Práctica de laboratorio 8.5.3: Resolución de problemas de redes empresariales 3

Diagrama de topología

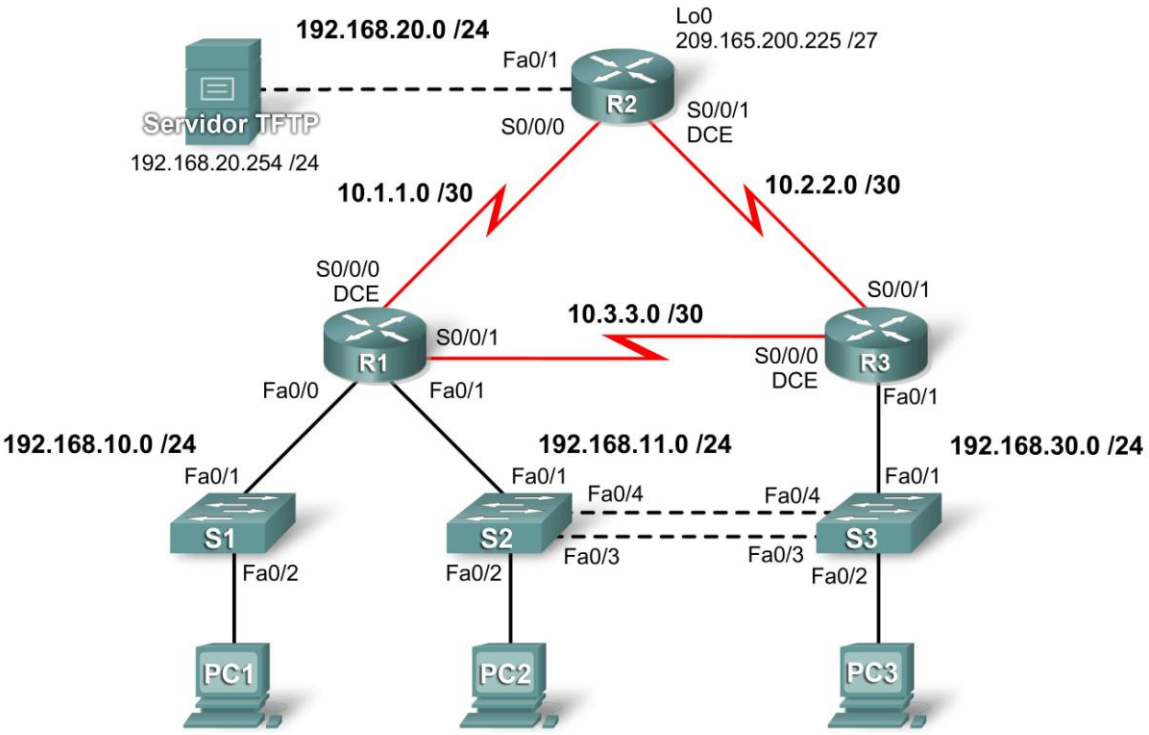

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/0	192.168.10.1	255.255.255.0	N/C
	Fa0/1	192.168.11.1	255.255.255.0	N/C
	S0/0/0	10.1.1.1	255.255.255.252	N/C
	S0/0/1	10.3.3.1	255.255.255.252	N/C
R2	Fa0/1	192.168.20.1	255.255.255.0	N/C
	S0/0/0	10.1.1.2	255.255.255.252	N/C
	S0/0/1	10.2.2.1	255.255.255.252	N/C
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226
R3	Fa0/1	N/C	N/C	N/C
	Fa0/1.11	192.168.11.3	255.255.255.0	N/C
	Fa0/1.30	192.168.30.1	255.255.255.0	N/C
	S0/0/0	10.3.3.2	255.255.255.252	N/C
	S0/0/1	10.2.2.2	255.255.255.252	N/C
S1	VLAN10	DHCP	255.255.255.0	N/C
S2	VLAN11	192.168.11.2	255.255.255.0	N/C
S3	VLAN30	192.168.30.2	255.255.255.0	N/C
PC1	NIC	192.168.10.10	255.255.255.0	192.168.10.1

PC2	**NIC**	192.168.11.10	255.255.255.0	192.168.11.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1
Servidor TFTP	**NIC**	192.168.20.254	255.255.255.0	192.168.20.1

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, el usuario podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración de inicio y recargar un router al estado por defecto
- Cargar los routers y switches con los guiones suministrados
- Detectar y corregir todos los errores de red
- Documentar la red corregida

Escenario

Para esta práctica de laboratorio no se debe utilizar la protección por contraseña o por inicio de sesión en ninguna línea de consola para evitar que se produzca un bloqueo accidental. Use **ciscoccna** para todas las contraseñas de esta situación.

Nota: Debido a que esta práctica de laboratorio es acumulativa, se utilizarán todos los conocimientos y las técnicas de resolución de problemas que se hayan adquirido en materiales anteriores para completarla con éxito.

Requisitos

- S2 es la raíz de spanning tree para la VLAN 11 y S3 es la raíz de spanning tree para la VLAN 30.
- S3 es un servidor VTP con S2 como cliente.
- El enlace serial entre R1 y R2 es Frame Relay.
- El enlace serial entre R2 y R3 utiliza encapsulación HDLC.
- El enlace serial entre R1 y R3 se autentica mediante CHAP.
- R2 debe tener procedimientos seguros de inicio de sesión, ya que es el router extremo de Internet.
- Todas las líneas vty, excepto las que pertenecen a R2, permiten conexiones sólo desde las subredes que se muestran en el diagrama de topología, sin incluir la dirección pública.
- Se debería impedir la suplantación de identidad (spoofing) de la dirección IP de origen en todos los enlaces que no se conectan al resto de los routers.
- Los protocolos de enrutamiento deben utilizarse de manera segura. En esta situación se usa OSPF.
- R3 no debe poder establecer una conexión telnet a R2 a través del enlace serial conectado en forma directa.
- R3 tiene acceso a las VLAN 11 y 30 a través de su puerto 0/1 Fast Ethernet.
- El servidor TFTP no debería recibir ningún tipo de tráfico que tenga una dirección de origen fuera de la subred. Todos los dispositivos tienen acceso al servidor TFTP.
- Todos los dispositivos de la subred 192.168.10.0 deben poder obtener sus direcciones IP de DHCP en R1. Esto incluye a S1.
- Se debe poder acceder a todas las direcciones que se muestran en el diagrama desde cada dispositivo.

Tarea 1: Cargar los routers con los guiones suministrados

```
!-----------------------------------------
!                  R1
!-----------------------------------------
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.11.0 255.255.255.0
      default-router 192.168.10.1
!
no ip domain lookup
!
ip dhcp excluded-address 192.168.10.2 192.168.10.254
!
frame-relay switching
!
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 no keepalive
 clockrate 128000
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast

no frame-relay inverse-arp
 frame-relay intf-type dce
 no shutdown
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
```

```
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
interface Serial0/1/0
 no ip address
 shutdown
 clockrate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.255 area 0
 network 10.2.2.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.10.0 0.0.0.255
 deny any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
line vty 0 4
 access-class VTY in
 login local
!
end
!----------------------------------------
!                  R2
!----------------------------------------
no service password-encryption
!
hostname R2
!
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
aaa session-id common
```

```
!
ip cef
!
no ip domain lookup
!
username ccna password 0 ciscoccna
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip access-group TFTP out
 ip access-group Anti-spoofing in
 ip nat inside
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat outside
 encapsulation frame-relay
 no keepalive
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no frame-relay inverse-arp
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 ip nat outside
!
!
router ospf 1
 passive-interface FastEthernet0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
no ip http server
ip nat inside source list nat interface FastEthernet0/0
!
ip access-list standard Anti-spoofing
 permit 192.168.20.0 0.0.0.255
 deny any
ip access-list standard NAT
 permit 10.0.0.0 0.255.255.255
 permit 192.168.0.0 0.0.255.255
ip access-list standard private
 deny   127.0.0.1
 deny   10.0.0.0 0.255.255.255
 deny   172.0.0.0 0.31.255.255
```

```
 deny   192.168.0.0 0.0.255.255
 permit any
!
ip access-list extended R3-telnet
 deny   tcp host 10.2.2.2 host 10.2.2.1 eq telnet
 deny   tcp host 10.3.3.2 host 10.2.2.1 eq telnet
 deny   tcp host 192.168.11.3 host 10.2.2.1 eq telnet
 deny   tcp host 192.168.30.1 host 10.2.2.1 eq telnet
 permit ip any any
!
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
!----------------------------------------
!                  R3
!----------------------------------------
no service password-encryption
!
hostname R3
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username R1 password ciscoccna
username ccna password ciscoccna
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 12
 ip address 192.168.11.3 255.255.255.0
```

```
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group Anti-spoofing in
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 encapsulation ppp
 clockrate 125000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 encapsulation lapb
 no shutdown
!
router ospf 1
 passive-interface FastEthernet0/1.30
 network 10.2.2.0 0.0.0.3 area 1
 network 10.3.3.0 0.0.0.3 area 1
 network 192.168.11.0 0.0.0.255 area 1
 network 192.168.30.0 0.0.0.255 area 1
 !
ip classless
!
ip http server
!
ip access-list standard Anti-spoofing
 permit 192.168.30.0 0.0.0.255
 deny any
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
line con 0
 exec-timeout 5 0
 logging synchronous
line aux 0
 exec-timeout 15 0
 logging synchronous
line vty 0 4
 access-class VTY in
 exec-timeout 15 0
 logging synchronous
 login local
!
end
!----------------------------------------
!                S1
```

```
!-----------------------------------------
no service password-encryption
!
hostname S1
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
!
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface range FastEthernet0/3-24
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan10
 ip address dhcp
 no ip route-cache
!
ip default-gateway 192.168.10.1
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
```

```
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S2
!----------------------------------------
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode client
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
 switchport access vlan 11
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 11
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface range FastEthernet0/5-24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
```

```
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan11
 ip address 192.168.11.2 255.255.255.0
 no ip route-cache
!
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S3
!----------------------------------------
no service password-encryption
!
hostname S3
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode Server
vtp password ciscoccna
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
vlan internal allocation policy ascending
!
vlan 30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11
 switchport mode trunk
```

```
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk native vlan 99
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface range FastEthernet0/5-24
 shutdown
!
interface GigabitEthernet0/1
 shutdown
!
interface GigabitEthernet0/2
 shutdown
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan30
 ip address 192.168.30.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.30.1
ip http server
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
```

Tarea 2: Buscar y corregir todos los errores de red

Tarea 3: Verificar que se cumpla totalmente con los requisitos

Debido a que las limitaciones de tiempo impiden resolver un problema sobre cada tema, sólo una cantidad selecta de temas tiene problemas. Sin embargo, para reforzar y fortalecer las habilidades de resolución de problemas, el usuario debería verificar que se cumpla con cada uno de los requisitos. Para ello, presente un ejemplo de cada requisito (por ejemplo, un comando **show** o **debug**).

Tarea 4: Documentar la red corregida

Tarea 5: Limpiar

Borre las configuraciones y recargue los routers. Desconecte y guarde los cables. Para los equipos PC host que normalmente se conectan a otras redes (tal como la LAN de la escuela o Internet), reconecte los cables correspondientes y restablezca las configuraciones TCP/IP.