Cisco | Networking Academy®
Mind Wide Open™

CCNA Exploration 4.0

Acceso a la WAN

Manual de prácticas de laboratorio para el instructor

Práctica de laboratorio 1.4.1: Revisión de reto
(Versión para el instructor)

Diagrama de topología

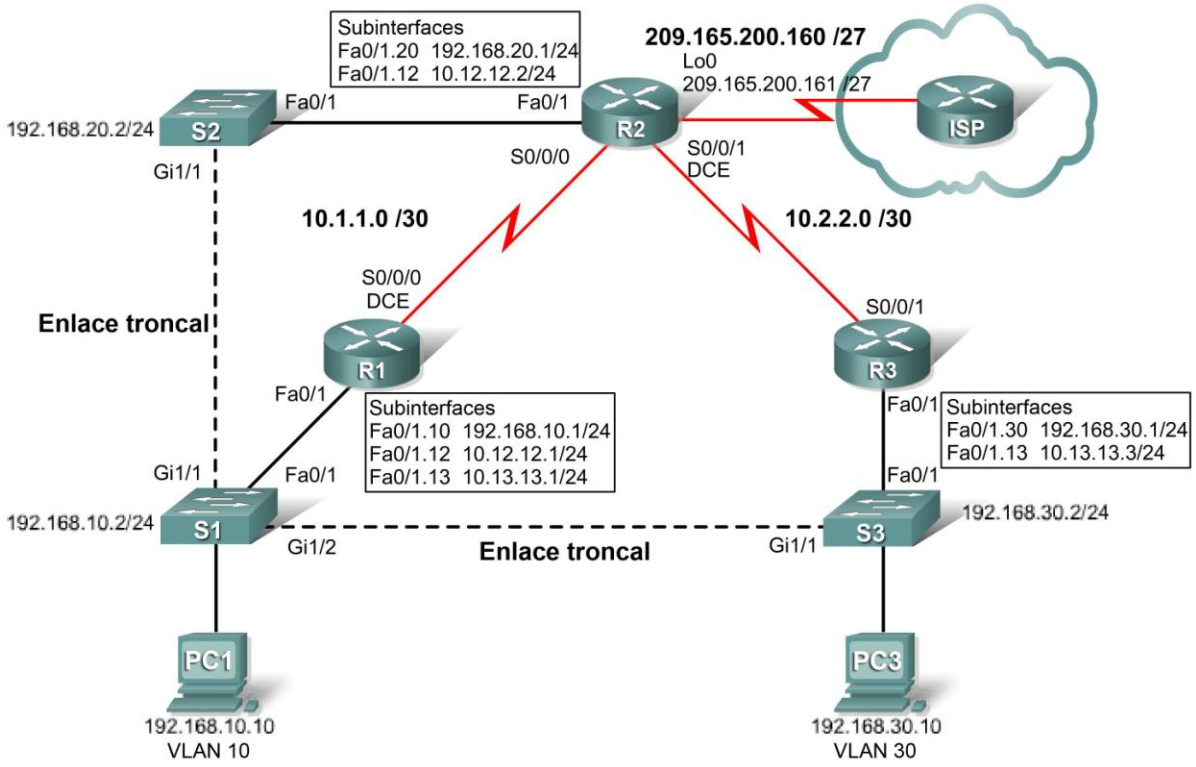


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/1**	N/C	N/C	N/C
	Fa0/1.10	192.168.10.1	255.255.255.0	N/C
	Fa0/1.12	10.12.12.1	255.255.255.0	N/C
	Fa0/1.13	10.13.13.1	255.255.255.0	N/C
	S0/0/0	10.1.1.1	255.255.255.252	N/C
R2	**Fa0/1**	N/C	N/C	N/C
	Fa0/1.12	10.12.12.2	255.255.255.0	N/C
	Fa0/1.20	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

R3	**Fa0/1**	N/C	N/C	N/C
	Fa0/1.13	10.13.13.3	255.255.255.0	N/C
	Fa0/1.30	192.168.30.1	255.255.255.0	N/C
	S0/0/1	10.2.2.2	255.255.255.252	N/C
S1	**VLAN10**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**VLAN20**	192.168.20.2	255.255.255.0	192.168.20.1
S3	**VLAN30**	192.168.30.2	255.255.255.0	192.168.30.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1

Objetivos de aprendizaje

Para completar esta práctica de laboratorio:

- Cablear una red según el diagrama de topología
- Borrar la configuración de inicio y recargar un router al estado por defecto
- Realizar tareas de configuración básicas en un router
- Configurar y activar interfaces
- Configurar el protocolo Spanning Tree
- Configurar el cliente y los servidores VTP
- Configurar las VLAN en los switches
- Configurar el enrutamiento RIP en todos los routers
- Configurar el enrutamiento OSPF en todos los routers
- Configurar el enrutamiento EIGRP en todos los routers

Escenario

En esta práctica de laboratorio se revisarán conceptos básicos sobre enrutamiento y conmutación. El usuario debería intentar hacer todo lo posible por su cuenta. Debería consultar el material anterior cuando no pueda seguir solo.

Nota: Configurar tres protocolos de enrutamiento por separado (RIP, OSPF y EIGRP) para enrutar la misma red no es categóricamente un buen ejemplo a seguir. Debería considerarse un mal ejemplo y no es algo que se haría en una red de producción. Aquí se hace para que el usuario pueda revisar los principales protocolos de enrutamiento antes de continuar y vea una sorprendente ilustración del concepto de distancia administrativa.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas de dispositivos

Configure los routers R1, R2 y R3, y los switches S1, S2 y S3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de Modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure el registro de datos sincrónico.
- Configure una contraseña para las conexiones de vty.

```
enable
configure terminal
no ip domain-lookup
enable secret class
banner motd ^CUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
end
copy running-config startup-config
```

Tarea 3: Configurar y activar las direcciones serial y Ethernet

Paso 1: Configurar las interfaces de R1, R2 y R3.

R1

```
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.12.12.1 255.255.255.0
!
interface FastEthernet0/1.13
```

```
 encapsulation dot1Q 13
 ip address 10.13.13.1 255.255.255.0
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
 clock rate 64000
!
```

R2

```
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.12.12.2 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
 no snmp trap link-status
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clock rate 64000
 no shutdown
```

R3

```
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.13
 encapsulation dot1Q 13
 ip address  10.13.13.3 255.255.255.0
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
!
```

Paso 2: Verificar el direccionamiento IP y las interfaces.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES unset  up                    up
FastEthernet0/1.10     192.168.10.1    YES manual up                    up
FastEthernet0/1.12     10.12.12.1      YES manual up                    up
FastEthernet0/1.13     10.13.13.1      YES manual up                    up
Serial0/0/0            10.1.1.1        YES unset  up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down

R2#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/1.12     10.12.12.2      YES manual up                    up
FastEthernet0/1.20     192.168.20.1    YES manual up                    up
Serial0/0/0            10.1.1.2        YES manual up                    up
Serial0/0/1            10.2.2.1        YES manual up                    up

R3#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        unassigned      YES manual up                    up
FastEthernet0/1.10     192.168.30.1    YES manual up                    up
FastEthernet0/1.13     10.13.13.3      YES manual up                    up
Serial0/0/0            unassigned      YES unset  administratively down down
Serial0/0/1            10.2.2.2        YES manual up                    up
```

Paso 3: Configurar la interfaz de la VLAN de administración en S1, S2 y S3.

```
S1(config)#interface vlan10
S1(config-if)#ip address 192.168.10.2 255.255.255.0

S2(config)#interface vlan20
S2(config-if)#ip address 192.168.20.2 255.255.255.0

S3(config)#interface vlan30
S3(config-if)#ip address 192.168.30.2 255.255.255.0
```

Paso 4: Configurar las interfaces Ethernet de PC1 y PC3.

Paso 5: Probar la conectividad entre los equipos PC.

Tarea 4: Configurar STP

Paso 1: Configurar S1 para que siempre sea raíz.

```
S1(config)#spanning-tree vlan 1-1000 root primary
```

Paso 2: Verificar que S1 sea raíz.

```
S1#show spanning-tree summary
Switch is in pvst mode
Root bridge for: VLAN0001
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          2          2
---------------------- -------- --------- -------- ---------- ----------
1 vlans                     0         0        0          7          7
```

Tarea 5: Configurar VTP

Paso 1: Configurar S1 como servidor VTP y crear un nombre de dominio y una contraseña.

```
S1(config)#vtp mode server
Setting device to VTP SERVER mode
S1(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Paso 2: Configurar S2 y S3 como clientes VTP y asignar nombres de dominio y contraseñas.

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
S2(config)#vtp password cisco
Setting device VLAN database password to cisco

S3(config)#vtp mode client
Setting device to VTP CLIENT mode
S3(config)#vtp domain cisco
Changing VTP domain name from NULL to cisco
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
```

Paso 3: Verificar la configuración.

```
S1#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x97 0xB7 0xCF 0xD2 0xDD 0x77 0x88 0x34
Configuration last modified by 0.0.0.0 at 3-1-93 00:25:29
Local updater ID is 192.168.10.2 on interface Vl10 (lowest numbered VLAN
interface found)

S2#show vtp stat
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE7 0xD7 0x24 0xC0 0x33 0x80 0xF7 0xAA
Configuration last modified by 0.0.0.0 at 3-1-93 00:19:03

S3#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 10
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0xE7 0xD7 0x24 0xC0 0x33 0x80 0xF7 0xAA
Configuration last modified by 0.0.0.0 at 3-1-93 06:52:33
```

Tarea 6: Configurar las VLAN

Paso 1: Configurar S1 con las VLAN.

```
S1(config)# vlan 10,12,13,20,30
```

Paso 2: Verificar que S2 y S3 hayan recibido las configuraciones VLAN de S1.

```
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24
10   VLAN0010                          active
12   VLAN0012                          active
13   VLAN0013                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

S2#show vlan brief
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/2
10   VLAN0010                          active
12   VLAN0012                          active
13   VLAN0013                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

```
S3#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12,
Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16,Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20,Fa0/21
                                                 Fa0/22, Fa0/23, Fa0/24, Gi0/2
10   VLAN0010                          active
12   VLAN0012                          active
13   VLAN0013                          active
20   VLAN0020                          active
30   VLAN0030                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup
```

Paso 3: Asignar puertos a las VLAN apropiadas.

S1:

```
interface FastEthernet0/1
 switchport trunk allowed vlan 10,12,13
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 swotchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 1,12
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 1,13
 switchport mode trunk
!
```

S2:

```
interface FastEthernet0/1
 switchport trunk allowed vlan 12,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 20
 switchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 12
 switchport mode trunk
!
```

```
S2:
interface FastEthernet0/1
 switchport trunk allowed vlan 13,30
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 swotchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 13
 switchport mode trunk
!
```

Tarea 7: Configurar el enrutamiento RIP

Paso 1: Configurar el enrutamiento RIP en R1, R2 y R3.

R1

```
!
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 192.168.10.0
!
```

R2

```
!
router rip
 version 2
 no auto-summary
 network 10.0.0.0
 network 192.168.20.0
!
```

R3

```
!
router rip
 version 2
 not auto-summary
 network 10.0.0.0
 network 192.168.30.0
```

Paso 2: Probar la conectividad haciendo ping.

R1:

```
R1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 10.12.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 10.13.13.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.13.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 192.168.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

```
R1#ping 192.168.30.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

R2:

```
R2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1., timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 10.2.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 10.12.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 10.13.13.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.13.13.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 10.13.13.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.13.13.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

```
R3#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 192.168.30.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 192.168.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R2#ping 192.168.30.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

R3:

```
R3#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 10.2.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 10.12.12.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 10.12.12.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.12.12.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

```
R3#ping 10.13.13.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.13.13.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.20.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.30.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 192.168.30.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

Paso 3: Verificar la tabla de enrutamiento.

```
R1#sh ip route
<output omitted>

R    192.168.30.0/24 [120/1] via 10.13.13.3, 00:00:03, FastEthernet0/1.13
C    192.168.10.0/24 is directly connected, FastEthernet0/1.10
```

```
R    192.168.20.0/24 [120/1] via 10.12.12.2, 00:00:00, FastEthernet0/1.12
                     [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.13.13.0/24 is directly connected, FastEthernet0/1.13
C       10.12.12.0/24 is directly connected, FastEthernet0/1.12
R       10.2.2.0/30 [120/1] via 10.13.13.3, 00:00:03, FastEthernet0/1.13
                    [120/1] via 10.12.12.2, 00:00:00, FastEthernet0/1.12
                    [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
C       10.1.1.0/30 is directly connected, Serial0/0/0
```

R2#sh ip route

```
<output omitted>

Gateway of last resort is not set

R    192.168.30.0/24 [120/1] via 10.2.2.2, 00:00:05, Serial0/0/1
R    192.168.10.0/24 [120/1] via 10.12.12.1, 00:00:17, FastEthernet0/1.12
                     [120/1] via 10.1.1.1, 00:00:17, Serial0/0/0
C    192.168.20.0/24 is directly connected, FastEthernet0/1.20
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
R       10.13.13.0/24 [120/1] via 10.12.12.1, 00:00:17, FastEthernet0/1.12
                      [120/1] via 10.2.2.2, 00:00:05, Serial0/0/1
                      [120/1] via 10.1.1.1, 00:00:17, Serial0/0/0
C       10.12.12.0/24 is directly connected, FastEthernet0/1.12
C       10.2.2.0/30 is directly connected, Serial0/0/1
C       10.1.1.0/30 is directly connected, Serial0/0/0
```

R3#sh ip route

```
<output omitted>

Gateway of last resort is not set

C    192.168.30.0/24 is directly connected, FastEthernet0/1.30
R    192.168.10.0/24 [120/1] via 10.13.13.1, 00:00:08, FastEthernet0/1.13
R    192.168.20.0/24 [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.13.13.0/24 is directly connected, FastEthernet0/1.13
R       10.12.12.0/24 [120/1] via 10.13.13.1, 00:00:08, FastEthernet0/1.13
                      [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
R       10.1.1.0/30 [120/1] via 10.13.13.1, 00:00:08, FastEthernet0/1.13
                    [120/1] via 10.2.2.1, 00:00:10, Serial0/0/1
```

Tarea 8: Configurar el enrutamiento OSPF

Paso 1: Configurar el enrutamiento OSPF en R1, R2 y R3.

R1

```
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.12.12.0 0.0.0.255 area 0
 network 10.13.13.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
```

R2

```
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 10.12.12.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
```

R3

```
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 10.13.13.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
```

Paso 2: Verificar que las rutas OSPF hayan reemplazado a las rutas RIP debido a una distancia administrativa más baja.

```
R1#show ip route
<output omitted>

O    192.168.30.0/24 [110/2] via 10.13.13.3, 00:00:13, FastEthernet0/1.13
C    192.168.10.0/24 is directly connected, FastEthernet0/1.10
O    192.168.20.0/24 [110/2] via 10.12.12.2, 00:00:13, FastEthernet0/1.12
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.13.13.0/24 is directly connected, FastEthernet0/1.13
C       10.12.12.0/24 is directly connected, FastEthernet0/1.12
O       10.2.2.0/30 [110/782] via 10.13.13.3, 00:00:13, FastEthernet0/1.13
                    [110/782] via 10.12.12.2, 00:00:13, FastEthernet0/1.12
C       10.1.1.0/30 is directly connected, Serial0/0/0

R2#show ip route
<output omitted>

O    192.168.30.0/24 [110/3] via 10.12.12.1, 00:00:39, FastEthernet0/1.12
O    192.168.10.0/24 [110/2] via 10.12.12.1, 00:00:39, FastEthernet0/1.12
C    192.168.20.0/24 is directly connected, FastEthernet0/1.20
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O       10.13.13.0/24 [110/2] via 10.12.12.1, 00:00:39, FastEthernet0/1.12
C       10.12.12.0/24 is directly connected, FastEthernet0/1.12
C       10.2.2.0/30 is directly connected, Serial0/0/1
C       10.1.1.0/30 is directly connected, Serial0/0/0

R3#show ip route
<output omitted>

C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
O    192.168.10.0/24 [110/2] via 10.13.13.1, 00:01:03, FastEthernet0/1.13
O    192.168.20.0/24 [110/3] via 10.13.13.1, 00:01:03, FastEthernet0/1.13
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.13.13.0/24 is directly connected, FastEthernet0/1.13
O       10.12.12.0/24 [110/2] via 10.13.13.1, 00:01:03, FastEthernet0/1.13
C       10.2.2.0/30 is directly connected, Serial0/0/1
O       10.1.1.0/30 [110/782] via 10.13.13.1, 00:01:03, FastEthernet0/1.13
```

¿En qué se diferencian las decisiones de enrutamiento ahora que se ejecuta OSPF?

Antes de que se agregara OSPF, los routers tomaban la ruta con la menor cantidad de saltos. Por ejemplo, R3 usaba su interfaz Serial0/0/0 para alcanzar la subred 192.168.20.0, ya que está a un salto. Una vez que se ejecuta OSPF, la ruta que se tomará se determina según la ruta más rápida. Si se utiliza el ejemplo anterior, R3 usa Fast Ethernet 0/0.13 para alcanzar la subred 192.168.20.0.

Paso 3: Verificar que RIP sigue en ejecución.

```
R1#show ip rip database
10.0.0.0/8    auto-summary
10.1.1.0/30    directly connected, Serial0/0/0
10.12.12.0/24    directly connected, FastEthernet0/1.12
10.13.13.0/24    directly connected, FastEthernet0/1.13
192.168.10.0/24    auto-summary
192.168.10.0/24    directly connected, FastEthernet0/1.10

R2#show ip rip database
10.0.0.0/8    auto-summary
10.1.1.0/30    directly connected, Serial0/0/0
10.2.2.0/30    directly connected, Serial0/0/1
10.12.12.0/24    directly connected, FastEthernet0/1.12
192.168.20.0/24    auto-summary
192.168.20.0/24    directly connected, FastEthernet0/1.20

R3#show ip rip database
10.0.0.0/8    auto-summary
10.2.2.0/30    directly connected, Serial0/0/1
10.13.13.0/24    directly connected, FastEthernet0/1.13
192.168.30.0/24    auto-summary
192.168.30.0/24    directly connected, FastEthernet0/1.30
```

Tarea 9: Configurar el enrutamiento EIGRP

Paso 1: Configurar el enrutamiento EIGRP en R1, R2 y R3.

R1

```
!
router eigrp 10
 no auto-summary
 network 10.1.1.0 0.0.0.3
 network 10.12.12.0 0.0.0.255
 network 10.13.13.0 0.0.0.255
 network 192.168.10.0
!
```

R2

```
!
router eigrp 10
 no auto-summary
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 10.12.12.0 0.0.0.255
 network 192.168.20.0
!
```

R3

```
!
router eigrp 10
 no auto-summary
 network 10.2.2.0 0.0.0.3
 network 10.13.13.0 0.0.0.255
 network 192.168.30.0
!
```

Paso 2: Verificar que las rutas EIGRP hayan reemplazado a las rutas OSPF debido a una distancia administrativa más baja.

```
R1#show ip route
<output omitted>

D    192.168.30.0/24 [90/30720] via 10.13.13.3, 00:00:24, FastEthernet0/1.13
C    192.168.10.0/24 is directly connected, FastEthernet0/1.10
D    192.168.20.0/24 [90/30720] via 10.12.12.2, 00:00:48, FastEthernet0/1.12
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.13.13.0/24 is directly connected, FastEthernet0/1.13
C       10.12.12.0/24 is directly connected, FastEthernet0/1.12
D       10.2.2.0/30 [90/20514560] via 10.13.13.3, 00:00:24,
FastEthernet0/1.13
                    [90/20514560] via 10.12.12.2, 00:00:24,
FastEthernet0/1.12
C       10.1.1.0/30 is directly connected, Serial0/0/0

R2#show ip route
<output omitted>

D    192.168.30.0/24 [90/33280] via 10.12.12.1, 00:00:29, FastEthernet0/1.12
D    192.168.10.0/24 [90/30720] via 10.12.12.1, 00:00:30, FastEthernet0/1.12
C    192.168.20.0/24 is directly connected, FastEthernet0/1.20
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
D       10.13.13.0/24 [90/30720] via 10.12.12.1, 00:00:30, FastEthernet0/1.12
C       10.12.12.0/24 is directly connected, FastEthernet0/1.12
C       10.2.2.0/30 is directly connected, Serial0/0/1
C       10.1.1.0/30 is directly connected, Serial0/0/0
```

```
R3#show ip route
<output omitted>

C    192.168.30.0/24 is directly connected, FastEthernet0/0.30
D    192.168.10.0/24 [90/30720] via 10.13.13.1, 00:00:08, FastEthernet0/1.13
D    192.168.20.0/24 [90/33280] via 10.13.13.1, 00:00:08, FastEthernet0/1.13
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.13.13.0/24 is directly connected, FastEthernet0/1.13
D       10.12.12.0/24 [90/30720] via 10.13.13.1, 00:00:08, FastEthernet0/1.13
C       10.2.2.0/30 is directly connected, Serial0/0/1
D       10.1.1.0/30 [90/20514560] via 10.13.13.1, 00:00:08,
FastEthernet0/0.13
```

Paso 3: Verificar que OSPF sigue en ejecución.

```
R1#sh ip ospf database
            OSPF Router with ID (192.168.10.1) (Process ID 1)
                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.10.1    192.168.10.1    1038        0x80000005 0x0056F6 5
192.168.20.1    192.168.20.1    1039        0x80000004 0x00B9F7 6
192.168.30.1    192.168.30.1    1048        0x80000003 0x00C99A 4

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.12.12.2      192.168.20.1    1039        0x80000001 0x004D5A
10.13.13.3      192.168.10.1    1052        0x80000001 0x003175

R2#sh ip ospf database
            OSPF Router with ID (192.168.20.1) (Process ID 1)
                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.10.1    192.168.10.1    1084        0x80000005 0x0056F6 5
192.168.20.1    192.168.20.1    1083        0x80000004 0x00B9F7 6
192.168.30.1    192.168.30.1    1092        0x80000003 0x00C99A 4

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.12.12.2      192.168.20.1    1083        0x80000001 0x004D5A
10.13.13.13     192.168.10.1    1098        0x80000001 0x003175

R3#sh ip ospf database
            OSPF Router with ID (192.168.30.1) (Process ID 1)
                Router Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum Link count
192.168.10.1    192.168.10.1    1135        0x80000005 0x0056F6 5
192.168.20.1    192.168.20.1    1135        0x80000004 0x00B9F7 6
192.168.30.1    192.168.30.1    1143        0x80000003 0x00C99A 4

                Net Link States (Area 0)

Link ID         ADV Router      Age         Seq#       Checksum
10.12.12.2      192.168.20.1    1136        0x80000001 0x004D5A
10.13.13.3      192.168.10.1    1149        0x80000001 0x003175
```

Tarea 10: Documentar las configuraciones del router

R1

```
R1#show run

!<resultado omitido>
!
hostname R1
!
!
enable secret class
!
!
no ip domain lookup
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.12.12.1 255.255.255.0
!
interface FastEthernet0/1.13
 encapsulation dot1Q 13
 ip address 10.13.13.1 255.255.255.0
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.0
 no fair-queue
 clockrate 64000
 no shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
router eigrp 10
 network 10.1.1.0 0.0.0.3
 network 10.12.12.0 0.0.0.255
 network 10.13.13.0 0.0.0.255
 network 192.168.10.0
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
```

```
 network 10.12.12.0 0.0.0.255 area 0
 network 10.13.13.0 0.0.0.255 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!!
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R2

```
R2#show run
!<resultado omitido>
!
hostname R2
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 no ip address
 shutdown
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.20.1 255.255.255.0
!
interface FastEthernet0/1.12
 encapsulation dot1Q 12
 ip address 10.12.12.2 255.255.255.0
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.0
 no shutdown
```

```
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.0
 no shutdown
!
router eigrp 10
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 10.12.12.0 0.0.0.255
 network 192.168.20.0
 no auto-summary
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 10.12.12.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 no auto-summary
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R3

```
R3#show run
!<resultado omitido>
!
hostname R3
!
!
enable secret class
!
no ip domain lookup
!
!
interface FastEthernet0/0
 no ip address
 shutdown
```

```
!
interface FastEthernet0/1
 no ip address
 no shutdown
!
interface FastEthernet0/1.13
 encapsulation dot1Q 13
 ip address  10.13.13.3 255.255.255.0
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
!
interface Serial0/0/0
 no ip address
 shutdown
 clockrate 125000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
!
router eigrp 10
 network 10.2.2.0 0.0.0.3
 network 10.13.13.0 0.0.0.255
 network 192.168.30.0
 no auto-summary
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 10.13.13.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
End

S1#show run
!<resultado omitido>
```

```
!
hostname S1
!
!
enable secret class
!
!
no ip domain lookup
!
vlan 10,12,13,20,30
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1-1000 priority 24576
!
vtp mode server
vtp domain cisco
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,12,13
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access 10
 swotchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 12
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport trunk allowed vlan 13
 switchport mode trunk
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
End

S2#show run
!<resultado omitido>
hostname S2
!
enable secret class
!
```

```
no ip domain lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vtp mode client
vtp domain cisco
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk allowed vlan 12,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access 20
 swotchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 12
 switchport mode trunk
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
End

S3#show run
!<resultado omitido>
!
hostname S3
!
enable secret class
!
no ip domain lookup
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vtp mode client
vtp domain cisco
vtp password cisco
!
interface FastEthernet0/1
 switchport trunk allowed vlan 13,30
 switchport mode trunk
```

```
!
interface FastEthernet0/2
 switchport access 30
 swotchport mode access
!
interface GigabitEthernet0/1
 switchport trunk allowed vlan 13
 switchport mode trunk
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Tarea 11: 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.

Práctica de laboratorio 2.5.1: Configuración básica de PPP (Versión para el instructor)

Diagrama de topología

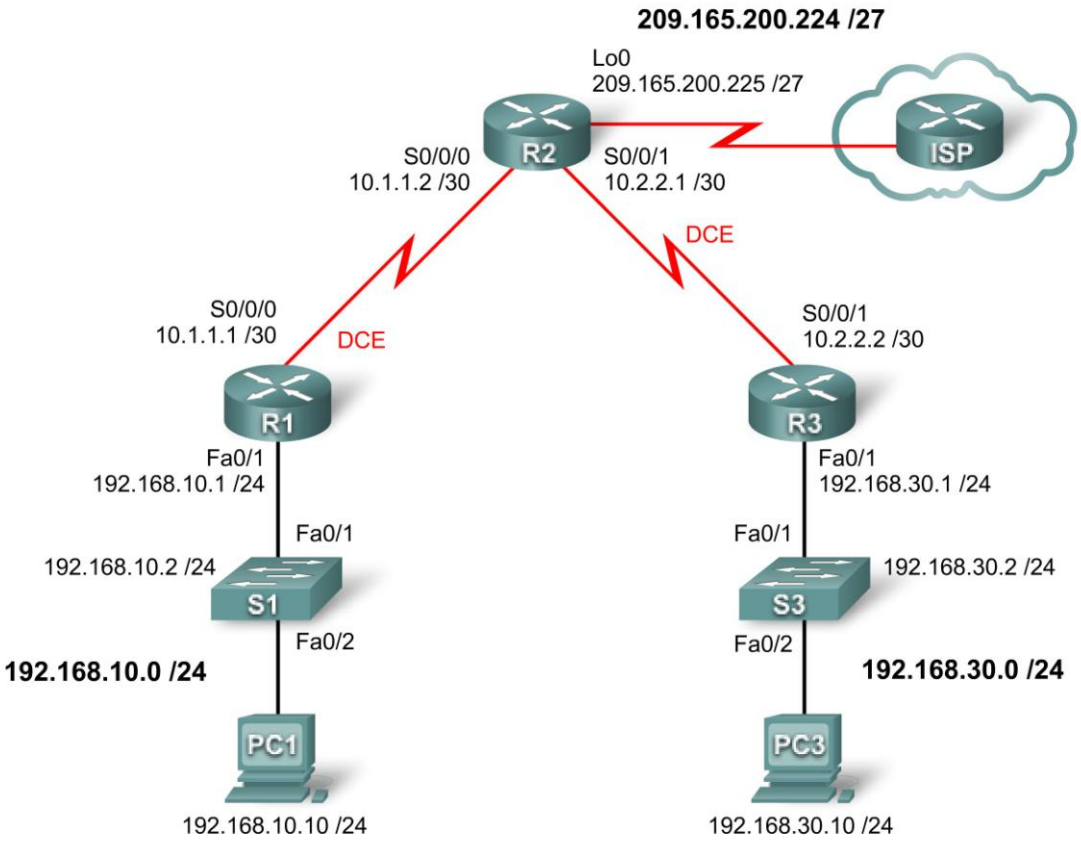


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/1**	192.168.10.1	255.255.255.0	N/C
	S0/0/0	10.1.1.1	255.255.255.252	N/C
R2	**Lo0**	209.165.200.225	255.255.255.224	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
R3	**Fa0/1**	192.168.30.1	255.255.255.0	N/C
	S0/0/1	10.2.2.2	255.255.255.252	N/C
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
PC3	**NIC**	192.168.30.10	255.255.255.0	192.168.30.1

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
- Realizar tareas de configuración básicas en un router
- Configurar y activar interfaces
- Configurar el enrutamiento OSPF en todos los routers
- Configurar la encapsulación PPP en todas las interfaces seriales
- Aprender acerca de los comandos **debug ppp negotiation** y **debug ppp packet**
- Aprender cómo cambiar la encapsulación en las interfaces seriales de PPP a HDLC
- Interrumpir intencionalmente y restablecer la encapsulación PPP
- Configurar la autenticación CHAP y PAP de PPP
- Interrumpir intencionalmente y restablecer la autenticación PAP y CHAP de PPP

Escenario

En esta práctica de laboratorio, se aprenderá a configurar la encapsulación PPP en enlaces seriales a través de la red que se muestra en el diagrama de topología. También se aprenderá a restaurar los enlaces seriales a su encapsulación HDLC por defecto. Se debe prestar especial atención al aspecto del resultado del router cuando se interrumpe intencionalmente la encapsulación PPP. Esto ayudará en la práctica de laboratorio de resolución de problemas relacionada con este capítulo. Por último, se configurará la autenticación PPP PAP y la autenticación PPP CHAP.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en el diagrama de topología.

Nota: Si se utilizan los routers 1700, 2500 ó 2600, los resultados del router y las descripciones tienen un aspecto diferente.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar la configuración básica del router

Configure los routers R1, R2 y R3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de Modo EXEC.
- Configure un mensaje del día.

- Configure una contraseña para las conexiones de la consola.
- Configure el registro de datos sincrónico.
- Configure una contraseña para las conexiones de vty.

```
enable
configure terminal
no ip domain-lookup
enable secret class
banner motd ^CUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
end
copy running-config starting-config
```

Tarea 3: Configurar y activar las direcciones serial y Ethernet

Paso 1: Configurar las interfaces de R1, R2 y R3.

Configure las interfaces de los routers R1, R2 y R3 con las direcciones IP de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio. Asegúrese de incluir la frecuencia de reloj en las interfaces DCE seriales.

R1

```
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!

interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
 clock rate 64000
```

R2

```
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
```

```
 ip address 10.2.2.1 255.255.255.252
 clock rate 64000
 no shutdown
```

R3

```
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
```

Paso 2: Verificar el direccionamiento IP y las interfaces.

Utilice el comando **show ip interface brief** para verificar que el direccionamiento IP es correcto y que las interfaces están activas.

```
R1#show ip interface brief
Interface        IP-Address    OK? Method Status
Protocol
FastEthernet0/0  unassigned    YES NVRAM  administratively down down
FastEthernet0/1  192.168.10.1  YES manual up                    up
Serial0/0/0      10.1.1.1      YES manual up                    up
Serial0/0/1      unassigned    YES NVRAM  administratively down down

R2#show ip interface brief
Interface        IP-Address     OK? Method Status              Protocol
FastEthernet0/0  unassigned     YES NVRAM  administratively down down
FastEthernet0/1  unassigned     YES NVRAM  administratively down down
Serial0/0/0      10.1.1.2       YES manual up                    up
Serial0/0/1      10.2.2.1       YES manual up                    up
Loopback0        209.165.200.225YES manual up                    up

R3#show ip interface brief
Interface       IP-Address   OK? Method Status              Protocol
FastEthernet0/0 unassigned   YES NVRAM  administratively down down
FastEthernet0/1 192.168.30.1 YES manual up                    up
Serial0/0/0     unassigned   YES NVRAM  administratively down down
Serial0/0/1     10.2.2.2     YES manual up                    up
```

Cuando haya finalizado, asegúrese de guardar la configuración en ejecución para la NVRAM del router.

Paso 3: Configurar las interfaces Ethernet de PC1 y PC3.

Configure las interfaces Ethernet de lPC1 y PC3 con las direcciones IP y gateways por defecto que se indican en la tabla de direccionamiento.

Paso 4: Probar la configuración al hacer ping desde el equipo PC a la gateway por defecto.

Tarea 4: Configurar OSPF en los routers

Si se necesita repasar los comandos de OSPF, consulte el módulo 11 de Exploration 2.

Paso 1: Activar el enrutamiento OSPF en R1, R2 y R3.

Use el comando **router ospf** con un ID de proceso de 1. Asegúrese de publicar las redes.

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
*Aug 17 17:49:14.689: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from LOADING to FULL, Loading Done
R1(config-router)#

R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
*Aug 17 17:48:40.645: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.224 0.0.0.31 area 0
R2(config-router)#
*Aug 17 17:57:44.729: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-router)#

R3(config)#router ospf 1
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
*Aug 17 17:58:02.017: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-router)#network 192.168.30.0 0.0.0.255 area 0
R3(config-router)#
```

Paso 2: Verificar que hay conectividad completa en la red.

Use los comandos **show ip route** y **ping** para verificar la conectividad.

```
R1#show ip route

<output omitted>

O    192.168.30.0/24 [110/1563] via 10.1.1.2, 00:33:56, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/782] via 10.1.1.2, 00:33:56, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.2/32 is directly connected, Serial0/0/0
O       10.2.2.0/30 [110/1562] via 10.1.1.2, 00:33:56, Serial0/0/0
C       10.1.1.0/30 is directly connected, Serial0/0/0

R1#ping 192.168.30.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R1#

R2#show ip route

<output omitted>

O    192.168.30.0/24 [110/782] via 10.2.2.2, 00:33:04, Serial0/0/1
O    192.168.10.0/24 [110/782] via 10.1.1.1, 00:33:04, Serial0/0/0
     209.165.200.0/27 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.2.2.2/32 is directly connected, Serial0/0/1
C       10.2.2.0/30 is directly connected, Serial0/0/1
C       10.1.1.0/30 is directly connected, Serial0/0/0
C       10.1.1.1/32 is directly connected, Serial0/0/0

R2#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#ping 192.168.10.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R2#

R3#show ip route

<output omitted>

C    192.168.30.0/24 is directly connected, FastEthernet0/1
O    192.168.10.0/24 [110/1563] via 10.2.2.1, 00:32:01, Serial0/0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.225 [110/782] via 10.2.2.1, 00:32:01, Serial0/0/1
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.2.2.0/30 is directly connected, Serial0/0/1
O       10.1.1.0/30 [110/1562] via 10.2.2.1, 00:32:01, Serial0/0/1
C       10.2.2.1/32 is directly connected, Serial0/0/1

R3#ping 209.165.200.225

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms
R3#ping 192.168.10.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms
R3#
```

Tarea 5: Configurar la encapsulación PPP en interfaces seriales

Paso 1: Utilizar el comando show interface para verificar si HDLC es la encapsulación serial por defecto.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<output omitted>

R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<output omitted>

R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<output omitted>

R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set

<output omitted>
```

Paso 2: Utilice los comandos debug en R1 y R2 para ver los efectos que produce la configuración PPP.

```
R1#debug ppp negotiation
PPP protocol negotiation debugging is on
R1#debug ppp packet
PPP packet display debugging is on
R1#

R2#debug ppp negotiation
PPP protocol negotiation debugging is on
R2#debug ppp packet
PPP packet display debugging is on
R2#
```

Paso 3: Cambiar la encapsulación de las interfaces seriales de HDLC a PPP.

Cambie el tipo de encapsulación en el enlace entre R1 y R2, y observe los efectos. Si se comienza a recibir demasiados datos de depuración, use el comando **undebug all** para desactivar la depuración.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Aug 17 19:02:53.412: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
R1(config-if)#
*Aug 17 19:02:53.416: Se0/0/0 PPP: Phase is DOWN, Setup
*Aug 17 19:02:53.416: Se0/0/0 PPP: Using default call direction
*Aug 17 19:02:53.416: Se0/0/0 PPP: Treating connection as a dedicated
line
*Aug 17 19:02:53.416: Se0/0/0 PPP: Session handle[E4000001] Session
id[0]
*Aug 17 19:02:53.416: Se0/0/0 PPP: Phase is ESTABLISHING, Active Open
*Aug 17 19:02:53.424: Se0/0/0 LCP: O CONFREQ [Closed] id 1 len 10
*Aug 17 19:02:53.424: Se0/0/0 LCP:    MagicNumber 0x63B994DE
(0x050663B994DE)
R1(config-if)#
*Aug 17 19:02:55.412: Se0/0/0 PPP: Outbound cdp packet dropped
*Aug 17 19:02:55.432: Se0/0/0 LCP: TIMEout: State REQsent
*Aug 17 19:02:55.432: Se0/0/0 LCP: O CONFREQ [REQsent] id 2 len 10
*Aug 17 19:02:55.432: Se0/0/0 LCP:    MagicNumber 0x63B994DE
(0x050663B994DE)
*Aug 17 19:02:56.024: Se0/0/0 PPP: I pkt type 0x008F, datagramsize 24
link[illegal]
*Aug 17 19:02:56.024: Se0/0/0 UNKNOWN(0x008F): Non-NCP packet,
discarding
R1(config-if)#
*Aug 17 19:02:57.252: Se0/0/0 PPP: I pkt type 0x000F, datagramsize 84
link[illegal]
*Aug 17 19:02:57.252: Se0/0/0 UNKNOWN(0x000F): Non-NCP packet,
discarding
*Aug 17 19:02:57.448: Se0/0/0 LCP: TIMEout: State REQsent
*Aug 17 19:02:57.448: Se0/0/0 LCP: O CONFREQ [REQsent] id 3 len 10
*Aug 17 19:02:57.448: Se0/0/0 LCP:    MagicNumber 0x63B994DE
```

```
(0x050663B994DE)
R1(config-if)#
*Aug 17 19:02:58.412: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down

R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#
*Aug 17 19:06:48.848: Se0/0/0 PPP: Phase is DOWN, Setup
*Aug 17 19:06:48.848: Se0/0/0 PPP: Using default call direction
*Aug 17 19:06:48.848: Se0/0/0 PPP: Treating connection as a dedicated
line
*Aug 17 19:06:48.848: Se0/0/0 PPP: Session handle[C6000001] Session
id[0]
*Aug 17 19:06:48.848: Se0/0/0 PPP: Phase is ESTABLISHING, Active Open
*Aug 17 19:06:48.856: Se0/0/0 LCP: O CONFREQ [Closed] id 1 len 10
*Aug 17 19:06:48.856: Se0/0/0 LCP:    MagicNumber 0x63BD388C
(0x050663BD388C)
*Aug 17 19:06:48.860: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14
link[ppp]
*Aug 17 19:06:48.860: Se0/0/0 LCP: I CONFACK [REQsent] id 1 len 10
R2(config-if)#
*Aug 17 19:06:48.860: Se0/0/0 LCP:    MagicNumber 0x63BD388C
(0x050663BD388C)
R2(config-if)#
*Aug 17 19:06:50.864: Se0/0/0 LCP: TIMEout: State ACKrcvd
*Aug 17 19:06:50.864: Se0/0/0 LCP: O CONFREQ [ACKrcvd] id 2 len 10
*Aug 17 19:06:50.864: Se0/0/0 LCP:    MagicNumber 0x63BD388C
(0x050663BD388C)
*Aug 17 19:06:50.868: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14
link[ppp]
*Aug 17 19:06:50.868: Se0/0/0 LCP: I CONFREQ [REQsent] id 61 len 10
*Aug 17 19:06:50.868: Se0/0/0 LCP:    MagicNumber 0x63BDB9A8
(0x050663BDB9A8)
*Aug 17 19:06:50.868: Se0/0/0 LCP: O CONFACK [REQsent] id 61 len 10
*Aug 17 19:06:50.868: Se0/0/0 LCP:    MagicNumber 0x63BDB9A8
(0x050663BDB9A8)
*Aug 17 19:06:50.868: Se0/0/0 PPP: I pkt type 0xC021, datagramsize 14
link[ppp]
*Aug 17 19:06:50.868: Se0/0/0 LCP: I CONFACK [ACKsent] id 2 len 10
*Aug 17 19:06:50.868: Se0/0/0 LCP:    MagicNumber 0x63BD388C
(0x050663BD388C)
*Aug 17 19:06:50.868: Se0/0/0 LCP: State is Open
*Aug 17 19:06:50.872: Se0/0/0 PPP: Phase is FORWARDING, Attempting
Forward
*Aug 17 19:06:50.872: Se0/0/0 PPP: Phase is ESTABLISHING, Finish LCP
*Aug 17 19:06:50.872: Se0/0/0 PPP: Phase is UP
*Aug 17 19:06:50.872: Se0/0/0 IPCP: O CONFREQ [Closed] id 1 len 10
*Aug 17 19:06:50.872: Se0/0/0 IPCP:    Address 10.1.1.2
(0x03060A010102)
*Aug 17 19:06:50.872: Se0/0/0 CDPCP: O CONFREQ [Closed] id 1 len 4
*Aug 17 19:06:50.872: Se0/0/0 PPP: Process pending ncp packets
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14
link[ip]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: I CONFREQ [REQsent] id 1 len 10
*Aug 17 19:06:50.876: Se0/0/0 IPCP:    Address 10.1.1.1
```

```
(0x03060A010101)
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8
link[cdp]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: O CONFACK [REQsent] id 1 len 10
*Aug 17 19:06:50.876: Se0/0/0 IPCP:    Address 10.1.1.1
(0x03060A010101)
*Aug 17 19:06:50.876: Se0/0/0 CDPCP: I CONFREQ [REQsent] id 1 len 4
*Aug 17 19:06:50.876: Se0/0/0 CDPCP: O CONFACK [REQsent] id 1 len 4
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8021, datagramsize 14
link[ip]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: I CONFACK [ACKse
R2(config-if)#nt] id 1 len 10
*Aug 17 19:06:50.876: Se0/0/0 IPCP:    Address 10.1.1.2
(0x03060A010102)
*Aug 17 19:06:50.876: Se0/0/0 IPCP: State is Open
*Aug 17 19:06:50.876: Se0/0/0 PPP: I pkt type 0x8207, datagramsize 8
link[cdp]
*Aug 17 19:06:50.876: Se0/0/0 IPCP: Install route to 10.1.1.1
*Aug 17 19:06:50.880: Se0/0/0 CDPCP: I CONFACK [ACKsent] id 1 len 4
*Aug 17 19:06:50.880: Se0/0/0 CDPCP: State is Open
*Aug 17 19:06:50.880: Se0/0/0 PPP: O pkt type 0x0021, datagramsize 80
*Aug 17 19:06:50.880: Se0/0/0 IPCP: Add link info for cef entry
10.1.1.1
*Aug 17 19:06:50.884: Se0/0/0 PPP: I pkt type 0x0021, datagramsize 80
link[ip]
*Aug 17 19:06:51.848: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#
*Aug 17 19:06:51.888: Se0/0/0 LCP-FS: I ECHOREQ [Open] id 1 len 12
magic 0x63BDB9A8
*Aug 17 19:06:51.888: Se0/0/0 LCP-FS: O ECHOREP [Open] id 1 len 12
magic 0x63BD388C

<output omitted>

*Aug 17 19:07:00.936: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
```

¿Qué sucede cuando un extremo del enlace serial se encapsula con PPP y el otro extremo del enlace se encapsula con HDLC?

_____

_____

_____

El enlace deja de funcionar y se interrumpe la adyacencia OSPF. PPP sigue intentando establecer una conexión con el extremo opuesto del enlace. Sin embargo, dado que sigue recibiendo un paquete no NCP, descarta el paquete y no activa el enlace.

¿Cuáles son los pasos que atraviesa PPP cuando el otro extremo del enlace serial en R2 se configura con la encapsulación PPP?

_____

_____

_____

_____

_____

_____

PPP atraviesa las siguientes etapas:

DOWN

ESTABLISHING, Active Open

LCP: State is Open

ESTABLISHING, Finish LCP

UP

¿Qué sucede cuando la encapsulación PPP se configura en cada extremo del enlace serial?

_____

_____

El enlace se activa y se restablece la adyacencia OSPF.

Paso 4: Desactivar la depuración.

Desactive la depuración si aún no utilizó el comando **undebug all**.

```
R1#undebug all
Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off
R1#

R2#undebug all
Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off
R2#
```

Paso 5: Cambiar la encapsulación de HDLC a PPP en ambos extremos del enlace serial entre R2 y R3.

```
R2(config)#interface serial0/0/1
R2(config-if)#encapsulation ppp
R2(config-if)#
*Aug 17 20:02:08.080: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
R2(config-if)#
*Aug 17 20:02:13.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
*Aug 17 20:02:58.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 17 20:03:03.644: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-if)#

*Aug 17 20:03:46.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R3(config)#interface serial 0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#
*Aug 17 20:04:27.152: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
*Aug 17 20:04:30.952: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
```

¿Cuándo se activa el protocolo de línea en el enlace serial y se restablece la adyacencia OSPF?

_____

_____

Sólo después de que **ambos** extremos del enlace serial se encapsulan con PPP.

Paso 7: Verificar que PPP sea ahora la encapsulación en las interfaces seriales.

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>
```

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>

R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.2.2.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

<output omitted>
```

Tarea 7: Interrumpir y restablecer la encapsulación PPP

Al interrumpir intencionalmente la encapsulación PPP, se aprenderá acerca de los mensajes de error que se generan. Esto ayudará más adelante en la práctica de laboratorio de resolución de problemas.

Paso 1: Restablecer ambas interfaces seriales en R2 a su encapsulación HDLC por defecto.

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:36:48.432: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
*Aug 17 20:36:49.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R2(config-if)#
*Aug 17 20:36:51.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#interface serial 0/0/1
*Aug 17 20:37:14.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R2(config-if)#encapsulation hdlc
```

```
R2(config-if)#
*Aug 17 20:37:17.368: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
*Aug 17 20:37:18.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
*Aug 17 20:37:20.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 17 20:37:44.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
```

¿Por qué resulta útil interrumpir intencionalmente una configuración?

_____

_____

_____

La familiarización con las distintas maneras en que se puede interrumpir intencionalmente un protocolo ayudará a ver de qué manera se puede interrumpir un protocolo involuntariamente. Esto es muy útil cuando deba resolver los problemas en la práctica de laboratorio de resolución de problemas.

¿Por qué ambas interfaces se desactivan, luego se activan y finalmente vuelven a desactivarse?

_____

_____

_____

Las interfaces se desactivan inicialmente porque no hay concordancia entre sus tipos de encapsulación. Luego, las interfaces vuelven a activarse para que puedan tratar de restablecer una conexión. Cuando las interfaces no pueden reestablecer una conexión correctamente, se desactivan otra vez.

¿Hay otra forma de cambiar la encapsulación de una interfaz serial de PPP a la encapsulación HDLC por defecto que no sea mediante el comando **encapsulation hdlc**? (Ayuda: está relacionada con el comando **no**).

_____

_____

_____

_____

_____

_____

```
R2(config)#interface serial 0/0/0
R2(config-if)#no encapsulation ppp
R2(config-if)#interface serial 0/0/1
R2(config-if)#no encapsulation ppp
```

Paso 2: Restablecer ambas interfaces seriales en R2 a la encapsulación PPP.

```
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
*Aug 17 20:53:06.612: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#interface s0/0/1
*Aug 17 20:53:10.856: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#encapsulation ppp
*Aug 17 20:53:23.332: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 17 20:53:24.916: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-if)#
```

Tarea 8: Configurar la autenticación PPP

Paso 1: Configurar la autenticación PPP PAP en el enlace serial entre R1 y R2.

```
R1(config)#username R1 password cisco
R1(config)#int s0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#
*Aug 22 18:58:57.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R1(config-if)#
*Aug 22 18:58:58.423: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Interface down or
detached
R1(config-if)#ppp pap sent-username R2 password cisco
```

¿Qué sucede cuando la autenticación PPP PAP sólo se configura en un extremo del enlace serial?

_____

_____

El protocolo de línea de la interfaz serial 0/0/0 se desactiva y la adyacencia OSPF ingresa al estado DOWN.

```
R2(config)#username R2 password cisco
R2(config)#interface Serial0/0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R1 password cisco
R2(config-if)#
*Aug 23 16:30:33.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to up
R2(config-if)#
*Aug 23 16:30:40.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#
```

¿Qué sucede cuando la autenticación PPP PAP se configura en ambos extremos del enlace serial?

_____

_____

El protocolo de línea de la interfaz serial 0/0/0 se activa y se establece la adyacencia OSPF.

Paso 2: Configurar la autenticación PPP CHAP en el enlace serial entre R2 y R3.

En la autenticación PAP, la contraseña no está encriptada. Aunque sin dudas esto es mejor que la falta total de autenticación, es aún mucho mejor encriptar la contraseña que se envía a través del enlace. CHAP encripta la contraseña.

```
R2(config)#username R3 password cisco
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 23 18:06:00.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#
*Aug 23 18:06:01.947: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
R2(config-if)#

R3(config)#username R2 password cisco
*Aug 23 18:07:13.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#int s0/0/1
R3(config-if)#
*Aug 23 18:07:22.174: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-if)#ppp authentication chap
R3(config-if)#
```

Observe que el protocolo de línea en la interfaz serial 0/0/1 cambia su estado a UP incluso antes de que se configure la interfaz para la autenticación CHAP. ¿Puede adivinar por qué sucede esto?

_____

_____

_____

CHAP puede realizar una autenticación unidireccional y bidireccional. Por lo tanto, el enlace se activa cuando se configuran el nombre de usuario y la contraseña correctos.

Paso 3: Revisar el resultado de la depuración.

Para comprender mejor el proceso CHAP, observe el resultado del comando **debug ppp authentication** en R2 y R3. Luego desactive la interfaz serial 0/0/1 en R2 y ejecute el comando **no shutdown** en la interfaz serial 0/0/1 en R2.

```
R2#debug ppp authentication
PPP authentication debugging is on
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#shutdown
R2(config-if)#
*Aug 23 18:19:21.059: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
R2(config-if)#
*Aug 23 18:19:23.059: %LINK-5-CHANGED: Interface Serial0/0/1, changed
state to administratively down
*Aug 23 18:19:24.059: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R2(config-if)#no shutdown

*Aug 23 18:19:55.059: Se0/0/1 PPP: Using default call direction
*Aug 23 18:19:55.059: Se0/0/1 PPP: Treating connection as a dedicated
line
*Aug 23 18:19:55.059: Se0/0/1 PPP: Session handle[5B000005] Session
id[49]
*Aug 23 18:19:55.059: Se0/0/1 PPP: Authorization required
*Aug 23 18:19:55.063: %LINK-3-UPDOWN: Interface Serial0/0/1, changed
state to up
*Aug 23 18:19:55.063: Se0/0/1 CHAP: O CHALLENGE id 48 len 23 from "R2"
*Aug 23 18:19:55.067: Se0/0/1 CHAP: I CHALLENGE id 2 len 23 from "R3"
*Aug 23 18:19:55.067: Se0/0/1 CHAP: Using hostname from unknown source
*Aug 23 18:19:55.067: Se0/0/1 CHAP: Using password from AAA
*Aug 23 18:19:55.067: Se0/0/1 CHAP: O RESPONSE id 2 len 23 from "R2"
*Aug 23 18:19:55.071: Se0/0/1 CHAP: I RESPONSE id 48 len 23 from "R3"
*Aug 23 18:19:55.071: Se0/0/1 PPP: Sent CHAP LOGIN Request
*Aug 23 18:19:55.071: Se0/0/1 PPP: Received LOGIN Response PASS
*Aug 23 18:19:55.071: Se0/0/1 PPP: Sent LCP AUTHOR Request
*Aug 23 18:19:55.075: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*Aug 23 18:19:55.075: Se0/0/1 LCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:55.075: Se0/0/1 IPCP: Received AAA AUTHOR Response PASS
```

```
*Aug 23 18:19:55.075: Se0/0/1 CHAP: O SUCCESS id 48 len 4
*Aug 23 18:19:55.075: Se0/0/1 CHAP: I SUCCESS id 2 len 4
*Aug 23 18:19:55.075: Se0/0/1 PPP: Sent CDPCP AUTHOR Request
*Aug 23 18:19:55.075: Se0/0/1 CDPCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:55.079: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*Aug 23 18:19:56.075: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 23 18:20:05.135: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done

R3#debug ppp authentication
PPP authentication debugging is on
R3#
*Aug 23 18:19:04.494: %LINK-3-UPDOWN: Interface Serial0/0/1, changed
state to down
R3#
*Aug 23 18:19:04.494: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Interface down or
detached
*Aug 23 18:19:05.494: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
R3#
*Aug 23 18:19:36.494: %LINK-3-UPDOWN: Interface Serial0/0/1, changed
state to up
*Aug 23 18:19:36.494: Se0/0/1 PPP: Using default call direction
*Aug 23 18:19:36.494: Se0/0/1 PPP: Treating connection as a dedicated
line
*Aug 23 18:19:36.494: Se0/0/1 PPP: Session handle[3C000034] Session
id[52]
*Aug 23 18:19:36.494: Se0/0/1 PPP: Authorization required
*Aug 23 18:19:36.498: Se0/0/1 CHAP: O CHALLENGE id 2 len 23 from "R3"
*Aug 23 18:19:36.502: Se0/0/1 CHAP: I CHALLENGE id 48 len 23 from "R2"
*Aug 23 18:19:36.502: Se0/0/1 CHAP: Using hostname from unknown source
*Aug 23 18:19:36.506: Se0/0/1 CHAP: Using password from AAA
*Aug 23 18:19:36.506: Se0/0/1 CHAP: O RESPONSE id 48 len 23 from "R3"
*Aug 23 18:19:36.506: Se0/0/1 CHAP: I RESPONSE id 2 len 23 from "R2"
R3#
*Aug 23 18:19:36.506: Se0/0/1 PPP: Sent CHAP LOGIN Request
*Aug 23 18:19:36.506: Se0/0/1 PPP: Received LOGIN Response PASS
*Aug 23 18:19:36.510: Se0/0/1 PPP: Sent LCP AUTHOR Request
*Aug 23 18:19:36.510: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*Aug 23 18:19:36.510: Se0/0/1 LCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:36.510: Se0/0/1 IPCP: Received AAA AUTHOR Response PASS
*Aug 23 18:19:36.510: Se0/0/1 CHAP: O SUCCESS id 2 len 4
*Aug 23 18:19:36.510: Se0/0/1 CHAP: I SUCCESS id 48 len 4
*Aug 23 18:19:36.514: Se0/0/1 PPP: Sent CDPCP AUTHOR Request
*Aug 23 18:19:36.514: Se0/0/1 PPP: Sent IPCP AUTHOR Request
*Aug 23 18:19:36.514: Se0/0/1 CDPCP: Received AAA AUTHOR Response PASS
R3#
*Aug 23 18:19:37.510: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3#
*Aug 23 18:19:46.570: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3#
```

Tarea 9: Interrumpir intencionalmente y restablecer la autenticación PPP CHAP

Paso 1: Interrumpir la autenticación PPP CHAP.

En el enlace serial entre R2 y R3, cambie el protocolo de autenticación de la interfaz serial 0/0/1 a PAP.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication pap
R2(config-if)#^Z
R2#
*Aug 24 15:45:47.039: %SYS-5-CONFIG_I: Configured from console by
console
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
```

¿El cambio de protocolo de autenticación a PAP en la interfaz serial 0/0/1 produce la interrupción de la autenticación entre R2 y R3?

_____

_____

_____

Sí. Verifique que el protocolo esté desactivo mediante el comando **show ip interface brief**. Si no se recarga el router, el protocolo de línea permanece activo.

```
R2#show ip int brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES NVRAM  administratively down down
FastEthernet0/1 unassigned   YES NVRAM  administratively down down
Serial0/0/0     10.1.1.2     YES NVRAM  up                    up
Serial0/0/1     10.2.2.1     YES NVRAM  up                    down
Serial0/1/0     unassigned   YES NVRAM  administratively down down
Serial0/1/1     unassigned   YES NVRAM  administratively down down
Loopback0    209.165.200.225 YES NVRAM  up                    up
```

Paso 2: Restablecer la autenticación PPP CHAP en el enlace serial.

Tenga en cuenta que no es necesario recargar el router para que este cambio surta efecto.

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 24 15:50:00.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R2(config-if)#
*Aug 24 15:50:07.467: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOADING to FULL, Loading Done
R2(config-if)#
```

Paso 3: Interrumpir intencionalmente la autenticación PPP CHAP al cambiar la contraseña en R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password ciisco
R3(config)#^Z
R3#
*Aug 24 15:54:17.215: %SYS-5-CONFIG_I: Configured from console by
console
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
```

Después de la recarga, ¿cuál es el estado del protocolo de línea en serial 0/0/1?

_____

_____

Down. Verifique esto mediante el comando **show ip interface brief**.

```
R3#show ip int brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES NVRAM  administratively down down
FastEthernet0/1 192.168.30.1 YES NVRAM  up                    up
Serial0/0/0     unassigned   YES NVRAM  administratively down down
Serial0/0/1     10.2.2.2     YES NVRAM  up                    down
```

Paso 4: Restablecer la autenticación PPP CHAP al cambiar la contraseña en R3.

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password cisco
R3(config)#
*Aug 24 16:11:10.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#
*Aug 24 16:11:19.739: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
```

Tarea 10: Documentar las configuraciones del router

En cada router, ejecute el comando **show run** y capture las configuraciones.

```
R1#show run
!<resultado omitido>
!
hostname R1
!
!
enable secret class
!
!
!
no ip domain lookup
!
username R1 password 0 cisco
!
!
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication pap
 ppp pap sent-username R2 password 0 cisco
 no shutdown
!
!
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

```
R2#show run
!<resultado omitido>

!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
username R3 password 0 cisco
username R2 password 0 cisco
!
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp pap sent-username R1 password 0 cisco
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to
the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
```

```
end

R3#show run
!<resultado omitido>

!
hostname R3
!
!
enable secret class
!
!
!
no ip domain lookup
!
username R2 password 0 cisco
!
!
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to
the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Tarea 11: 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.

Práctica de laboratorio 2.5.2: Reto de configuración de PPP (Versión para el instructor)

Diagrama de topología

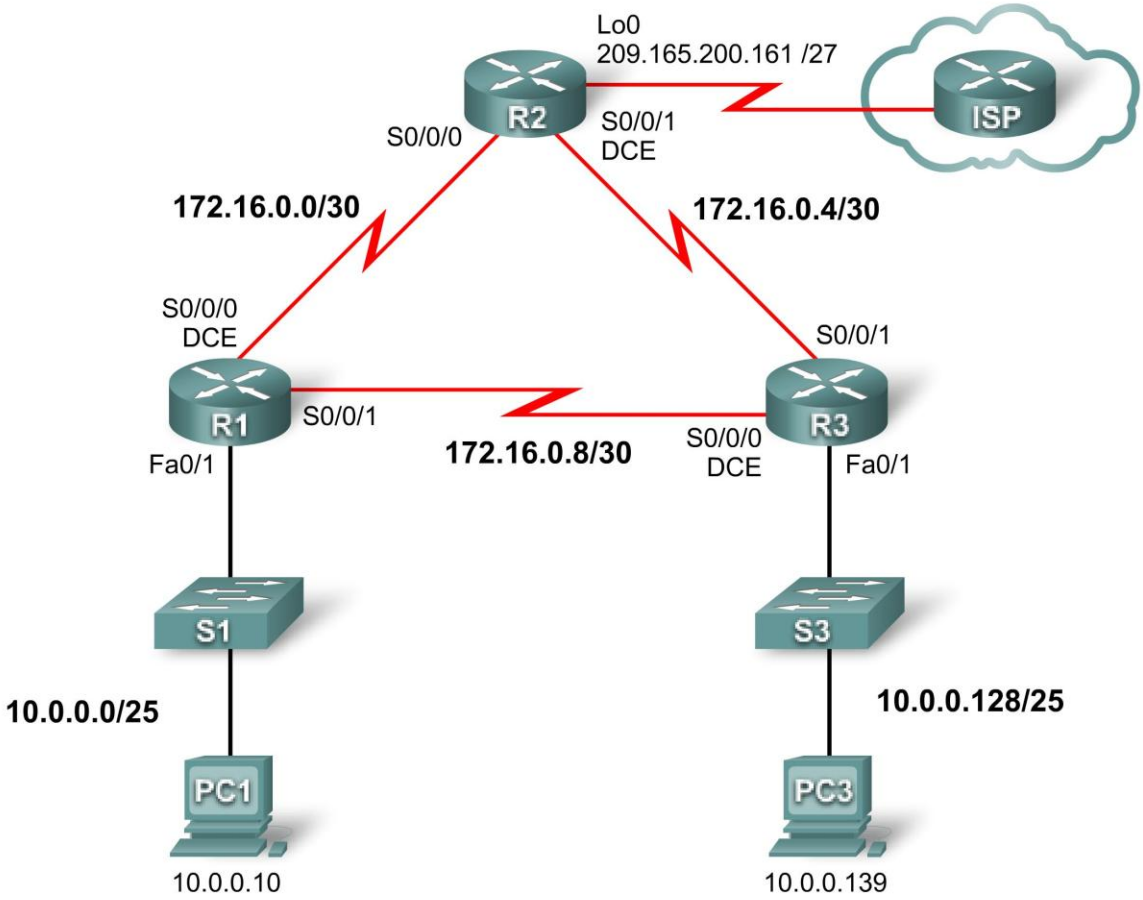


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/1**	10.0.0.1	255.255.255.128	N/C
	S0/0/0	172.16.0.1	255.255.255.252	N/C
	S0/0/1	172.16.0.9	255.255.255.252	N/C
R2	**Lo0**	209.165.200.161	255.255.255.224	N/C
	S0/0/0	172.16.0.2	255.255.255.252	N/C
	S0/0/1	172.16.0.5	255.255.255.252	N/C

R3	**Fa0/1**	10.0.0.129	255.255.255.128	N/C
	S0/0/0	172.16.0.10	255.255.255.252	N/C
	S0/0/1	172.16.0.6	255.255.255.252	N/C
PC1	**NIC**	10.0.0.10	255.255.255.128	10.0.0.1
PC3	**NIC**	10.0.0.139	255.255.255.128	10.0.0.129

Objetivos de aprendizaje

Para completar esta práctica de laboratorio:

- Cablear una red según el diagrama de topología
- Borrar la configuración de inicio y recargar un router al estado por defecto
- Realizar tareas de configuración básicas en un router
- Configurar y activar interfaces
- Configurar el enrutamiento OSPF en todos los routers
- Configurar la encapsulación PPP en todas las interfaces seriales
- Cambiar la encapsulación de las interfaces seriales de PPP a HDLC.
- Interrumpir intencionalmente y restablecer la encapsulación PPP
- Configurar la autenticación PPP CHAP
- Interrumpir intencionalmente y restablecer la autenticación PPP CHAP

Escenario

En esta práctica de laboratorio, se aprenderá a configurar la encapsulación PPP en enlaces seriales a través de la red que se muestra en el diagrama de topología. Además, se configurará la autenticación PPP CHAP. Si se necesita ayuda, se debería volver a consultar la práctica de laboratorio de configuración básica de PPP. Sin embargo, el usuario debería intentar resolver todo lo que pueda por su cuenta.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar la configuración básica del router

Configure los routers R1, R2 y R3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de Modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.

- Configure el registro de datos sincrónico.
- Configure una contraseña para las conexiones de vty.

```
enable
configure terminal
no ip domain-lookup
enable secret class
banner motd ^CUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
end
copy running-config starting-config
```

Tarea 3: Configurar y activar las direcciones serial y Ethernet

Paso 1: Configurar las interfaces de R1, R2 y R3.

R1

```
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 no shutdown
!

interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 no shutdown
 clock rate 64000
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 no shutdown
```

R2

```
!
interface Loopback0
 ip address 209.165.200.161 255.255.255.224
!
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
```

```
 clock rate 64000
 no shutdown
```

R3

```
!
interface FastEthernet0/1
 ip address 10.0.0.129 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.6 255.255.255.252
 clock rate 64000
 no shutdown
```

Paso 2: Verificar el direccionamiento IP y las interfaces.

```
R1#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES manual administratively down down
FastEthernet0/1 10.0.0.1     YES manual up                    up
Serial0/0/0     172.16.0.1   YES manual up                    up
Serial0/0/1     172.16.0.9   YES manual up                    up

R2#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES unset  administratively down down
FastEthernet0/1 unassigned   YES unset  administratively down down
Serial0/0/0     172.16.0.2   YES manual up                    up
Serial0/0/1     172.16.0.5   YES manual up                    up
Loopback0    209.165.200.161 YES manual up                    up

R3#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES unset  administratively down down
FastEthernet0/1 10.0.0.129   YES manual up                    up
Serial0/0/0     172.16.0.10  YES manual up                    up
Serial0/0/1     172.16.0.6   YES manual up                    up
```

Paso 3: Configurar las interfaces Ethernet de PC1 y PC3.

Paso 4: Probar la conectividad entre los equipos PC.

Tarea 4: Configurar OSPF en los routers

Paso 1: Configurar el enrutamiento OSPF en los routers.

R1

```
!
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
```

```
!
R2
!
router ospf 1
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.160 0.0.0.31 area 0
!
R3
!
router ospf 1
 network 10.0.0.128 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
```

Paso 2: Verificar que haya conectividad completa en la red.

```
R1#show ip route

<output omitted>

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.0.8 is directly connected, Serial0/0/1
O       172.16.0.4 [110/1562] via 172.16.0.10, 00:09:11, Serial0/0/1
                   [110/1562] via 172.16.0.2, 00:09:11, Serial0/0/0
C       172.16.0.0 is directly connected, Serial0/0/0
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.161 [110/782] via 172.16.0.2, 00:09:11, Serial0/0/0
     10.0.0.0/25 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
O       10.0.0.128 [110/782] via 172.16.0.10, 00:09:11, Serial0/0/1

R1#ping 209.165.200.161

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.161, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1#ping 10.0.0.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R2#show ip route

<output omitted>

     172.16.0.0/30 is subnetted, 3 subnets
O       172.16.0.8 [110/1562] via 172.16.0.6, 00:12:42, Serial0/0/1
                   [110/1562] via 172.16.0.1, 00:12:42, Serial0/0/0
C       172.16.0.4 is directly connected, Serial0/0/1
C       172.16.0.0 is directly connected, Serial0/0/0
     209.165.200.0/27 is subnetted, 1 subnets
```

```
C       209.165.200.160 is directly connected, Loopback0
     10.0.0.0/25 is subnetted, 2 subnets
O       10.0.0.0 [110/782] via 172.16.0.1, 00:12:42, Serial0/0/0
O       10.0.0.128 [110/782] via 172.16.0.6, 00:12:42, Serial0/0/1

R2#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R2#ping 10.0.0.129

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.129, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R3#show ip route

<output omitted>

     172.16.0.0/30 is subnetted, 3 subnets
C       172.16.0.8 is directly connected, Serial0/0/0
C       172.16.0.4 is directly connected, Serial0/0/1
O       172.16.0.0 [110/1562] via 172.16.0.9, 00:14:14, Serial0/0/0
                   [110/1562] via 172.16.0.5, 00:14:14, Serial0/0/1
     209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.161 [110/782] via 172.16.0.5, 00:14:14, Serial0/0/1
     10.0.0.0/25 is subnetted, 2 subnets
O       10.0.0.0 [110/782] via 172.16.0.9, 00:14:14, Serial0/0/0
C       10.0.0.128 is directly connected, FastEthernet0/1

R3#ping 209.165.200.161

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.161, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R3#ping 10.0.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

Tarea 5: Configurar la encapsulación PPP en interfaces seriales

Paso 1: Configurar PPP en las interfaces seriales de los tres routers.

R1

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

R2

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

R3

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

Paso 2: Verificar que todas las interfaces seriales utilicen la encapsulación PPP.

R1

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

R1#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.9/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

R2

```
R2#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

R2#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.5/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

R3

```
R3#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.10/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set

R3#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.6/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

Tarea 6: Interrumpir intencionalmente y restablecer la encapsulación PPP

Paso 1: Elegir una manera de interrumpir la encapsulación PPP en la red.

R1

```
interface Serial0/0/0
 encapsulation hdlc
```

R2

```
interface Serial0/0/1
 encapsulation hdlc
```

R3

```
interface Serial0/0/0
 encapsulation hdlc
```

Paso 2: Restablecer la conectividad completa en la red.

R1

```
interface Serial0/0/0
 encapsulation ppp
```

R2

```
interface Serial0/0/1
 encapsulation ppp
```

R3

```
interface Serial0/0/0
 encapsulation ppp
```

Paso 3: Verificar la conectividad completa en la red.

```
R1#show ip route
R2#show ip route
R3#show ip route
username R2 password cisco
username R3 password cisco
interface serial0/0/0
ppp authentication chap
interface serial0/0/1
ppp authentication chap
```

Tarea 7: Configurar la autenticación PPP CHAP

Paso 1: Configurar la autenticación PPP CHAP en todos los enlaces seriales.

R1

```
username R2 password cisco
username R3 password cisco
interface serial0/0/0
ppp authentication chap
interface serial0/0/1
ppp authentication chap
```

R2

```
username R1 password cisco
username R3 password cisco
interface serial0/0/0
ppp authentication chap
interface serial0/0/1
ppp authentication chap
```

R3

```
username R1 password cisco
username R2 password cisco
interface serial0/0/0
ppp authentication chap
interface serial0/0/1
ppp authentication chap
```

Paso 2: Verificar la autenticación PPP CHAP en todos los enlaces seriales.

```
R1#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES manual administratively down down
FastEthernet0/1 10.0.0.1     YES manual up                    up
Serial0/0/0     172.16.0.1   YES manual up                    up
Serial0/0/1     172.16.0.9   YES manual up                    up

R2#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES unset  administratively down down
FastEthernet0/1 unassigned   YES unset  administratively down down
Serial0/0/0     172.16.0.2   YES manual up                    up
Serial0/0/1     172.16.0.5   YES manual up                    up
Loopback0    209.165.200.161 YES manual up                    up

R3#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES unset  administratively down down
FastEthernet0/1 10.0.0.129   YES manual up                    up
Serial0/0/0     172.16.0.10  YES manual up                    up
Serial0/0/1     172.16.0.6   YES manual up                    up
```

Tarea 8: Interrumpir intencionalmente y restablecer la autenticación PPP CHAP

Paso 1: Elegir una manera de interrumpir la autenticación PPP CHAP en uno o más enlaces seriales.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial 0/0/0
R1(config-if)#no ppp authentication chap
R1(config-if)#ppp authentication pap
R1(config-if)#interface serial0/0/1
R1(config-if)#no ppp authentication chap
R1(config-if)#ppp authentication pap
R1(config-if)#^Z
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#reload
```

Paso 2: Verificar que la autenticación PPP CHAP se interrumpa.

```
R1#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES NVRAM  administratively down down
FastEthernet0/1 10.0.0.1     YES NVRAM  up                    up
Serial0/0/0     172.16.0.1   YES NVRAM  up                    down
Serial0/0/1     172.16.0.9   YES NVRAM  up                    down
```

Paso 3: Restablecer la autenticación PPP CHAP en todos los enlaces seriales.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial0/0/0
R1(config-if)#ppp authentication chap
R1(config-if)#interface serial0/0/1
R1(config-if)#ppp authentication chap
R1(config-if)#^Z
R1#
```

Paso 4: Verificar la autenticación PPP CHAP en todos los enlaces seriales.

```
R1#show ip interface brief
Interface       IP-Address   OK? Method Status                Protocol
FastEthernet0/0 unassigned   YES NVRAM  administratively down down
FastEthernet0/1 10.0.0.1     YES NVRAM  up                    up
Serial0/0/0     172.16.0.1   YES NVRAM  up                    up
Serial0/0/1     172.16.0.9   YES NVRAM  up                    up
```

Tarea 9: Documentar las configuraciones del router

R1

```
R1#show run

!<resultado omitido>
!
hostname R1
!
!
enable secret class
!
!
no ip domain lookup
!
username R3 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
```

```
!
!
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R2

```
R2#show run

!<resultado omitido>
!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R3 password 0 cisco
!
!
!
interface Loopback0
 ip address 209.165.200.161 255.255.255.224
!
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
 encapsulation ppp
 clockrate 64000
```

```
 ppp authentication chap
 no shutdown
!
!
router ospf 1
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.160 0.0.0.31 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R3

```
R3#show run
!<resultado omitido>
!
hostname R3
!
!
enable secret class
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.129 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
```

```
interface Serial0/0/1
 ip address 172.16.0.6 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
router ospf 1
 network 10.0.0.128 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted
to the full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Tarea 10: 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.

Práctica de laboratorio 2.5.3: Resolución de problemas de la configuración PPP (Versión para el instructor)

Diagrama de topología

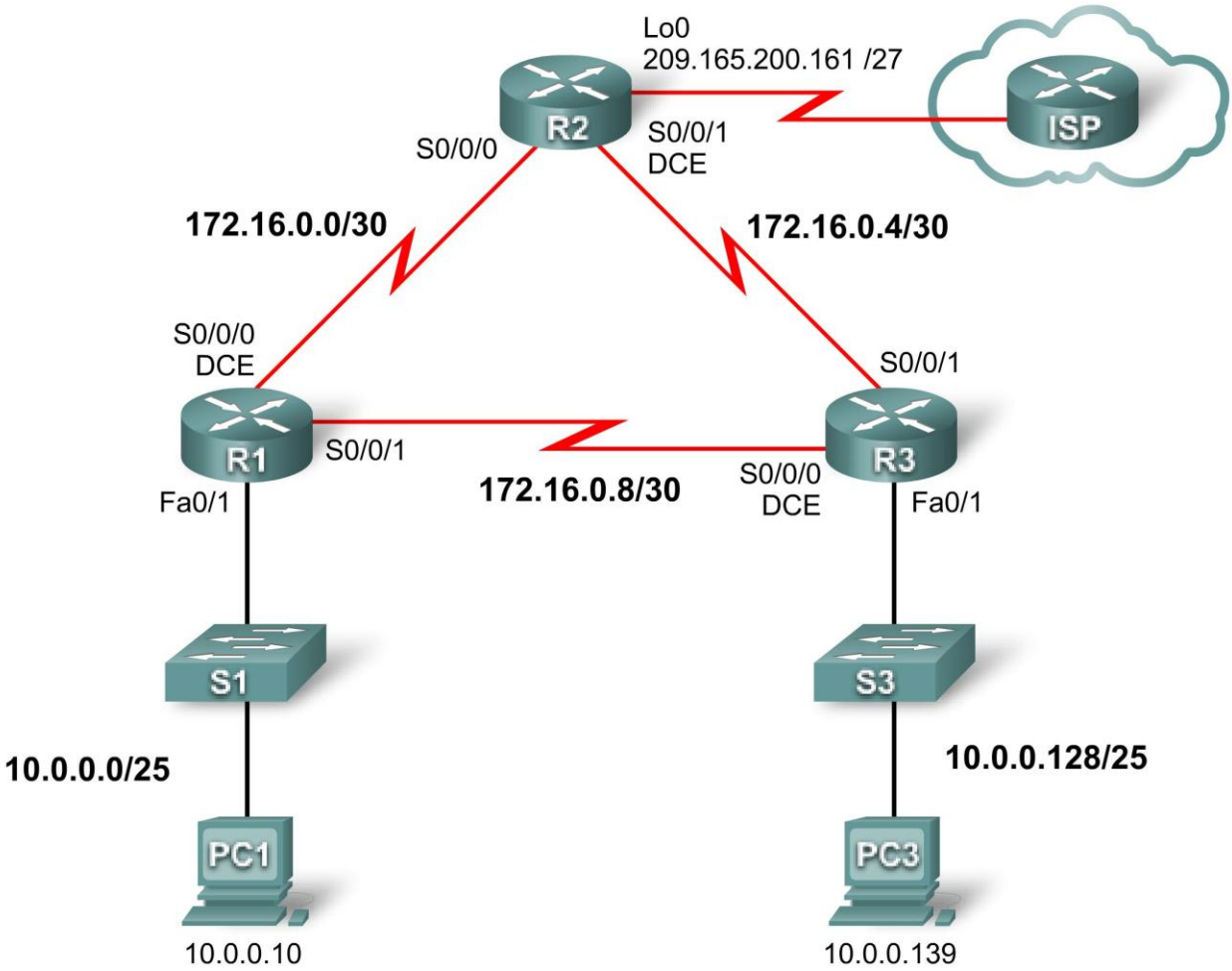


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/1**	10.0.0.1	255.255.255.128	N/C
	S0/0/0	172.16.0.1	255.255.255.252	N/C
	S0/0/1	172.16.0.9	255.255.255.252	N/C
R2	**Lo0**	209.165.200.161	255.255.255.224	N/C
	S0/0/0	172.16.0.2	255.255.255.252	N/C
	S0/0/1	172.16.0.5	255.255.255.252	N/C

R3	**Fa0/1**	10.0.0.129	255.255.255.128	N/C
	S0/0/0	172.16.0.10	255.255.255.252	N/C
	S0/0/1	172.16.0.6	255.255.255.252	N/C
PC1	**NIC**	10.0.0.10	255.255.255.128	10.0.0.1
PC3	**NIC**	10.0.0.139	255.255.255.128	10.0.0.129

Objetivos de aprendizaje

Para completar esta práctica de laboratorio:

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

Escenario

Un ingeniero de redes inexperto configuró los routers de la compañía. Diversos errores en la configuración produjeron problemas de conectividad. El jefe le solicitó al usuario que resuelva y corrija los errores de configuración y que documente su trabajo. Según los conocimientos de PPP y los métodos de prueba estándar, busque y corrija los errores. Asegúrese de que todos los enlaces seriales utilicen la autenticación PPP CHAP y de que todas las redes sean alcanzables.

Tarea 1: Cargar los routers con los guiones suministrados

[Nota para el instructor: Los comandos faltantes o mal configurados se muestran en rojo].

R1

```
enable
configure terminal
!
hostname R1
!
!
enable secret class
!
!
!
no ip domain lookup
!
username R2 password 0 cisco
username R3 password 0 cisco
!Este comando se omitió
!
!
!
```

```
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.128
 !Un error habitual al configurar redes es colocar la configuración correcta
en el lugar incorrecto. En este caso, un análisis minucioso del diagrama
revela que FastEthernet0/1 debería tener esta dirección IP.
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.248
 !máscara de subred incorrecta. La máscara de subred correcta es 255.255.255.252
 no fair-queue
 clockrate 64000
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp authentication chap
!Por error, en lugar de la autenticación CHAP se configuró la autenticación
PPP PAP
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
 network 172.16.0.0 0.0.0.3 area 0
!En OSPF se anunciaba una subred incorrecta
!
ip classless
!
ip http server
!
!
control-plane
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R2

```
enable
configure terminal
!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
username R11 password 0 cisco
!R1 se escribió como R11.  Éste es un error común en la configuración.
username R1 password 0 cisco
username R3 password 0 class
!
!
!
interface Loopback0
 no ip address
 ip address 209.165.200.161 255.255.255.224
!La dirección IP correcta se colocó en la interfaz equivocada
(FastEthernet0/1)
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 209.165.200.161 255.255.255.224
 ip address 10.0.0.1 255.255.255.128
!Un análisis minucioso del diagrama de topología revela que la dirección IP
correcta se colocó en la interfaz equivocada. Esta dirección IP pertenece a
la interfaz Loopback0
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 encapsulation ppp
 no fair-queue
 ppp authentication chap
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
!Se dejó la encapsulación serial HDLC por defecto.  Se omitieron los
siguientes comandos:
encapsulation ppp
 clockrate 64000
 ppp authentication chap

!
```

```
router ospf 1
 log-adjacency-changes
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.128 0.0.0.31 area 0
 network 209.165.200.160 0.0.0.31 area 0
!En OSPF se anunció la subred incorrecta para la red 209
ip classless
!
ip http server
!
!
control-plane
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R3

```
enable
configure terminal
!
hostname R3
!
!
enable secret class
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R3 password 0 ciscco
username R3 password 0 cisco
!Otro error tipográfico. Esta vez la contraseña interrumpe esta
configuración.
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.0.0.129 255.255.255.0
```

```
 ip address 10.0.0.129 255.255.255.128
!Debido a que tantas prácticas de laboratorio usan la subred /24, es fácil
acostumbrarse a escribir esta subred sin verificar el diagrama y sin pensar.
duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 no fair-queue
 clockrate 64000
!PPP y CHAP NO se configuraron en esta interfaz. Faltan los siguientes
comandos:
 encapsulation ppp
 ppp authentication chap
!
interface Serial0/0/1
 no ip address
 ip address 172.16.0.6 255.255.255.252
 encapsulation ppp
 ppp authentication pap
 ppp authentication chap
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.128 0.0.0.127 area 0
 network 192.16.0.4 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 192.16.0.8 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
ip classless
!
ip http server
!
!
control-plane
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Tarea 2: Buscar y corregir errores de red

Detecte, documente y corrija cada uno de los errores mediante métodos estándar de resolución de problemas.

Nota: Si se estuviese haciendo la resolución de problemas de una red de producción y la tarea de configuración consistiera en configurar PPP CHAP, y esto no funcionara, lo primero que se verificaría sería la configuración PPP CHAP. Sin embargo, en las configuraciones de la red dividida de esta práctica de laboratorio, eso sólo dejaría al usuario a mitad de camino en su propósito de restablecer la red. A menudo hay ingenieros de red muy avanzados que cuando realizan la resolución problemas se centran sólo en la tarea principal de configuración y no verifican los principios básicos. ¿Se escribieron correctamente las direcciones de red? ¿Se escribieron correctamente las subredes? ¿Funciona el enrutamiento básico? Si el enfoque en la tarea principal de resolución de problemas resolviera el problema, sería excelente. De lo contrario, debería volver a los principios básicos. Ésta es una metodología segura de resolución de problemas.

Tarea 3: Documentar la red corregida

Ahora que se corrigieron todos los errores y se probó la conectividad en toda la red, debe documentarse la configuración final de cada dispositivo.

R1

```
R1#show run

!<resultado omitido>
!
hostname R1
!
!
enable secret class
!
!
no ip domain lookup
!
username R3 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
!
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
```

```
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R2

```
R2#show run

!<resultado omitido>
!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R3 password 0 cisco
!
!
!
interface Loopback0
 ip address 209.165.200.161 255.255.255.224
!
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
!
router ospf 1
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.160 0.0.0.31 area 0
```

```
!
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

R3

```
R3#show run
!<resultado omitido>
!
hostname R3
!
!
enable secret class
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.129 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.6 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
router ospf 1
 network 10.0.0.128 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
!
```

```
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Tarea 4: 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.

Práctica de laboratorio 3.5.1: Frame Relay básico (Versión para el instructor)

Diagrama de topología

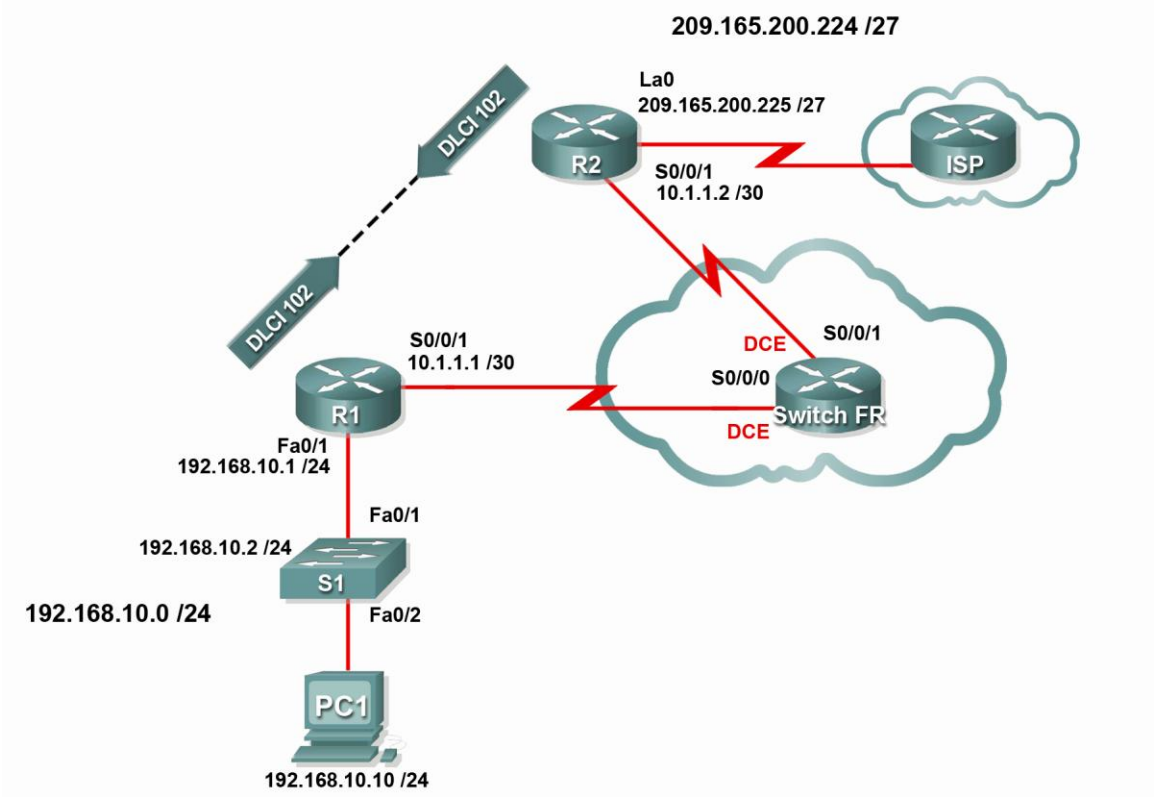


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/0**	192.168.10.1	255.255.255.0	N/C
	S0/0/1	10.1.1.1	255.255.255.252	N/C
R2	**S0/0/1**	10.1.1.2	255.255.255.252	N/C
	Lo 0	209.165.200.225	255.255.255.224	N/A
S1	**VLAN1**	192.168.10.2	255.255.255.0	192.168.10.1
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1

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
- Realizar tareas de configuración básicas en un router
- Configurar y activar interfaces
- Configurar el enrutamiento EIGRP en todos los routers
- Configurar la encapsulación Frame Relay en todas las interfaces seriales
- Configurar un router como switch Frame Relay
- Comprender los resultados de los comandos **show frame-relay**
- Aprender los efectos del comando **debug frame-relay lmi**
- Interrumpir intencionalmente y restaurar un enlace Frame Relay
- Cambiar el tipo de encapsulación Frame Relay del tipo por defecto de Cisco a IETF
- Cambiar el tipo de LMI Frame Relay de Cisco a ANSI
- Configurar una subinterfaz Frame Relay

Escenario

En esta práctica de laboratorio, se aprenderá a configurar la encapsulación Frame Relay en enlaces seriales a través de la red que se muestra en el diagrama de topología. También se aprenderá a configurar un router como switch Frame Relay. Existen estándares tanto de Cisco como abiertos que se aplican a Frame Relay. Se aprenderán ambos. Se debe prestar especial atención a la sección de práctica de laboratorio en donde se deben interrumpir intencionalmente las configuraciones Frame Relay. Esto ayudará en la práctica de laboratorio de resolución de problemas relacionada con este capítulo.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en la topología. Las prácticas de laboratorio de Frame Relay, a diferencia de cualquier otra práctica de Exploration 4, tienen dos enlaces DCE en el mismo router. Asegúrese de cambiar el cableado para que refleje el diagrama de topología.

Nota: Si se utilizan los routers 1700, 2500 ó 2600, el resultado del router y las descripciones tienen un aspecto diferente.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar la configuración básica del router

Configure los routers R1 y R2, y el switch S1 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de Modo EXEC.
- Configure un mensaje del día.

- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para las conexiones de vty.
- Configure las direcciones IP en R1 y R2.

  Importante: Deje las interfaces seriales desactivadas.
- Active el EIGRP AS 1 en R1 y R2 para todas las redes.

```
enable
configure terminal
no ip domain-lookup
enable secret class
banner motd ^CUnauthorized access strictly prohibited, violators
will be prosecuted to the full extent of the law^C
!
!
!
line console 0
logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
end
copy running-config startup-config
```

!R1

```
interface serial 0/0/1
ip address 10.1.1.1 255.255.255.252
shutdown
!Las interfaces seriales deberían permanecer desactivadas hasta que
!se configure el switch Frame Relay

interface fastethernet 0/0
ip address 192.168.10.1 255.255.255.0
no shutdown
router eigrp 1
no auto-summary
network 10.0.0.0
network 192.168.10.0
!
```

!R2

```
interface serial 0/0/1
ip address 10.1.1.2 255.255.255.252
shutdown
!Las interfaces seriales deberían permanecer desactivadas hasta que
!se configure el switch Frame Relay
```

```
interface loopback 0
ip address 209.165.200.225 255.255.255.224
router eigrp 1
no auto-summary
network 10.0.0.0
network 209.165.200.0
!
```

Tarea 3: Configurar Frame Relay

Ahora se debe configurar una conexión Frame Relay punto a punto básica entre los routers 1 y 2. Primero se debe configurar el switch FR como switch Frame Relay y crear los DLCI.

¿Qué significa DLCI?

_____

Identificador de conexión de enlace de datos

¿Para qué se usa el DLCI?

_____

_____

Un DLCI es una dirección de la capa 2 que se asigna a una dirección IP de la capa 3.

¿Qué es un PVC y cómo se utiliza?

_____

_____

_____

Un PVC es un circuito virtual permanente, una conexión de la capa 2 creada entre extremos a través de una nube Frame Relay. Pueden existir varios PVC por interfaz física, lo que permite múltiples conexiones punto a punto o conexiones punto a multipunto.

Paso 1: Configurar el switch FR como switch Frame Relay y crear un PVC entre R1 y R2.

Este comando activa la conmutación Frame Relay en forma global en el router, lo que permite enviar tramas sobre según el DLCI entrante en lugar de la dirección IP:

```
FR-Switch(config)#frame-relay switching
```

Cambie el tipo de encapsulación de la interfaz a Frame Relay. Al igual que HDLC o PPP, Frame Relay es un protocolo de capa de enlace de datos que especifica el entramado del tráfico de la capa 2.

```
FR-Switch(config)#interface serial 0/0/0
FR-Switch(config)#clock rate 64000

FR-Switch(config-if)#encapsulation frame-relay
```

El cambio del tipo de interfaz a DCE le indica al router que envíe mensajes de actividad LMI y permite que se apliquen sentencias de ruta Frame Relay. No se pueden configurar los PVC mediante el comando **frame-relay route** entre dos interfaces DTE Frame Relay.

```
FR-Switch(config-if)#frame-relay intf-type dce
```

Nota: Los tipos de interfaz Frame Relay no tienen que coincidir con el tipo de la interfaz física subyacente. Una interfaz serial DTE física puede funcionar como una interfaz DCE Frame Relay y una interfaz DCE física puede funcionar como una interfaz DTE Frame Relay lógica.

Configure el router para que envíe el tráfico entrante en la interfaz serial 0/0/0 con DLCI 102 a serial 0/0/1 con un DLCI saliente de 201.

```
FR-Switch(config-if)#frame-relay route 102 interface serial 0/0/1 201
FR-Switch(config-if)#no shutdown
```

Esta configuración crea dos PVC: uno de R1 a R2 (DLCI 102) y el otro de R2 a R1 (DLCI 201). La configuración se puede verificar mediante el comando **show frame-relay pvc**.

```
FR-Switch(config-if)#interface serial 0/0/1
FR-Switch(config)#clock rate 64000
FR-Switch(config-if)#encapsulation frame-relay
FR-Switch(config-if)#frame-relay intf-type dce
FR-Switch(config-if)#frame-relay route 201 interface serial 0/0/0 102
FR-Switch(config-if)#no shutdown
```

```
FR-Switch#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

             Active     Inactive      Deleted       Static
  Local         0           0           0            0
  Switched      0           1           0            0
  Unused        0           0           0            0

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE =
Serial0/0/0

  input pkts 0             output pkts 0           in bytes 0
  out bytes 0              dropped pkts 0          in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0          out FECN pkts 0
  out BECN pkts 0          in DE pkts 0            out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
  Detailed packet drop counters:
  no out intf 0            out intf down 0         no out PVC 0
  in PVC down 0            out PVC down 0          pkt too big 0
  shaping Q full 0         pkt above DE 0          policing drop 0
  pvc create time 00:03:33, last time pvc status changed 00:00:19

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

             Active     Inactive      Deleted       Static
  Local         0           0           0            0
  Switched      0           1           0            0
  Unused        0           0           0            0
```

```
DLCI = 201, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE =
Serial0/0/1

  input pkts 0             output pkts 0           in bytes 0
  out bytes 0              dropped pkts 0          in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0          out FECN pkts 0
  out BECN pkts 0          in DE pkts 0            out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
  Detailed packet drop counters:
  no out intf 0            out intf down 0         no out PVC 0
  in PVC down 0            out PVC down 0          pkt too big 0
  shaping Q full 0         pkt above DE 0          policing drop 0
  pvc create time 00:02:02, last time pvc status changed 00:00:18
```

Observe el 1 en la columna Inactive (inactivo). El PVC que se creó no tiene ningún extremo configurado. El switch Frame Relay detecta esta situación y marcó el PVC como Inactive.

Ejecute el comando **show frame-relay route**. Este comando muestra las rutas Frame Relay existentes, sus interfaces, DLCI y estado. Ésta es la ruta de capa 2 que transporta el tráfico Frame Relay a través de la red. No confunda esto con el enrutamiento IP de la capa 3.

```
FR-Switch#show frame-relay route

Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial0/0/0     102             Serial0/0/1     201             inactive
Serial0/0/1     201             Serial0/0/0     102             inactive
```

Paso 2: Configurar R1 para Frame Relay.

El ARP inverso permite que los extremos distantes de un enlace Frame Relay se detecten dinámicamente entre sí y proporciona un método dinámico de asignación de direcciones IP a los DLCI. A pesar de que el ARP inverso es útil, no siempre es confiable. La práctica más recomendable consiste en asignar las direcciones IP a los DLCI en forma estática y desactivar inverse-arp.

```
R1(config)#interface serial 0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay inverse-arp
```

¿Por qué asignaría una dirección IP a un DLCI?

_____

_____

_____

_____

Cuando el router desea enviar tráfico a una dirección IP a través de un enlace Frame Relay, se debe indicar al switch de trama qué PVC debe atravesar el tráfico. Un switch de trama descarta todo el tráfico que reciba sin DLCI en el encabezado, ya que no tiene manera de determinar cómo enrutar los datos.

El comando **frame-realy map** asigna estáticamente una dirección IP a un DLCI. Además de asignar IP a un DLCI, el software IOS de Cisco permite asignar diversas direcciones del protocolo de capa 3. La palabra clave **broadcast** en el siguiente comando envía todo el tráfico multicast o broadcast destinado para este link a través del DLCI. La mayoría de los protocolos de enrutamiento requieren la palabra clave **broadcast** para funcionar correctamente sobre Frame Relay. También se puede utilizar la palabra clave **broadcast** en varios DLCI de la misma interfaz. El tráfico se reproduce a todos los PVC.

```
R1(config-if)#frame-relay map ip 10.1.1.2 102 broadcast
```

¿El DLCI está asignado a la dirección IP local o a la dirección IP del otro extremo del PVC?

_____

El DLCI está asignado a la dirección IP del extremo remoto del PVC.

```
R1(config-if)#no shutdown
```

¿Por qué se utiliza el comando **no shutdown** después del comando **no frame-relay inverse-arp**?

_____

_____

_____

_____

Si se escribe primero el comando **no shutdown**, es posible que ARP inverso permita que el Frame Relay aprenda las asignaciones de capa 2 a capa 3 que quizá el usuario no desea que aprenda. Al desactivar el ARP inverso de Frame Relay antes de ejecutar el comando **no shutdown**, se asegura de que sólo las conexiones asignadas en forma estática deseadas formen parte de las asignaciones de Frame Relay.

Paso 3: Configurar R2 para Frame Relay.

```
R2(config)#interface serial 0/0/1
R2(config-if)#encapsulation frame-relay
R2(config-if)#no frame-relay inverse-arp
R2(config-if)#frame-relay map ip 10.1.1.1 201 broadcast
R2(config-if)#no shutdown
```

En ese momento, se reciben mensajes que indican que las interfaces se activaron y que se estableció la adyacencia vecina de EIGRP.

```
R1#*Sep  9 17:05:08.771: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.2 (Serial0/0/1) is up: new adjacency
```

```
R2#*Sep  9 17:05:47.691: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Serial0/0/1) is up: new adjacency
```

El comando **show ip route** muestra tablas de enrutamiento completas.

R1:

```
R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0
D    209.165.200.0/24 [90/20640000] via 10.1.1.2, 00:00:07, Serial0/0/1
     10.0.0.0/30 is subnetted, 1 subnets
C    10.1.1.0 is directly connected, Serial0/0/1
```

R2:

```
R2#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static
route
       o - ODR, P - periodic downloaded static route


Gateway of last resort is not set

D    192.168.10.0/24 [90/20514560] via 10.1.1.1, 00:26:03, Serial0/0/1
     209.165.200.0/27 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Serial0/0/1
```

Tarea 4: Verificar la configuración

Ahora se debería poder hacer ping de R1 a R2. Una vez que se activen las interfaces, es posible que el PVC demore varios segundos en activarse. También se pueden ver las rutas EIGRP de cada router.

Paso 1: Hacer ping a R1 y R2.

Asegúrese de poder hacer ping al router R2 desde el router R1.

```
R1#ping 10.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32
ms
R2#ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32
ms
```

Paso 2: Obtener información del PVC.

El comando **show frame-relay pvc** muestra información sobre todos los PVC configurados en el router. El resultado también incluye el DLCI asociado.

R1:

```
R1#show frame-relay pvc

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

  input pkts 5             output pkts 5            in bytes 520
  out bytes 520            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 10:26:41, last time pvc status changed 00:01:04
```

R2:

```
R2#show frame-relay pvc

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

               Active     Inactive      Deleted       Static
  Local           1            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1
```

```
  input pkts 5             output pkts 5            in bytes 520
  out bytes 520            dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 10:25:31, last time pvc status changed 00:00:00
```

Switch FR:

```
FR-Switch#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

              Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       1            0            0            0
  Unused         0            0            0            0

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/0

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 10:28:31, last time pvc status changed 00:03:57

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

              Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       1            0            0            0
  Unused         0            0            0            0

DLCI = 201, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

  input pkts 0             output pkts 0            in bytes 0
  out bytes 0              dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0         out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
```

```
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 0
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 10:27:00, last time pvc status changed 00:04:03
```

Paso 3: Verificar las asignaciones Frame Relay.

El comando **show frame-relay map** muestra a los DLCI información sobre las asignaciones estáticas y dinámicas de direcciones de capa 3. Debido a que se desactivó el ARP inverso, sólo hay asignaciones estáticas.

R1:

```
R1#show frame-relay map
Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
              CISCO, status defined, active
```

R2:

```
R2#show frame-relay map
Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,
              CISCO, status defined, active
```

Switch FR:

El switch FR funciona como un dispositivo de capa 2, de modo que no es necesario asignar direcciones de capa 3 a los DLCI de capa 2.

Paso 4: Depurar la LMI Frame Relay.

¿Para qué sirve la LMI en una red Frame Relay?

_____

_____

_____

_____

La LMI o interfaz de administración local es un protocolo de señalización que intercambia información entre un router y un switch Frame Relay. La LMI intercambia información sobre mensajes de actividad, estado de los PVC (activo, inactivo, eliminado, no utilizado) y direcciones IP (cuando el ARP inverso está activo).

¿Cuáles son los tres tipos diferentes de LMI?

_____

ansi, cisco, q933a

¿En qué DLCI funciona la LMI?

_____

1023

Ejecute el comando **debug frame-relay lmi**. El resultado proporciona información detallada sobre todos los datos de la LMI. Los mensajes de actividad se envían cada 10 segundos, de modo que es posible que sea necesario esperar para ver un resultado.

El resultado de la depuración muestra dos paquetes LMI: el primero saliente, el segundo entrante.

```
R1#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
R1#
*Aug 24 06:19:15.920: Serial0/0/1(out): StEnq, myseq 196, yourseen
195, DTE up
*Aug 24 06:19:15.920: datagramstart = 0xE73F24F4, datagramsize = 13
*Aug 24 06:19:15.920: FR encap = 0xFCF10309
*Aug 24 06:19:15.920: 00 75 01 01 00 03 02 C4 C3
*Aug 24 06:19:15.920:
*Aug 24 06:19:15.924: Serial0/0/1(in): Status, myseq 196, pak size 21
*Aug 24 06:19:15.924: RT IE 1, length 1, type 0
*Aug 24 06:19:15.924: KA IE 3, length 2, yourseq 196, myseq 196
*Aug 24 06:19:15.924: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2
, bw 0
R1#undebug all
Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off
```

Observe que el resultado muestra un paquete LMI saliente con el número de secuencia 196. El último mensaje LMI recibido del switch FR tenía el número de secuencia 195.

```
*Aug 24 06:19:15.920: Serial0/0/1(out): StEnq, myseq 196, yourseen
195, DTE up
```

Esta línea indica un mensaje LMI entrante del switch FR a R1 con el número de secuencia 196.

```
*Aug 24 06:19:15.924: Serial0/0/1(in): Status, myseq 196, pak size 21
```

El switch FR envió esto como número de secuencia 196 (myseq) y el último mensaje LMI que recibió el switch FR desde R1 tenía el número de secuencia 196 (yourseq).

```
*Aug 24 06:19:15.924: KA IE 3, length 2, yourseq 196, myseq 196
```

DLCI 102 es el único DLCI en este enlace y actualmente está activo.

```
*Aug 24 06:19:15.924: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2 ,
bw 0
```

Tarea 4: Resolución de problemas de Frame Relay

Existe una variedad de herramientas disponibles para la resolución de problemas de conectividad de Frame Relay. Para aprender acerca de la resolución de problemas, se interrumpirá la conexión Frame Relay establecida anteriormente y luego se restablecerá.

Paso 1: Eliminar la asignación de tramas de R1.

```
R1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#no frame-relay map ip 10.1.1.2 102 broadcast
```

Ahora que se ha eliminado la sentencia de asignación de tramas de R1, intente hacer ping al router R1 desde el router R2. No se obtendrá ninguna respuesta.

```
R2#ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Además, se deberían recibir mensajes de consola que notifican que la adyacencia EIGRP se activa y se desactiva.

```
R1(config-if)#*Sep  9 17:28:36.579: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: Interface Goodbye received

R1(config-if)#*Sep  9 17:29:32.583: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is up: new adjacency

R1(config-if)#*Sep  9 17:32:37.095: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: retry limit exceeded

R2#*Sep  9 17:29:15.359: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Serial0/0/1) is down: holding time expired
```

Ejecute el comando **debug ip icmp** en R1:

```
R1#debug ip icmp

ICMP packet debugging is on
```

Ahora haga ping nuevamente a la interfaz serial de R1. En R1 aparece el siguiente mensaje de depuración:

```
R2#ping 10.1.1.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)
R1#*Sep  9 17:42:13.415: ICMP: echo reply sent, src 10.1.1.1, dst
10.1.1.2
R1#*Sep  9 17:42:15.411: ICMP: echo reply sent, src 10.1.1.1, dst
10.1.1.2
R1#*Sep  9 17:42:17.411: ICMP: echo reply sent, src 10.1.1.1, dst
10.1.1.2
R1#*Sep  9 17:42:19.411: ICMP: echo reply sent, src 10.1.1.1, dst
10.1.1.2
R1#*Sep  9 17:42:21.411: ICMP: echo reply sent, src 10.1.1.1, dst
10.1.1.2
```

Tal como se muestra en este mensaje de depuración, el paquete ICMP de R2 alcanza a R1.

¿Por qué no se realizó correctamente el ping?

_____

_____

El ping falla porque R1 no tiene manera de responder. Al no tener ninguna manera de asignar la dirección IP de R2 al DLCI de capa 2, no puede enrutar la respuesta y descarta el paquete.

La emisión del comando **show frame-relay map** devuelve una línea en blanco.

```
R1#show frame-relay map

R1#
```

Desactive la depuración mediante el comando **undebug all** y vuelva a aplicar el comando **frame-relay map ip**, pero sin usar la palabra clave **broadcast.**

```
R1#undebug all

Port Statistics for unclassified packets is not turned on.

All possible debugging has been turned off

R1#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay map ip 10.1.1.2 102
R2#ping 10.1.1.1


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/41/44 ms
```

Observe que a pesar de que los pings se realizan correctamente, la adyacencia EIGRP continúa activándose y desactivándose.

```
R1(config-if)#*Sep  9 17:47:58.375: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is up: new adjacency

R1(config-if)#*Sep  9 17:51:02.887: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: retry limit exceeded

R1(config-if)#*Sep  9 17:51:33.175: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is up: new adjacency

R1(config-if)#*Sep  9 17:54:37.687: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1:
Neighbor 10.1.1.2 (Serial0/0/1) is down: retry limit exceeded
```

¿Por qué continúa activándose y desactivándose la adyacencia EIGRP?

_____

_____

No se envía tráfico multicast a través del DLCI especificado en la sentencia de asignación de trama.

Reemplace la sentencia de asignación Frame Relay y, esta vez, incluya la palabra clave **broadcast**. Verifique que se restablece toda la tabla de enrutamiento y que hay conectividad completa de extremo a extremo.

```
R1#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface serial0/0/1
R1(config-if)#encapsulation frame-relay
R1(config-if)#frame-relay map ip 10.1.1.2 102 broadcast

R1#show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static  route  o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0
     209.165.200.0/27 is subnetted, 1 subnets

D    209.165.200.224 [90/20640000] via 10.1.1.2, 00:00:05, Serial0/0/1
     10.0.0.0/30 is subnetted, 1 subnets

C    10.1.1.0 is directly connected, Serial0/0/1
```

Paso 2: Cambiar el tipo de encapsulación Frame Relay.

El software IOS de Cisco admite dos tipos de encapsulación Frame Relay: la encapsulación Cisco por defecto y la encapsulación IETF basada en estándares. Cambie la encapsulación Frame Relay en serial 0/0/1 de R2 a IETF.

```
R2(config-if)#encapsulation frame-relay ietf
```

Observe que la interfaz no deja de funcionar. Tal vez esto sea sorprendente. Los routers Cisco pueden interpretar correctamente las tramas Frame Relay que utilizan tanto la encapsulación Frame Relay por defecto de Cisco como la encapsulación Frame Relay estándar de IETF. Si la red está compuesta completamente de routers Cisco, entonces se puede utilizar tanto la encapsulación Frame Relay por defecto de Cisco como el estándar de IETF. Los routers Cisco comprenden ambos tipos de tramas entrantes. Sin embargo, si hay routers de distintos fabricantes que utilizan Frame Relay, se debe utilizar el estándar de IETF. El comando **encapsulation frame-relay ietf** obliga al router Cisco a encapsular las tramas salientes mediante el estándar de IETF. El router de otro fabricante puede comprender correctamente este estándar.

```
R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY IETF, loopback not set

<output omitted>
```

```
FR-Switch#show int s0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
```

Observe la diferencia de resultados entre los dos comandos **show interface**. Además, se debe tener en cuenta que la adyacencia EIGRP aún está activada. A pesar de que el switch FR y R2 utilizan distintos tipos de encapsulación, siguen pasando tráfico.

Cambie nuevamente el tipo de encapsulación al tipo por defecto:

```
R2(config-if)#encapsulation frame-relay
```

Paso 3: Cambiar el tipo de LMI.

En R2, cambie el tipo de LMI a ANSI.

```
R2#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface serial 0/0/1
R2(config-if)#encapsulation frame-relay
R2(config-if)#frame-relay lmi-type ansi
R2(config-if)#^Z
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]

*Sep  9 18:41:08.351: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down

*Sep  9 18:41:08.351: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor
10.1.1.1 (Serial0/0/1) is down: interface down

R2#show interface serial 0/0/1

Serial0/0/1 is up, line protocol is down

R2#show frame-relay lmi

LMI Statistics for interface Serial0/0/1 (Frame Relay DTE) LMI TYPE =
ANSI
  Invalid Unnumbered info 0               Invalid Prot Disc 0
  Invalid dummy Call Ref 0                Invalid Msg Type 0
  Invalid Status Message 0                Invalid Lock Shift 0
  Invalid Information ID 0                Invalid Report IE Len 0
  Invalid Report Request 0                Invalid Keep IE Len 0
  Num Status Enq. Sent 1391               Num Status msgs Rcvd 1382
  Num Update Status Rcvd 0                Num Status Timeouts 10
  Last Full Status Req 00:00:27          Last Full Status Rcvd 00:00:27
```

Si se sigue ejecutando el comando **show frame-relay lmi**, se observará que las horas resaltadas se incrementan. Una vez transcurridos los 60 segundos, la interfaz cambiará su estado a Up Down (activado desactivado), ya que R2 y el switch FR han dejado de intercambiar mensajes de actividad u otro tipo de información acerca del estado de enlace.

Ejecute el comando **debug frame-relay lmi**. Observe que los paquetes LMI ya no aparecen en pares. Aunque se registran todos los mensajes LMI salientes, no se muestra ningún mensaje entrante. Esto se debe a que R2 espera una LMI de ANSI y el switch FR envía una LMI de Cisco.

```
R2#debug frame-relay lmi

*Aug 25 04:34:25.774: Serial0/0/1(out): StEnq, myseq 20, yourseen 0,
DTE down
*Aug 25 04:34:25.774: datagramstart = 0xE73F2634, datagramsize = 14
*Aug 25 04:34:25.774: FR encap = 0x00010308
*Aug 25 04:34:25.774: 00 75 95 01 01 00 03 02 14 00
*Aug 25 04:34:25.774:
```

Deje la depuración activada y restablezca el tipo de LMI a Cisco en R2.

```
R2(config-if)#frame-relay lmi-type cisco
*Aug 25 04:42:45.774: Serial0/0/1(out): StEnq, myseq 2, yourseen 1, DTE
down
*Aug 25 04:42:45.774: datagramstart = 0xE7000D54, datagramsize = 13
*Aug 25 04:42:45.774: FR encap = 0xFCF10309
*Aug 25 04:42:45.774: 00 75 01 01 01 03 02 02 01
*Aug 25 04:42:45.774:
*Aug 25 04:42:45.778: Serial0/0/1(in): Status, myseq 2, pak size 21
*Aug 25 04:42:45.778: RT IE 1, length 1, type 0
*Aug 25 04:42:45.778: KA IE 3, length 2, yourseq 2 , myseq 2
*Aug 25 04:42:45.778: PVC IE 0x7 , length 0x6 , dlci 201, status 0x2 ,
bw 0
*Aug 25 04:42:55.774: Serial0/0/1(out): StEnq, myseq 3, yourseen 2, DTE
up
*Aug 25 04:42:55.774: datagramstart = 0xE7001614, datagramsize = 13
*Aug 25 04:42:55.774: FR encap = 0xFCF10309
*Aug 25 04:42:55.774: 00 75 01 01 01 03 02 03 02
*Aug 25 04:42:55.774:
*Aug 25 04:42:55.778: Serial0/0/1(in): Status, myseq 3, pak size 21
*Aug 25 04:42:55.778: RT IE 1, length 1, type 0
*Aug 25 04:42:55.778: KA IE 3, length 2, yourseq 1 , myseq 3
*Aug 25 04:42:55.778: PVC IE 0x7 , length 0x6 , dlci 201, status 0x2 ,
bw 0
*Aug 25 04:42:56.774: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
```

Como se puede observar, el número de secuencia de LMI se ha restablecido en 1 y R2 comenzó a comprender los mensajes LMI provenientes del switch FR. Después de que el switch FR y R2 intercambiaron correctamente los mensajes LMI, la interfaz cambió su estado a Up (activado).

Tarea 5: Configurar una subinterfaz Frame Relay

Frame Relay admite dos tipos de subinterfaces: punto a punto y punto a multipunto. Las subinterfaces punto a multipunto admiten topologías multiacceso sin broadcast. Por ejemplo, una topología hub-and-spoke usaría una subinterfaz punto a multipunto. En esta práctica de laboratorio, se creará una subinterfaz punto a punto.

Paso 1: En el switch FR, crear un nuevo PVC entre R1 y R2.

```
FR-Switch(config)#interface serial 0/0/0
FR-Switch(config-if)#frame-relay route 112 interface serial 0/0/1 212
FR-Switch(config-if)#interface serial 0/0/1
FR-Switch(config-if)#frame-relay route 212 interface serial 0/0/0 112
```

Paso 2: Crear y configurar una subinterfaz punto a punto en R1.

Cree la subinterfaz 112 como interfaz punto a punto. Para poder crear subinterfaces, primero se debe especificar la encapsulación Frame Relay en la interfaz física.

```
R1(config)#interface serial 0/0/1.112 point-to-point
R1(config-subif)#ip address 10.1.1.5 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 112
```

Paso 3: Crear y configurar una subinterfaz punto a punto en R2.

```
R2(config)#interface serial 0/0/1.212 point-to-point
R2(config-subif)#ip address 10.1.1.6 255.255.255.252
R2(config-subif)#frame-relay interface-dlci 212
```

Paso 4: Verificar la conectividad.

Se debería poder hacer ping a través del nuevo PVC.

```
R1#ping 10.1.1.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R2#ping 10.1.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

La configuración también se puede verificar mediante los comandos **show frame-relay pvc** y **show frame-relay** en la Tarea 4.

R1:

```
R1#show frame-relay pvc

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

               Active     Inactive      Deleted       Static
  Local           2            0            0            0
  Switched        0            0            0            0
  Unused          0            0            0            0

DLCI = 102, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

  input pkts 319            output pkts 279          in bytes 20665
  out bytes 16665          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                 out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 193       out bcast bytes 12352
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 04:43:35, last time pvc status changed 01:16:05
```

```
DLCI = 112, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1.112


  input pkts 15            output pkts 211          in bytes 2600
  out bytes 17624          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 200       out bcast bytes 16520
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:19:16, last time pvc status changed 00:18:56
```

R2:

```
R2#show frame-relay pvc

PVC Statistics for interface Serial0/0/1 (Frame Relay DTE)

              Active     Inactive      Deleted       Static
  Local          2            0            0            0
  Switched       0            0            0            0
  Unused         0            0            0            0

DLCI = 201, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

  input pkts 331            output pkts 374          in bytes 19928
  out bytes 24098          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 331       out bcast bytes 21184
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 05:22:55, last time pvc status changed 01:16:36

DLCI = 212, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1.212

  input pkts 217            output pkts 16           in bytes 18008
  out bytes 2912          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 6       out bcast bytes 1872
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  pvc create time 00:19:37, last time pvc status changed 00:18:57
```

Switch FR:

```
FR-Switch#show frame-relay pvc

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

              Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       2            0            0            0
  Unused         0            0            0            0

DLCI = 102, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/0

  input pkts 335            output pkts 376          in bytes 20184
  out bytes 24226          dropped pkts 2           in pkts dropped 2
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0       out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 333
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 2           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 05:23:43, last time pvc status changed 01:18:32

DLCI = 112, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/0

  input pkts 242            output pkts 18          in bytes 20104
  out bytes 3536          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0       out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 242
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 00:21:41, last time pvc status changed 00:21:22

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

              Active     Inactive      Deleted       Static
  Local          0            0            0            0
  Switched       2            0            0            0
  Unused         0            0            0            0
```

```
DLCI = 201, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

  input pkts 376            output pkts 333          in bytes 24226
  out bytes 20056          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0       out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 376
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 05:23:14, last time pvc status changed 01:39:39

DLCI = 212, DLCI USAGE = SWITCHED, PVC STATUS = ACTIVE, INTERFACE =
Serial0/0/1

  input pkts 18             output pkts 243          in bytes 3536
  out bytes 20168          dropped pkts 0           in pkts dropped 0
  out pkts dropped 0                out bytes dropped 0
  in FECN pkts 0           in BECN pkts 0           out FECN pkts 0
  out BECN pkts 0          in DE pkts 0             out DE pkts 0
  out bcast pkts 0       out bcast bytes 0
  30 second input rate 0 bits/sec, 0 packets/sec
  30 second output rate 0 bits/sec, 0 packets/sec
  switched pkts 18
  Detailed packet drop counters:
  no out intf 0            out intf down 0          no out PVC 0
  in PVC down 0            out PVC down 0           pkt too big 0
  shaping Q full 0         pkt above DE 0           policing drop 0
  pvc create time 00:21:36, last time pvc status changed 00:21:20
```

R1:

```
R1#show frame-relay map

Serial0/0/1 (up): ip 10.1.1.2 dlci 102(0x66,0x1860), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/1.112 (up): point-to-point dlci, dlci 112(0x70,0x1C00),
broadcast
          status defined, active
```

R2:

```
R2#show frame-relay map

Serial0/0/1 (up): ip 10.1.1.1 dlci 201(0xC9,0x3090), static,
              broadcast,
              CISCO, status defined, active
Serial0/0/1.212 (up): point-to-point dlci, dlci 212(0xD4,0x3440),
broadcast
          status defined, active
```

Switch FR:

```
FR-Switch#show frame-relay route

Input Intf      Input Dlci      Output Intf     Output Dlci     Status
Serial0/0/0     102             Serial0/0/1     201             active
Serial0/0/0     112             Serial0/0/1     212             active
Serial0/0/1     201             Serial0/0/0     102             active
Serial0/0/1     212             Serial0/0/0     112             active
```

Ahora depure la LMI Frame Relay.

```
R1#debug frame-relay lmi

*Aug 25 05:58:50.902: Serial0/0/1(out): StEnq, myseq 136, yourseen 135,
DTE up
*Aug 25 05:58:50.902: datagramstart = 0xE7000354, datagramsize = 13
*Aug 25 05:58:50.902: FR encap = 0xFCF10309
*Aug 25 05:58:50.902: 00 75 01 01 00 03 02 88 87
*Aug 25 05:58:50.902:
*Aug 25 05:58:50.906: Serial0/0/1(in): Status, myseq 136, pak size 29
*Aug 25 05:58:50.906: RT IE 1, length 1, type 0
*Aug 25 05:58:50.906: KA IE 3, length 2, yourseq 136 , myseq 136
*Aug 25 05:58:50.906: PVC IE 0x7 , length 0x6 , dlci 102, status 0x2 ,
bw 0
*Aug 25 05:58:50.906: PVC IE 0x7 , length 0x6 , dlci 112, status 0x2 ,
bw 0
```

Observe que dos DLCI figuran en el mensaje LMI del switch FR a R1.

```
R2#debug frame-relay lmi

*Aug 25 06:08:35.774: Serial0/0/1(out):StEnq, myseq 7,yourseen 4,DTE up
*Aug 25 06:08:35.774: datagramstart = 0xE73F28B4, datagramsize = 13
*Aug 25 06:08:35.774: FR encap = 0xFCF10309
*Aug 25 06:08:35.774: 00 75 01 01 00 03 02 07 04
*Aug 25 06:08:35.774:
*Aug 25 06:08:35.778: Serial0/0/1(in): Status, myseq 7, pak size 29
*Aug 25 06:08:35.778: RT IE 1, length 1, type 0
*Aug 25 06:08:35.778: KA IE 3, length 2, yourseq 5 , myseq 7
*Aug 25 06:08:35.778: PVC IE 0x7,length 0x6, dlci 201, status 0x2, bw 0
*Aug 25 06:08:35.778: PVC IE 0x7,length 0x6, dlci 212, status 0x2, bw 0
```

Configuraciones finales

```
R1#show run
<output omitted>
!
hostname R1

enable secret class
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
```

```
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.2 102 broadcast
 no frame-relay inverse-arp
 no shutdown
!
interface Serial0/0/1.112 point-to-point
 ip address 10.1.1.5 255.255.255.252
 frame-relay interface-dlci 112
!
router eigrp 1
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
!
banner motd ^CUnauthorized access prohibited, violators will be
prosecuted to the full extent of the law.^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 login
 password cisco
!
end


R2#show run
<output omitted>
!
hostname R2
!
!
enable secret class
!
!
no ip domain lookup
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
!
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 clockrate 64000
 frame-relay map ip 10.1.1.1 201 broadcast
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
 no shutdown
```

```
!
interface Serial0/0/1.212 point-to-point
 ip address 10.1.1.6 255.255.255.252
 frame-relay interface-dlci 212
!
router eigrp 1
 network 10.0.0.0
 network 209.165.200.224 0.0.0.31
 no auto-summary
!
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end

FR-Switch#show run
<output omitted>
!
hostname FR-Switch
!
enable secret class
!
no ip domain lookup
frame-relay switching
!
!
!
!
interface Serial0/0/0
 no ip address
 encapsulation frame-relay

 clockrate 64000
 frame-relay intf-type dce
 frame-relay route 102 interface Serial0/0/1 201
 frame-relay route 112 interface Serial0/0/1 212
 no shutdown
!
interface Serial0/0/1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 201 interface Serial0/0/0 102
 frame-relay route 212 interface Serial0/0/0 112
 no shutdown
!
!
line con 0
 password cisco
```

```
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Práctica de laboratorio 3.5.2: Reto de configuración de Frame Relay (Versión para el instructor)

Diagrama de topología

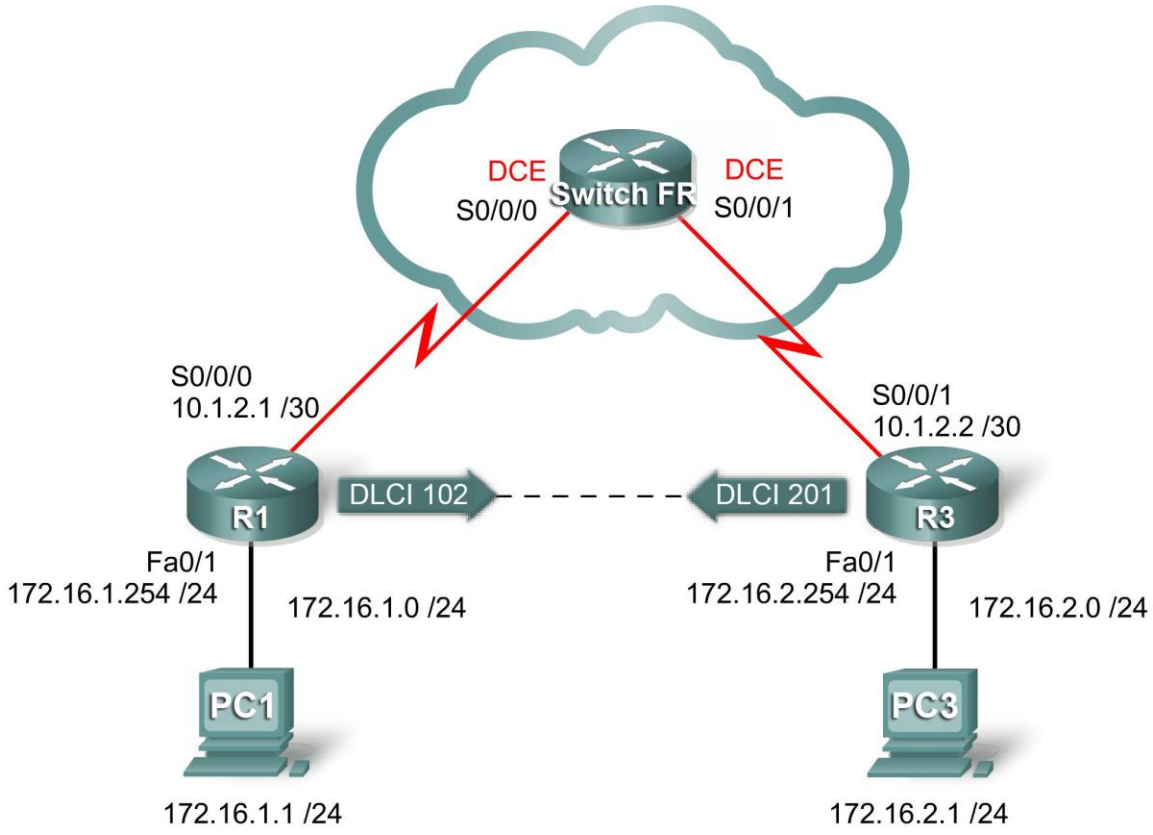


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Fa0/1**	172.16.1.254	255.255.255.0	N/C
	S0/0/0	10.1.2.1	255.255.255.252	N/C
R2	**Fa0/1**	172.16.2.254	255.255.255.0	N/C
	S0/0/1	10.1.2.2	255.255.255.252	N/C
PC1	**NIC**	172.16.1.1	255.255.255.0	172.16.1.254
PC3	**NIC**	172.16.2.1	255.255.255.0	172.16.2.254

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
- Realizar tareas de configuración básicas en un router
- Configurar y activar interfaces
- Configurar el enrutamiento EIGRP en todos los routers
- Configurar la encapsulación Frame Relay en todas las interfaces seriales
- Configurar un PVC en Frame Relay
- Interrumpir intencionalmente y restablecer un PVC en Frame Relay
- Configurar las subinterfaces Frame Relay
- Interrumpir intencionalmente y restaurar el PVC

Escenario

En esta práctica de laboratorio se configurará Frame Relay según la red que se muestra en el diagrama de topología. Si se necesita ayuda, se puede consultar la práctica de laboratorio de Frame Relay básico. Sin embargo, el usuario debe intentar hacer todo lo posible por su cuenta.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar la configuración básica del router

Configure los routers R1, R2 y R3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de Modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure el registro de datos sincrónico.
- Configure una contraseña para las conexiones de vty.

Tarea 3: Configurar las direcciones IP

Paso 1: Configurar las direcciones IP en todos los enlaces de acuerdo con la tabla de direccionamiento.

R1

```
R1(config)#int s0/0/0
R1(config-if)#ip address 10.1.2.1 255.255.255.252
R1(config-if)#int fa0/1
R1(config-if)#ip address 172.16.1.254 255.255.255.0
```

```
R2:
R2(config)#int s0/0/1
R2(config-if)#ip address 10.1.2.2 255.255.255.252
R2(config-if)#int fa0/1
R2(config-if)#ip address 172.16.1.254 255.255.255.0
```

Paso 2: Verificar el direccionamiento IP y las interfaces.

```
show ip int brief
```

Paso 3: Activar las interfaces Ethernet en R1 y R2. No activar las interfaces seriales.

```
R1(config-if)#int fa0/1
R1(config-if)#no shut
```

```
R2(config-if)#int fa0/1
R2(config-if)#no shut
```

Paso 4: Configurar las interfaces Ethernet de PC1 y PC3.

Paso 5: Probar la conectividad entre los equipos PC y sus routers locales.

```
ping
```

Tarea 4: Configurar EIGRP en los routers R1 y R2

Paso 1: Activar EIGRP en R1 y R2 para todas las subredes.

```
router eigrp 1
network 10.1.2.0 0.0.0.3
network 172.16.0.0 0.0.15.255.255
no auto-summary
```

Tarea 5: Configurar un PVC en Frame Relay entre R1 y R2

Paso 1: Configurar las interfaces en el switch FR para crear el PVC entre R1 y R2.

Use los DLCI del diagrama de topología.

```
Switch FR:
interface serial0/0/0
encapsulation frame-relay
frame-relay route 102 interface s0/0/1 201
frame-relay intf-type dce
interface serial0/0/1
encapsulation frame-relay
frame-relay route 201 interface s0/0/0 102
frame-relay intf-type dce
```

Paso 2: Configurar interfaces físicas en R1 y R2 para la encapsulación Frame Relay.

No detecte automáticamente las direcciones IP en el extremo de los enlaces. Active el enlace después de la configuración completa.

R1

```
interface serial0/0/0
encapsulation frame-relay
no frame-relay inverse-arp
no shut
```

R2

```
int s0/0/1
encapsulation frame-relay
no frame-relay inverse-arp
no shut
```

Paso 3: Configurar las asignaciones Frame Relay en R1 y R2 con DLCI adecuados. Permitir el tráfico broadcast en los DLCI.

R1

```
interface serial0/0/0
frame=relay map ip 10.1.2.2 102 broadcast
```

R2

```
interface serial0/0/1
frame-relay map ip 10.1.2.1 201 broadcast
```

Paso 4: Verificar la conectividad de extremo a extremo mediante PC1 y PC2

```
ping
```

Tarea 6: Interrumpir intencionalmente el PVC y luego restablecerlo

Paso 1: Interrumpir el PVC entre R1 y R2 mediante el método preferido.

Paso 2: Restablecer la conectividad completa en la red.

Paso 3: Verificar la conectividad completa en la red.

Tarea 7: Configurar las subinterfaces de Frame Relay

Paso 1: Eliminar la dirección IP y la configuración de la asignación de tramas de las interfaces físicas de R1 y R2.

R1

```
interface serial0/0/0
no frame-relay map ip 10.1.2.2 102 broadcast
no ip address
```

R2

```
int s0/0/1
no frame-relay map ip 10.1.2.1 201 broadcast
```

Paso 2: Configurar subinterfaces Frame Relay punto a punto en R1 y R2 con las mismas direcciones IP y DLCI que se utilizaron anteriormente en las interfaces físicas.

R1

```
interface serial0/0/0.102 point-to-point
ip address 10.1.2.1 255.255.255.252
frame-relay interface-dlci 102
```

R2

```
int s0/0/1.102 point-to-point
ip add 10.1.2.2 255.255.255.252
frame-relay interface-dlci 201
```

Paso 3: Verificar la conectividad de extremo a extremo completa.

```
Haga ping de PC a PC.
```

Tarea 8: Interrumpir intencionalmente el PVC y luego restablecerlo

Paso 1: Interrumpir el PVC mediante un método diferente al que se utilizó en la tarea 6.

Paso 2: Restablecer el PVC.

Paso 3: Verificar la conectividad de extremo a extremo completa.

Tarea 9: Documentar las configuraciones del router

En cada router, ejecute el comando **show run** y capture las configuraciones.

Tarea 10: 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.

Práctica de laboratorio 3.5.3: Resolución de problemas de Frame Relay (Versión para el instructor)

Diagrama de topología

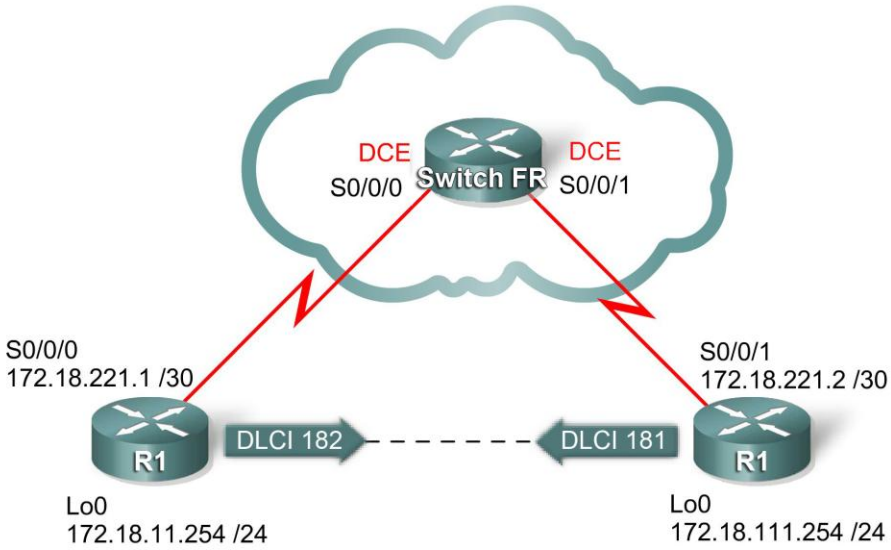


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**Lo0**	172.18.11.254	255.255.255.0	N/C
	S0/0/0	172.18.221.1	255.255.255.252	N/C
R2	**Lo0**	172.18.111.254	255.255.255.0	N/C
	S0/0/1	172.18.221.2	255.255.255.252	N/C

Objetivos de aprendizaje

Practicar las aptitudes de resolución de problemas de Frame Relay.

Escenario

En esta práctica de laboratorio el usuario practicará la resolución de problemas en un entorno de Frame Relay mal configurado. Cargue o solicítele al instructor que cargue las configuraciones que aparecen a continuación en los routers. Localice y repare todos los errores en las configuraciones y establezca la conectividad de extremo a extremo. La configuración final debe coincidir con el diagrama de topología y la tabla de direccionamiento. Todas las contraseñas están establecidas en **cisco**, excepto la contraseña secreta de enable que está establecida en **class**.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Paso 2: Borrar todas las configuraciones de los routers.

Paso 3: Importar las configuraciones.

Router 1

```
!
hostname R1
!
enable secret class
!
no ip domain lookup
!
!
!
!
interface Loopback0
 ip address 172.18.11.254 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/1
 no ip address
 shutdown
 no fair-queue
 clockrate 125000
!
interface Serial0/0/0
 ip address 172.18.221.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 172.18.221.2 678 broadcast
 frame-relay map ip 172.18.221.2 182 broadcast
 ! El DLCI se escribió incorrectamente y se debe corregir para que haya
conectividad.
 frame-relay map ip 172.18.221.1 182
! A menudo no se considera la asignación Frame Relay para la dirección
IP de la interfaz,
 ! ya que la mayoría de los otros tipos de interfaces pueden alcanzar
su propia dirección.
 no frame-relay inverse-arp
 no shutdown
!
```

```
router eigrp 1
 network 172.18.221.0
 network 172.18.11.0
 no auto-summary
!
!
!
line con 0
 password cisco
 logging synchronous
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Router 2

```
!
hostname R2
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 172.18.111.254 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/0/1
 ip address 172.18.221.2 255.255.255.252
 encapsulation frame-relay
 clockrate 125000
 frame-relay map ip 172.18.221.1 181 broadcast
 ! Se olvidó la palabra clave broadcast. Sin la palabra clave broadcast,
 ! los paquetes multicast no se envían con este DLCI. Esto impide que
 ! EIGRP forme adyacencias.
 frame-relay map ip 172.18.221.2 181
 ! A menudo no se considera la asignación Frame Relay para la dirección
IP de la interfaz,
```

```
 ! ya que la mayoría de los otros tipos de interfaces pueden alcanzar
su propia dirección.
 no frame-relay inverse-arp
 frame-relay lmi-type ansi
 ! El switch Frame Relay utiliza el tipo de LMI por defecto, que es
 ! cisco. Debe eliminarse este comando para que el enlace funcione.
 no shutdown
! Es habitual olvidar que las interfaces de un router
! se desactivan por defecto.
!
router eigrp 1
 network 172.18.221.0
 network 172.18.111.0
 no auto-summary
!
!
!
line con 0
 password cisco
 logging synchronous
line aux 0
line vty 0 4
 login
!
end
```

Switch FR:

```
!
hostname FR-Switch
!
!
enable secret class
!
!
!
no ip domain lookup
frame-relay switching
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 125000
 frame-relay intf-type dce
 frame-relay route 182 interface Serial0/0/1 181
 no shutdown
!
interface Serial0/0/1
 no ip address
 clockrate 125000
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 181 interface Serial0/0/1 182
 ! Sin una sentencia de ruta, el switch Frame Relay no sabe cómo
 ! conmutar los paquetes Frame Relay.
 no shutdown
!
!
!
!
line con 0
 password cisco
 logging synchronous
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Tarea 2: Resolver los problemas y reparar la conexión Frame Relay entre R1 y R2

Tarea 3: Documentar las configuraciones del router

En cada router, ejecute el comando **show run** y capture las configuraciones.

Tarea 4: 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.

Práctica de laboratorio 4.6.1: Configuración básica de seguridad (Versión para el instructor)

Diagrama de topología

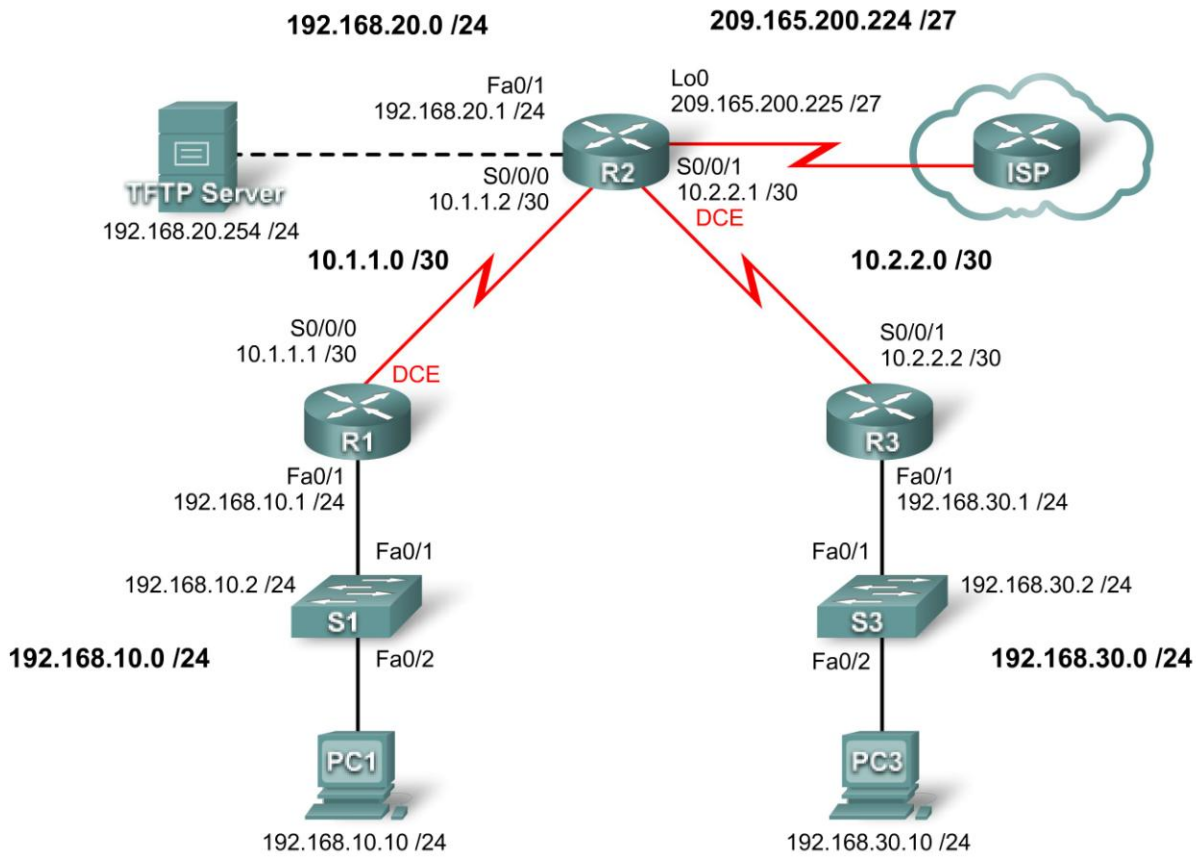


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/1	192.168.10.1	255.255.255.0	N/C
	S0/0/0	10.1.1.1	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	N/C
R3	Fa0/1	192.168.30.1	255.255.255.0	N/C
	S0/0/1	10.2.2.2	255.255.255.252	N/C

S1	**VLAN10**	192.168.10.2	255.255.255.0	N/C
S3	**VLAN20**	192.168.30.2	255.255.255.0	N/C
PC1	**NIC**	192.168.10.10	255.255.255.0	192.168.10.1
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
- Realizar tareas de configuración básicas en un router
- Configurar la seguridad básica de router
- Deshabilitar las interfases y los servicios de Cisco que no se utilicen
- Proteger las redes empresariales de ataques básicos internos y externos
- Comprender y administrar los archivos de configuración IOS de Cisco y el sistema de archivos Cisco
- Establecer y utilizar el SDM (Security Device Manager) de Cisco y el SDM Express para configurar la seguridad básica de router
- Configurar las VLAN en los switches

Escenario

En esta práctica de laboratorio, se aprenderá a configurar la seguridad básica de red mediante la red que se muestra en el diagrama de topología. Se aprenderá a configurar la seguridad del router de tres maneras diferentes: mediante la CLI, la función de seguridad automática y SDM de Cisco. Además, se aprenderá a administrar el software IOS de Cisco.

Notas para el instructor:

Esta práctica de laboratorio sobre seguridad básica les permite a los estudiantes practicar las principales aptitudes que se presentan en este capítulo. Si bien muchos instructores preferirán permitir que los estudiantes completen esta práctica de laboratorio en su totalidad, algunos instructores quizá deseen dividir la práctica de laboratorio para programar prácticas más breves. Por este motivo, aquí se proporcionan pautas para mostrar la mejor manera de dividir esta práctica de laboratorio.

La práctica de laboratorio puede dividirse de la siguiente manera:

- Parte 1: los estudiantes completan las tareas 1 a 7 y guardan sus configuraciones. Las respuestas a las configuraciones figuran en este documento después de la tarea 7.
- Parte 2: los estudiantes utilizan las configuraciones guardadas de la parte 1 y completan la tarea 8. Al final de este documento se proporcionan las respuestas a las configuraciones para toda la práctica de laboratorio.

En caso de que se requiera una mayor especificidad, los estudiantes pueden completar la tarea 6 de manera independiente con respecto a las demás tareas de esta práctica de laboratorio.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en la topología.

Nota: Esta práctica de laboratorio se desarrolló y probó mediante routers 1841. Si se utilizan routers serie 1700, 2500 ó 2600, los resultados y las descripciones del router pueden ser diferentes.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Paso 1: Configurar los routers.

Configure los routers R1, R2 y R3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router según el diagrama de topología.
- Deshabilite la búsqueda DNS.
- Configure un mensaje del día.
- Configure las direcciones IP de R1, R2 y R3.
- Habilite RIP versión 2 en todos los routers para todas las redes.
- Cree una interfaz loopback en R2 para simular la conexión a Internet.
- Configure un servidor TFTP en R2. Si necesita descargar el software del servidor TFTP, una opción es: http://tftpd32.jounin.net/

R1

```
hostname R1
no ip domain-lookup
banner motd ^Unauthorized access strictly prohibited and prosecuted to
the full extent of the law.^
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no shutdown
 clock rate 64000
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
```

R2

```
hostname R2
no ip domain-lookup
banner motd ^Unauthorized access strictly prohibited and prosecuted to
the full extent of the law.^
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
Interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clock rate 115200
 no shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.20.0
 network 209.165.200.0
 no auto-summary
!
```

R3

```
hostname R3
no ip domain-lookup
banner motd ^Unauthorized access strictly prohibited and prosecuted to
the full extent of the law.^
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
!
router rip
 version 2
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
```

Paso 2: Configurar las interfaces Ethernet.

Configure las interfaces Ethernet de PC1, PC3 y el servidor TFTP con las direcciones IP y las gateways por defecto de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio.

Paso 3: Probar la configuración de los equipos PC al hacer ping a la gateway por defecto desde cada PC y el servidor TFTP.

Tarea 3: Proteger al router del acceso no autorizado

Paso 1: Configurar contraseñas seguras y autenticación AAA.

Utilice una base de datos local en R1 para configurar contraseñas seguras. Utilice **ciscoccna** para todas las contraseñas en esta práctica de laboratorio.

```
R1(config)#enable secret ciscoccna
```

¿Cómo ayuda la configuración de una contraseña secreta de enable a proteger un router para que no se vea afectado por un ataque?

_____

_____

_____

El objetivo es impedir que los usuarios no autorizados accedan a un dispositivo mediante Telnet, SSH o a través de la consola. Si por algún motivo un pirata informático alcanza penetrar esta primera capa de defensa, al utilizar una contraseña secreta de enable puede impedir la modificación de la configuración del dispositivo. Esto proporciona una capa adicional de seguridad.

El comando **username** crea un nombre de usuario y una contraseña que se almacenan localmente en el router. El nivel privilegiado por defecto del usuario es 0 (la menor cantidad de acceso). Se puede cambiar el nivel de acceso de un usuario al agregar la palabra clave **privilege** *0-15* antes de la palabra clave **password**.

```
R1(config)#username ccna password ciscoccna
```

El comando **aaa** habilita la AAA (autenticación, autorización y contabilidad) globalmente en el router. Esto se utiliza para conectarse al router.

```
R1(config)#aaa new-model
```

Puede crear una lista de autenticación a la que pueda accederse cuando alguien intenta iniciar sesión en el dispositivo después de aplicarla a las líneas vty y líneas de consola. La palabra clave **local** indica que la base de datos del usuario se encuentra almacenada en forma local en el router.

```
R1(config)#aaa authentication login LOCAL_AUTH local
```

Los siguientes comandos le indican al router que los usuarios que intentan conectarse al router deben autenticarse mediante la lista recién creada.

```
R1(config)#line console 0
R1(config-lin)#login authentication LOCAL_AUTH
R1(config-lin)#line vty 0 4
R1(config-lin)#login authentication LOCAL_AUTH
```

¿Qué elemento no seguro observa en la siguiente sección de la configuración en ejecución?:

```
R1#show run
<output omitted>
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 0 ciscoccna
!
<output omitted>
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 logging synchronous
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

_____

_____

_____

La contraseña secreta de enable está encriptada, pero la contraseña para el usuario ccna no lo es. Esto es menos seguro.

Para aplicar encriptación simple a las contraseñas, ingrese el siguiente comando en el modo de configuración global:

```
R1(config)#service password-encryption
```

Verifique esto con el comando **show run**.

```
R1#show run
service password-encryption
!
enable secret 5 $1$.DB7$DunHvguQH0EvLqzQCqzfr1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
username ccna password 7 0822455D0A1606141C0A
<output omitted>
!
```

```
banner motd ^CCUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law^C
!
line con 0
 logging synchronous
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 login authentication LOCAL_AUTH
!
```

Paso 2: Establecer la seguridad de las líneas de consola y las líneas VTY.

Puede hacer que el router desconecte una línea que ha estado inactiva durante un determinado período de tiempo. Si un ingeniero de red estaba conectado a un dispositivo de red y tuvo que ausentarse repentinamente, este comando desconecta al usuario automáticamente después de un determinado período de tiempo. Los siguientes comandos hacen que la línea se desconecte después de 5 minutos.

```
R1(config)#line console 0
R1(config-lin)#exec-timeout 5 0
R1(config-lin)#line vty 0 4
R1(config-lin)#exec-timeout 5 0
```

El siguiente comando dificulta los intentos de conexión de fuerza bruta. El router bloquea los intentos de conexión durante 5 minutos si una persona intenta sin éxito conectarse 5 veces en 2 minutos. Esto se configura en un valor bajo específicamente a los fines de esta práctica de laboratorio. Otra medida es el registro de estos eventos cada vez que suceden.

```
R1(config)#login block-for 300 attempt 2 within 120
R1(config)#security authentication failure rate 5 log
```

Para verificar esto, intente conectarse a R1 desde R2 a través de Telnet con un nombre de usuario y una contraseña incorrectos.

En R2:

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted to the
full extent of the law

User Access Verification

Username: cisco
Password:

% Authentication failed

User Access Verification

Username: cisco
Password:

% Authentication failed
```

```
[Connection to 10.1.1.1 closed by foreign host]
R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```

En R1:

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF, because
block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

Tarea 4: Establecer la seguridad de acceso a la red

Paso 1: Impedir la propagación de la actualización del enrutamiento RIP.

¿Quién puede recibir actualizaciones RIP en un segmento de red en el que RIP está habilitado? ¿Es ésta la configuración preferida?

_____

_____

_____

Cualquier dispositivo que escuche puede recibir actualizaciones RIP. Esto no es seguro, ya que proporciona información acerca de la estructura de la red. El primer paso para acceder sin autorización a una red es el reconocimiento de la red, en el que se debe intentar conocer la estructura la red existente antes de decidir cómo atacarla.

El comando **passive-interface** impide que los routers envíen actualizaciones de enrutamiento a todas las interfaces, excepto a aquellas que se configuraron para participar en las actualizaciones de enrutamiento. Este comando se ejecuta como parte de la configuración RIP.

El primer comando coloca todas las interfaces en modo pasivo (la interfaz sólo recibe actualizaciones RIP). El segundo comando hace que determinadas interfaces regresen del modo pasivo al modo activo (mediante el envío y la recepción de actualizaciones RIP).

R1

```
R1(config)#router rip
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
```

R2

```
R2(config)#router rip
R2(config-router)#passive-interface default
R2(config-router)#no passive-interface s0/0/0
R2(config-router)#no passive-interface s0/0/1
```

R3

```
R3(config)#router rip
R3(config-router)#passive-interface default
R3(config-router)#no passive-interface s0/0/1
```

Paso 2: Impedir la recepción no autorizada de actualizaciones RIP.

El primer paso en la seguridad de RIP es impedir las actualizaciones RIP innecesarias hacia toda la red. El próximo paso es proteger las actualizaciones RIP con contraseñas. Para ello, primero se debe configurar la clave que se utilizará.

```
R1(config)#key chain RIP_KEY
R1(config-keychain)#key 1
R1(config-keychain-key)#key-string cisco
```

Esto debe agregarse a cada router que recibirá actualizaciones RIP.

```
R2(config)#key chain RIP_KEY
R2(config-keychain)#key 1
R2(config-keychain-key)#key-string cisco
```

```
R3(config)#key chain RIP_KEY
R3(config-keychain)#key 1
R3(config-keychain-key)#key-string cisco
```

Para utilizar la clave, debe configurarse cada interfaz que participe en las actualizaciones RIP. Éstas son las mismas interfaces que se habilitaron anteriormente mediante el comando **no passive-interface**.

R1

```
R1(config)#int s0/0/0
R1(config-if)#ip rip authentication mode md5
R1(config-if)#ip rip authentication key-chain RIP_KEY
```

En este punto, R1 no recibe más actualizaciones RIP desde R2, ya que R2 todavía no se configuró para utilizar una clave para las actualizaciones de enrutamiento. Puede visualizar esto en R1 mediante el comando **show ip route** y al confirmar que no aparezca ninguna ruta de R2 en la tabla de enrutamiento.

Borre las rutas IP con el comando **clear ip route *** o espere que se agote el tiempo de espera de las rutas.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *- candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 1 subnets, 1 masks
C       10.1.1.0/24 is directly connected, Serial0/0/0
C    192.168.10.0 is directly connected, Serial0/0/0
```

Configure R2 y R3 para que utilicen autenticación de enrutamiento. Recuerde que se debe configurar cada una de las interfaces activas.

R2

```
R2(config)#int s0/0/0
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
R2(config)#int s0/0/1
R2(config-if)#ip rip authentication mode md5
R2(config-if)#ip rip authentication key-chain RIP_KEY
```

R3

```
R3(config)#int s0/0/1
R3(config-if)#ip rip authentication mode md5
R3(config-if)#ip rip authentication key-chain RIP_KEY
```

Paso 3: Verificar que el enrutamiento RIP sigue funcionando.

Después de haber configurado los tres routers para que utilicen autenticación de enrutamiento, las tablas de enrutamiento deben volver a cargarse con todas las rutas RIP. R1 ahora debe tener todas las rutas a través de RIP. Confirme esto con el comando **show ip route**.

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, *-candidate default, U-per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R       10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/0
C       10.1.1.0/24 is directly connected, Serial0/0/0
```

Tarea 5: Registrar la actividad con SNMP (Protocolo simple de administración de red)

Paso 1: Configurar el registro de SNMP en el servidor syslog.

El registro de SNMP puede ser de utilidad para controlar la actividad de red. La información capturada puede enviarse a un servidor syslog en la red, donde dicha información podrá analizarse y archivarse. Se debe tener cuidado al configurar el registro (syslog) en el router. A la hora de elegir el host de registro designado, se debe recordar que el host de registro debe estar conectado a una red confiable o protegida, o a una interfaz de router aislada y dedicada.

En esta práctica de laboratorio, se configurará PC1 como el servidor syslog para R1. Utilice el comando **logging** para seleccionar la dirección IP del dispositivo al que se enviarán los mensajes SNMP. En este ejemplo, se utiliza la dirección IP de PC1.

```
R1(config)#logging 192.168.10.10
```

Nota: PC1 debe tener software de syslog instalado y en ejecución para poder ver los mensajes syslog.

En el próximo paso, se definirá el nivel de gravedad para los mensajes que se enviarán al servidor syslog.

Paso 2: Configurar el nivel de gravedad de SNMP.

El nivel de los mensajes SNMP puede ajustarse para permitir al administrador determinar qué tipos de mensajes se enviarán al dispositivo syslog. Los routers admiten distintos niveles de registro. Los ocho niveles abarcan desde 0 (emergencia), que indica que el sistema es inestable, hasta 7 (depuración), que envía mensajes que incluyen información del router. Para configurar los niveles de gravedad, se utiliza la palabra clave asociada con cada nivel, tal como se muestra en la tabla.

Nivel de gravedad	Palabra clave	Descripción
0	emergencias	Sistema no utilizable
1	alertas	Se requiere acción inmediata
2	crítico	Condiciones críticas
3	errores	Condiciones de error
4	advertencias	Condiciones de advertencia
5	notificaciones	Condición normal pero significativa
6	información	Mensajes informativos
7	depuración	Mensajes de depuración

El comando **logging trap** establece el nivel de gravedad. El nivel de gravedad incluye el nivel especificado y cualquier otro nivel por debajo de éste (en cuanto a gravedad). Establezca R1 en el nivel 4 para capturar mensajes con niveles de gravedad 4, 5, 6 y 7.

```
R1(config)#logging trap warnings
```

¿Cuál es el riesgo de establecer el nivel de gravedad en un nivel demasiado alto o demasiado bajo?

_____

_____

_____

Si el nivel de gravedad es demasiado alto, el router puede generar demasiados mensajes como para que sean útiles. Es más difícil encontrar los mensajes importantes entre otros mensajes de menor utilidad. Además, puede provocar la congestión de la red. El riesgo de establecer el nivel demasiado bajo es que no se proporciona información suficiente cuando se intenta identificar un problema.

Nota: Si instaló el software de syslog en PC1, genere y observe el software de syslog para detectar mensajes.

Tarea 6: Deshabilitar los servicios de red de Cisco que no se utilizan

Paso 1: Deshabilitar las interfaces que no se utilizan.

¿Por qué se deberían deshabilitar las interfaces que no se utilizan en los dispositivos de red?

_____

_____

_____

Si se dejan habilitadas las interfaces que no se utilizan, otras personas podrían obtengan acceso inesperado a la red si logran obtener acceso físico al dispositivo. Deshabilitar estas interfaces impide que se utilicen para ataques de intermediarios o suplantación DHCP.

En el diagrama de topología, se puede observar que R1 sólo debería utilizar la interfaz S0/0/0 y Fa0/1. Todas las demás interfaces de R1 deben desactivarse administrativamente mediante el comando de configuración de interfaz **shutdown**.

```
R1(config)#interface fastethernet0/0
R1(config-if)#shutdown
R1(config-if)# interface s0/0/1
R1(config-if)#shutdown

*Sep 10 13:40:24.887: %LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to administratively down
*Sep 10 13:40:25.887: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to down
```

Para verificar que el R1 tenga desconectadas todas las interfaces inactivas, utilice el comando **show ip interface brief**. Las interfaces desactivadas manualmente se indican como "administratively down".

```
R1#sh ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  administratively down down
FastEthernet0/1        192.168.10.1    YES manual up                    up
Serial0/0/0            10.1.0.1        YES manual up                    up
Serial0/0/1            unassigned      YES unset  administratively down down
```

Paso 2: Deshabilitar los servicios globales que no se utilizan.

La mayoría de las redes modernas no necesitan muchos servicios. Si se deja habilitados los servicios que no se utilizan, se dejarán los puertos abiertos que podrán utilizarse para poner en riesgo la red. Deshabilite cada uno de estos servicios de R1.

```
R1(config)#no service pad
R1(config)#no service finger
R1(config)#no service udp-small-server
R1(config)#no service tcp-small-server
R1(config)#no ip bootp server
R1(config)#no ip http server
R1(config)#no ip finger
R1(config)#no ip source-route
R1(config)#no ip gratuitous-arps
R1(config)#no cdp run
```

Paso 3: Desactivar los servicios de interfaz que no se utilizan.

Estos comandos se ingresan en el nivel de interfaz y deberían aplicarse a cada una de las interfaces del R1.

```
R1(config-if)#no ip redirects
R1(config-if)#no ip proxy-arp
R1(config-if)#no ip unreachables
R1(config-if)#no ip directed-broadcast
R1(config-if)#no ip mask-reply
R1(config-if)#no mop enabled
```

¿Qué tipo de ataque mitiga la desactivación de redireccionamientos IP, IP inalcanzables y broadcasts dirigidos a IP?

_____

_____

_____

Los redireccionamientos IP, IP inalcanzables y broadcasts dirigidos a IP se utilizan en el los ataques de reconocimiento. Al hacer ping a una gran cantidad de direcciones, un atacante puede obtener información acerca de la estructura de una red. La deshabilitación de estos servicios reduce la cantidad de información que se recibe en dichos intentos.

Paso 4: Utilizar AutoSecure para establecer la seguridad de un router Cisco.

Mediante la utilización de un solo comando en el modo CLI, la función AutoSecure permite deshabilitar servicios IP comunes que pueden explotarse para ataques de red y habilitar los servicios y las funciones IP que pueden ayudar a defender una red en riesgo de ataque. AutoSecure simplifica la configuración de seguridad de un router y refuerza la configuración del router.

Mediante función AutoSecure, se pueden aplicar a un router las mismas características de seguridad recién aplicadas (excepto la seguridad de RIP) de manera mucho más rápida. Debido a que ya se estableció la seguridad de R1, utilice el comando **`auto secure`** en R3.

```
R3#auto secure
               --- Configuración AutoSecure ---

*** La configuración AutoSecure aumenta la seguridad del
router, pero no hace que sea absolutamente resistente
a todos los ataques de seguridad ***

AutoSecure modifica la configuración del dispositivo.
Se muestran todos los cambios de configuración. Para obtener una explicación
detallada sobre la manera en que los cambios de configuración aumentan la
seguridad
y cualquier posible efecto secundario, consulte Cisco.com para
obtener la documentación de AutoSecure.
Puede ingresar "?" en cualquier indicador para obtener ayuda.
Use ctrl-c para cancelar esta sesión en cualquier indicador.

Recopilación de información sobre el router para AutoSecure

¿Está este router conectado a Internet? [no]: sí
Especifique la cantidad de interfaces orientadas a Internet [1]: 1

Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0/0            unassigned      YES unset  down        down
FastEthernet0/1            192.168.30.1    YES manual up          up
Serial0/0/0                unassigned      YES manual down        down
Serial0/0/1                10.2.2.2        YES manual up          up
Especifique el nombre de la interfaz orientada a Internet: Serial0/0/1
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
```

```
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enable secret is either not configured or
 Is the same as enable password
Enter the new enable password: ciscoccna
Confirm the enable password: ciscoccna
Enter the new enable password: ccnacisco
Confirm the enable password: ccnacisco

Configuration of local user database
Enter the username: ccna
Enter the password: ciscoccna
Confirm the password: ciscoccna
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 300

Maximum Login failures with the device: 5

Maximum time period for crossing the failed login attempts: 120

Configure SSH server? Yes
Enter domain-name: cisco.com

Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected to internet

Configure CBAC firewall feature: no
Tcp intercept feature is used prevent tcp syn attack
On the servers in the network. Create autosec_tcp_intercept_list
To form the list of servers to which the tcp traffic is to be observed
```

```
Enable TCP intercept feature: yes

This is the configuration generated:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
line tty 192
 login authentication local_auth
 exec-timeout 15 0
login block-for 300 attempts 5 within 120
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
```

```
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip cef
access-list 100 permit udp any any eq bootpc
interface Serial0/0/1
 ip verify unicast source reachable-via rx allow-default 100
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept drop-mode random
ip tcp intercept watch-timeout 15
ip tcp intercept connection-timeout 3600
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
!
end

Apply this configuration to running-config? [yes]:yes

The name for the keys will be: R3.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R3#
000045: *Nov 16 15:39:10.991 UTC: %AUTOSEC-1-MODIFIED: AutoSecure
configuration has been Modified on this device
```

Como se puede observar, la función AutoSecure es mucho más rápida que la configuración línea por línea. Sin embargo, existen ventajas para hacer esto manualmente, tal como se verá en la práctica de laboratorio de resolución de problemas. Cuando utilice AutoSecure, es posible que desactive un servicio que necesite. Tenga cuidado en todo momento y considere los servicios requeridos antes de utilizar AutoSecure.

Tarea 7: Administrar IOS de Cisco y los archivos de configuración

Paso 1: Mostrar los archivos de IOS de Cisco.

IOS de Cisco es el software que los routers utilizan para funcionar. El router puede tener memoria suficiente para almacenar múltiples imágenes de IOS de Cisco. Es importante saber qué archivos se almacenan en el router.

Ejecute el comando **show flash** para visualizar el contenido de la memoria flash del router.

Precaución: Se debe tener mucho cuidado al ejecutar comandos que impliquen la memoria flash. Si se escribe mal un comando, puede llegar a eliminar la imagen de IOS de Cisco.

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:25:14 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:40:28 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:41:02 +00:00 sdm.tar
4       833024 May 05 2007 21:41:24 +00:00 es.tar
5      1052160 May 05 2007 21:41:48 +00:00 common.tar

8679424 bytes available (23252992 bytes used)
```

Al observar esta lista, se puede determinar lo siguiente:

- La imagen es para un router 1841 (c**1841**-ipbase-mz.124-1c.bin).
- El router utiliza una imagen basada en IP (c1841-**ipbase**-mz.124-1c.bin).
- El IOS de Cisco es versión 12.4(1c) (c1841-ipbase-mz.**124-1c**.bin).
- Este dispositivo tiene instalado SDM (**sdm**config-18xx.cfg, **sdm**.tar).

Puede utilizar el comando **dir all** para mostrar todos los archivos en el router.

```
R2#dir all
Directory of archive:/

No files in directory

No space information available
Directory of system:/

 3  dr-x           0                    <no date>  memory
 1  -rw-         979                    <no date>  running-config
 2  dr-x           0                    <no date>  vfiles

No space information available
Directory of nvram:/

 189  -rw-         979                      <no date>  startup-config
 190  ----           5                      <no date>  private-config
 191  -rw-         979                      <no date>  underlying-config
   1  -rw-           0                      <no date>  ifIndex-table
```

```
196600 bytes total (194540 bytes free)
Directory of flash:/

 1 -rw- 13937472  May 05 2007 20:08:50 +00:00  c1841-ipbase-mz.124-1c.bin
 2 -rw-     1821  May 05 2007 20:25:00 +00:00  sdmconfig-18xx.cfg
 3 -rw-  4734464  May 05 2007 20:25:38 +00:00  sdm.tar
 4 -rw-   833024  May 05 2007 20:26:02 +00:00  es.tar
 5 -rw-  1052160  May 05 2007 20:26:30 +00:00  common.tar
 6 -rw-     1038  May 05 2007 20:26:56 +00:00  home.shtml
 7 -rw-   102400  May 05 2007 20:27:20 +00:00  home.tar
 8 -rw-   491213  May 05 2007 20:27:50 +00:00  128MB.sdf
 9 -rw-   398305  May 05 2007 20:29:08 +00:00  sslclient-win-1.1.0.154.pkg
 10 -rw- 1684577  May 05 2007 20:28:32 +00:00  securedesktop-ios-3.1.1.27-
k9.pkg

31932416 bytes total (8679424 bytes free)
```

Paso 2: Transferir archivos con TFTP.

TFTP se utiliza para archivar y actualizar el software IOS de Cisco de un dispositivo. Sin embargo, en esta práctica de laboratorio no se utilizan archivos reales de IOS de Cisco porque cualquier error que se cometa al ingresar los comandos puede hacer que se elimine la imagen de IOS de Cisco del dispositivo. Al final de esta sección se incluye un ejemplo de una transferencia a través de TFTP del IOS de Cisco.

¿Por qué es importante tener una versión actualizada del software IOS de Cisco?

_____

_____

_____

El software puede actualizarse para corregir un defecto o reemplazar una versión que ya no se admite. Disponer de una versión actualizada garantiza que las características de seguridad más actuales se incluyen en el software IOS de Cisco en ejecución.

Cuando se transfieren archivos a través de TFTP, es importante asegurarse de que el servidor TFTP y el router puedan comunicarse. Una manera de probar esto es hacer ping entre estos dispositivos.

Para comenzar la transferencia del software IOS de Cisco, cree un archivo en el servidor TFTP denominado **test** en la carpeta raíz del TFTP. Este archivo puede ser un archivo de texto en blanco, ya que este paso sólo sirve para ilustrar los pasos necesarios. Cada programa TFTP varía en cuanto a dónde se almacenan los archivos. Consulte el archivo de ayuda del servidor TFTP para determinar cuál es la carpeta raíz.

Desde R1, recupere el archivo y guárdelo en la memoria flash.

```
R2#copy tftp flash
Address or name of remote host []? 192.168.20.254 (IP address of the TFTP
server)
Source filename []? Test (name of the file you created and saved to TFTP
server)
Destination filename [test]? test-server (An arbitrary name for the file when
saved to the router)
Accessing tftp://192.168.20.254/test...
Loading test from 192.168.20.254 (via FastEthernet0/1): !
[OK - 1192 bytes]

1192 bytes copied in 0.424 secs (2811 bytes/sec)
```

Verifique la existencia del archivo en la memoria flash mediante el comando **show flash**.

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server

8675328 bytes available (23257088 bytes used)
```

Los routers también pueden actuar como servidores TFTP. Esto puede ser de utilidad si hay un dispositivo que necesita una imagen y ya existe uno que utiliza dicha imagen. R2 se convertirá en un servidor TFTP para R1. Debe recordarse que las imágenes de IOS de Cisco son específicas según las plataformas del router y los requisitos de memoria. Se debe tener cuidado a la hora de transferir una versión superior de imagen de IOS de Cisco desde un router hacia otro.

La sintaxis de comandos es: **tftp-server nvram:** [*nombre de archivo1* [**alias** *nombre de archivo2*]

El comando que aparece a continuación configura R2 como servidor TFTP. R2 suministra su archivo de configuración inicial a los dispositivos que lo soliciten a través de TFTP (se utiliza el archivo de configuración inicial para los fines de simplicidad y facilidad). La palabra clave **alias** permite a los dispositivos solicitar el archivo mediante el alias **test** en lugar del nombre completo del archivo.

```
R2(config)#tftp-server nvram:startup-config alias test
```

Ahora se puede solicitar el archivo a R2 mediante R1.

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? test
Destination filename []? test-router
Accessing tftp://10.1.1.2/test...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]

1192 bytes copied in 0.452 secs (2637 bytes/sec)
```

Una vez más, verifique que el archivo **test** se haya copiado correctamente mediante el comando **show flash**.

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
```

```
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        1192 Sep 12 2007 07:38:18 +00:00 test-server
12        1192 Sep 12 2007 07:51:04 +00:00 test-router

8671232 bytes available (23261184 bytes used)
```

Dado que no se desea que los archivos sin utilizar ocupen espacio valioso en la memoria, se deben eliminar ahora de la memoria flash de R1. **Hay que tener mucho cuidado al hacerlo.** El borrado accidental de la memoria flash significará que se deberá volver a instalar toda la imagen de IOS para el router. Si el router indica que se borrase la memoria flash (**erase flash**), significa que existe un error. Pocas veces se querrá borrar toda la memoria flash. La única ocasión legítima en que esto sucederá es cuando se actualice el IOS a una imagen de IOS grande. Si aparece al indicador **erase flash**, tal como se muestra en el ejemplo, DETÉNGASE DE INMEDIATO. NO presione Intro. Pida ayuda al instructor DE INMEDIATO.

```
Erase flash: ?[confirm] no
```

```
R1#delete flash:test-server
Delete filename [test-server]?
Delete flash:test? [confirm]
R1#delete flash:test-router
Delete filename [test-router]?
Delete flash:test-router? [confirm]
```

Ejecute el comando **show flash** para verificar que los archivos se hayan eliminado. **Esto es sólo un ejemplo. No complete esta tarea.**

```
R1#show flash
-#- --length-- -----date/time------ path
1     13937472 May 05 2007 21:13:20 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg

8679424 bytes available (23252992 bytes used)
```

A continuación se proporciona un ejemplo de una transferencia TFTP de un archivo de imagen de IOS de Cisco.

NO complete esta tarea en los routers. Sólo debe leerse.

```
R1#copy tftp flash
Address or name of remote host []? 10.1.1.2
Source filename []? c1841-ipbase-mz.124-1c.bin
Destination filename []? flash:c1841-ipbase-mz.124-1c.bin
Accessing tftp://10.1.1.2/c1841-ipbase-mz.124-1c.bin...
```

```
Loading c1841-ipbase-mz.124-1c.bin from 10.1.1.2 (via Serial0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 13937472 bytes]

13937472 bytes copied in 1113.948 secs (12512 bytes/sec)
```

Paso 3: Recuperar una contraseña mediante ROMmon.

Si por algún motivo ya no puede se acceder a un dispositivo debido a que se desconoce, se perdió o se olvidó una contraseña, todavía se puede acceder si se cambia el registro de configuración. El registro de configuración le indica al router qué configuración debe cargar en el arranque. En el registro de configuración, se puede indicar al router que arranque desde una configuración en blanco que no esté protegida con contraseña.

El primer paso para cambiar el registro de configuración es visualizar la configuración actual mediante el comando **show version**. Estos pasos se realizan en R3.

```
R3#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.4(1c), RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 25-Oct-05 17:10 by evmiller

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

R3 uptime is 25 minutes
System returned to ROM by reload at 08:56:50 UTC Wed Sep 12 2007
System image file is "flash:c1841-ipbase-mz.124-1c.bin"

Cisco 1841 (revisión 7.0) with 114688K/16384K bytes de memoria.
Processor board ID FTX1118X0BN
2 FastEthernet interfaces
2 Low-speed serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes de NVRAM.
31.360K bytes de ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

A continuación, vuelva a cargar el router y envíe una pausa durante el arranque. La tecla **Pausa** puede variar de un equipo a otro. Generalmente, se encuentra en la esquina superior derecha del teclado. La pausa permite que el dispositivo entre a un modo denominado ROMmon. Este modo no requiere que el dispositivo tenga acceso al archivo de imagen de IOS de Cisco.

```
R3#reload
Proceed with reload? [confirm]

*Sep 12 08:27:28.670: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload command.
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
```



```
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Readonly ROMMON initialized
rommon 1 >
```

Cambie el registro de configuración por un valor que cargue la configuración inicial del router. Esta configuración no tiene una contraseña configurada, pero admite los comandos de IOS de Cisco. Cambie el valor del registro de configuración en 0x2142.

```
rommon 1 > confreg 0x2142
```

Ahora que ya se cambió, se puede iniciar el dispositivo mediante el comando **reset**.

```
rommon 2 > reset
program load complete, entry point: 0x8000f000, size: 0xcb80
program load complete, entry point: 0x8000f000, size: 0xcb80

program load complete, entry point: 0x8000f000, size: 0xd4a9a0
Self decompressing the image :
############################################################
################################################################################
# [OK]

<output omitted>


         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!
```

Paso 4: Restablecer el router.

Ahora se copia la configuración de inicio en la configuración en ejecución, se restablece la configuración y luego se vuelve a cambiar el registro de configuración al valor por defecto (0x2102).

Para copiar la configuración de inicio desde NVRAM en la memoria en ejecución, escriba **copy startup-config running-config**. Tenga cuidado. *No* escriba `copy running-config startup-config` porque borrará la configuración de inicio.

```
Router#copy startup-config running-config
Destination filename [running-config]? {enter}

2261 bytes copied in 0.576 secs (3925 bytes/sec)

R3#:show running-config
<output omitted>
enable secret 5 $1$31P/$cyPgoxc0R9y93Ps/N3/kg.
!
<output omitted>
!
```

```
key chain RIP_KEY
 key 1
  key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
<output omitted>
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication
 transport output telnet
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
```

En esta configuración, el comando **shutdown** aparece debajo de todas las interfaces, ya que éstas se encuentran actualmente desactivadas. Lo más importante es que ahora se pueden ver las contraseñas (contraseña de enable, contraseña secreta de enable, contraseña de VTY, contraseña de consola), ya sea en formato encriptado o sin encriptar. Puede volver a utilizar contraseñas sin encriptar. Debe cambiar las contraseñas encriptadas por una contraseña nueva.

```
R3#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#enable secret ciscoccna
R3(config)#username ccna password ciscoccna
```

Ejecute el comando **no shutdown** en cada una de las interfaces que desee utilizar.

```
R3(config)#interface FastEthernet0/1
R3(config-if)#no shutdown
R3(config)#interface Serial0/0/0
R3(config-if)#no shutdown
```

Puede ejecutar el comando **show ip interface brief** para confirmar que la configuración de interfaz sea correcta. Todas las interfaces que desee utilizar deben mostrarse como up up.

```
R3#show ip interface brief
Interface                  IP-Address      OK? Method Status      Protocol
FastEthernet0/0            unassigned      YES NVRAM  administratively down down
FastEthernet0/1            192.168.30.1    YES NVRAM  up                    up
Serial0/0/0                10.2.2.2        YES NVRAM  up                    up
Serial0/0/1                unassigned      YES NVRAM  administratively down down
```

Escriba **config-register** *valor de registro de configuración*. La variable *valor de registro de configuración* es el valor que registró en el paso 3 ó 0x2102. Guarde la configuración en ejecución.

```
R3(config)#config-register 0x2102
R3(config)#end
R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

¿Cuáles son las desventajas de la recuperación de contraseñas?

_____

_____

_____

En primer lugar, si las contraseñas están encriptadas, no se pueden ver ni recuperar. Esto es por lo que siempre debe tener una copia de seguridad de todas las configuraciones en funcionamiento para los dispositivos en una red de producción. La segunda desventaja es que cualquier persona que tenga acceso físico a un dispositivo puede seguir estos pasos y tomar control del dispositivo. Por lo tanto, la seguridad física de los dispositivos de red es fundamental.

Configuraciones para la parte 1

R1

```
!
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
security authentication failure rate 5 log
enable secret 5 $1$0Ch/$fp.BLSjtqOwxL7VyBwURB1
!
aaa new-model
!
```

```
aaa authentication login LOCAL_AUTH local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
no ip source-route
no ip gratuitous-arps
!
no ip bootp server
no ip domain lookup
login block-for 300 attempts 2 within 120
!
!
key chain RIP_KEY
 key 1
  key-string 7 05080F1C2243
!
username ccna password 7 070C285F4D061A061913
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no mop enabled
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
!
```

```
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
no ip http server
no ip http secure-server
!
logging trap warnings
logging 192.168.10.10
no cdp run
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law.^C
!
line con 0
 exec-timeout 5 0
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 exec-timeout 5 0
 login authentication LOCAL_AUTH
!
scheduler allocate 20000 1000
!
end
```

R2

```
hostname R2
!
no ip domain lookup
!
key chain RIP_KEY
 key 1
  key-string cisco
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clock rate 115200
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 network 209.165.200.0
 no auto-summary
!
no ip http server
no ip http secure-server
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law.^C
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

R3

```
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname R3
!
security authentication failure rate 10 log
security passwords min-length 6
logging buffered 4096 debugging
logging console critical
enable secret 5 $1$ZT.e$0rWCK4DgdK5sz7tThM16S0
enable password 7 141411050D0723382727
!
aaa new-model
!
```

```
aaa authentication login local_auth local
!
aaa session-id common
!
no ip source-route
no ip gratuitous-arps
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept connection-timeout 3600
ip tcp intercept watch-timeout 15
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
ip tcp intercept drop-mode random
!
no ip bootp server
no ip domain lookup
ip domain name cisco.com
ip ssh time-out 60
ip ssh authentication-retries 2
login block-for 300 attempts 5 within 120
!
key chain RIP_KEY
 key 1
  key-string 7 05080F1C2243
!
username ccna password 7 070C285F4D061A061913
archive
 log config
  logging enable
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no mop enabled
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
```

```
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip verify unicast source reachable-via rx allow-default 100
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
interface Serial0/1/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
no ip http server
no ip http secure-server
!
logging trap debugging
logging facility local2
access-list 100 permit udp any any eq bootpc
no cdp run
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law.^C
!
line con 0
 exec-timeout 5 0
 login authentication local_auth
 transport output telnet
line aux 0
 exec-timeout 15 0
 login authentication local_auth
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet ssh
!
```

```
scheduler allocate 20000 1000
!
end
```

Tarea 8: Utilizar el SDM para establecer la seguridad de un router

Si el SDM no está instalado en los routers, consulte el **Apéndice "Cómo instalar el SDM"** para obtener instrucciones sobre cómo instalar el SDM. Estas instrucciones no se incluyen en la versión para el estudiante de esta práctica de laboratorio.

En esta tarea, se utilizará Security Device Manager (SDM), la interfaz GUI, para establecer la seguridad del router R2. El SDM es más rápido que la escritura de cada uno de los comandos y proporciona más control que la función AutoSecure.

Verifique si el SDM está instalado en el router:

```
R2#show flash
-#- --length-- -----date/time------ path
1     13937472 Sep 12 2007 08:31:42 +00:00 c1841-ipbase-mz.124-1c.bin
2         1821 May 05 2007 21:29:36 +00:00 sdmconfig-18xx.cfg
3      4734464 May 05 2007 21:30:14 +00:00 sdm.tar
4       833024 May 05 2007 21:30:42 +00:00 es.tar
5      1052160 May 05 2007 21:31:10 +00:00 common.tar
6         1038 May 05 2007 21:31:36 +00:00 home.shtml
7       102400 May 05 2007 21:32:02 +00:00 home.tar
8       491213 May 05 2007 21:32:30 +00:00 128MB.sdf
9      1684577 May 05 2007 21:33:16 +00:00 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 May 05 2007 21:33:50 +00:00 sslclient-win-1.1.0.154.pkg
11        2261 Sep 25 2007 23:20:16 +00:00 Tr(RIP)
12        2506 Sep 26 2007 17:11:58 +00:00 save.txt
```

Si el SDM no está instalado en el router, es necesario instalarlo para poder continuar. Consulte con el instructor para obtener instrucciones.

Paso 1: Conectar R2 mediante el servidor TFTP.

Cree un nombre de usuario y una contraseña en R2.

```
R2(config)#username ccna password ciscoccna
```

Habilite el servidor seguro http en R2 y conecte R2 mediante un explorador Web en el servidor TFTP.

```
R2(config)#ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R2(config)#
*Nov 16 16:01:07.763: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Nov 16 16:01:08.731: %PKI-4-NOAUTOSAVE: Configuration was modified.  Issue
"write memory" to save new certificate
R2(config)#end
R2#copy run start
```

Desde el servidor TFTP, abra un explorador Web y navegue hasta https://192.168.20.1/. Inicie sesión con el usuario y la contraseña configurados anteriormente:

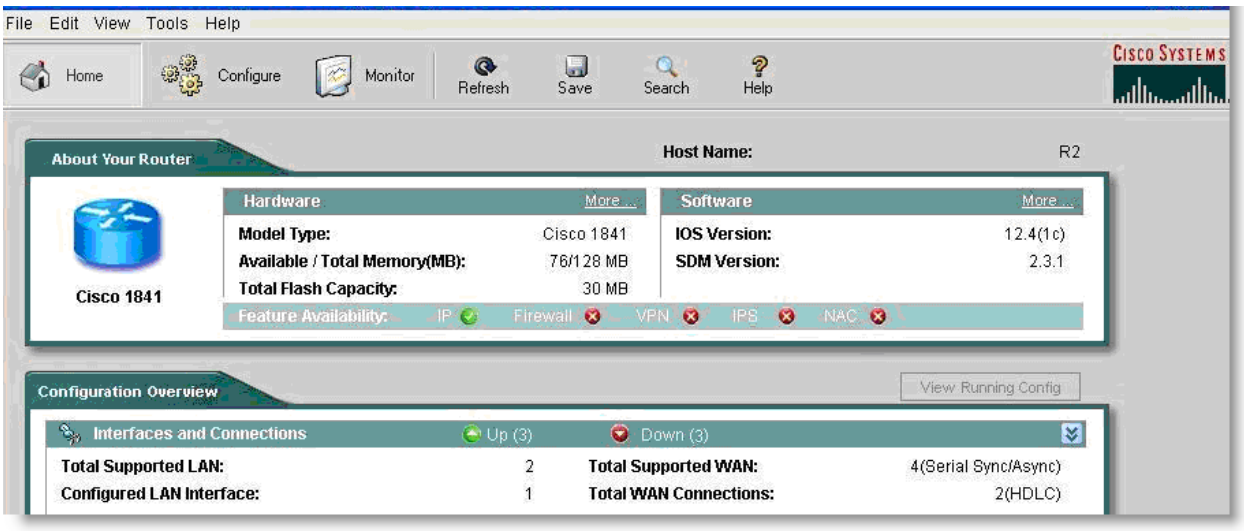
nombre de usuario: **ccna**

contraseña: **ciscoccna**

Seleccione **Cisco Router and Security Device Manager**

Abra Internet Explorer y especifique la dirección IP para R2 en la barra de dirección. Se abre una nueva ventana. Asegúrese de haber desactivado todos los bloqueadores de elementos emergentes del explorador. Además, asegúrese de tener JAVA instalado y actualizado.

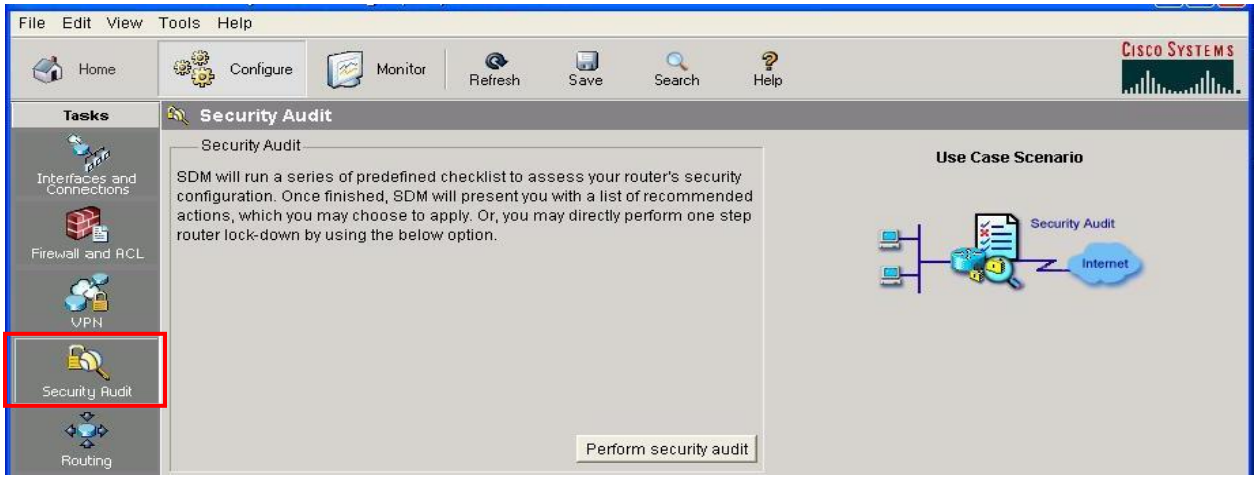
Una vez que haya terminado de cargarse, se abre una nueva ventana para el SDM.



Paso 2: Navegar hacia la función Security Audit.

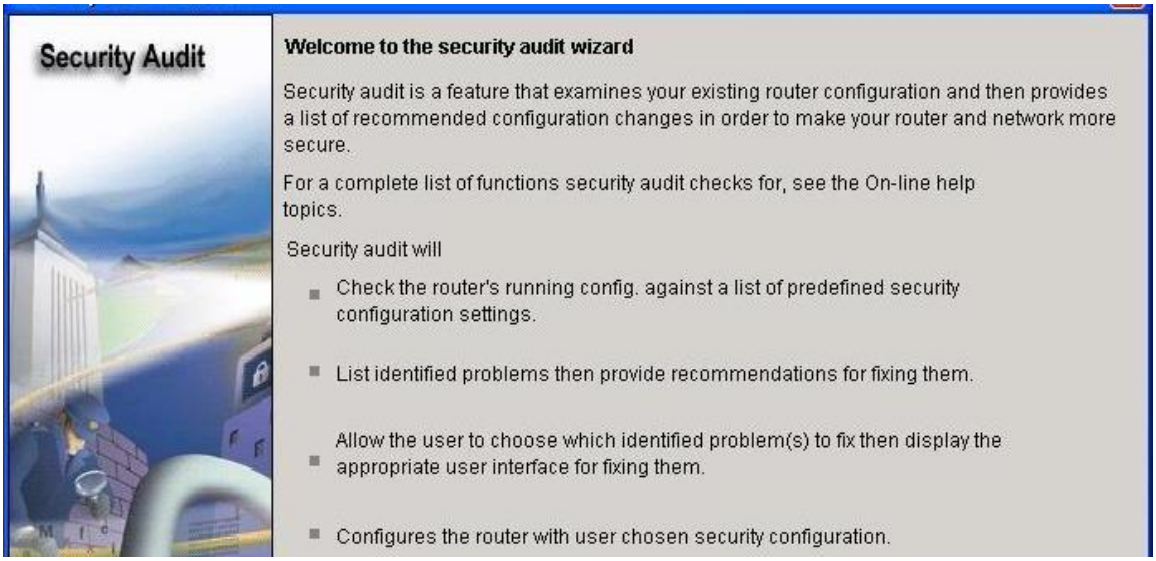
Haga clic en el botón **Configure**, que se encuentra en la esquina superior izquierda de la ventana.

Navegue hacia abajo en el panel izquierdo hasta llegar a **Security Audit** y haga clic en esta opción.

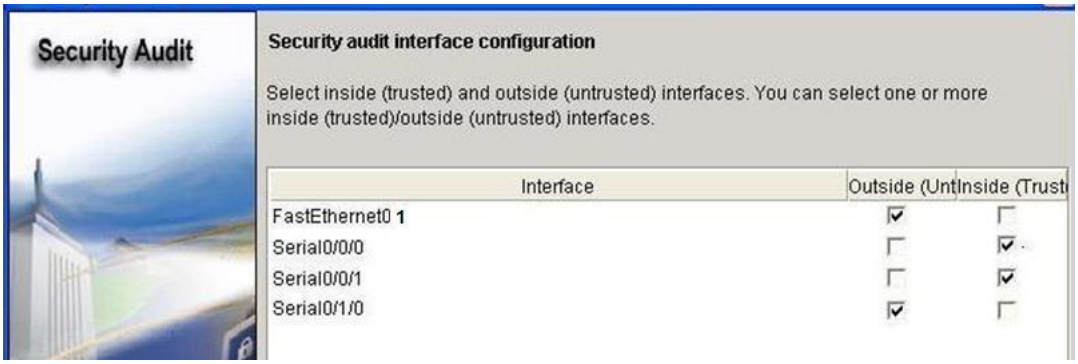


Al hacer clic en **Security Audit**, se abre otra ventana.

Paso 3: Realizar una auditoría de seguridad.

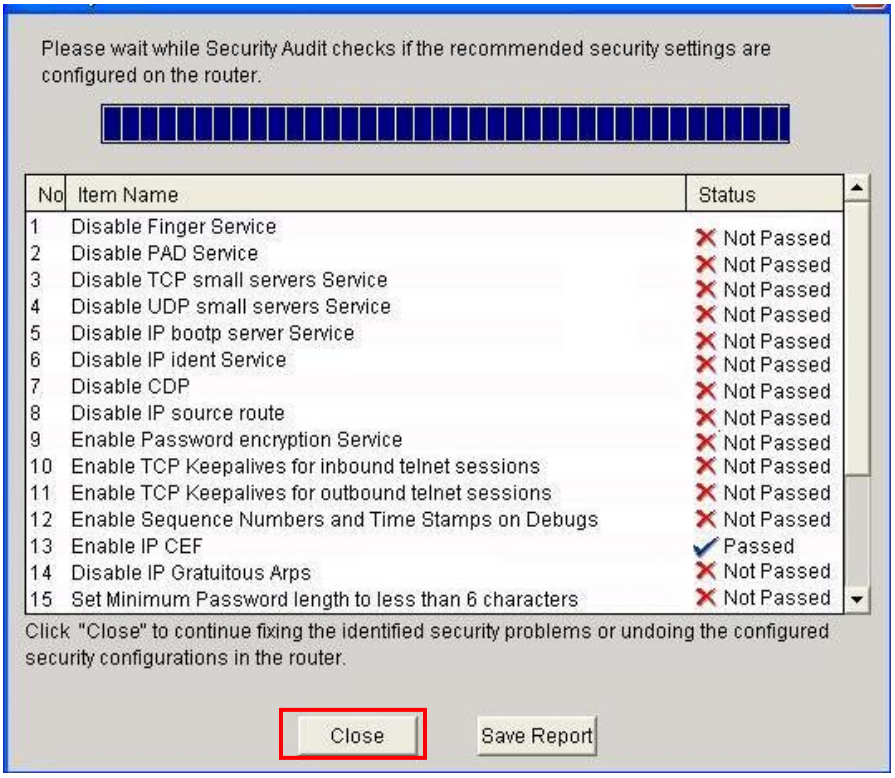


Esto proporciona una explicación breve acerca de cómo funciona la opción Security Audit. Haga clic en **Next** para abrir la ventana de configuración Security Audit Interface.



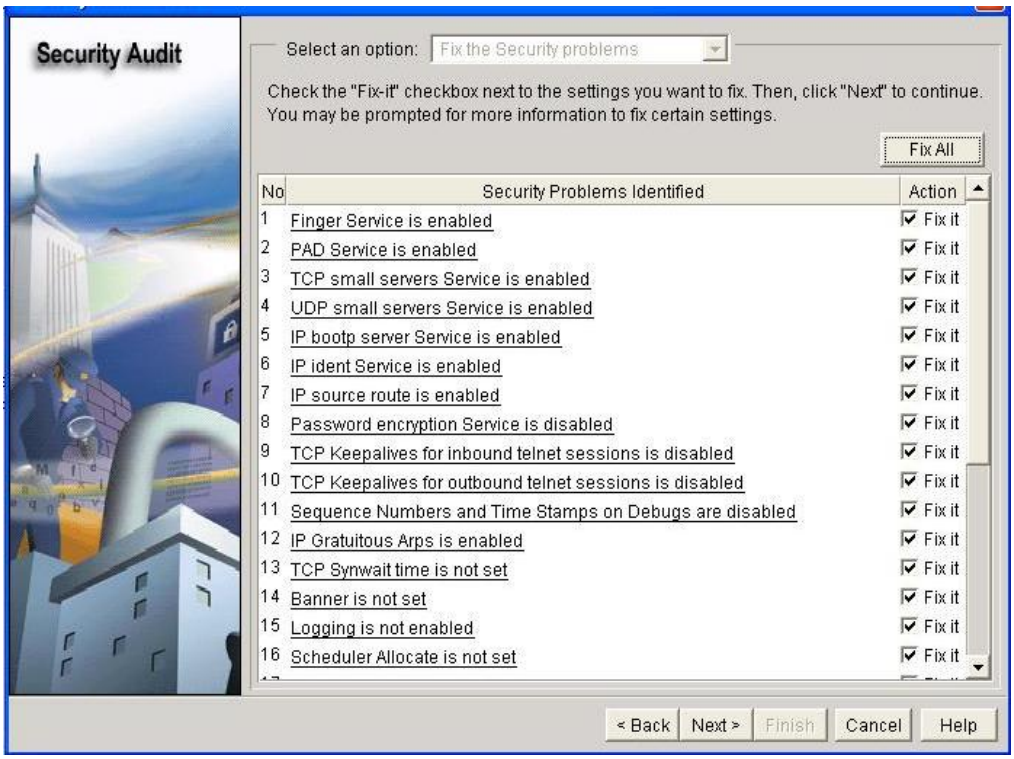
Si el usuario no está seguro acerca de la legitimidad del tráfico que ingresa a la interfaz, ésta debe calificarse como externa (no confiable). En este ejemplo, ni FastEthernet0/1 ni Serial0/1/0 son confiables porque Serial0/1/0 apunta a Internet mientras que Fastethernet0/1 apunta al acceso de la red y podría generarse tráfico ilegítimo.

Una vez que se hayan seleccionado las interfaces internas y externas, haga clic en **Next**. Se abre una nueva ventana que indica que SDM está realizando una auditoría de seguridad.

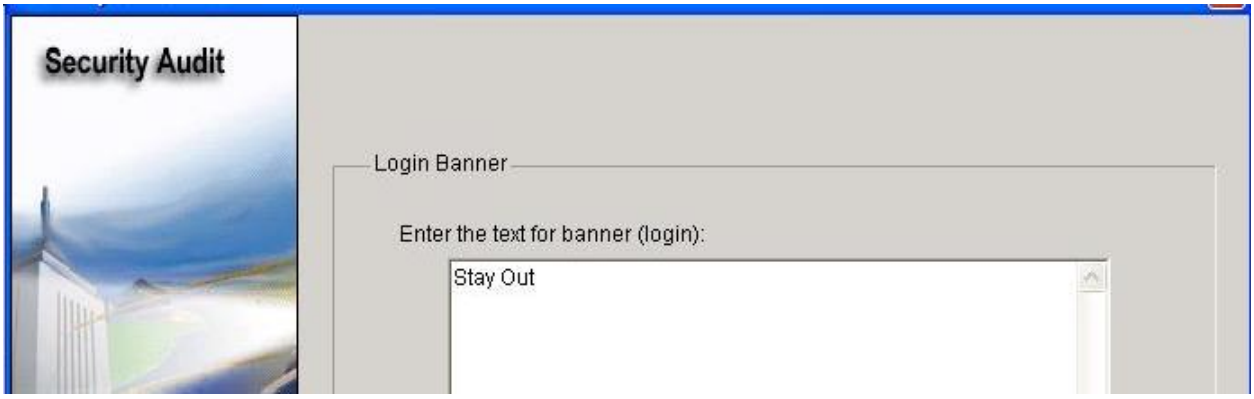


Como se puede observar, la configuración por defecto no es segura. Haga clic en el botón **Close** para continuar.

Paso 4: Aplicar la configuración al router.



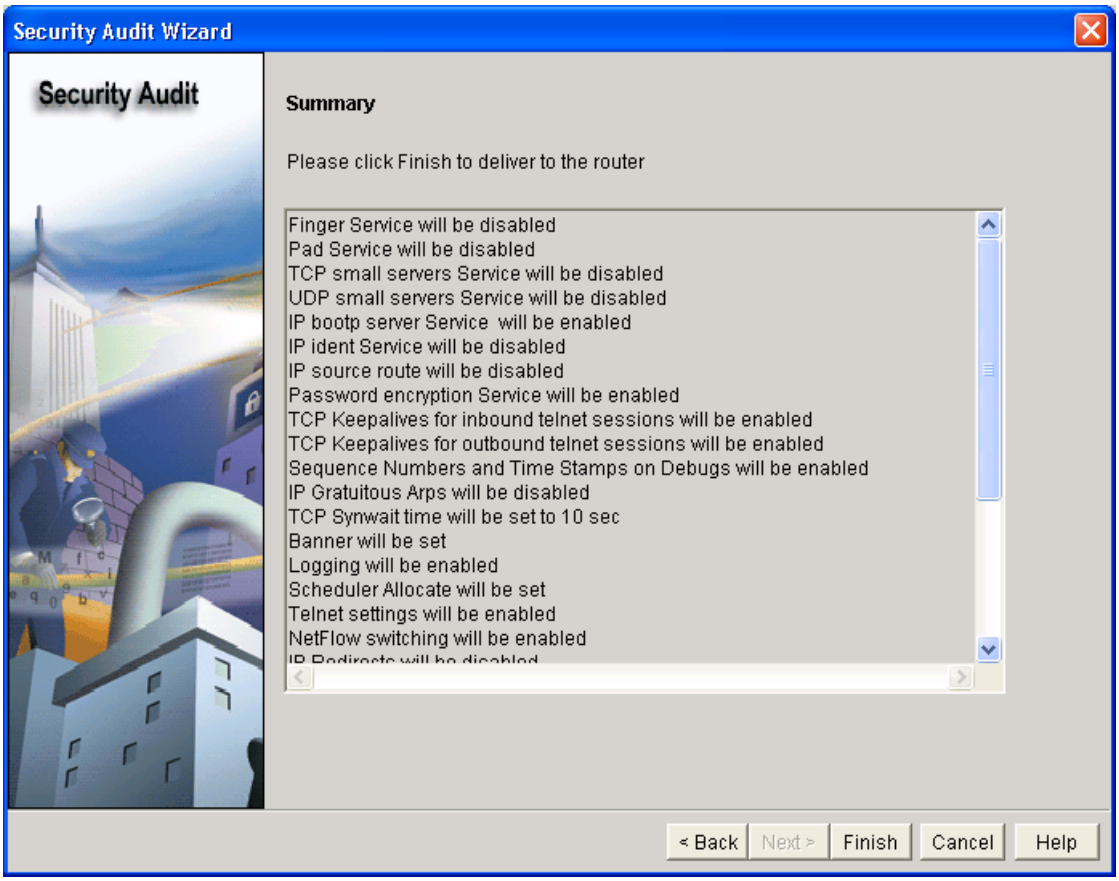
Haga clic en el botón **Fix All** para que se realicen todos los cambios de seguridad sugeridos. A continuación, haga clic en el botón **Next**.



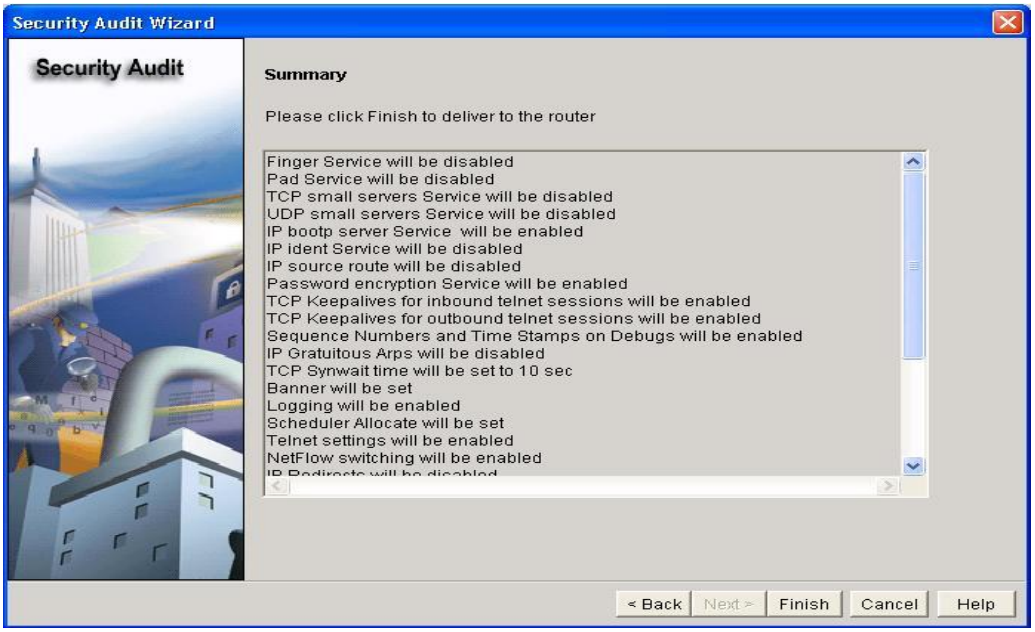
Escriba un mensaje para utilizarlo como mensaje del día para el router y después haga clic en **Next**.

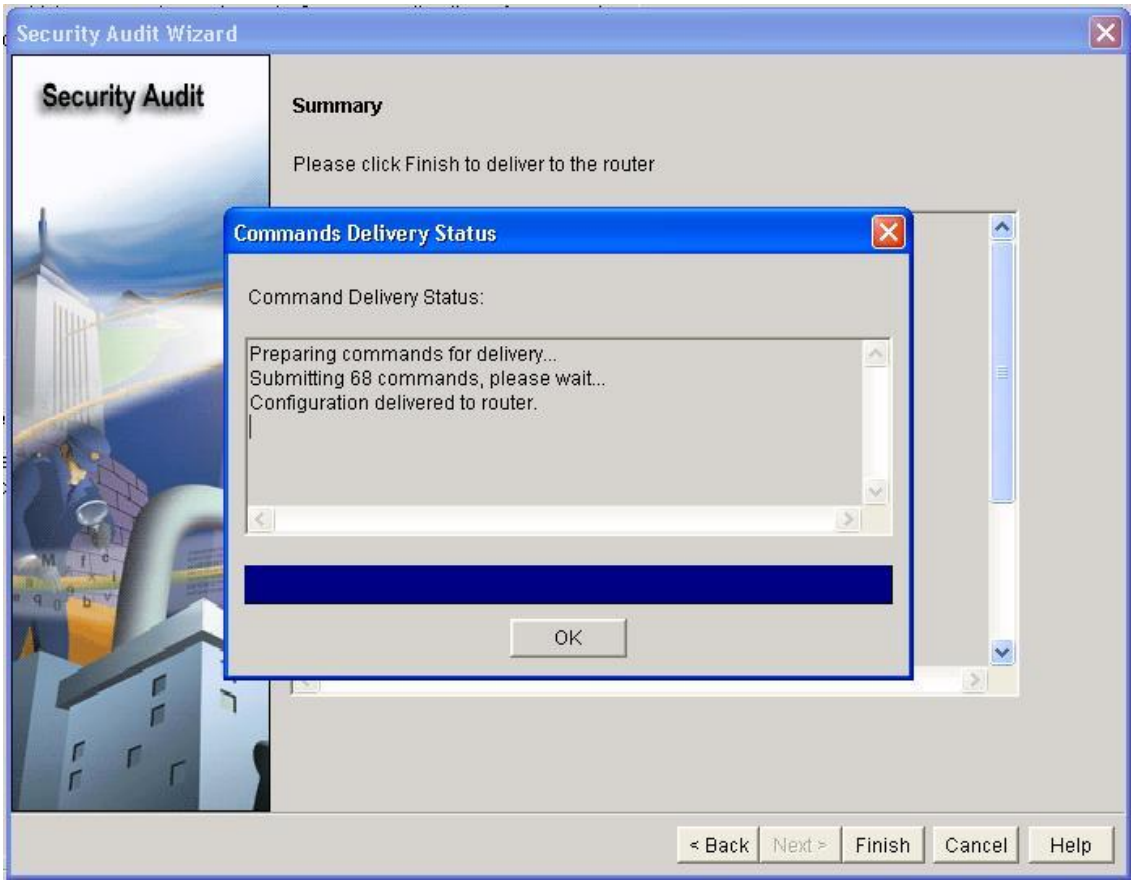
A continuación, establezca el nivel de gravedad de las traps de registro que el router debe enviar al servidor syslog. El nivel de gravedad se establece en depuración para esta situación. Haga clic en **Next** para ver un resumen de los cambios que se realizarán en el router.

Paso 5: Aplicar la configuración al router.



Una vez que haya revisado los cambios que se realizarán, haga clic en **Finish**.





Haga clic en **OK** y salga de SDM.

Tarea 9: Documentar las configuraciones del router

En cada router, ejecute el comando **`show run`** y capture las configuraciones.

R1

```
!
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
security authentication failure rate 5 log
enable secret 5 $1$0Ch/$fp.BLSjtqOwxL7VyBwURB1
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
no ip source-route
no ip gratuitous-arps
!
no ip bootp server
no ip domain lookup
login block-for 300 attempts 2 within 120
!
!
key chain RIP_KEY
 key 1
  key-string 7 05080F1C2243
!
username ccna password 7 070C285F4D061A061913
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no mop enabled
!
interface Serial0/0/0
```

```
 ip address 10.1.1.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
no ip http server
no ip http secure-server
!
logging trap warnings
logging 192.168.10.10
no cdp run
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law.^C
!
line con 0
 exec-timeout 5 0
 login authentication LOCAL_AUTH
line aux 0
line vty 0 4
 exec-timeout 5 0
 login authentication LOCAL_AUTH
!
scheduler allocate 20000 1000
!
end
```

R2

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
```

```
hostname R2
no ip domain-lookup
banner motd ^Unauthorized access strictly prohibited and prosecuted to the
full extent of the law.^
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
no ip finger
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password ciscoccna
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no fair-queue
!
```

```
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
 no shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 network 209.165.200.224
 no auto-summary
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication local_auth
 transport output telnet
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 pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
```

```
!
hostname R3
!
security authentication failure rate 10 log
security passwords min-length 6
logging buffered 4096 debugging
logging console critical
enable secret 5 $1$ZT.e$0rWCK4DgdK5sz7tThM16S0
enable password 7 141411050D0723382727
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
no ip source-route
no ip gratuitous-arps
ip tcp intercept list autosec_tcp_intercept_list
ip tcp intercept connection-timeout 3600
ip tcp intercept watch-timeout 15
ip tcp intercept max-incomplete low 450
ip tcp intercept max-incomplete high 550
ip tcp intercept drop-mode random
!
no ip bootp server
no ip domain lookup
ip domain name cisco.com
ip ssh time-out 60
ip ssh authentication-retries 2
login block-for 300 attempts 5 within 120
!
key chain RIP_KEY
 key 1
  key-string 7 05080F1C2243
!
username ccna password 7 070C285F4D061A061913
archive
 log config
  logging enable
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
```

```
 duplex auto
 speed auto
 no mop enabled
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip verify unicast source reachable-via rx allow-default 100
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
interface Serial0/1/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clock rate 2000000
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
no ip http server
no ip http secure-server
!
logging trap debugging
logging facility local2
access-list 100 permit udp any any eq bootpc
no cdp run
!
banner motd ^CUnauthorized access strictly prohibited and prosecuted to the
full extent of the law.^C
!
```

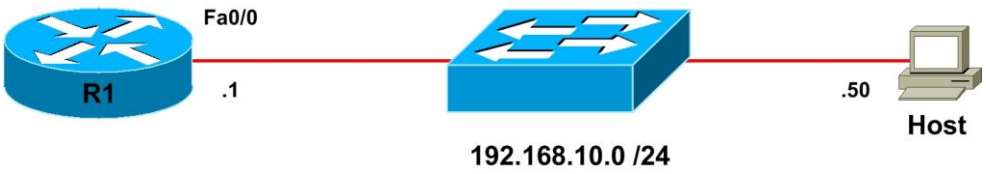
```
line con 0
 exec-timeout 5 0
 login authentication local_auth
 transport output telnet
line aux 0
 exec-timeout 15 0
 login authentication local_auth
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Tarea 10: 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.

Apéndice: Cómo instalar SDM

Diagrama de topología



Escenario

En esta práctica de laboratorio, se preparará un router para su acceso a través de Security Device Manager (SDM) de Cisco mediante algunos comandos básicos con el fin de permitir la conectividad desde SDM hacia el router. A continuación, se instalará la aplicación SDM localmente en un equipo host. Por último, se instalará SDM en la memoria flash de un router.

Paso 1: Preparación

Comience esta práctica de laboratorio mediante la eliminación de cualquier configuración anterior y luego vuelva a cargar los dispositivos. Una vez que los dispositivos se hayan cargado nuevamente, establezca los nombres de host apropiados. Asegúrese de que el switch esté configurado de modo tal que el router y el host se encuentren en la misma VLAN. Por defecto, todos los puertos del switch se asignan a la VLAN 1.

Asegúrese de que el equipo PC cumpla con los requisitos mínimos para admitir SDM. SDM puede ejecutarse en un equipo PC que funcione con cualquiera de los siguientes sistemas operativos:

- Microsoft Windows ME
- Microsoft Windows NT 4.0 Workstation con Service Pack 4
- Microsoft Windows XP Professional
- Microsoft Windows 2003 Server (Standard Edition)
- Microsoft Windows 2000 Professional con Service Pack 4

Nota: Windows 2000 Advanced Server no es compatible.

Además, debe habilitarse un explorador Web con SUN JRE 1.4 o superior, o un explorador controlado por ActiveX.

Paso 2: Preparar el router para SDM

En primer lugar, cree un nombre de usuario y una contraseña en el router para que los utilice SDM. Este inicio de sesión requerirá un nivel privilegiado de 15 para que SDM pueda cambiar la configuración del router.

```
R1(config)# username ciscosdm privilege 15 password 0 ciscosdm
```

Para que funcione SDM, se debe configurar acceso HTTP al router. Si la imagen lo admite (se necesita una imagen de IOS que admita la funcionalidad de criptografía), también se debe habilitar el acceso HTTPS seguro mediante el comando **ip http secure-server**. La habilitación de HTTPS genera algunos resultados acerca de las claves de encriptación RSA. Esto es normal. Además, asegúrese de que el servidor HTTP utilice la base de datos local para la autenticación.

```
R1(config)# ip http server
R1(config)# ip http secure-server
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Jan 14 20:19:45.310: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jan 14 20:19:46.406: %PKI-4-NOAUTOSAVE: Configuration was modified.
Issue "write memory" to save new certificate
R1(config)# ip http authentication local
```

Por último, configure las líneas de terminal virtual del router para la autenticación mediante la base de datos de autenticación local. Permita entradas del terminal virtual desde telnet y SSH.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet ssh
```

Paso 3: Configurar el direccionamiento

Configure la interfaz Fast Ethernet del router con la dirección IP que se muestra en el diagrama. Si ya configuró la dirección IP correcta, omita este paso.

```
R1(config)# interface fastethernet0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
```

A continuación, asigne una dirección IP al equipo PC. Si el equipo PC ya tiene una dirección IP en la misma subred que la del router, puede omitir este paso.

Desde el equipo PC, haga ping a la interfaz Ethernet de R1. Se deberían recibir respuestas. Si no se recibe ninguna respuesta, realice la resolución de problemas. Para ello, verifique la VLAN de los puertos del switch, la dirección IP y la máscara de subred de cada uno de los dispositivos conectados al switch.

Paso 4: Extraer SDM en el host

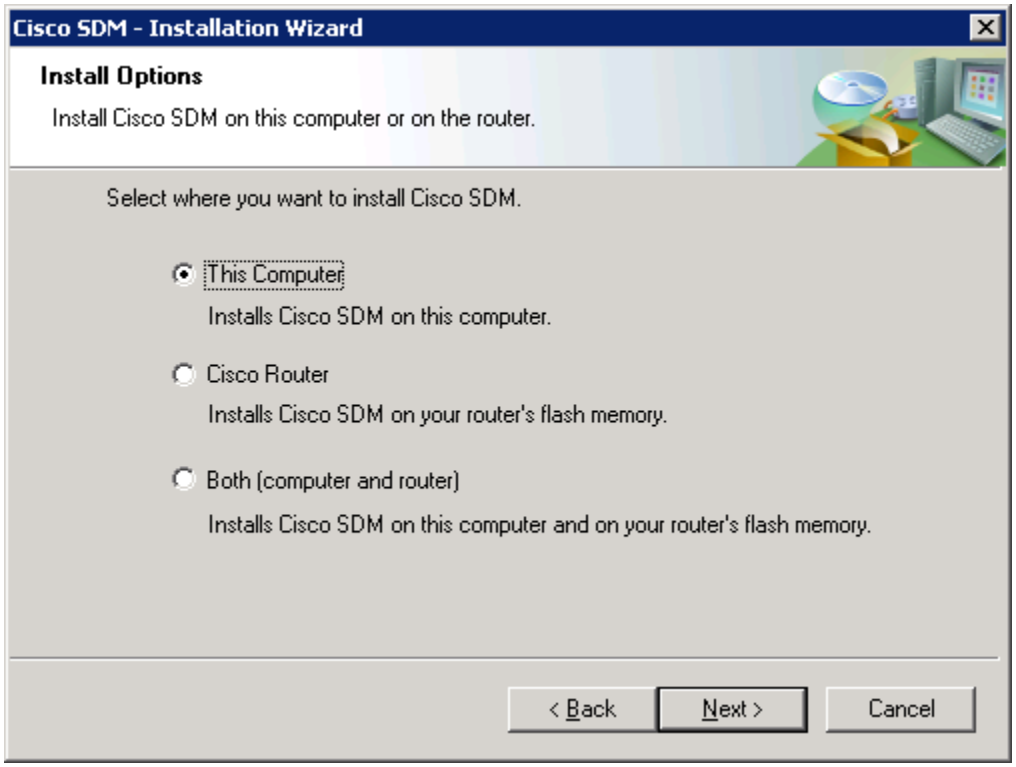
Ahora que el router está listo para su acceso desde SDM y que hay conectividad entre el router y el equipo PC, se puede utilizar SDM para configurar el router. Se debería comenzar por la extracción del archivo comprimido de SDM en un directorio del disco duro. En este ejemplo, el directorio utilizado es “C:\sdm\”, aunque se puede utilizar cualquier ruta deseada.

Está casi listo para utilizar SDM para configurar el router. El último paso es la instalación de la aplicación SDM en el equipo PC.

Paso 5: Instalar SDM en el equipo PC

Haga doble clic en el programa ejecutable **setup.exe** para abrir el asistente de instalación. Una vez que se abra la pantalla del asistente de instalación, haga clic en **Next**. Acepte las condiciones del acuerdo de licencia y haga clic en **Next**.

La siguiente pantalla solicita que se elija de entre las tres opciones para la ubicación de la instalación de SDM.



Al instalar SDM, se puede instalar la aplicación en el equipo sin colocarla en la memoria flash del router, se puede instalar en el router sin afectar al equipo o bien se puede instalar en ambos. Ambos tipos de instalaciones son muy similares. Si se desea instalar SDM en el equipo, vaya directamente al paso 7.

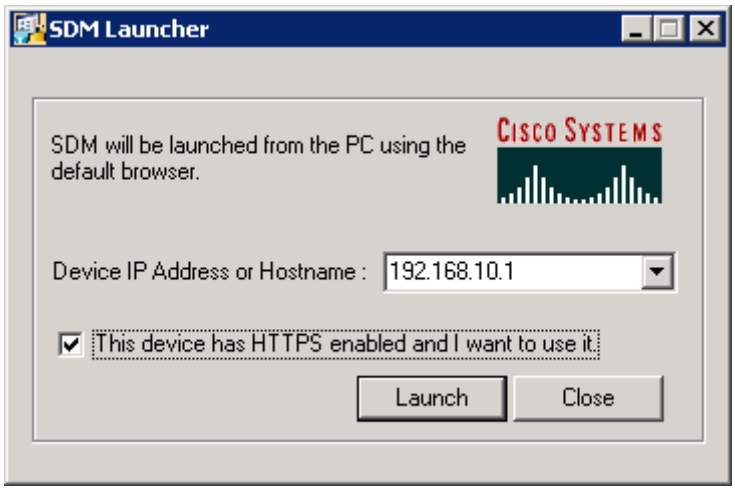
Por ahora, haga clic en **This Computer** y a continuación en **Next**. Utilice la carpeta de destino por defecto y haga clic en **Next** otra vez.

Haga clic en **Install** para iniciar la instalación.

El software se instala y después aparece un cuadro de diálogo final que solicita que se inicie SDM. Active la casilla **Launch Cisco SDM** y luego haga clic en **Finish**.

Paso 6: Ejecutar SDM desde el equipo PC

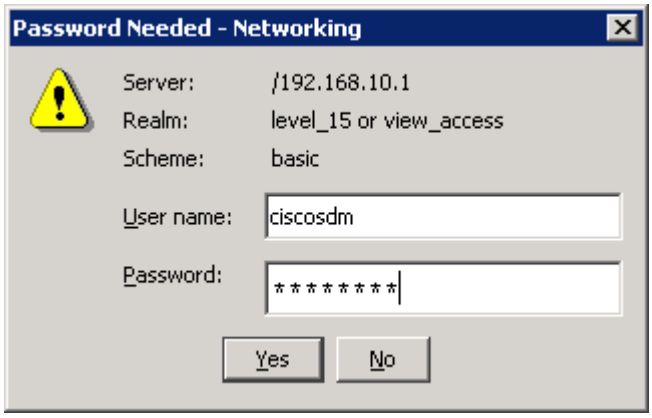
Si se activó la opción la opción Launch Cisco SDM, SDM debería iniciarse desde el instalador una vez que haya completado el paso 5. En caso contrario, o bien si ejecuta SDM sin haberlo instalado recientemente, haga clic en el icono del escritorio con el nombre **Cisco SDM**. Se abre el cuadro de diálogo SDM Launcher. Escriba la dirección IP del router que se muestra en el diagrama como una dirección IP del dispositivo. Si se habilitó el servidor seguro HTTP en el paso 2, active la casilla **This device has HTTPS enabled and I want to use it**. A continuación, haga clic en el botón **Launch**.



Cuando aparezca la advertencia de seguridad, haga clic en **Yes**. Observe que es posible que, inicialmente, Internet Explorer bloquee SDM y que se deberá permitir o adaptar las opciones de seguridad de Internet Explorer según sea necesario para poder utilizarlo. Según la versión de Internet Explorer que se ejecute, una de estas opciones es especialmente importante para ejecutar SDM localmente y se encuentra en el menú Herramientas, en Opciones de Internet… Haga clic en la ficha **Opciones avanzadas** y, en la sección Seguridad, active la casilla **Permitir que el contenido activo se ejecute en los archivos de Mi equipo**, en caso de que no esté activada.

Escriba el nombre de usuario y la contraseña creados anteriormente.

Es posible que se solicite la aceptación de un certificado de este router. Acepte el certificado para continuar. A continuación, proporcione el nombre de usuario y la contraseña para el router y haga clic en **Yes**.

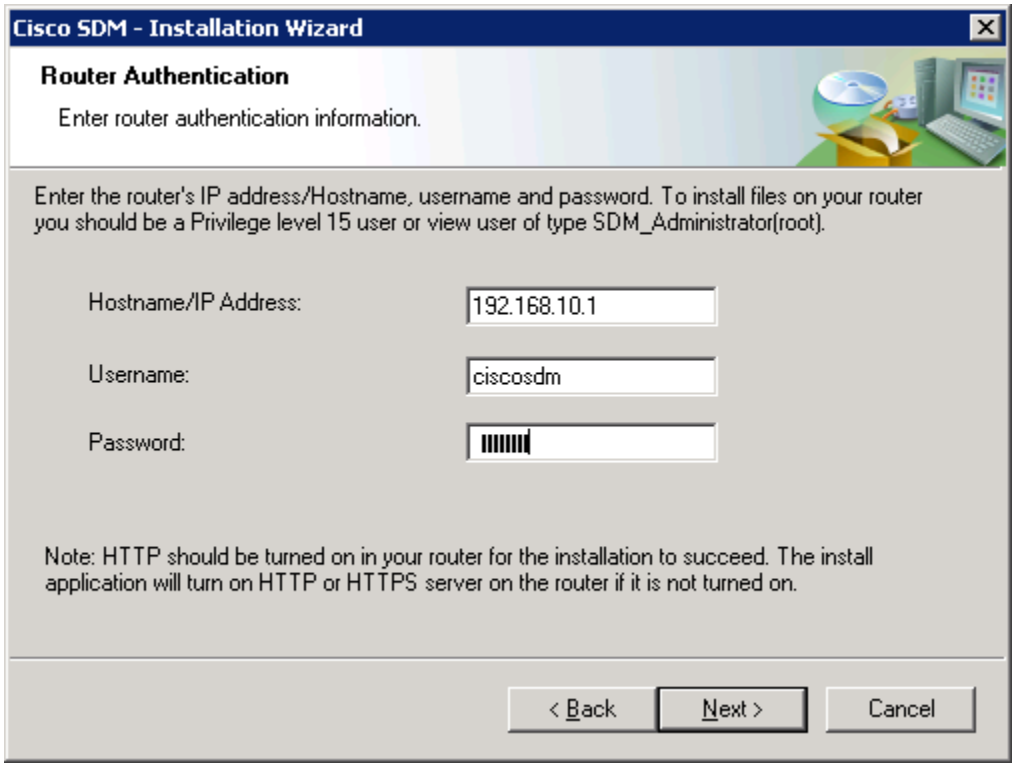


SDM lee la configuración del router. Si las configuraciones se realizaron correctamente, se podrá acceder al panel de control de SDM. Si la configuración es correcta, significa que configuró SDM y se conectó a éste correctamente. La información puede variar según la versión de SDM que se ejecute.

Paso 7: Instalar SDM en el router

Siga el paso 6 hasta que aparezca la solicitud que se muestra en la siguiente figura. Cuando aparezca esta ventana, haga clic en **Cisco Router** para instalar SDM en la memoria flash del router. Si no desea instalar SDM en la memoria flash del router o si no tiene el espacio disponible en la memoria flash, no intente instalar el SDM en el router.

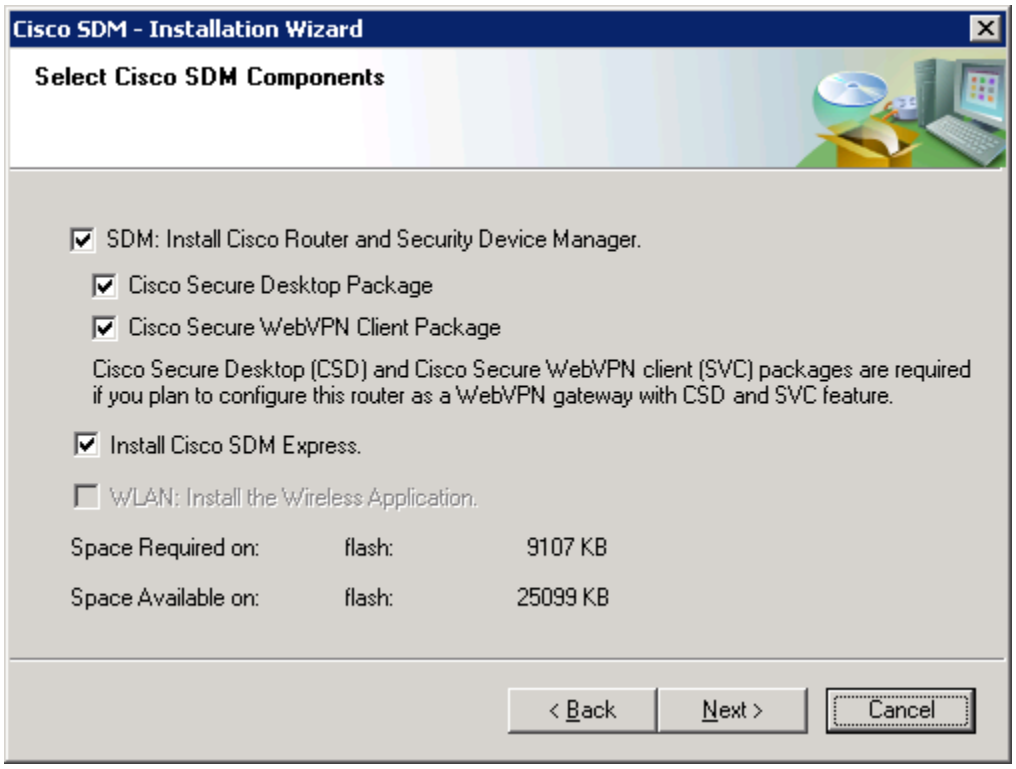
Escriba la información del router para que el instalador pueda acceder de manera remota e instalar SDM en el router.



SDM de Cisco se conecta al router. Es posible que se observe que algunos mensajes se registran en la consola. Esto es normal.

```
Jan 14 16:15:26.367: %SYS-5-CONFIG_I: Configured from console by
ciscosdm on vty0 (192.168.10.50)
```

Elija **Typical** como el tipo de instalación y haga clic en **Next**. Deje las opciones de instalación por defecto que están marcadas y haga clic en **Next**.



Por último, haga clic en **Install** para iniciar el proceso de instalación. Durante la instalación, es posible que se registren más mensajes en la consola. Este proceso de instalación demora un tiempo (observe las marcas horarias en los resultados de la consola que aparecen a continuación para calcular la duración en un Cisco 2811). El tiempo variará según el modelo de router.

```
Jan 14 16:19:40.795: %SYS-5-CONFIG_I: Configured from console by
ciscosdm on vty0 (192.168.10.50)
```

Al final de la instalación, se solicita que se inicie SDM en el router. Antes de hacerlo, vaya a la consola y ejecute el comando **show flash:**. Observe todos los archivos que SDM instaló en la memoria flash. Antes de la instalación, el único archivo de la lista era el primer archivo, la imagen de IOS.

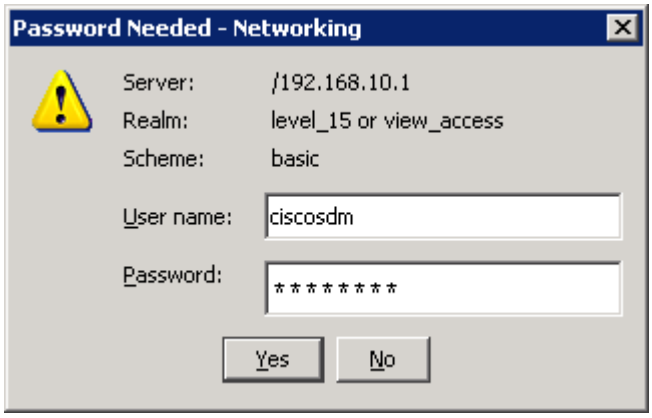
```
R1# show flash:

CompactFlash directory:
File  Length    Name/status
  1   38523272  c2800nm-advipservicesk9-mz.124-9.T1.bin
  2   1038      home.shtml
  3   1823      sdmconfig-2811.cfg
  4   102400    home.tar
  5   491213    128MB.sdf
  6   1053184   common.tar
  7   4753408   sdm.tar
  8   1684577   securedesktop-ios-3.1.1.27-k9.pkg
  9   398305    sslclient-win-1.1.0.154.pkg
 10   839680    es.tar
[47849552 bytes used, 16375724 available, 64225276 total]
62720K bytes of ATA CompactFlash (Read/Write)
```

Paso 8: Ejecutar SDM desde el router

Abra Internet Explorer y navegue hasta el URL “https://<dirección IP>/” o “http://<dirección IP>/”, según si se habilitó o no el servidor seguro HTTP en el paso 2. Cuando se solicite la aceptación del certificado, haga clic en **Yes**.

Pase por alto las advertencias de seguridad y haga clic en **Run**.

Escriba el nombre de usuario y la contraseña configurados en el paso 2.



SDM leerá la configuración del router.

Una vez que SDM haya terminado de cargar la configuración actual del router, aparecerá la página de inicio de SDM. Si la configuración es correcta, significa que configuró SDM y se conectó a éste correctamente. Lo que se observa puede variar de lo que aparece en la figura a continuación, según el número de modelo del router, la versión de IOS y otras variables.

Práctica de laboratorio 4.6.2: Reto de configuración de seguridad (Versión para el instructor)

Diagrama de topología

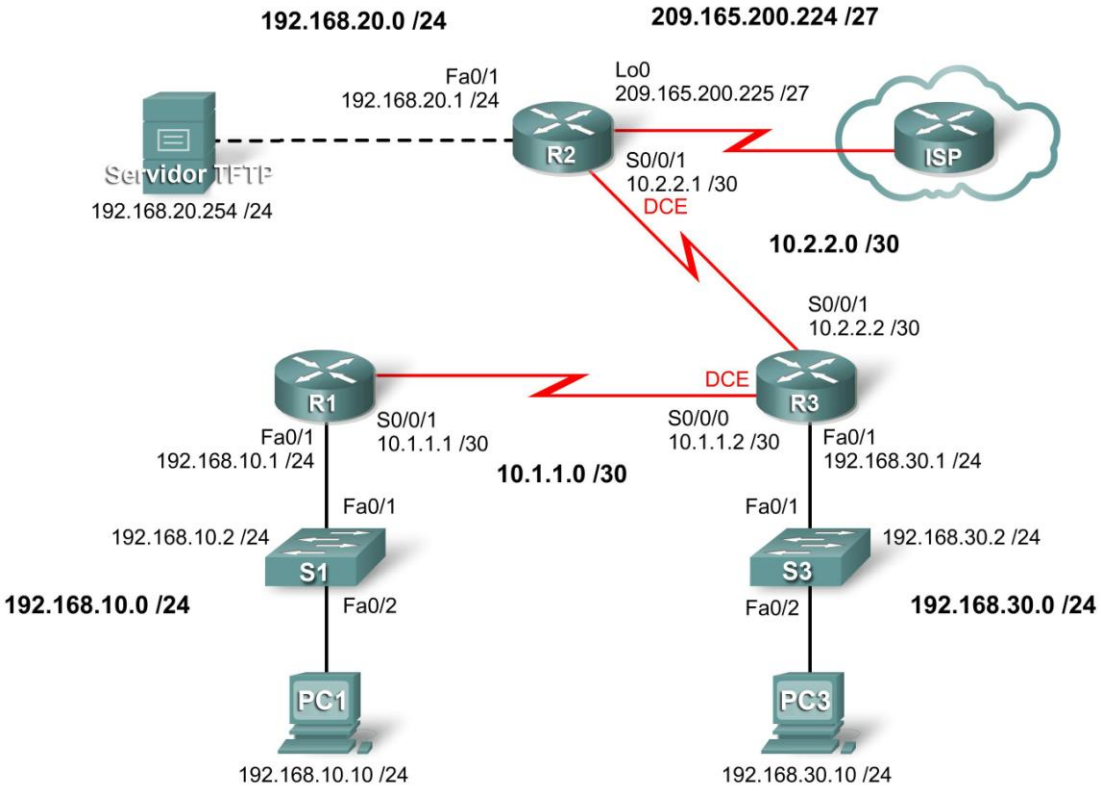


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/1	192.168.10.1	255.255.255.0	N/C
	S0/0/1	10.1.1.1	255.255.255.252	N/C
R2	Fa0/1	192.168.20.1	255.255.255.0	N/C
	S0/0/1	10.2.2.1	255.255.255.252	N/C
	Lo0	209.165.200.225	255.255.255.224	N/C
R3	Fa0/1	192.168.30.1	255.255.255.0	N/C
	S0/0/1	10.2.2.2	255.255.255.252	N/C
	S0/0/0	10.1.1.2	255.255.255.252	N/C
S1	VLAN10	192.168.10.2	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
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
- Realizar tareas de configuración básicas en un router
- Configurar y activar interfaces
- Configurar la seguridad básica de router
- Deshabilitar las interfases y los servicios de Cisco que no se utilicen
- Proteger las redes empresariales de ataques básicos internos y externos
- Comprender y administrar los archivos de configuración IOS de Cisco y el sistema de archivos Cisco
- Establecer y utilizar el SDM (Security Device Manager) de Cisco para configurar la seguridad básica de router

Escenario

En esta práctica de laboratorio se configurará la seguridad mediante la red que se muestra en el diagrama de topología. Si se necesita ayuda, se puede consultar la práctica de laboratorio de seguridad básica. Sin embargo, el usuario debe intentar hacer todo lo posible por su cuenta. Para esta actividad no se debe utilizar la protección por contraseña o por inicio de sesión en ninguna línea de consola porque se podría provocar una desconexión accidental. No obstante, aún así se debería establecer la seguridad de la línea de consola mediante otros métodos. Utilice **ciscoccna** para todas las contraseñas en esta práctica de laboratorio.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Paso 1: Configurar los routers.

Configure los routers R1, R2 y R3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router según el diagrama de topología.
- Deshabilite la búsqueda DNS.
- Configure un mensaje del día.
- Configure las direcciones IP en las interfaces de R1, R2 y R3.
- Active RIPv2 en todos los routers para todas las redes.
- Cree una interfaz loopback en R2 para simular la conexión a Internet.
- Cree las VLAN en los switches S1 y S3, y configure las interfaces respectivas para participar en las VLAN.
- Configure el router R3 para la conectividad segura de SDM.
- Instale SDM en el equipo PC3 o en R3 si aún no está instalado.

Paso 2: Configurar las interfaces Ethernet.

Configure las interfaces Ethernet de PC1, PC3 y el servidor TFTP con las direcciones IP y las gateways por defecto de la tabla de direccionamiento que se encuentra al comienzo de esta práctica de laboratorio.

Paso 3: Probar la configuración de los equipos PC al hacer ping a la gateway por defecto desde cada PC y el servidor TFTP.

Tarea 3: Establecer la seguridad el acceso a los routers

Paso 1: Configurar contraseñas seguras y autenticación AAA mediante una base de datos local.

Cree una contraseña segura para el acceso a los routers. Cree el nombre de usuario **ccna** para guardar de manera local en el router. Configure el router para que use la base de datos de autenticación local. Recuerde usar **ciscoccna** para todas las contraseñas de esta práctica de laboratorio.

```
service password-encryption
enable secret ciscoccna
username ccna password ciscoccna
aaa new-model
aaa authentication login local_auth local
```

Paso 2: Establecer la seguridad de las líneas de consola y las líneas VTY.

Configure la consola y las líneas vty para que los usuarios no puedan ingresar un nombre de usuario ni una contraseña incorrectos cinco veces en un periodo de 2 minutos. Bloquee todos los intentos adicionales de conexión durante 2 minutos.

```
line con 0
 exec-timeout 5 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
login block-for 300 attempt 2 within 120
security authentication failure rate 10 log
```

Paso 3: Verificar que se denieguen los intentos de conexión una vez que se llegue al límite de intentos fallidos.

R2:

```
R2#telnet 10.1.1.1
Trying 10.1.1.1 ... Open
Unauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law

User Access Verification

Username: cisco
Password:

% Authentication failed
```

```
User Access Verification

Username: cisco
Password:

% Authentication failed

[Connection to 10.1.1.1 closed by foreign host]

R2#telnet 10.1.1.1
Trying 10.1.1.1 ...
% Connection refused by remote host
```

R1:

```
*Sep 10 12:40:11.211: %SEC_LOGIN-5-QUIET_MODE_OFF: Quiet Mode is OFF,
because block period timed out at 12:40:11 UTC Mon Sep 10 2007
```

Tarea 4: Establecer la seguridad de acceso a la red

Paso 1: Establecer la seguridad del protocolo de enrutamiento RIP.

No envíe actualizaciones RIP a routers que no pertenezcan a la red (cualquier router que no se mencione en esta situación). Autentique las actualizaciones RIP y encríptelas.

R1:

```
key chain RIP_KEY
 key 1
  key-string cisco
!
int s0/0/0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
router rip
 version 2
 passive-interface default
 no passive-interface s0/0/0
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
```

R2:

```
key chain RIP_KEY
 key 1
  key-string cisco
!
int s0/0/1
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
```

```
router rip
 version 2
 passive-interface default
 no passive-interface s0/0/1
 network 10.0.0.0
 network 192.168.20.0
 no auto-summary
```

R3:

```
key chain RIP_KEY
 key 1
  key-string cisco
!
int s0/0/1
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
int s0/0/0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
router rip
 version 2
 passive-interface default
 no passive-interface s0/0/0
 no passive-interface s0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
```

Paso 2: Verificar que el enrutamiento RIP sigue funcionando.

R1:

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.30.0/24 [120/2] via 10.1.1.2, 00:00:16, Serial0/0/1
C    192.168.10.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.1.1.2, 00:00:13, Serial0/0/1
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R       10.2.2.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/1
C       10.1.1.0/24 is directly connected, Serial0/0/1
```

R2:

```
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.30.0/24 [120/2] via 10.2.2.2, 00:00:16, Serial0/0/1
C    192.168.20.0/24 is directly connected, FastEthernet0/1
R    192.168.10.0/24 [120/1] via 10.2.2.2, 00:00:13, Serial0/0/1
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
R       10.1.1.0/24 [120/1] via 10.1.0.2, 00:00:16, Serial0/0/1
C       10.2.2.0/24 is directly connected, Serial0/0/1
C     209.165.200.224 is directly connected, Loopback0
```

R3:

```
R3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS
level-2
       ia - IS-IS inter area, * - candidate default, U - per-user
static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.10.0/24 [120/2] via 10.1.1.1, 00:00:16, Serial0/0/1
C    192.168.30.0/24 is directly connected, FastEthernet0/1
R    192.168.20.0/24 [120/1] via 10.2.2.1, 00:00:13, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 1 masks
C       10.2.2.0/24 is directly connected, Serial0/0/0
C       10.1.1.0/24 is directly connected, Serial0/0/1
```

Tarea 5: Registrar la actividad con SNMP (Protocolo simple de administración de red)

Paso 1: Configurar el registro SNMP en el servidor syslog en 192.168.10.250 en todos los dispositivos.

```
logging 192.168.10.250
```

Paso 2: Registrar todos los mensajes con nivel de gravedad 4 en el servidor syslog.

```
logging trap warnings
```

Tarea 6: Deshabilitar los servicios de red de Cisco que no se utilizan

Paso 1: Deshabilitar las interfaces que no se utilicen en todos los dispositivos.

R1:

```
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
```

R2:

```
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
```

R3:

```
interface FastEthernet0/0
 no ip address
 shutdown
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
!
```

Paso 2: Deshabilitar los servicios globales que no se utilicen en R1.

```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no cdp run
```

Paso 3: Deshabilitar los servicios de interfaz que no se utilicen en R1.

```
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
interface Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
```

Paso 4: Utilizar la función AutoSecure para establecer la seguridad de R2.

Recuerde usar **ciscoccna** para todas las contraseñas de esta práctica de laboratorio.

```
R2#auto secure
                --- Configuración AutoSecure ---

*** La configuración AutoSecure aumenta la seguridad del
router, pero no hace que sea absolutamente resistente
a todos los ataques de seguridad ***
```

```
AutoSecure modifica la configuración del dispositivo.
Se muestran todos los cambios de configuración. Para obtener una
explicación
detallada sobre la manera en que los cambios de configuración aumentan
la seguridad
y cualquier posible efecto secundario, consulte Cisco.com para
obtener la documentación de AutoSecure.
Puede ingresar "?" en cualquier indicador para obtener ayuda.
Use ctrl-c para cancelar esta sesión en cualquier indicador.

Recopilación de información sobre el router para AutoSecure

¿Está este router conectado a Internet? [no]: sí
Especifique la cantidad de interfaces orientadas a Internet [1]: 1

Interface                  IP-Address      OK? Method Status
Protocol
FastEthernet0/0            unassigned     YES manual up          up
FastEthernet0/1            192.168.30.1   YES unset  down         down
Serial0/0/0                10.2.2.2        YES manual up          up
Serial0/0/1                10.2.2.2        YES manual up          up
Serial0/1/0                unassigned      YES manual down        down
Serial0/1/1                unassigned      YES unset  down        down
Especifique el nombre de la interfaz orientada a Internet: Serial0/1/0
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
Enter the new enable password: ciscoccna
Confirm the enable password: ciscoccna
Configuration of local user database
Enter the username: ccna
Enter the password: ciscoccna
Confirm the password: ciscoccna
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for
local authentication, exec-timeout, and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 300

Maximum Login failures with the device: 5
Maximum time period for crossing the failed login attempts: 120
```

```
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling CEF (This might impact the memory requirements for your
platform)
Enabling unicast rpf on all interfaces connected
to internet

Ésta es la configuración generada:

no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 070C285F4D061A061913
username ccna password 7 045802150C2E4F4D0718
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
line tty 1
 login authentication local_auth
 exec-timeout 15 0
line tty 192
 login authentication local_auth
 exec-timeout 15 0
```

```
login block-for 300 attempts 5 within 120
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
interface Serial0/0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
interface Serial0/1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
ip cef
access-list 101 permit udp any any eq bootpc
interface Serial0/0/0
 ip verify unicast source reachable-via rx allow-default 101
!
end

Apply this configuration to running-config? [yes]:yes
```

Tarea 7: Administrar IOS de Cisco y los archivos de configuración

Paso 1: Identificar dónde se ubica el archivo de configuración en ejecución en la memoria del router.

```
R1#dir system:
Directory of system:/

    3  dr-x           0                    <no date>  memory
    1  -rw-        1232                    <no date>  running-config
    2  dr-x           0                    <no date>  vfiles

No space information available
```

Paso 2: Transferir el archivo de configuración en ejecución de R1 a R2 mediante TFTP.

R1:

```
R1(config)#tftp-server system:running-config alias run
```

R2:

```
R2#copy tftp flash
Address or name of remote host []? 10.2.2.1
Source filename []? run
Destination filename [test]? run
Accessing tftp://10.2.2.1/run...
Loading test from 10.2.2.1 (via Serial0/0/0): !
[OK - 1192 bytes]

1192 bytes copied in 0.424 secs (2811 bytes/sec)
```

Paso 3: Interrumpir R1 y recuperarlo mediante ROMmon.

Copie y pegue los siguientes comandos en R1 y luego recupere R1 mediante ROMmon.

```
line vty 0 4
 exec-timeout 0 20
line console 0
 exec-timeout 0 20
end
copy run start
exit
```

```
rommon 1 > confreg 0x2142
rommon 2 > reset
```

```
R1#copy running-config startup-config
R1#configure terminal
R1(config)#config-register 0x2102
R1(config)#end
R2#reload
```

Paso 4: Restablecer la configuración guardada a R1 desde R2 mediante TFTP.

Debido a que R1 y R2 no están directamente conectados, se debe configurar nuevamente RIP en R1. Sin embargo, R1 no recibirá las actualizaciones a menos que se configure la autenticación RIP.

R2:

```
R2(config)#tftp-server flash:run alias run
```

R1:

```
key chain RIP_KEY
 key 1
  key-string cisco
!
int s0/0/1
 ip address 10.1.1.2 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no shut
!
router rip
 version 2
 passive-interface default
 no passive-interface s0/0/1
 network 10.0.0.0
 no auto-summary
```

```
R1#copy tftp nvram
Address or name of remote host []? 10.2.2.1
Source filename []? run
Destination filename []? nvram:startup-config
Accessing tftp://10.1.1.2/run...
Loading test from 10.1.1.2 (via Serial0/0/0): !
[OK - 1192 bytes]

1192 bytes copied in 0.452 secs (2637 bytes/sec)
```

Paso 5: Borrar la configuración guardada de R2.

```
R2#delete flash:run
```

Tarea 8: Usar SDM para establecer la seguridad de R2

Paso 1: Conectarse a R2 mediante PC1.

Paso 2: Navegar hacia la función Security Audit.

Paso 3: Realizar una auditoría de seguridad.

Paso 4: Elegir la configuración que se debe aplicar al router.

Paso 5: Aplicar la configuración al router.

Tarea 9: Documentar las configuraciones del router

En cada router, ejecute el comando **show run** y capture las configuraciones.

```
----------------------------------------
                R1
----------------------------------------
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
no ip finger
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip bootp server
!
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password ciscoccna
!
!
```

```
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 no fair-queue
 clockrate 125000
!
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no fair-queue
 clockrate 125000
!
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
ip classless
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
```

```
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
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
```

```
----------------------------------------
                R2
----------------------------------------
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
hostname R2
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
```

```
no ip gratuitous-arps
no ip finger
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip bootp server
!
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password ciscoccna
!
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arpshutdown
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 no fair-queue
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
 no shutdown
```

```
!
interface Serial0/1/0
 ip address 209.165.200.224 255.255.255.224
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clockrate 2000000
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 network 209.165.200.224
 no auto-summary
!
ip classless
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
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 pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
hostname R3
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
no ip finger
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip bootp server
!
!
key chain RIP_KEY
 key 1
  key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
```

```
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 clockrate 125000
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 login authentication
 transport output telnet
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
```

Tarea 10: 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.

Práctica de laboratorio 4.6.3: Resolución de problemas de configuración de seguridad (Versión para el instructor)

Diagrama de topología

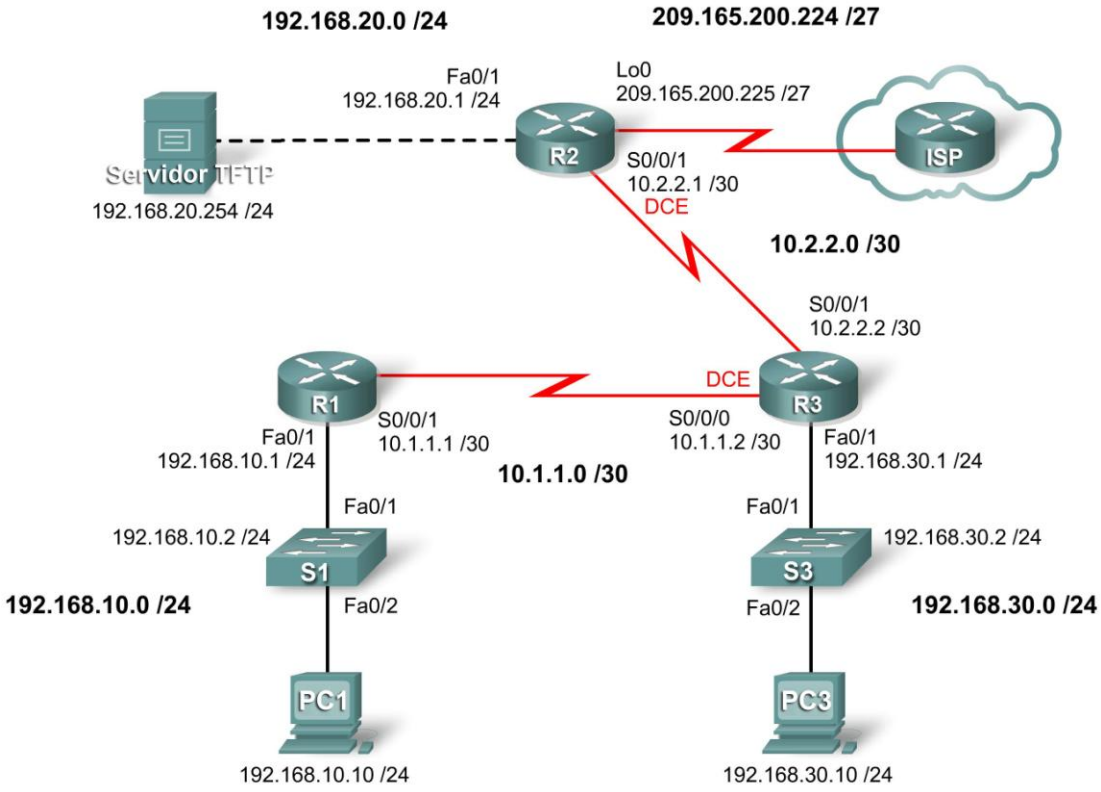


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/1	192.168.10.1	255.255.255.0	N/C
	S0/0/1	10.1.1.1	255.255.255.252	N/C
R2	Fa0/1	192.168.20.1	255.255.255.0	N/C
	S0/0/1	10.2.2.1	255.255.255.252	N/C
	Lo0	209.165.200.225	255.255.255.224	N/C
R3	Fa0/1	192.168.30.1	255.255.255.0	N/C
	S0/0/1	10.2.2.2	255.255.255.252	N/C
	S0/0/0	10.1.1.2	255.255.255.252	N/C
S1	VLAN10	192.168.10.2	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
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
- Eliminar la configuración de inicio y restablecer todos los routers al estado por defecto
- Cargar los routers con los guiones suministrados
- Detectar y corregir todos los errores de red
- Documentar la red corregida

Escenario

Una empresa acaba de contratar un nuevo ingeniero en redes que ha generado algunos problemas de seguridad en la red debido a errores de configuración y descuidos. El jefe le solicitó al usuario que corrija los errores que ha cometido el nuevo ingeniero al configurar los routers. Mientras se corrigen los problemas, debe garantizarse la seguridad de todos los dispositivos así como el acceso a ellos para los administradores y todas las redes se deben poder alcanzar. Se debe poder acceder a todos los routers con SDM desde PC1. Verifique la seguridad de un dispositivo mediante herramientas tales como Telnet y ping. El uso no autorizado de estas herramientas debe bloquearse, pero se debe garantizar el uso autorizado. 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.

Tarea 1: Cargar los routers con los guiones suministrados

Cargue las siguientes configuraciones en los dispositivos de la topología. Las líneas en color rojo se incluyen en la práctica de laboratorio del instructor pero en la del estudiante. Tampoco se cargan en el router al comienzo de esta práctica. Las líneas que se deben eliminar se resaltan con color amarillo y las que se deben agregar, con rojo. Utilice las anotaciones para ayudar a los estudiantes a identificar correctamente las respuestas.

R1:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login LOCAL_AUTH local
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
```

Los nombres que distinguen entre mayúsculas y minúsculas pueden crear errores comunes de configuración. Aquí la política debería ser usar minúsculas.

```
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password ciscoccna
!
 interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcasts
 duplex auto
 speed auto
 no shutdown
!
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
 shutdown
 no fair-queue
 clockrate 125000
!
```

Todas las interfaces que no se usan deberían estar desactivadas.

El comando **no ip directed-broadcast** está omitido en todas las interfaces. Es un error común olvidarse un comando cuando se ingresan muchas veces muchos comandos similares.

```
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
 shutdown
!
interface Serial0/1/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
 shutdown
 clockrate 2000000
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
ip classless
!
no ip http server
ip http server
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
```

Por error serial 0/0/0 se configuró como activo cuando la actualización RIP tiene que enviarse desde S0/0/1.

Por razones de seguridad, este comando normalmente está desactivado (automáticamente si se usa AutoSecure). Sin embargo, este escenario requiere SDM, y SDM requiere que haya un servidor HTTP activado.

A pesar de que el registro está habilitado y el destino establecido, hay que configurar el tipo de registros que se deben enviar al servidor.

```
 exec-timeout 5 0
 logging synchronous
 login authentication local_auth
!
end
```

El comando **show run** revela que esto no está activado, porque todas las contraseñas excepto la contraseña secreta de enable estarán en texto sin encriptar.

R2:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R2
!
security authentication failure rate 10 log
security passwords min-length 6
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip source-route
no ip gratuitous-arps
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string cisco
!
username ccna password ciscoccna
!
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 duplex auto
 speed auto
!
```

Es habitual olvidarse de crear la keychain que debe utilizarse en la autenticación RIP, incluso después de configurar las interfaces.

```
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 duplex auto
 speed auto
 no shutdown
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 no fair-queue
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
 no shutdown
!
interface Serial0/1/0
 ip address 209.165.200.224 255.255.255.224
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 shutdown
 clockrate 2000000
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 no auto-summary
```

Las interfaces RIP deben ponerse en passive (pasiva), a menos que estén configuradas de otro modo.

```
!
ip classless
!
no ip http server
ip http server
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
line aux 0
 exec-timeout 15 0
 logging synchronous
 login authentication local_auth
 transport output telnet
line vty 0 4
 exec-timeout 0 0
 exec-timeout 5 0
 logging synchronous
 login authentication local_auth
 transport input telnet
!
end
```

Por razones de seguridad este comando normalmente está desactivado (está desactivado automáticamente si se usa **AutoSecure**). Sin embargo, este escenario requiere SDM y SDM requiere que el servidor HTTP esté activado.

CDP debería estar desactivado a menos que se lo necesite.

El límite de tiempo se cambió a infinito, lo que permite conexiones indefinidas.

R3:

```
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
```

```
no ip source-route
no ip gratuitous-arps
ip cef
!
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string Cisco
  key-string cisco
username ccna password ciscoccna
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip proxy-arp
 no ip directed-broadcast
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 no shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 125000
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 no ip directed-broadcast
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
```

Otro error de diferencia entre mayúsculas y minúsculas. Las cadenas de claves reconocen mayúsculas y minúsculas, y por consiguiente son propensas a que se las escriba mal.

La autenticación local está configurada, pero se omitieron una contraseña y un nombre de usuario locales, de modo que la autenticación no es posible.

La autenticación RIP se configuró en R1 y R2, pero no en R3, lo que impide que se propaguen las actualizaciones RIP.

Configuraciones faltantes para la autenticación RIP.

```
router rip
 version 2
 passive-interface default
 passive-interface Serial0/0/0
 passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
no ip http server
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
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
```

Tarea 2: Buscar y corregir todos los errores de red

Detecte, documente y corrija cada uno de los errores mediante métodos estándar de resolución de problemas.

Nota: Cuando se realice la resolución problemas de una red de producción que no funcione, muchos errores muy pequeños pueden impedir que todo funcione correctamente. El primer punto que se debe controlar es la ortografía y las mayúsculas o minúsculas de todas las contraseñas, nombres de keychain y claves y nombres de listas de autenticación. Por lo general, lo que provoca la falla total es el uso de una mayúscula en lugar de una minúscula o viceversa, o un error de ortografía. Se recomienda comenzar por lo más básico y continuar con lo más difícil. Primero pregunte si coinciden todos los nombres y las claves. Luego, si la configuración usa una lista, una keychain u otro elemento, verifique si el elemento mencionado realmente existe y si es el mismo en todos los dispositivos. Realizar una configuración una vez en uno de los dispositivos y luego copiarla y pegarla en el otro es la mejor manera de asegurarse de que la configuración sea exactamente la misma. Luego, en el momento de deshabilitar o restringir servicios, debe preguntarse para qué se utilizan tales servicios y si son necesarios. También debe averiguar qué información debería enviar el router. Quién debería recibir esa información y quién no. Por último, debe averiguar qué permiten hacer los servicios y si se desea que los usuarios puedan hacerlo. Por lo general, si se considera que existe alguna manera de abusar de un servicio, entonces se deben tomar medidas para evitar que esto ocurra.

Tarea 3: Documentar la red corregida

```
----------------------------------------
            R1
----------------------------------------
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
no ip finger
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password ciscoccna
!
interface FastEthernet0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 duplex auto
```

```
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.10.1 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 no fair-queue
 clockrate 125000
!
interface Serial0/0/1
 ip address 10.1.1.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no fair-queue
 clockrate 125000
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.10.0
 no auto-summary
!
ip classless
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
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

----------------------------------------
                R2
----------------------------------------
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
hostname R2
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 10 log
security passwords min-length 6
enable secret ciscoccna
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
no ip source-route
no ip gratuitous-arps
no ip finger
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string cisco
```

```
username ccna password ciscoccna
!
interface FastEthernet0/0
 no ip address
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arpshutdown
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 duplex auto
 speed auto
 no shutdown
!
!
interface Serial0/0/0
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 no fair-queue
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
 no shutdown
!
interface Serial0/1/0
 ip address 209.165.200.224 255.255.255.224
 no ip redirects
 no ip unreachables
 no ip proxy-arp
!
interface Serial0/1/1
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 shutdown
 clockrate 2000000
!
```

```
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 no auto-summary
!
ip classless
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
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 pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service finger
no service udp-small-server
no service tcp-small-server
!
hostname R3
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 5 log
security passwords min-length 6
enable secret ciscoccna
```

```
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no ip source-route
no ip gratuitous-arps
no ip finger
ip cef
!
no ip dhcp use vrf connected
!
no ip bootp server
!
key chain RIP_KEY
 key 1
  key-string 7 01100F175804
username ccna password 7 094F471A1A0A1411050D
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 clockrate 125000
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
```

```
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.30.0
 no auto-summary
!
ip classless
!
no ip http server
!
login block-for 300 attempt 2 within 120
!
logging trap debugging
logging 192.168.10.150
no cdp run
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
 transport output telnet
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
```

Tarea 4: 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.

Práctica de laboratorio 5.5.1: Listas de control de acceso básicas (Versión para el instructor)

Diagrama de topología

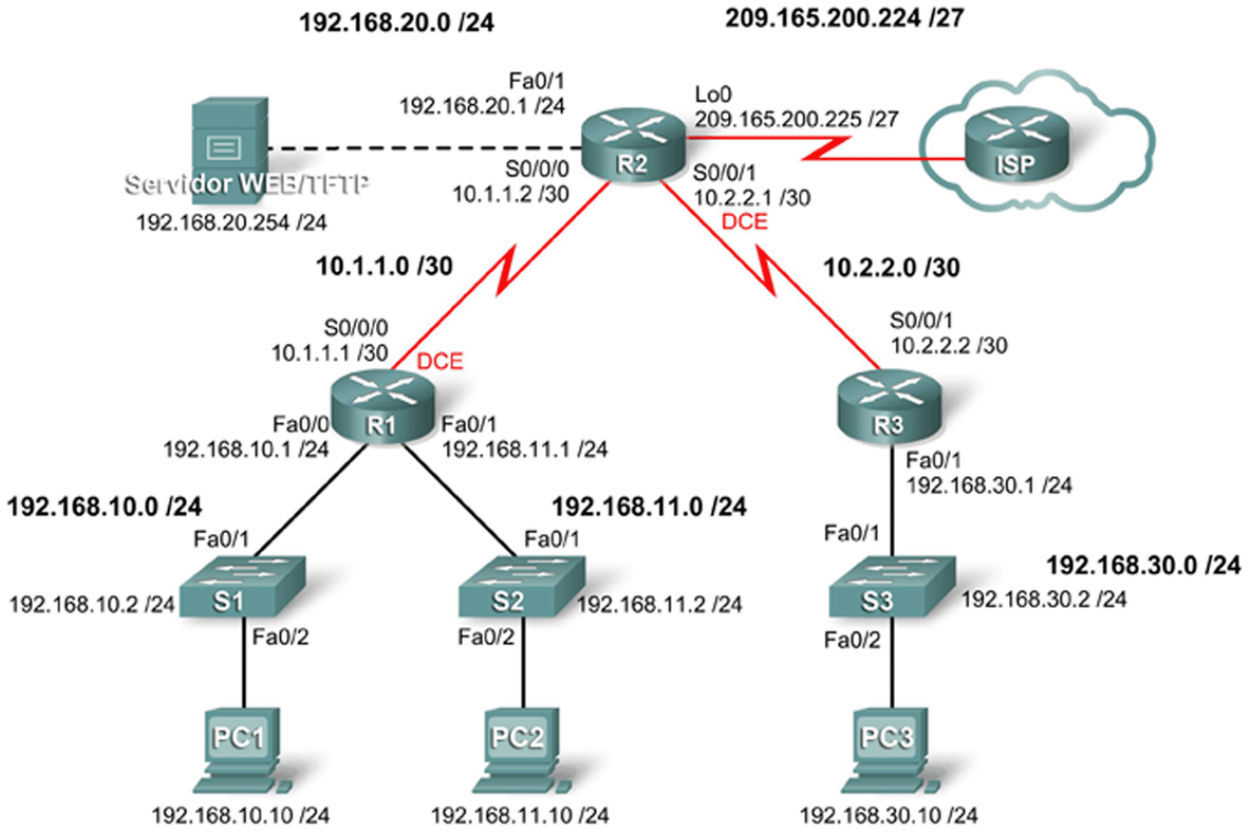


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	Fa0/0	192.168.10.1	255.255.255.0	
	Fa0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
R2	Fa0/1	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	Fa0/1	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	

S1	**Vlan1**	192.168.10.2	255.255.255.0	192.168.10.1
S2	**Vlan1**	192.168.11.2	255.255.255.0	192.168.11.1
S3	**Vlan1**	192.168.30.2	255.255.255.0	192.168.30.1
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
Web Server	**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:

- Diseñar ACL nombradas estándar y nombradas ampliadas
- Aplicar ACL nombradas estándar y nombradas ampliadas
- Probar ACL nombradas estándar y nombradas ampliadas
- Realizar la resolución de problemas relacionados con ACL nombradas estándar y nombradas ampliadas

Escenario

En esta práctica de laboratorio, se aprenderá a configurar la seguridad básica de red mediante listas de control de acceso. Se aplicarán ACL estándar y ampliadas.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en el diagrama de topología.

Nota: Esta práctica de laboratorio se desarrolló y probó mediante routers 1841. Si se utilizan routers serie 1700, 2500 ó 2600, los resultados y las descripciones del router pueden ser diferentes. En routers más antiguos o en versiones de IOS anteriores a la 12.4, es posible que algunos comandos sean diferentes o que no existan.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Configure los routers R1, R2, R3 y los switches S1, S2 y S3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router de modo que coincida con el diagrama de topología.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de **class** en el Modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña de cisco para las conexiones de consola.
- Configure una contraseña para las conexiones de vty.
- Configure máscaras y direcciones IP en todos los dispositivos.

- Habilite OSPF área 0 en todos los routers para todas las redes.
- Configure una interfaz loopback en R2 para simular el ISP.
- Configure direcciones IP para la interfaz VLAN 1 en cada switch.
- Configure cada switch con la gateway por defecto apropiada.
- Verifique que la conectividad IP sea total mediante el comando **ping**.

R1

```
hostname R1
!
no ip domain-lookup
enable secret class
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
interface fa0/0
 ip address 192.168.10.1 255.255.255.0
 no shut
!
interface fa0/1
 ip address 192.168.11.1 255.255.255.0
 no shut
!
interface s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 125000
 no shut
!
router ospf 1
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.3 area 0
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
```

R2

```
hostname R2
!
no ip domain-lookup
enable secret class
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
interface fa0/1
 ip address 192.168.20.1 255.255.255.0
 no shut
!
```

```
interface s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
!
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 clock rate 64000
 no shut
!
interface Lo0
 ip address 209.165.200.225 255.255.255.224
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.255.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
```

R3

```
hostname R3
!
no ip domain-lookup
enable secret class
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
interface fa0/1
 ip add 192.168.30.1 255.255.255.0
 no shut
!
interface s0/0/1
 ip add 10.2.2.2 255.255.255.252
 no shut
!
router ospf 1
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.30.1 0.0.0.255 area 0
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
password cisco
login
```

S1

```
interface vlan 1
 ip address 192.168.10.2 255.255.255.0
 no shut
!
ip default-gateway 192.168.10.1
```

S2

```
interface vlan 1
 ip address 192.168.11.2 255.255.255.0
 no shut
!
ip default-gateway 192.168.11.1
```

S3

```
interface vlan 1
 ip add 192.168.30.2 255.255.255.0
 no shut
!
ip default-gateway 192.168.30.1
```

Tarea 3: Configurar una ACL estándar

Las ACL estándar pueden filtrar tráfico sólo según la dirección IP de origen. Una práctica recomendada típica es configurar una ACL estándar tan cerca del destino como sea posible. En esta tarea, se configurará una ACL estándar. La ACL está diseñada para impedir que el tráfico desde la red 192.168.11.0/24, ubicada en un laboratorio de estudiantes, acceda a cualquiera de las redes locales de R3.

Esta ACL se aplicará en dirección entrante en la interfaz serial de R3. Se debe recordar que cada ACL tiene un comando “deny all” implícito que hace que se bloquee todo el tráfico que no coincida con una sentencia de la ACL. Por esta razón, se debe agregar la sentencia **permit any** al final de la ACL.

Antes de configurar y aplicar esta ACL, asegúrese de probar la conectividad desde PC1 (o la interfaz Fa0/1 de R1) a PC3 (o la interfaz Fa0/1del R3). Las pruebas de conectividad deberían realizarse correctamente antes de aplicar la ACL.

Paso 1: Crear la ACL en el router R3.

En el modo de configuración global, cree una ACL nombrada estándar denominada **STND-1**.

```
R3(config)#ip access-list standard STND-1
```

En el modo de configuración de ACL estándar, agregue una sentencia que deniegue cualquier paquete con una dirección de origen de 192.168.11.0 /24 e imprima un mensaje a la consola por cada paquete coincidente.

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255 log
```

Permita todo el tráfico restante.

```
R3(config-std-nacl)#permit any
```

Paso 2: Aplicar la ACL.

Aplique la ACL **STND-1** como filtro en los paquetes que ingresan a R3 a través de la interfaz serial 0/0/1.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 in
R3(config-if)#end
R3#copy run start
```

Paso 3: Probar la ACL.

Antes de probar la ACL, asegúrese de que la consola de R3 esté visible. De este modo, se podrán ver los mensajes de registro de la lista de acceso cuando se deniegue el acceso al paquete.

Pruebe la ACL haciendo ping de PC2 a PC3. Debido a que la ACL está diseñada para bloquear el tráfico con direcciones de origen de la red 192.168.11.0 /24, PC2 (192.168.11.10) no debería poder hacer ping a PC3.

También se puede utilizar un ping ampliado desde la interfaz Fa0/1 del R1 a la interfaz Fa0/1 del R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.11.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.11.1
U.U.U
Success rate is 0 percent (0/5)
```

Se debería poder ver el siguiente mensaje en la consola de R3:

```
*Sep  4 03:22:58.935: %SEC-6-IPACCESSLOGNP: list STND-1 denied 0
0.0.0.0 -> 192.168.11.1, 1 packet
```

En el modo EXEC privilegiado de R3, ejecute el comando **show access-lists**. El resultado debe ser similar al siguiente. Cada línea de una ACL tiene un contador asociado que muestra cuántos paquetes coinciden con la regla.

```
Standard IP access list STND-1
    10 deny   192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)
    20 permit any (25 matches)
```

El objetivo de esta ACL era bloquear los hosts de la red 192.168.11.0/24. Cualquier otro host, como por ejemplo, los de la red 192.168.10.0/24, debería tener acceso a las redes de R3. Realice otra prueba de PC1 a PC3 para asegurarse de que este tráfico no se bloquee.

También se puede utilizar un ping ampliado desde la interfaz Fa0/0 del R1 a la interfaz Fa0/1 del R3.

```
R1#ping ip
Target IP address: 192.168.30.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.10.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/43/44 ms
```

Tarea 4: Configurar una ACL ampliada

Cuando se requiere un mayor nivel de detalle, se debe usar una ACL ampliada. Las ACL ampliadas pueden filtrar el tráfico teniendo en cuenta otros aspectos, además de la dirección de origen. Las ACL ampliadas pueden filtrar según el protocolo, las direcciones IP de origen y destino y los números de puerto de origen y destino.

Una política adicional para esta red establece que los dispositivos de la LAN 192.168.10.0/24 sólo pueden alcanzar las redes internas. Los equipos de esta LAN no pueden acceder a Internet. Por lo tanto, estos usuarios deben bloquearse para que no alcancen la dirección IP 209.165.200.225. Debido a que este requisito debe cumplirse tanto en el origen como en el destino, se necesita una ACL ampliada.

En esta tarea, se configurará una ACL ampliada en R1 que impide que el tráfico que se origina en cualquier dispositivo de la red 192.168.10.0/24 acceda al host 209.165.200.255 (el ISP simulado). Esta ACL se aplicará en dirección saliente en la interfaz Serial 0/0/0 de R1. Una práctica recomendada típica para la aplicación de ACL ampliada es ubicarlas tan cerca del origen como sea posible.

Antes de comenzar, verifique que se pueda hacer ping a 209.165.200.225 desde PC1.

Paso 1: Configurar una ACL ampliada y nombrada.

En el modo de configuración global, cree una ACL nombrada y ampliada, denominada **EXTEND-1**.

```
R1(config)#ip access-list extended EXTEND-1
```

Observe que el indicador del router cambia para señalar que ahora se encuentra en el modo de configuración de ACL ampliada. Desde este indicador, agregue las sentencias necesarias para bloquear el tráfico desde la red 192.168.10.0 /24 al host. Utilice la palabra clave **host** cuando defina el destino.

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

Recuerde que el comando “deny all” implícito bloquea cualquier otro tráfico sin la sentencia adicional **permit**. Agregue la sentencia **permit** para asegurarse de que no se bloquee el tráfico restante.

```
R1(config-ext-nacl)#permit ip any any
```

Paso 2: Aplicar la ACL.

Con las ACL estándar, lo más conveniente es ubicar a la ACL lo más cerca posible del destino. Las ACL ampliadas generalmente se ubican cerca del origen. La ACL **EXTEND-1** se ubicará en la interfaz serial y filtrará el tráfico saliente.

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip access-group EXTEND-1 out log
R1(config-if)#end
R1#copy run start
```

Paso 3: Probar la ACL.

Desde PC1, haga ping a la interfaz loopback de R2. Estos ping deberían fallar porque todo el tráfico proveniente de la red 192.168.10.0/24 se filtra cuando el destino es 209.165.200.225. Si el destino es cualquier otra dirección, los pings deberían realizarse correctamente. Confirme esto haciendo ping al R3 desde el dispositivo de red 192.168.10.0/24.

Nota: La función de ping ampliado de R1 no puede utilizarse para probar esta ACL, ya que el tráfico se originará dentro de R1 y no volverá probarse con la ACL aplicada a la interfaz serial de R1.

Es posible verificarlo nuevamente al ejecutar **show ip access-list** en R1 después de hacer ping.

```
R1#show ip access-list
Extended IP access list EXTEND-1
    10 deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 matches)
    20 permit ip any any
```

Tarea 5: Controlar el acceso a las líneas VTY con una ACL estándar

Es conveniente restringir el acceso a las líneas VTY del router para la administración remota. Puede aplicarse una ACL a las líneas VTY, lo que permite restringir el acceso a hosts o redes específicos. En esta tarea, se configurará una ACL estándar para permitir que los hosts de dos redes accedan a las líneas VTY. Se le negará el acceso a todos los demás hosts.

Verifique que pueda establecer una conexión telnet a R2 desde R1 y R3.

Paso 1: Configurar la ACL.

Configure una ACL estándar nombrada en R2 que permita el tráfico desde 10.2.2.0/30 y 192.168.30.0/24. Debe denegarse todo el tráfico restante. Denomine la ACL **TASK-5**.

```
R2(config)#ip access-list standard TASK-5
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```

Paso 2: Aplicar la ACL.

Entre al modo de configuración de línea para las líneas VTY de 0 a 4.

```
R2(config)#line vty 0 4
```

Utilice el comando **access-class** para aplicar la ACL a las líneas vty en dirección entrante. Observe que esto difiere del comando que se utiliza para aplicar las ACL a otras interfaces.

```
R2(config-line)#access-class TASK-5 in
R2(config-line)#end
R2#copy run start
```

Paso 3: Probar la ACL.

Establezca una conexión telnet a R2 desde R1. Observe que R1 no tiene direcciones IP en su rango de direcciones que aparece en las sentencias de permiso de la ACL TASK-5. Los intentos de conexión deberían fallar.

```
R1# telnet 10.1.1.2
Trying 10.1.1.2 …
% Connection refused by remote host
```

Desde R3, establezca una conexión telnet a R2. Aparece una petición de entrada para la contraseña de la línea VTY.

```
R3# telnet 10.1.1.2
Trying 10.1.1.2 … Open
CUnauthorized access strictly prohibited, violators will be prosecuted
to the full extent of the law.

User Access Verification

Password:
```

¿Por qué los intentos de conexión desde otras redes fallan aunque no se enumeren específicamente en la ACL?

_____

_____

Todas las ACL incluyen un comando deny all implícito como sentencia final. Se niega el acceso a todo el tráfico que no esté explícitamente permitido.

Tarea 6: Resolución de problemas en las ACL

Cuando se configura incorrectamente una ACL o se la aplica a la interfaz incorrecta o en la dirección incorrecta, el tráfico de red puede verse afectado de manera no deseada.

Paso 1: Eliminar la ACL STND-1 de S0/0/1 de R3.

En una tarea anterior, se creó y aplicó una ACL nombrada y estándar en R3. Utilice el comando **show running-config** para visualizar la ACL y su ubicación. Se debería ver que una ACL llamada **STND-1** se configuró y aplicó en dirección entrante en Serial 0/0/1. Recuerde que esta ACL se diseñó para impedir que todo el tráfico de red con una dirección de origen de la red 192.168.11.0/24 acceda a la LAN del R3.

Para eliminar la ACL, entre al modo de configuración de la interfaz para Serial 0/0/1 de R3. Utilice el comando **no ip access-group STND-1** para eliminar la ACL de la interfaz.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 in
```

Use el comando **show running-config** para confirmar que la ACL se haya eliminado de la Serial 0/0/1.

Paso 2: Aplicar la ACL STND-1 en S0/0/1 saliente.

Para probar la importancia de la dirección de filtrado de la ACL, aplique nuevamente la ACL **STND-1** a la interfaz Serial 0/0/1. Esta vez, la ACL filtrará el tráfico saliente en lugar del tráfico entrante. Recuerde utilizar la palabra clave **out** cuando aplique la ACL.

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group STND-1 out
```

Paso 3: Probar la ACL.

Pruebe la ACL haciendo ping de PC2 a PC3. Como alternativa, utilice un ping ampliado desde R1. Observe que esta vez los pings se realizan correctamente y que los contadores de la ACL no aumentan. Confirme esto mediante el comando **show ip access-list** en R3.

Paso 4: Restablecer la configuración original de la ACL.

Elimine la ACL de la dirección saliente y aplíquela nuevamente a la dirección entrante.

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group STND-1 out
R3(config-if)#ip access-group STND-1 in
```

Paso 5: Aplicar TASK-5 a la interfaz serial 0/0/0 entrante de R2.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group TASK-5 in
```

Paso 6: Probar la ACL.

Intente comunicarse con cualquier dispositivo conectado a R2 o R3 desde R1 o sus redes conectadas. Observe que toda la comunicación está bloqueada. Sin embargo, los contadores de la ACL no aumentan. Esto se debe al comando “deny all” implícito al final de todas las ACL. Esta sentencia deny impide todo el tráfico entrante a la serial 0/0/0 desde cualquier origen que no sea R3. Básicamente, esto hará que las rutas de R1 se eliminen de la tabla de enrutamiento.

Se deberían ver mensajes similares a los que aparecen a continuación impresos en las consolas de R1 y R2 (debe transcurrir un tiempo para que la relación vecina OSPF se desactive, por lo que deberá ser paciente):

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

Una vez recibido este mensaje, ejecute el comando **show ip route** tanto en R1 como en R2 para determinar qué rutas se eliminaron de la tabla de enrutamiento.

Elimine la ACL TASK-5 de la interfaz y guarde las configuraciones.

```
R2(config)#interface serial 0/0/0
R2(config-if)#no ip access-group TASK-5 in
R2(config)#exit
R2#copy run start
```

Tarea 7: Documentar las configuraciones del router

Configuraciones

Router 1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 no shutdown
```

```
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip access-group EXTEND-1 out
 clockrate 64000
 no shutdown
!
router ospf 1
 network 10.1.1.0 0.0.0.3 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 access-list extended EXTEND-1
 deny   ip 192.168.10.0 0.0.0.255 host 209.165.200.225
 permit ip any any
!
banner motd ^CUnauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

Router 2

```
hostname R2
!
enable secret class
!
no ip domain lookup
!
interface Loopback0
 ip address 209.165.200.225 255.255.255.224
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 clockrate 125000
 no shutdown
```

```
!
router ospf 1
 no auto-cost
 network 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 209.165.200.224 0.0.0.31 area 0
!
ip access-list standard TASK-5
 permit 10.2.2.0 0.0.0.3
 permit 192.168.30.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class TASK-5 in
 password cisco
 login
!
```

Router 3

```
hostname R3
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group STND-1 out
 no shutdown
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip access-list standard STND-1
 deny   192.168.11.0 0.0.0.255 log
 permit any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
```

```
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
end
```

Tarea 8: 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.

Práctica de laboratorio 5.5.2: Reto de listas de control de acceso (Versión para el instructor)

Diagrama de topología

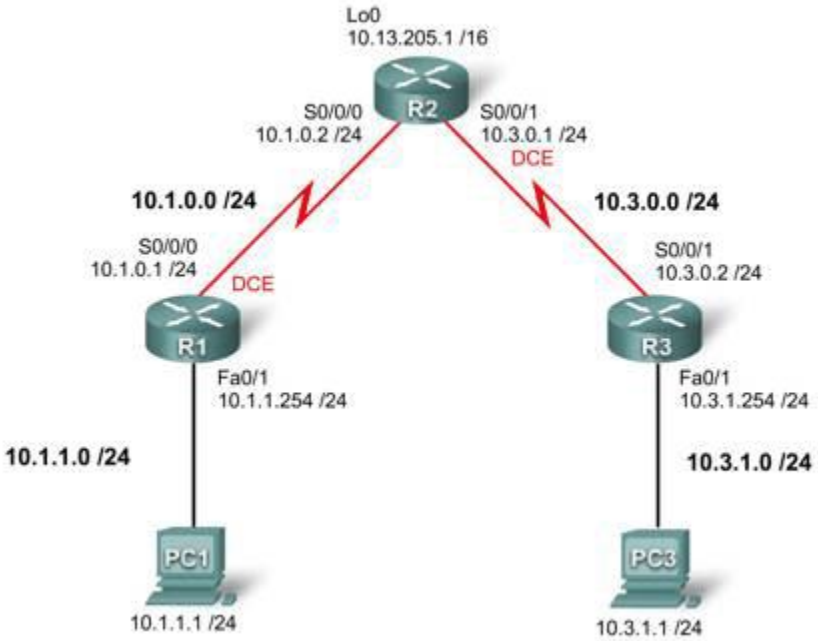


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**S0/0/0**	10.1.0.1	255.255.255.0	
	Fa0/1	10.1.1.254	255.255.255.0	
R2	**S0/0/0**	10.1.0.2	255.255.255.0	
	S0/0/1	10.3.0.1	255.255.255.0	
	Lo 0	10.13.205.1	255.255.0.0	
R3	**S0/0/1**	10.3.0.2	255.255.255.0	
	Fa0/1	10.3.1.254	255.255.255.0	
PC 1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Objetivos de aprendizaje

Para completar esta práctica de laboratorio:

- Diseñar ACL nombradas estándar y nombradas ampliadas
- Aplicar ACL nombradas estándar y nombradas ampliadas
- Probar ACL nombradas estándar y nombradas ampliadas
- Realizar la resolución de problemas relacionados con ACL nombradas estándar y nombradas ampliadas

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en el diagrama de topología.

Nota: Si utiliza routers 1700, 2500 ó 2600, los resultados del router y las descripciones de la interfaz pueden tener un aspecto diferente.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Configure los routers R1, R2 y R3 de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del router.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de Modo EXEC.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para las conexiones de vty.
- Configure direcciones IP en todos los dispositivos.
- Cree una interfaz loopback en R2.
- Habilite OSPF área 0 en todos los routers para todas las redes.
- Verifique que la conectividad IP sea total mediante el comando **ping**.

R1

```
hostname R1
no ip domain-lookup
 enable secret class
!
interface FastEthernet0/1
 ip address 10.1.1.254 255.255.255.0
 no shutdown
!
interface serial 0/0/0
 ip address 10.1.0.1 255.255.255.0
 clock rate 125000
```

```
 no shutdown
   !
router ospf 1
 network 10.1.0.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 logging synchronous
 password cisco
 login
!
line vty 0 4
 password cisco
 login
!
```

R2

```
hostname R2
enable secret class
no ip domain lookup
!
interface Loopback0
 ip address 10.13.205.1 255.255.0.0
!
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.3.0.1 255.255.255.0
 clockrate 125000
 no shutdown
!
router ospf 1
 network 10.1.0.0 0.0.0.255 area 0
 network 10.3.0.0 0.0.0.255 area 0
 network 10.13.0.0 0.0.255.255 area 0
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

R3

```
hostname R3
!
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.3.1.254 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.3.0.2 255.255.255.0
 no shutdown
!
router ospf 1
 network 10.3.0.0 0.0.0.255 area 0
 network 10.3.1.0 0.0.0.255 area 0
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

Tarea 3: Configurar las ACL estándar

Configure las ACL nombradas y estándar en las líneas VTY de R1 y R3 para permitir que los hosts conectados directamente a sus subredes FastEthernet tengan acceso Telnet. Deniegue el acceso a cualquier otro intento de conexión. Documente los procedimientos de prueba.

_____

_____

_____

_____

R1

```
ip access-list standard VTY_LOCAL
 permit 10.1.1.0 0.0.0.255
 deny any log
!
line vty 0 4
 access-class VTY_LOCAL in
!
```

R3

```
ip access-list standard VTY_LOCAL
 permit 10.3.1.0 0.0.0.255
 deny any log
!
line vty 0 4
 access-class VTY_LOCAL in
```

Intente establecer una conexión Telnet a R3 desde PC1, R1 y R2. Estas pruebas deberían fallar.

Intente establecer una conexión Telnet a R1 desde PC3, R2 y R3. Estas pruebas deberían fallar.

Intente establecer una conexión Telnet a R1 desde PC1. Esta prueba debería realizarse correctamente.

Intente establecer una conexión Telnet a R3 desde PC·. Esta prueba debería realizarse correctamente.

Tarea 4: Configurar las ACL ampliadas

Mediante ACL ampliadas en R2, complete los siguientes requisitos:

- Las LAN conectadas a R1 y R3 se utilizan para prácticas de laboratorio informáticas para estudiantes. El administrador de red observó que los estudiantes de estas prácticas de laboratorio juegan a través de la WAN con estudiantes remotos. Asegúrese de que la ACL impida que la LAN conectada a R1 alcance a la LAN de R3 y que la LAN de R3 no pueda alcanzar la LAN de R1. Debe ser específico en las sentencias, de modo que cualquier LAN nueva que se haya agregado a R1 o R3 no se verá afectada.
- Permita el ingreso del tráfico OSPF.
- Permita el ingreso del tráfico ICMP a las interfaces locales de R2.
- Se debe permitir el ingreso del tráfico de red destinado al puerto TCP 80. Debe negarse el acceso de todo tráfico restante y éste se debe registrar.
- Debe negarse el acceso a todo el tráfico que no se haya especificado anteriormente.

Nota: Es posible que esto requiera varias listas de acceso. Verifique la configuración y documente el procedimiento de prueba.

¿Por qué es tan importante el orden de las sentencias de las listas de acceso?

_____

_____

Las listas de acceso se procesan de arriba hacia abajo. Si un paquete coincide con una línea, se realiza la acción coincidente y se omiten las acciones siguientes.

R2

```
ip access-list extended BLOCK_R1
 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
 permit ospf any any
 permit icmp any host 10.1.0.2
 permit icmp any host 10.3.0.2
 permit icmp any host 10.13.205.1
 permit tcp any any eq 80 log
```

```
ip access-list extended BLOCK_R3
 deny ip 10.3.1.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ospf any any
 permit icmp any host 10.1.0.2
 permit icmp any host 10.3.0.2
 permit icmp any host 10.13.205.1
 permit tcp any any eq 80 log


interface serial 0/0/0
 ip access-group BLOCK_R1 in
!
interface serial 0/0/1
 ip access-group BLOCK_R3 in
```

Tarea 5: Verificar una ACL

Pruebe cada protocolo que se intenta bloquear y asegúrese de permitir el acceso del tráfico admitido. Esto requiere probar los pings, HTTP, Telnet y OSPF.

Paso 1: Probar R1 para tráfico de R3 y R3 para tráfico de R1.

Haga ping desde PC1 a PC3.
Haga ping desde PC3 a PC1.
Ambos pings deberían fallar.

Paso 2: Probar el acceso del puerto 80.

Para probar la funcionalidad del puerto 80, habilite el servidor HTTP en R2:

```
R2(config)#ip http server
```

En PC1, abra un explorador Web a la interfaz Serial 0/0/0 de R2. Esto debe realizarse correctamente.

Paso 3: Verificar las rutas OSPF.

Ninguna ruta debería perderse. Confirme esto mediante el comando **show ip route**.

Paso 4: Probar el ping a R2.

Haga ping a R2 desde R1 y PC1.
Haga ping a R2 desde R3 y PC3.
Ambos pings deberían realizarse correctamente.

Paso 5: Realizar otras pruebas de ping para confirmar que se haya denegado el resto del tráfico.

Tarea 6: Documentar las configuraciones del router

Configuraciones

R1

```
hostname R1
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.1.1.254 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.0
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.0.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
ip access-list standard VTY_LOCAL
 permit 10.1.1.0 0.0.0.255
 deny any log
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class VTY_LOCAL in
 password cisco
 login
!
```

R2

```
hostname R2
enable secret class
no ip domain lookup
!
interface Loopback0
 ip address 10.13.205.1 255.255.0.0
!
```

```
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.0
 ip access-group BLOCK_R1 in
 no shutdown
!
interface Serial0/0/1
 ip address 10.3.0.6 255.255.255.0
 ip access-group BLOCK_R3 in
 clockrate 125000
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.1.0.0 0.0.0.255 area 0
 network 10.3.0.0 0.0.0.255 area 0
 network 10.13.0.0 0.0.255.255 area 0
!
ip access-list extended BLOCK_R1
 deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
 permit ospf any any
 permit icmp any host 10.1.0.2
 permit icmp any host 10.3.0.2
 permit icmp any host 10.13.205.1
 permit tcp any any eq 80 log

ip access-list extended BLOCK_R3
 deny ip 10.3.1.0 0.0.0.255 10.1.1.0 0.0.0.255
 permit ospf any any
 permit icmp any host 10.1.0.2
 permit icmp any host 10.3.0.2
 permit icmp any host 10.13.205.1
 permit tcp any any eq 80 log
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

R3

```
hostname R3
!
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.3.1.254 255.255.255.0
 no shutdown
```

```
!
interface Serial0/0/1
 ip address 10.3.0.5 255.255.255.0
 no shutdown
!
router ospf 1
 no auto-cost
 network 10.3.0.0 0.0.0.255 area 0
 network 10.3.1.0 0.0.0.255 area 0
!
ip access-list standard VTY_LOCAL
 permit 10.3.1.0 0.0.0.255
 deny any log
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^C
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class VTY_LOCAL in
 password cisco
 login
!
```

Tarea 7: 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.

Práctica de laboratorio 5.5.3: Resolución de problemas de las listas de control de acceso (Versión para el instructor)

Diagrama de topología

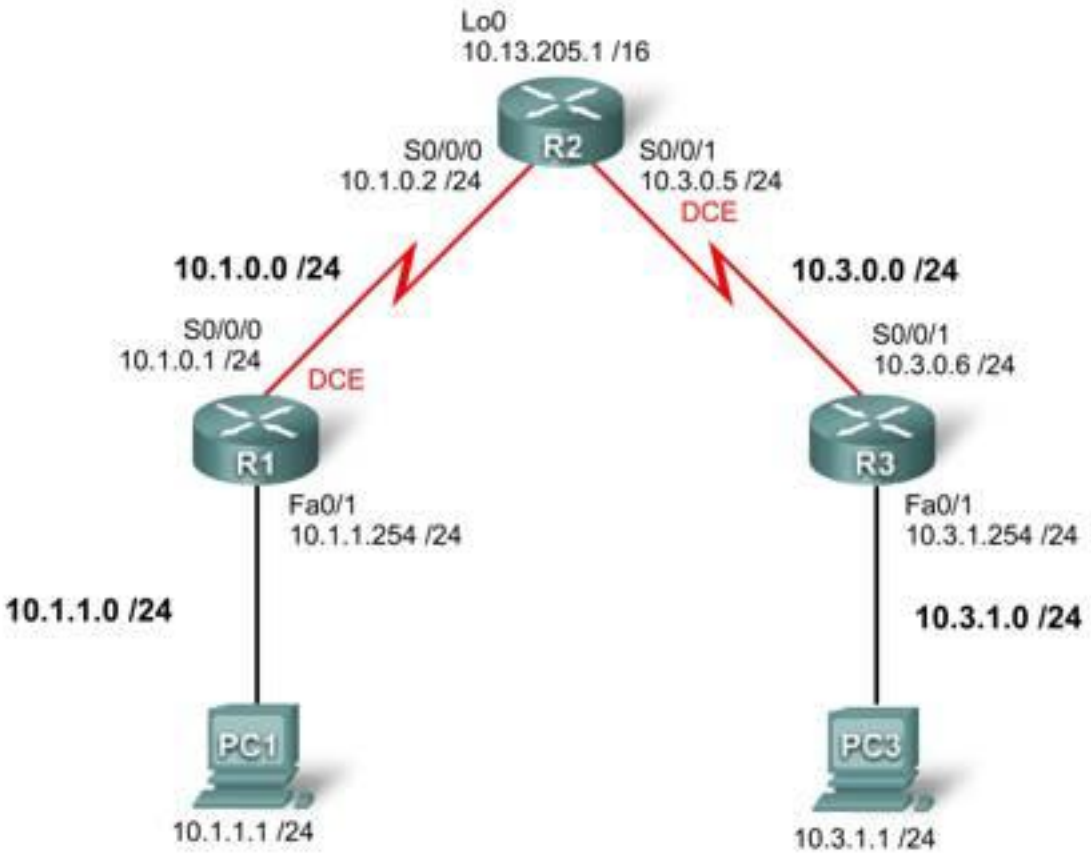


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway por defecto
R1	**S0/0/0**	10.1.0.1	255.255.255.0	
	Fa0/1	10.1.1.254	255.255.255.0	
R2	**S0/0/0**	10.1.0.2	255.255.255.0	
	S0/0/1	10.3.0.5	255.255.255.0	
	Lo 0	10.13.205.1	255.255.0.0	
R3	**S0/0/1**	10.3.0.6	255.255.255.0	
	Fa0/1	10.3.1.254	255.255.255.0	
PC 1	**NIC**	10.1.1.1	255.255.255.0	10.1.1.254
PC 3	**NIC**	10.3.1.1	255.255.255.0	10.3.1.254

Objetivos de aprendizaje

Para completar esta práctica de laboratorio:

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

Escenario

El usuario trabaja para un proveedor de servicios regional que tiene clientes que recientemente experimentaron diversas infracciones de seguridad. Se implementaron algunas políticas de seguridad que no satisfacen las necesidades específicas de los clientes. Se le solicitó al departamento del usuario que analice la configuración, realice pruebas y cambie la configuración, según sea necesario, para establecer la seguridad de los routers de los clientes.

Asegúrese de que en las configuraciones finales se implementen las siguientes políticas de seguridad:

- Los clientes de R1 y R3 solicitan que sólo los equipos PC locales puedan acceder a las líneas VTY. Registre todos los intentos de acceso a las líneas VTY por parte de otros dispositivos.
- No debe permitirse que las redes conectadas directamente de R1 y R3 envíen ni reciban tráfico entre sí. Debe permitirse el acceso a todo el tráfico restante desde R1 y R3, y hacia éstos.

Debe utilizarse y aplicarse de manera entrante un mínimo de sentencias de ACL en las interfaces seriales de R2. OSPF se utiliza para distribuir la información de enrutamiento. Todas las contraseñas, excepto la contraseña secreta de enable, se establecen en cisco. La contraseña secreta de enable se establece en class.

Tarea 1: Cargar los routers con los guiones suministrados

[Nota para el instructor: tanto el instructor como los estudiantes pueden cargar estos comandos en el router. Dichos comandos no se incluyen en la versión para el estudiante de la práctica de laboratorio].

R1

```
hostname R1
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.1.1.254 255.255.255.0
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.0
 clock rate 125000
 no shutdown
 ip access-group VTY-Local out
!
router ospf 1
 network 10.1.0.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
```

```
ip access-list standard VTY-Local
 deny any log
 permit 10.1.1.0 0.0.0.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
```

R2

```
hostname R2
enable secret class
!
interface Loopback0
 ip address 10.13.205.1 255.255.0.0
!
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.0
 no shutdown
 ip access-group block-R3 in
!
interface Serial0/0/1
 ip address 10.3.0.5 255.255.255.0
 clock rate 125000
 no shutdown
 ip access-group block-R1 out
!
router ospf 1
 network 10.1.0.0 0.0.0.255 area 0
 network 10.3.0.0 0.0.0.255 area 0
 network 10.13.0.0 0.0.255.255 area 0
!
ip access-list extended block-R1
 deny   ip 10.1.1.0 0.0.0.255 10.3.0.0 0.0.0.255
 permit ip any any
!
ip access-list extended block-R3
 deny   ip 10.3.0.0 0.0.1.255 10.1.0.0 0.0.1.255
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
```

```
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
```

R3

```
hostname R3
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.3.1.254 255.255.255.0
 no shutdown
!
interface Serial0/0/1
 ip address 10.3.0.6 255.255.255.0
 no shutdown
!
router ospf 1
 network 10.3.0.0 0.0.0.255 area 0
 network 10.3.1.0 0.0.0.255 area 0
!
ip access-list standard VTY-Local
 permit 10.3.11.0 0.0.0.255
 deny any log
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class VTY-Local in
 password cisco
login
```

Tarea 2: Buscar y corregir errores de red

Busque y corrija todos los errores de configuración. Documente los pasos realizados para la resolución de problemas de la red y anote cada error detectado.

Tarea 3: Documentar la red corregida

Ahora que se corrigieron todos los errores y se probó la conectividad en toda la red, debe documentarse la configuración final de cada dispositivo.

R1

```
hostname R1
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.1.1.254 255.255.255.0
!
interface Serial0/0/0
 ip address 10.1.0.1 255.255.255.0
 clockrate 125000
!
router ospf 1
 log-adjacency-changes
 network 10.1.0.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.255 area 0
!
ip access-list standard VTY-Local
 permit 10.1.1.0 0.0.0.255
 deny any log
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 access-class VTY-Local in
 password cisco
 login
!
```

R2

```
hostname R2
enable secret class
!
interface Loopback0
 ip address 10.13.205.1 255.255.0.0
!
interface Serial0/0/0
 ip address 10.1.0.2 255.255.255.0
 ip access-group block-R1 in
!
interface Serial0/0/1
 ip address 10.3.0.6 255.255.255.0
 clockrate 125000
 ip access-group block-R3 in
!
```

```
router ospf 1
 log-adjacency-changes
 network 10.1.0.0 0.0.0.255 area 0
 network 10.3.0.0 0.0.0.255 area 0
 network 10.13.0.0 0.0.255.255 area 0
!
ip access-list extended block-R1
 deny   ip 10.1.0.0 0.0.1.255 10.3.0.0 0.0.1.255
 permit ip any any
!
ip access-list extended block-R3
 deny   ip 10.3.0.0 0.0.1.255 10.1.0.0 0.0.1.255
 permit ip any any
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
 password cisco
 login
!
```

R3

```
hostname R3
enable secret class
no ip domain lookup
!
interface FastEthernet0/1
 ip address 10.3.1.254 255.255.255.0
!
interface Serial0/0/1
 ip address 10.3.0.5 255.255.255.0
!
router ospf 1
 network 10.3.0.0 0.0.0.255 area 0
 network 10.3.1.0 0.0.0.255 area 0
!
ip access-list standard VTY-Local
 permit 10.3.1.0 0.0.0.255
 deny any log
!
banner motd ^Unauthorized access strictly prohibited, violators will be
prosecuted to the full extent of the law.^
!
line con 0
 password cisco
 logging synchronous
 login
!
line vty 0 4
```

```
 access-class VTY-Local in
 password cisco
login
```

Tarea 4: 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.

Práctica de laboratorio 7.4.1: Configuración básica de DHCP y NAT (Versión para el instructor)

Diagrama de topología

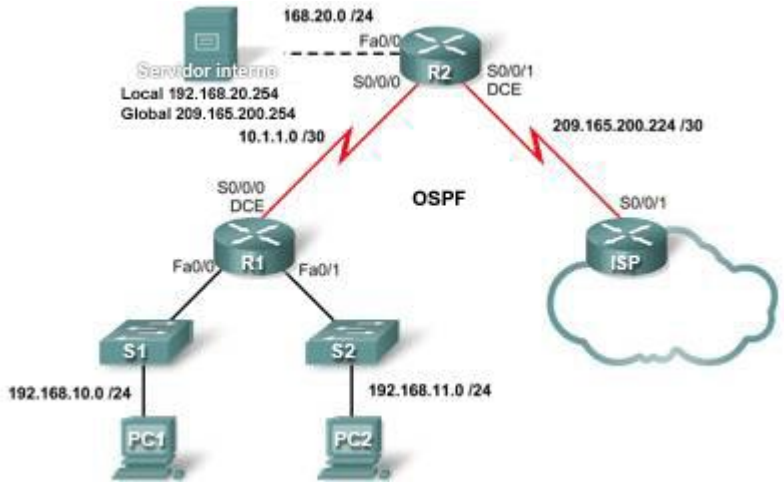


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.254	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, el usuario podrá:

- Preparar la red
- Realizar las configuraciones básicas del router
- Configurar un servidor de DHCP del IOS de Cisco
- Configurar el enrutamiento estático y por defecto
- Configurar NAT estática
- Configurar NAT dinámica con un conjunto de direcciones
- Configurar la sobrecarga de NAT

Escenario

En esta práctica de laboratorio, se configurarán los servicios IP de DHCP y NAT. Un router es el servidor de DHCP. El otro router envía solicitudes de DHCP al servidor. Además, se establecerán las configuraciones de NAT estática y dinámica, incluida la sobrecarga de NAT. Una vez finalizadas estas configuraciones, se verificará la conectividad entre las direcciones internas y externas.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en la topología.

Nota: Si se utilizan routers serie 1700, 2500 ó 2600, los resultados del router y las descripciones de la interfaz pueden ser diferentes. Es posible que en routers más antiguos algunos comandos sean diferentes o no existan.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Configure los routers R1, R2 e ISP de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del dispositivo.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC privilegiado.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para las conexiones de vty.
- Configure direcciones IP en todos los routers. Los equipos PC reciben direccionamiento IP desde DHCP más adelante en la práctica de laboratorio.
- Habilite OSPF con el ID de proceso 1 en R1 y R2. No publique la red 209.165.200.224/27.

Nota: En lugar de conectar un servidor a R2, se puede configurar una interfaz loopback en R2 para usar la dirección IP 192.168.20.254/24. De este modo, no hace falta configurar la interfaz Fast Ethernet.

Para todos los dispositivos:

```
enable
conf t
no ip domain-lookup
enable secret class
banner motd $Authorized Access Only!$
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
 password cisco
 login
end
copy run start
```

R1:

```
hostname R1
int fa0/0
 ip address 192.168.10.1 255.255.255.0
 no shut
int fa0/0
 ip address 192.168.11.1 255.255.255.0
 no shut
int s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 125000
!
router ospf 1
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.3 area 0
```

R2:

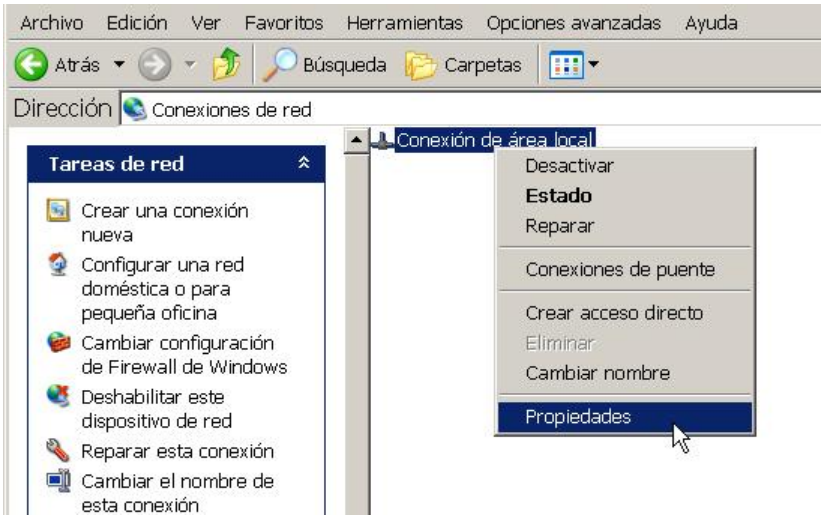
```
hostname R2
int fa0/0
 ip address 192.168.20.1 255.255.255.0
 no shut
int s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
int s0/0/1
 ip address 209.165.200.225 255.255.255.252
 clock rate 125000
 no shut
!optional loopback interface in place of server
 !interface loopback 0
 !ip address 192.168.20.254 255.255.255.0
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
```

ISP:

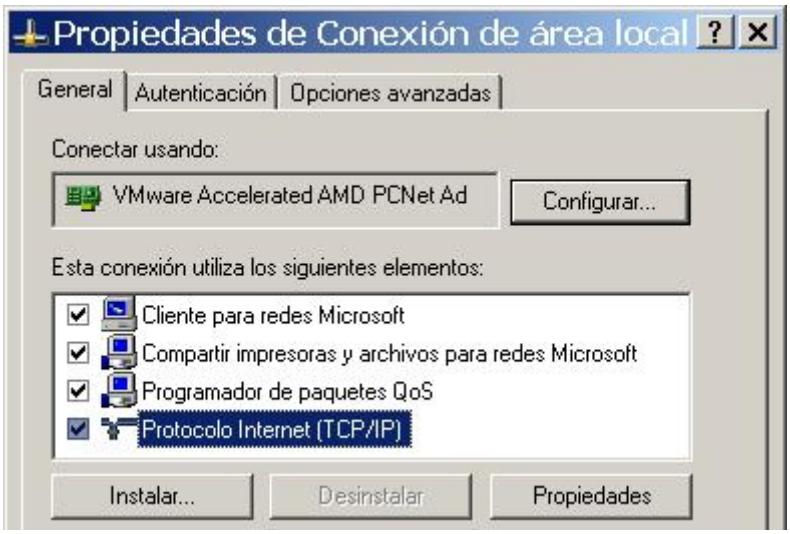
```
hostname ISP
int s0/0/1
 ip address 209.165.200.226 255.255.255.252
 no shut
!
```

Tarea 3: Configurar PC1 y PC2 para que reciban una dirección IP a través de DHCP

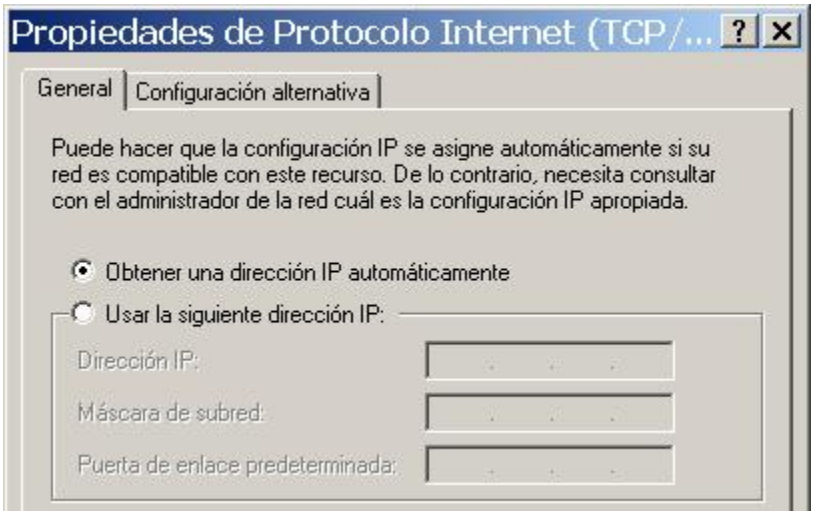
En un equipo PC de Windows, vaya a **Inicio** -> **Panel de control** -> **Conexiones de red** -> **Conexión de área local**. Haga clic con el botón derecho del mouse en **Conexión de área local** y seleccione **Propiedades.**



Desplácese hacia abajo y resalte **Protocolo de Internet (TCP/IP)**. Haga clic en el botón **Propiedades**.



Asegúrese de haber seleccionado la opción **Obtener una dirección IP automáticamente**.



Una vez que se haya hecho esto en PC1 y PC2, estos equipos estarán listos para recibir una dirección IP de un servidor de DHCP.

Tarea 4: Configurar un servidor de DHCP del IOS de Cisco

El software IOS de Cisco admite una configuración de servidor de DHCP denominada Easy IP. El objetivo de esta práctica de laboratorio es que los dispositivos en las redes 192.168.10.0/24 y 192.168.11.0/24 soliciten a R2 direcciones IP a través de DHCP.

Paso 1: Excluir las direcciones asignadas en forma estática.

El servidor de DHCP da por sentado que todas las direcciones IP en una subred de conjunto de direcciones DHCP están disponibles para la asignación a los clientes DHCP. Es necesario especificar las direcciones IP que el servidor de DHCP no debe asignar a los clientes. Estas direcciones IP generalmente son direcciones estáticas reservadas para la interfaz del router, la dirección IP para administración del switch, los servidores y la impresora de red local. El comando **ip dhcp excluded-address** impide que el router asigne direcciones IP dentro del rango configurado. Los siguientes comandos excluyen las primeras 10 direcciones IP de cada pool para las LAN conectadas a R1. Estas direcciones no se asignarán a ningún cliente DHCP.

```
R2(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R2(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

Paso 2: Configurar el pool.

Cree el pool de DHCP mediante el comando **ip dhcp pool** y asígnele el nombre **R1Fa0.**

```
R2(config)#ip dhcp pool R1Fa0
```

Especifique la subred que se utilizará al asignar las direcciones IP. Los pools de DHCP se asocian automáticamente con una interfaz según la sentencia de red. Ahora el router actúa como un servidor de DHCP, distribuyendo direcciones en la subred 192.168.10.0/24, comenzando con 192.168.10.1.

```
R2(dhcp-config)#network 192.168.10.0 255.255.255.0
```

Configure el router por defecto y el servidor de nombre de dominio para la red. Los clientes reciben estas configuraciones a través del DHCP, junto con la dirección IP.

```
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.10.1
```

Nota: No hay un servidor DNS en 192.168.11.5. El comando se configura a modo de práctica únicamente.

Debido a que los dispositivos de la red 192.168.11.0/24 también solicitan direcciones a R2, debe crearse un pool por separado para atender a los dispositivos en esa red. Los comandos son similares a los que se muestran anteriormente:

```
R2(config)#ip dhcp pool R1Fa1
R2(dhcp-config)#network 192.168.11.0 255.255.255.0
R2(dhcp-config)#dns-server 192.168.11.5
R2(dhcp-config)#default-router 192.168.11.1
```

Paso 3: Probar el DHCP.

En PC1 y PC2, pruebe si cada equipo recibió una dirección IP automáticamente. En cada equipo PC, vaya a **Inicio** -> **Ejecutar** -> **cmd** -> **ipconfig**

¿Cuál fue el resultado de la prueba? _____ Ninguna dirección IP se obtuvo automáticamente.

¿Por qué se obtienen estos resultados? _____ Debe configurarse una dirección IP de ayudante.

Paso 4: Configurar una dirección de ayudante.

Los servicios de red tales como DHCP dependen de los broadcasts de Capa 2 para funcionar. Cuando los dispositivos que proporcionan estos servicios existen en una subred distinta de la de los clientes, no pueden recibir los paquetes de broadcast. Debido a que el servidor de DHCP y los clientes DHCP no se encuentran en la misma subred, configure R1 para que envíe broadcasts de DHCP a R2, que es el servidor de DHCP, mediante el comando de configuración de interfaz **ip helper-address**.

Observe que el comando **ip helper-address** debe configurarse en cada una de las interfaces involucradas.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 10.1.1.2
R1(config)#interface fa0/1
R1(config-if)#ip helper-address 10.1.1.2
```

Paso 5: Liberar y renovar las direcciones IP de PC1 y PC2.

Si los equipos PC se utilizaron en otra práctica de laboratorio o se conectaron a Internet, quizá ya hayan obtenido información acerca de una dirección IP automáticamente de un servidor de DHCP diferente. Esta dirección IP se debe borrar mediante los comandos **ipconfig /release** e **ipconfig /renew**.

Paso 6: Verificar la configuración de DHCP.

La configuración del servidor de DHCP se puede verificar de diversas maneras. Ejecute el comando **ipconfig** en PC1 y PC2 para verificar que hayan recibido una dirección IP dinámicamente. A continuación, se pueden ejecutar comandos en el router para obtener más información. El comando **show ip dhcp binding** proporciona información acerca de las direcciones de DHCP asignadas actualmente. Por ejemplo, el siguiente resultado muestra que la dirección IP 192.168.10.11 se asignó a la dirección MAC 3031.632e.3537.6563. El arrendamiento de IP vence el 14 de septiembre de 2007 a las 19:33 horas.

```
R1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name
192.168.10.11       0063.6973.636f.2d30.    Sep 14 2007 07:33 PM    Automatic
                    3031.632e.3537.6563.
                    2e30.3634.302d.566c.
                    31
```

El comando **show ip dhcp pool** muestra información acerca de todos los pools de DHCP configurados actualmente en el router. En este resultado, el pool **R1Fa0** está configurado en R1. Se ha arrendado una dirección de este pool. El próximo cliente que solicite una dirección recibirá 192.168.10.12.

```
R2#show ip dhcp pool
Pool R1Fa0 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : ninguno
 1 subnet is currently in the pool :
 Current index        IP address range                  Leased addresses
 192.168.10.12        192.168.10.1     - 192.168.10.254    1
```

El comando **debug ip dhcp server events** puede resultar muy útil para la resolución de problemas de arrendamientos de DHCP con un servidor de DHCP del IOS de Cisco. A continuación se muestra el resultado de la depuración en R1 después de conectar un host. Observe que la parte resaltada muestra a DHCP otorgando al cliente una dirección de 192.168.10.12 y una máscara de subred de 255.255.255.0.

```
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80b01010000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: there is no address pool for 192.168.11.1.
*Sep 13 21:04:18.072: DHCPD: Sending notification of DISCOVER:
R1#
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
*Sep 13 21:04:18.072: DHCPD: Seeing if there is an internally specified pool
class:
*Sep 13 21:04:18.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:18.072:   DHCPD: remote id 020a0000c0a80a01000000000000
*Sep 13 21:04:18.072:   DHCPD: circuit id 00000000
R1#
*Sep 13 21:04:20.072: DHCPD: Adding binding to radix tree (192.168.10.12)
*Sep 13 21:04:20.072: DHCPD: Adding binding to hash tree
*Sep 13 21:04:20.072: DHCPD: assigned IP address 192.168.10.12 to client
0063.6973.636f.2d30.3031.632e.3537.6563.2e30.3634.302d.566c.31.
*Sep 13 21:04:20.072: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.072:  DHCPD: address 192.168.10.12 mask 255.255.255.0
*Sep 13 21:04:20.072:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.072:   DHCPD: lease time remaining (secs) = 86400
*Sep 13 21:04:20.076: DHCPD: Sending notification of ASSIGNMENT:
*Sep 13 21:04:20.076:  DHCPD: address 192.168.10.12 mask 255.255.255.0
R1#
*Sep 13 21:04:20.076:   DHCPD: htype 1 chaddr 001c.57ec.0640
*Sep 13 21:04:20.076:   DHCPD: lease time remaining (secs) = 86400
```

Tarea 5: Configurar el enrutamiento estático y por defecto

ISP utiliza enrutamiento estático para llegar a todas las redes más allá de R2. Sin embargo, R2 traduce direcciones privadas a direcciones públicas antes de enviar tráfico al ISP. Por consiguiente, el ISP debe configurarse con las direcciones públicas que forman parte de la configuración de NAT en R2. Ingrese la siguiente ruta estática en ISP:

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

Esta ruta estática incluye todas las direcciones asignadas a R2 para uso público.

Configure una ruta por defecto en R2 y propáguela en OSPF.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#router ospf 1
R2(config-router)#default-information originate
```

Espere unos segundos hasta que R1 aprenda la ruta por defecto desde R2 y luego verifique la tabla de enrutamiento de R1. También puede borrar la tabla de enrutamiento con el comando **clear ip route ***. En la tabla de enrutamiento de R1 debería aparecer una ruta por defecto que apunte a R2. Desde R1, haga ping a la interfaz serial 0/0/1 en el ISP (209.165.200.226). Los pings deberían realizarse correctamente. Si los pings fallan, realice la resolución de problemas según corresponda.

Tarea 6: Configurar NAT estática

Paso 1: Asignar una dirección IP pública en forma estática a una dirección IP privada.

Los hosts externos más allá del ISP pueden acceder al servidor interno conectado a R2. Asigne la dirección IP pública 209.165.200.254 en forma estática como la dirección que NAT utilizará para asignar paquetes a la dirección IP privada del servidor interno en 192.168.20.254.

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

Paso 2: Especificar las interfaces NAT internas y externas.

Antes de que NAT pueda funcionar, se deben especificar cuáles interfaces son internas y cuáles son externas.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Nota: Si se utiliza un servidor interno simulado, se debe asignar el comando **ip nat inside** a la interfaz loopback.

Paso 3: Verificar la configuración de NAT estática.

Desde el ISP, haga ping a la dirección IP pública 209.165.200.254.

Tarea 7: Configurar NAT dinámica con un conjunto de direcciones

Mientras que NAT estática proporciona una asignación permanente entre una dirección interna y una dirección pública específica, NAT dinámica asigna direcciones IP privadas a direcciones públicas. Estas direcciones IP públicas provienen de un pool de NAT.

Paso 1: Definir un conjunto de direcciones globales.

Cree un conjunto de direcciones a las que se puedan traducir las direcciones de origen coincidentes. El siguiente comando crea un pool denominado MY-NAT-POOL, que establece las direcciones globales disponibles para la traducción de las direcciones internas coincidentes a una dirección IP en el rango 209.165.200.241–209.165.200.246.

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Paso 2: Crear una lista de control de acceso ampliada para identificar las direcciones internas que se traducen.

```
R2(config)#ip access-list extended NAT
R2(config-ext-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-ext-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

Paso 3: Establecer la traducción dinámica de origen al crear un enlace entre el pool y la lista de control de acceso.

Un router puede tener más de un pool de NAT y más de una ACL. El siguiente comando le indica al router el conjunto de direcciones que debe usar para traducir hosts permitidos según la ACL.

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

Paso 4: Especificar las interfaces NAT internas y externas.

Ya se han especificado las interfaces internas y externas de la configuración de NAT estática. Ahora se debe agregar la interfaz serial conectada a R1 como interfaz interna.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Paso 5: Verificar la configuración.

Haga ping al ISP desde PC1 o la interfaz Fast Ethernet en R1 mediante un **ping** ampliado. Luego utilice los comandos **show ip nat translations** y **show ip nat statistics** en R2 para verificar NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.241:4 192.168.10.1:4     209.165.200.226:4  209.165.200.226:4
--- 209.165.200.241    192.168.10.1       ---                ---
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 23  Misses: 3
CEF Translated packets: 18, CEF Punted packets: 0
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 1] access-list NAT pool MY-NAT-POOL refcount 1
 pool MY-NAT-POOL: netmask 255.255.255.248
        start 209.165.200.241 end 209.165.200.246
        type generic, total addresses 6, allocated 1 (16%), misses 0
Queued Packets: 0
```

Para realizar la resolución de problemas relacionados con NAT, puede utilizar el comando **debug ip nat**. Active la depuración de NAT y repita el ping desde PC1.

```
R2#debug ip nat
IP NAT debugging is on
R2#
*Sep 13 21:15:02.215: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [25]
*Sep 13 21:15:02.231: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [25]
*Sep 13 21:15:02.247: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [26]
*Sep 13 21:15:02.263: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [26]
*Sep 13 21:15:02.275: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [27]
*Sep 13 21:15:02.291: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [27]
*Sep 13 21:15:02.307: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [28]
*Sep 13 21:15:02.323: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [28]
*Sep 13 21:15:02.335: NAT*: s=192.168.10.11->209.165.200.241, d=209.165.200.226 [29]
*Sep 13 21:15:02.351: NAT*: s=209.165.200.226, d=209.165.200.241->192.168.10.11 [29]
R2#
```

Tarea 8: Configurar la sobrecarga de NAT

En el ejemplo anterior, ¿qué sucedería si se necesitara más de las seis direcciones IP públicas que permite el pool?

_____

El séptimo usuario y los usuarios subsiguientes no podrían acceder a los destinos más allá de R2.

Al hacer un seguimiento de los números de puerto, la sobrecarga de NAT permite a varios usuarios internos volver a usar una dirección IP pública.

En esta tarea, se eliminará el pool y la sentencia de asignación configurada en la tarea anterior. A continuación, se configurará la sobrecarga de NAT en R2 de manera que todas las direcciones IP internas se traduzcan a la dirección S0/0/1 de R2 cuando se conecten a un dispositivo externo.

Paso 1: Eliminar el pool de NAT y la sentencia de asignación.

Use los siguientes comandos para eliminar el pool de NAT y la asignación a la ACL de NAT.

```
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

Si recibe el siguiente mensaje, borre las traducciones NAT.

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

Paso 2: Configurar PAT en R2 mediante la dirección IP pública de la interfaz serial 0/0/1.

La configuración es similar a NAT dinámica, excepto que en lugar de un conjunto de direcciones, se utiliza la palabra clave **interface** para identificar la dirección IP externa. Por lo tanto, no se define ningún pool de NAT. La palabra clave **overload** permite agregar el número de puerto a la traducción.

Debido a que ya se configuró una ACL para identificar las direcciones IP internas que deben traducirse y qué interfaces son internas y externas, sólo se debe configurar lo siguiente:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

Paso 3: Verificar la configuración.

Haga ping al ISP desde PC1 o la interfaz Fast Ethernet en R1 mediante un **ping** ampliado. Luego utilice los comandos **show ip nat translations** y **show ip nat statistics** en R2 para verificar NAT.

```
R2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.225:6 192.168.10.11:6    209.165.200.226:6  209.165.200.226:6
--- 209.165.200.254    192.168.20.254     ---                ---

R2#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0, Loopback0
Hits: 48  Misses: 6
CEF Translated packets: 46, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 2] access-list NAT interface Serial0/0/1 refcount 1
Queued Packets: 0
```

Nota: En la tarea anterior, se podría haber agregado la palabra clave **overload** al comando **ip nat inside source list NAT pool MY-NAT-POOL** para permitir más de seis usuarios simultáneos.

Tarea 9: Documentar la red

En cada router, ejecute el comando **show run** y capture las configuraciones.

```
R1#show run
<output omitted>
!
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip helper-address 10.1.1.2
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 ip helper-address 10.1.1.2
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 125000
!
interface Serial0/0/1
 no ip address
 shutdown
!
```

```
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
!
!
banner motd ^C
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
!
end

R2#show run
!
hostname R2
!
!
enable secret class
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.11.1 192.168.11.10
!
ip dhcp pool R1Fa0
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
   dns-server 192.168.11.5
!
ip dhcp pool R1Fa1
   network 192.168.11.0 255.255.255.0
   dns-server 192.168.11.5
   default-router 192.168.11.1
!
no ip domain lookup
!
```

```
interface Loopback0
 ip address 192.168.20.254 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 !
 !
 !
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 !
interface Serial0/0/1
 ip address 209.165.200.225 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 clock rate 125000
 !
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
 !
ip route 0.0.0.0 0.0.0.0 209.165.200.226
 !
 !
no ip http server
no ip http secure-server
ip nat inside source list NAT interface Serial0/0/1 overload
ip nat inside source static 192.168.20.254 209.165.200.254
 !
ip access-list extended NAT
 permit ip 192.168.10.0 0.0.0.255 any
 permit ip 192.168.11.0 0.0.0.255 any
 !
 !
banner motd ^C
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
 !
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
 exec-timeout 0 0
 password cisco
 logging synchronous
```

```
 login
!
end


ISP#show run
<output omitted>
!
hostname ISP
!
enable secret class
!
no ip domain lookup
!
interface Serial0/0/1
 ip address 209.165.200.226 255.255.255.252
 no shutdown
!
!
!
ip route 209.165.200.240 255.255.255.240 Serial0/0/1
!
banner motd ^C
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line vty 0 4
password cisco
 logging synchronous
 login
!
end
```

Tarea 10: 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.

Cisco | Networking Academy®
Mind Wide Open™

Práctica de laboratorio 7.4.2: Reto de configuración de DHCP y NAT (Versión para el instructor)

Diagrama de topología

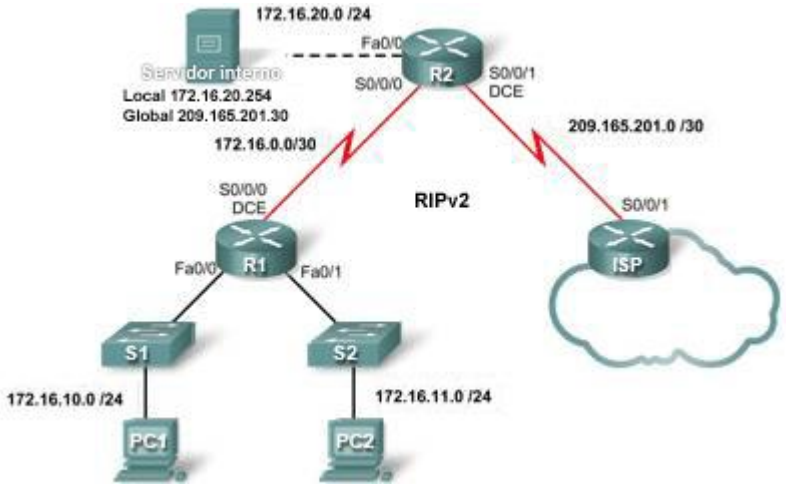


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**S0/0/0**	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	**S0/0/0**	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	**S0/0/1**	209.165.201.2	255.255.255.252

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, el usuario podrá:

- Preparar la red
- Realizar las configuraciones básicas del router
- Configurar un servidor de DHCP del IOS de Cisco
- Configurar el enrutamiento estático y por defecto
- Configurar NAT estática
- Configurar NAT dinámica con un conjunto de direcciones
- Configurar la sobrecarga de NAT

Escenario

En esta práctica de laboratorio, se configurarán los servicios de dirección IP con la red que se muestra en el diagrama de topología. Si se necesita ayuda, se debe volver a consultar la práctica de laboratorio de configuración básica de NAT y DHCP. Sin embargo, el usuario debe intentar hacer todo lo posible por su cuenta.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Se puede utilizar cualquier router del laboratorio, siempre y cuando éste disponga de las interfaces necesarias que se muestran en la topología.

Nota: Si se utilizan routers serie 1700, 2500 ó 2600, los resultados del router y las descripciones de la interfaz pueden ser diferentes.

Paso 2: Borrar todas las configuraciones de los routers.

Tarea 2: Realizar las configuraciones básicas del router

Configure los routers R1, R2 e ISP de acuerdo con las siguientes instrucciones:

- Configure el nombre de host del dispositivo.
- Deshabilite la búsqueda DNS.
- Configure una contraseña de modo EXEC privilegiado.
- Configure un mensaje del día.
- Configure una contraseña para las conexiones de la consola.
- Configure una contraseña para las conexiones de vty.
- Configure direcciones IP en todos los routers. Los equipos PC reciben direccionamiento IP desde DHCP más adelante en la práctica de laboratorio.
- Habilite OSPF con el ID de proceso 1 en R1 y R2. No publique la red 209.165.200.224/27.

Nota: En lugar de conectar un servidor a R2, se puede configurar una interfaz loopback en R2 para usar la dirección IP 192.168.20.254/24. De este modo, no hace falta configurar la interfaz Fast Ethernet.

Para todos los dispositivos:

```
enable
conf t
no ip domain-lookup
enable secret class
banner motd $Authorized Access Only!$
!
line con 0
logging synchronous
 password cisco
 login
!
line vty 0 4
 password cisco
 login
end
copy run start
```

R1:

```
hostname R1
int fa0/0
 ip address 172.16.10.1 255.255.255.0
 no shut
int fa0/1
 ip address 172.16.11.1 255.255.255.0
 no shut
int s0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shut
!
router rip
 version 2
 network 172.16.0.0
no auto-summary
```

R2:

```
hostname R2
int fa0/0
 ip address 172.16.20.1 255.255.255.0
 no shut
int s0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shut
int s0/0/1
 ip address 209.165.201.1 255.255.255.252
 clock rate 125000
 no shut
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

ISP:

```
hostname ISP
int s0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shut
!
```

Tarea 3: Configurar un servidor de DHCP del IOS de Cisco

Configure R2 como el servidor de DHCP para las dos LAN de R1.

Paso 1: Excluir las direcciones asignadas en forma estática.

Excluya las primeras tres direcciones de cada pool.

```
R2(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.3
R2(config)#ip dhcp excluded-address 172.16.11.1 172.16.11.3
```

Paso 2: Configurar el pool de DHCP.

Cree dos pools de DHCP. A uno de ellos asígnele el nombre **R1_LAN10** para la red 172.16.10.0/24, al asígnele el nombre **R1_LAN11** para la red 172.16.11.0/24.

Configure cada pool con una gateway por defecto y un DNS simulado en 172.16.20.254.

```
R2(config)#ip dhcp pool R1_LAN10
R2(dhcp-config)#network 172.16.10.0 255.255.255.0
R2(dhcp-config)#default-router 172.16.10.1
R2(dhcp-config)#dns-server 172.16.20.254
R2(dhcp-config)#ip dhcp pool R1_LAN11
R2(dhcp-config)#network 172.16.11.0 255.255.255.0
R2(dhcp-config)#default-router 172.16.11.1
R2(dhcp-config)#dns-server 172.16.20.254
```

Paso 3: Configurar una dirección de ayudante.

Configure direcciones de ayudantes de modo que los broadcasts de cliente se envíen al servidor de DHCP.

```
R1(config)#interface fa0/0
R1(config-if)#ip helper-address 172.16.0.2
R1(config-if)#interface fa0/1
R1(config-if)#ip helper-address 172.16.0.2
```

Paso 4: Verificar la configuración del DHCP.

Tarea 4: Configurar el enrutamiento estático y por defecto

Configure el ISP con una ruta estática para la red 209.165.201.0/27. Utilice la interfaz de salida como argumento.

```
ISP(config)#ip route 209.165.201.0 255.255.255.224 serial 0/0/1
```

Configure una ruta por defecto en R2 y propáguela en OSPF. Utilice la dirección IP del siguiente salto como argumento.

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#router rip
R2(config-router)#default-information originate
```

Tarea 5: Configurar NAT estática

Paso 1: Asignar una dirección IP pública en forma estática a una dirección IP privada.

Asigne en forma estática la dirección IP del servidor interno a la dirección pública 209.165.201.30.

```
R2(config)#ip nat inside source static 172.16.20.254 209.165.201.30
```

Paso 2: Especificar las interfaces NAT internas y externas.

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

Paso 3: Verificar la configuración de NAT estática.

Tarea 6: Configurar NAT dinámica con un conjunto de direcciones

Paso 1: Definir un conjunto de direcciones globales.

Cree un pool denominado **NAT_POOL** para las direcciones IP de 209.165.201.9 a 209.165.201.14 mediante una máscara de subred /29.

```
R2(config)#ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask
255.255.255.248
```

Paso 2: Crear una lista de control de acceso nombrada y estándar para identificar las direcciones internas que se traducen.

Utilice el nombre **NAT_ACL** y permita el acceso a todos los hosts conectados a las dos LAN de R1.

```
R2(config)#ip access-list standard NAT_ACL
R2(config-std-nacl)#permit 172.16.10.0 0.0.0.255
R2(config-std-nacl)#permit 172.16.11.0 0.0.0.255
```

Paso 3: Establecer la traducción dinámica de origen.

Enlace el pool de NAT a la ACL y permita la sobrecarga de NAT.

```
R2(config)#ip nat inside source list NAT_ACL pool NAT_POOL overload
```

Paso 4: Especificar las interfaces NAT internas y externas.

Verifique que todas las interfaces internas y externas se especifiquen correctamente.

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

Paso 5: Verificar la configuración.

Tarea 7: Documentar la red

En cada router, ejecute el comando **show run** y capture las configuraciones.

Tarea 8: 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.

Guiones finales

```
!--------------
!R1
!--------------
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
banner motd $
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
$
!
line con 0
password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end

!--------------
!R2
!--------------

hostname R2
!
enable secret class
!
```

```
ip dhcp excluded-address 172.16.10.1 172.16.10.3
ip dhcp excluded-address 172.16.11.1 172.16.11.3
!
ip dhcp pool R1_LAN10
   network 172.16.10.0 255.255.255.0
   default-router 172.16.10.1
   dns-server 172.16.20.254
!
ip dhcp pool R1_LAN11
   network 172.16.11.0 255.255.255.0
   default-router 172.16.11.1
   dns-server 172.16.20.254
!
no ip domain lookup
!
interface Loopback0
 ip address 172.16.20.254 255.255.255.0
 ip nat inside
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 ip nat inside
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.201.1 255.255.255.252
 ip nat outside
 clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NAT_POOL overload
ip nat inside source static 172.16.20.254 209.165.201.30
!
ip access-list standard NAT_ACL
 permit 172.16.10.0 0.0.0.255
 permit 172.16.11.0 0.0.0.255
!
banner motd $
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
$
!
```

```
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end

!--------------
!ISP
!--------------

hostname ISP
!
enable secret class
!
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shutdown
!
ip route 209.165.201.0 255.255.255.224 Serial0/0/1
!
banner motd $
**********************************
  !!!AUTHORIZED ACCESS ONLY!!!
**********************************
$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

Práctica de laboratorio 7.4.3: Resolución de problemas de DHCP y NAT (Versión para el instructor)

Diagrama de topología

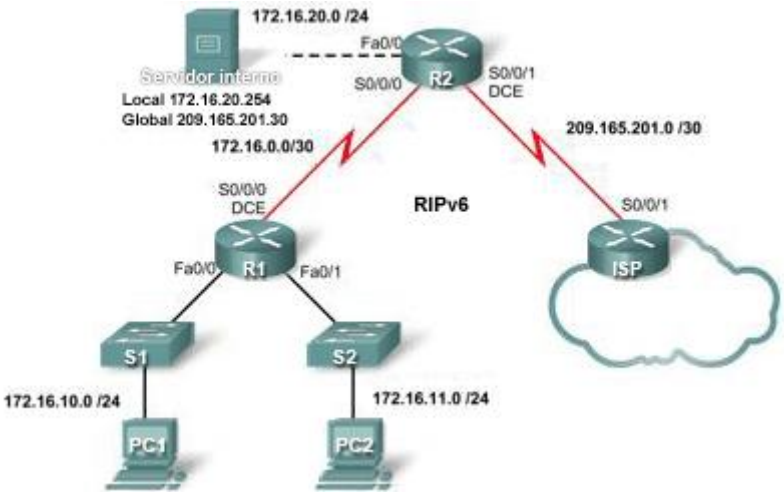


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	**S0/0/0**	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	**S0/0/0**	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	**S0/0/1**	209.165.201.2	255.255.255.252

Objetivos de aprendizaje

Al completar esta práctica de laboratorio, el usuario podrá:

- Preparar la red
- Cargar los routers con guiones
- Detectar y corregir errores de red
- Documentar la red corregida

Escenario

Un ingeniero de redes inexperto configuró los routers R1 y R2 de la compañía. Diversos errores en la configuración produjeron problemas de conectividad. El jefe le solicitó al usuario que resuelva y corrija los errores de configuración y que documente su trabajo. Según los conocimientos de DHCP, NAT y los métodos de prueba estándar, busque y corrija los errores. Asegúrese de que todos los clientes tengan conectividad total. El ISP se configuró correctamente.

Asegúrese de que la red admita lo siguiente:

1. El router R2 debería funcionar como el servidor de DHCP para las redes 172.16.10.0/24 y 172.16.11.0/24 conectadas a R1.
2. Todos los equipos PC conectados a R1 deberían recibir una dirección IP en la red apropiada a través de DHCP.
3. El tráfico desde las LAN de R1 que ingrese a la interfaz Serial 0/0/0 de R2 y que salga de la interfaz Serial 0/0/1 de R2 debería recibir una traducción NAT con un conjunto de direcciones que proporcione el ISP.
4. Las redes externas deberían poder alcanzar al servidor interno mediante la dirección IP 209.165.201.30 y las redes internas deberían poder alcanzar a dicho servidor mediante la dirección IP 172.16.20.254.

Tarea 1: Preparar la red

Paso 1: Conectar una red que sea similar a la del diagrama de topología.

Paso 2: Borrar todas las configuraciones de los routers.

Paso 3: Importar las configuraciones que aparecen a continuación.

[Nota para el instructor: Las configuraciones que aparecen a continuación incluyen comandos mal configurados. Estas configuraciones pueden cargarse en los routers de la topología. Las configuraciones finales que se encuentran al final de este documento incluyen los comandos faltantes, que se muestran de color rojo, y los comandos mal configurados, que se muestran ~~en color rojo y tachados~~ seguidos del comando correcto en color rojo].

R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 no shutdown
!
interface Serial0/0/0
```

```
 ip address 172.16.0.1 255.255.255.252
clock rate 125000
 no shutdown
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

R2

```
hostname R2
!
enable secret class
!
ip dhcp excluded-address 172.16.10.1 172.16.10.3
ip dhcp excluded-address 172.16.11.1 172.16.11.3
!
ip dhcp pool R1_LAN10
   network 172.16.10.0 255.255.255.0
   dns-server 172.16.20.254
!
ip dhcp pool R1_LAN11
   network 172.16.11.0 255.255.255.0
   dns-server 172.16.20.254
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.0
 ip nat inside
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.201.1 255.255.255.252
 ip nat outside
 clock rate 125000
 no shutdown
!
```

```
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL overload

!
ip access-list standard NAT_ACL
 permit 172.16.10.0 0.0.0.255
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

ISP

```
hostname ISP
!
enable secret class
!
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

Tarea 2: Buscar y corregir errores de red

Cuando la red se configura correctamente:

- Los equipos PC1 y PC2 deberían poder recibir direcciones IP desde el pool de DHCP correcto, según lo muestra el comando ipconfig en los equipos PC. Además, el comando `show ip dhcp bindings` en R2 debería mostrar que ambos equipos PC recibieron las direcciones IP.
- Los pings de prueba desde PC1 y PC2 hacia el ISP deberían recibir traducción de sobrecarga de NAT, tal como lo muestra el comando `show ip nat translations` en R2.
- Los pings de prueba desde el servidor interno al ISP deberían recibir la traducción de NAT estática que se indica en la topología. Utilice el comando `show ip nat translations` para verificar esto.
- Un ping desde el ISP hacia la dirección global del servidor interno debería realizarse correctamente.
- Los pings de prueba desde el ISP hacia R1 no deberían recibir traducción NAT, tal como lo muestran los comandos show `ip nat translations o debug ip nat` en R2.

Tarea 3: Documentar las configuraciones del router

En cada router, ejecute el comando **show run** y capture las configuraciones.

Tarea 4: 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.

Configuraciones finales

R1

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface FastEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 ip helper-address 172.16.0.2
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shutdown
!
```

```
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

R2

```
hostname R2
!
enable secret class
!
ip dhcp excluded-address 172.16.10.1 172.16.10.3
ip dhcp excluded-address 172.16.11.1 172.16.11.3
!
ip dhcp pool R1_LAN10
   network 172.16.10.0 255.255.255.0
   default-router 172.16.10.1
   dns-server 172.16.20.254
!
ip dhcp pool R1_LAN11
   network 172.16.11.0 255.255.255.0
   default-router 172.16.11.1
   dns-server 172.16.20.254
!
no ip domain lookup
!
interface FastEthernet0/0
 ip address 172.16.20.1 255.255.255.0
 ip nat inside
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 ip nat inside
 no shutdown
!
interface Serial0/0/1
 ip address 209.165.201.1 255.255.255.252
 ip nat outside
 clock rate 125000
 no shutdown
!
```

```
router rip
 version 2
 network 172.16.0.0
 default-information originate
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL overload
ip nat inside source list NAT_ACL pool NAT_POOL overload
ip nat inside source static 172.16.20.254 209.165.201.30
!
ip access-list standard NAT_ACL
 permit 172.16.10.0 0.0.0.255
 permit 172.16.11.0 0.0.0.255
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

ISP

```
hostname ISP
!
enable secret class
!
interface Serial0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 Serial0/0/1
!
banner motd $AUTHORIZED ACCESS ONLY$
!
line con 0
 password cisco
 logging synchronous
 login
line vty 0 4
 password cisco
 logging synchronous
 login
!
end
```

Práctica de laboratorio 8.5.1: Resolución de problemas de redes empresariales 1 (Versión para el instructor)

Diagrama de topología

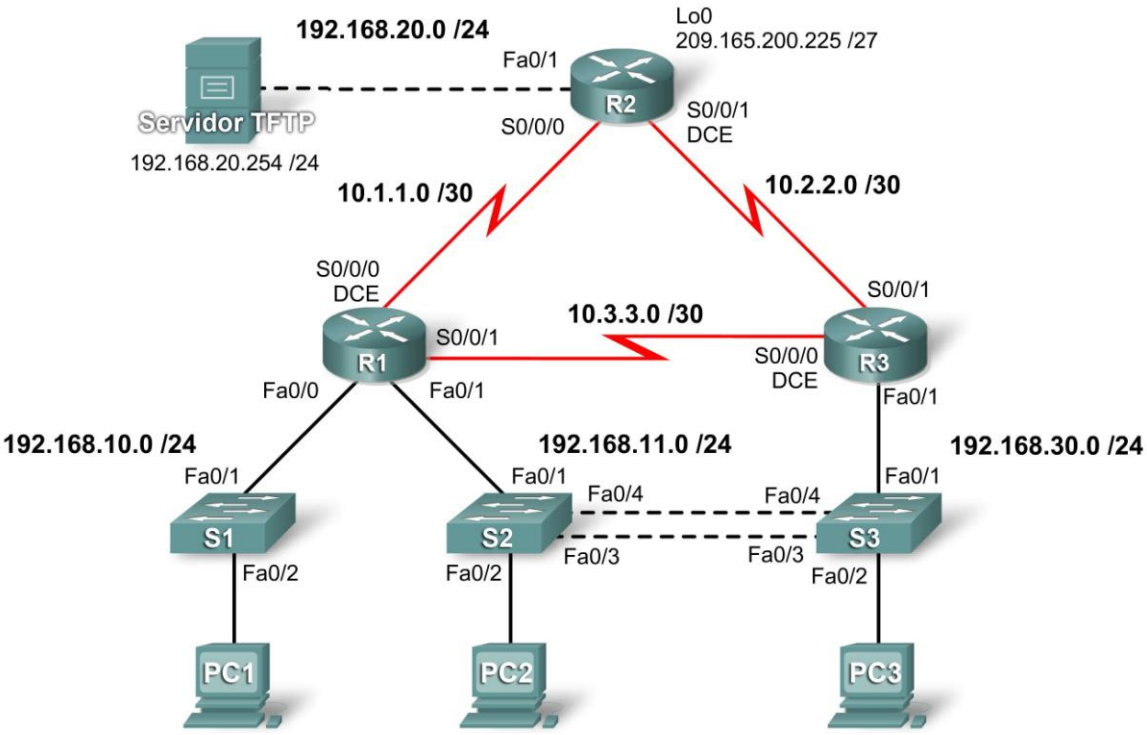


Tabla de direccionamiento

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

Se le solicita al usuario que corrija los errores de configuración de la red de la compañía. 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. Asegúrese de que cada router pueda hacer ping a su propia interfaz Frame Relay.
- El enlace serial entre R2 y R3 utiliza encapsulación HDLC.
- El enlace serial entre R1 y R3 utiliza PPP.
- 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.

Ayuda:

R2# **telnet 10.1.1.1 /source-interface loopback 0**

Trying 10.1.1.1 ...

% Connection refused by remote host

- 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.
- Se debe establecer la seguridad de los protocolos de enrutamiento. Todos los routers RIP deben utilizar autenticación MD5.
- 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 0/0 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.
- R1 debe ser accesible a través de SDM.
- Se debe poder acceder a todas las direcciones que se muestran en el diagrama desde cada dispositivo.

Notas para el instructor:

Los estudiantes reciben las configuraciones que deben cargarse en los routers. Las configuraciones de la práctica de laboratorio para estudiantes no contienen las líneas de color rojo. Como instructor, aquí se proporcionan estas líneas para que pueda guiar a los estudiantes a través del proceso de resolución de problemas.

La práctica de laboratorio, tal como se presenta aquí, ofrece práctica sobre la resolución de problemas y confirmación para muchas de las aptitudes presentadas a través de los cursos CCNA. Se encuentra disponible una configuración de inicio alternativa para una práctica de laboratorio menos extensa. La configuración alternativa tiene menos puntos de resolución de problemas y permite que los estudiantes completen la práctica de laboratorio en menos tiempo.

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 5 ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
frame-relay switching
!El enlace Frame Relay no funciona a menos que un lado conmute tramas
!
```

```
key chain RIP_KEY
 key 1
  key-string cisco
!Debe crear una keychain que se utilizará para que funcione la
autenticación de RIP.
!
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation frame-relay

 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
 no shutdown
 frame-relay intf-type dce
! El router que funciona como el switch Frame Relay debe incluir su
! interfaz
! serial designada en el lado DCE de la conexión.
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
! Las interfaces deben establecerse en un estado activo para que
! propaguen las
! actualizaciones RIP al ingresar el comando por defecto de la interfaz
```

```
! pasiva.
 network 10.1.1.0
 network 10.0.0.0
! En realidad, el comando network 10.1.1.0 funcionará. Sin embargo, RIP
! lo cambiará a 10.0.0.0. Ejecute el comando show run para confirmar
! este cambio.
 network 192.168.10.0
 network 192.168.11.0
 no auto-summary
!
ip classless
!
no ip http server
ip http server
! Es probable que se haya deshabilitado el servidor HTTP por razones de
! seguridad.
! Sin embargo, para que se pueda acceder a SDM, se debe habilitar el
! servidor HTTP.
!
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 0 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 authentication login local_auth local
! El nombre de la lista de autenticación distingue mayúsculas de
! minúsculas; por lo tanto, las líneas vty
! intentan autenticar según una lista inexistente. Los errores de
! ortografía, mayúsculas y minúsculas son los más comunes.
```

```
aaa session-id common
!
ip cef
!
no ip domain lookup
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password 0 ciscoccna
!
interface Loopback0
 description Simulated ISP Connection
 ip address 209.165.200.245 255.255.255.224
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
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 outside
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 encapsulation frame-relay
 no keepalive
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
! Sin este comando, el router no podrá hacer ping a su propia
! interfaz
 no frame-relay inverse-arp
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.0
 ip address 10.2.2.1 255.255.255.252
! Después de utilizar la subred /24 con tanta frecuencia, las máscaras
! de subred
! pueden escribirse incorrectamente con facilidad.
 ip access-group R3-telnet in
 ip nat inside
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
!
!
```

```
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 default-information originate
 no auto-summary
!
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 overload
!
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 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
!
control-plane
!
line con 0
 exec-timeout 0 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
!
key chain RIP_KEY
 key 1
  key-string cisco
username R1 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 ip access-group Anti-spoofing in
 no snmp trap link-status
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation ppp
 clockrate 125000
 ppp authentication chap
!
```

```
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
! Todos los demás routers utilizan autenticación. Por lo tanto, sin
! este comando en cada interfaz que envíe actualizaciones RIP, este
! router
! no podrá participar en RIP.
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/1.11
 no passive-interface FastEthernet0/1.30
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.11.0
 network 192.168.30.0
 no auto-summary
!
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
!
control-plane
!
line con 0
 exec-timeout 0 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
!
control-plane
!
```

```
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S2
!----------------------------------------
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp mode client
! NOTA: Debido a que el servidor ya se configuró, la información sobre
! VLAN
! no se transferirá a Switch3 hasta que se realice una nueva revisión.
! Esto puede
! suceder porque se crea y luego se elimina una VLAN en Switch2, el
! servidor
! VTP.
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 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 Vlan11
 ip address 192.168.11.2 255.255.255.0
 no ip route-cache
!
ip http server
!
control-plane
!
line con 0
 exec-timeout 0 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 domain CCNA_Troubleshooting
! El modo VTP distingue mayúsculas de minúsculas; por lo tanto,
! un error tipográfico como éste impediría que
! VTP funcione adecuadamente. El switch debe mostrar un error sobre la
! falta de concordancia de un dominio al activarse los enlaces
! troncales.
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 11,30
! Es un error común olvidarse de crear las VLAN, especialmente si
! ya tienen acceso a los enlaces troncales.
!
interface FastEthernet0/1
 switchport trunk allowed vlan 30
 switchport trunk allowed vlan 11,30
! VLAN 11 debe permitirse en el enlace troncal a R3 para lograr la
! conectividad a
! R2
 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
!
control-plane
!
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**).

Recuérdeles a los estudiantes la diversidad de comandos que han utilizado a lo largo de este curso y otros para verificar y resolver problemas. Entre algunos de los comandos más comunes y útiles se incluyen:

- show ip route
- show ip interface brief
- show spanning-tree
- show vtp status
- show interfaces serial
- debug ppp authentication
- show ip access-lists
- show ip dhcp binding

- show frame-relay map
- show run
- debug ppp authentication
- ping
- telnet

Esta tarea es intencionalmente poco clara, ya que existen diversas maneras de verificar los requisitos. A continuación se muestra un ejemplo para el requisito 1.

El requisito 1 establece que S2 debe ser la raíz de VLAN 11 y que S3 debe ser la raíz de VLAN 30. La ejecución del comando show spanning-tree permite confirmar que estos switches se configuraron correctamente.

```
S2#show spanning-tree
VLAN0011
Spanning tree enabled protocol rstp
Root ID     Priority    24587
            Address     001c.57ec.2480
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15

Bridge ID   Priority    24587  (priority 24576 sys-id-ext 11)
            Address     001c.57ec.2480
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
            Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0030
  Spanning tree enabled protocol rstp
  Root ID    Priority    24606
             Address     001c.57ec.1480
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15

  Bridge ID  Priority    28702  (priority 28672 sys-id-ext 30)
             Address     001c.57ec.2480
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

Tarea 4: Documentar la red corregida

```
!-----------------------------------------
!                  R1
!-----------------------------------------
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret 5 ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
frame-relay switching
!
key chain RIP_KEY
 key 1
  key-string cisco
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 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
```

```
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation ppp
 ppp authentication chap
!
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.10.0
 network 192.168.11.0
 no auto-summary
!
ip classless
!
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
!
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password 0 ciscoccna
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
!
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 outside
 duplex auto
 speed auto
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 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 inside
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
!
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
```

```
network 192.168.20.0
 default-information originate
 no auto-summary
!
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 overload
!
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 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
!
control-plane
!
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
!
!
key chain RIP_KEY
 key 1
  key-string cisco
username R1 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no snmp trap link-status
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 ip access-group Anti-spoofing in
 no snmp trap link-status
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation ppp
 clockrate 125000
 ppp authentication chap
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/1.11
 no passive-interface FastEthernet0/1.30
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.11.0
 network 192.168.30.0
 no auto-summary
```

```
!
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
!
control-plane
!
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
!
control-plane
!
!
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 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 Vlan11
 ip address 192.168.11.2 255.255.255.0
 no ip route-cache
!
ip http server
!
control-plane
!
```

```
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 11,30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 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
!
control-plane
!
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
```

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.

Configuraciones alternativas

Estas configuraciones pueden utilizarse como punto de partida y tienen menos errores. Una vez más, deben utilizarse los mismos métodos y comandos de resolución de problemas para aislar y resolver los problemas. Las configuraciones de red corregidas son iguales a las configuraciones originales.

```
!-----------------------------------------
!                  R1
!-----------------------------------------
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret 5 ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
frame-relay switching
!
key chain RIP_KEY
 key 1
  key-string cisco
!Debe crear una keychain que se utilizará para que funcione la
autenticación de RIP.
!
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no shutdown
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no shutdown
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation frame-relay
```

```
 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
 no shutdown
 frame-relay intf-type dce
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
! Las interfaces deben establecerse en un estado activo para que
! propaguen las
! actualizaciones RIP al ingresar el comando por defecto de la interfaz
! pasiva.
 network 10.0.0.0
 network 192.168.10.0
 network 192.168.11.0
 no auto-summary
!
ip classless
!
no ip http server
ip http server
! Es probable que se haya deshabilitado el servidor HTTP por razones de
! seguridad.
! Sin embargo, para que se pueda acceder a SDM, se debe habilitar el
! servidor HTTP.
!
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 0 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 authentication login local_auth local
! El nombre de la lista de autenticación distingue mayúsculas de
! minúsculas; por lo tanto, las líneas vty
! intentan autenticar según una lista inexistente. Los errores de
! ortografía, mayúsculas y minúsculas son los más comunes.
aaa session-id common
!
ip cef
!
no ip domain lookup
!
key chain RIP_KEY
 key 1
  key-string cisco
username ccna password 0 ciscoccna
!
interface Loopback0
 description Simulated ISP Connection
 ip address 209.165.200.245 255.255.255.224
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 ip access-group TFTP out
 ip access-group Anti-spoofing in
 ip nat outside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 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 10.2.2.1 255.255.255.0
 ip address 10.2.2.1 255.255.255.252
! Después de utilizar la subred /24 con tanta frecuencia, las máscaras
! de subred
! pueden escribirse incorrectamente con facilidad.
 ip access-group R3-telnet in
 ip nat inside
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 clockrate 128000
!
!
router rip
 version 2
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 default-information originate
 no auto-summary
!
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 overload
!
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 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
!
control-plane
!
line con 0
 exec-timeout 0 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
!
key chain RIP_KEY
 key 1
  key-string cisco
username R1 password 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 ip address 192.168.11.3 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 no snmp trap link-status
!
```

```
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 ip access-group Anti-spoofing in
 no snmp trap link-status
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
 encapsulation ppp
 clockrate 125000
 ppp authentication chap
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip rip authentication mode md5
 ip rip authentication key-chain RIP_KEY
! Todos los demás routers utilizan autenticación. Por lo tanto, sin
! este comando en cada interfaz que envíe actualizaciones RIP, este
! router
! no podrá participar en RIP.
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/0.11
 no passive-interface FastEthernet0/0.30
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.11.0
 network 192.168.30.0
 no auto-summary
!
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
!
control-plane
!
```

```
line con 0
 exec-timeout 0 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
!
control-plane
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
!----------------------------------------
!                S2
!----------------------------------------
no service password-encryption
!
hostname S2
!
security passwords min-length 6
enable secret ciscoccna
!
no aaa new-model
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp mode client
! NOTA: Debido a que el servidor ya se configuró, la información sobre
! VLAN
! no se transferirá a Switch3 hasta que se realice una nueva revisión.
! Esto puede
! suceder porque se crea y luego se elimina una VLAN en Switch2, el
! servidor
! VTP.
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 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 Vlan11
 ip address 192.168.11.2 255.255.255.0
 no ip route-cache
!
ip http server
!
control-plane
!
line con 0
 exec-timeout 0 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 domain CCNA_Troubleshooting
! El modo VTP distingue mayúsculas de minúsculas; por lo tanto, un
! error tipográfico como éste impediría que
! VTP funcione adecuadamente. El switch debe mostrar un error sobre la
! falta de concordancia de un dominio al activarse los enlaces
! troncales.
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 11,30
! Es un error común olvidarse de crear las VLAN, especialmente si
! ya tienen acceso a los enlaces troncales.
!
interface FastEthernet0/1
 switchport trunk allowed vlan 30
 switchport trunk allowed vlan 11,30
! VLAN 11 debe permitirse en el enlace troncal a R3 para lograr la
! conectividad a
! R2
 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
!
control-plane
!
line con 0
 exec-timeout 5 0
 logging synchronous
line vty 0 4
 password ciscoccna
 login
line vty 5 15
 no login
!
end
```

Práctica de laboratorio 8.5.2: Resolución de problemas de redes empresariales 2 (Versión para el instructor)

Diagrama de topología

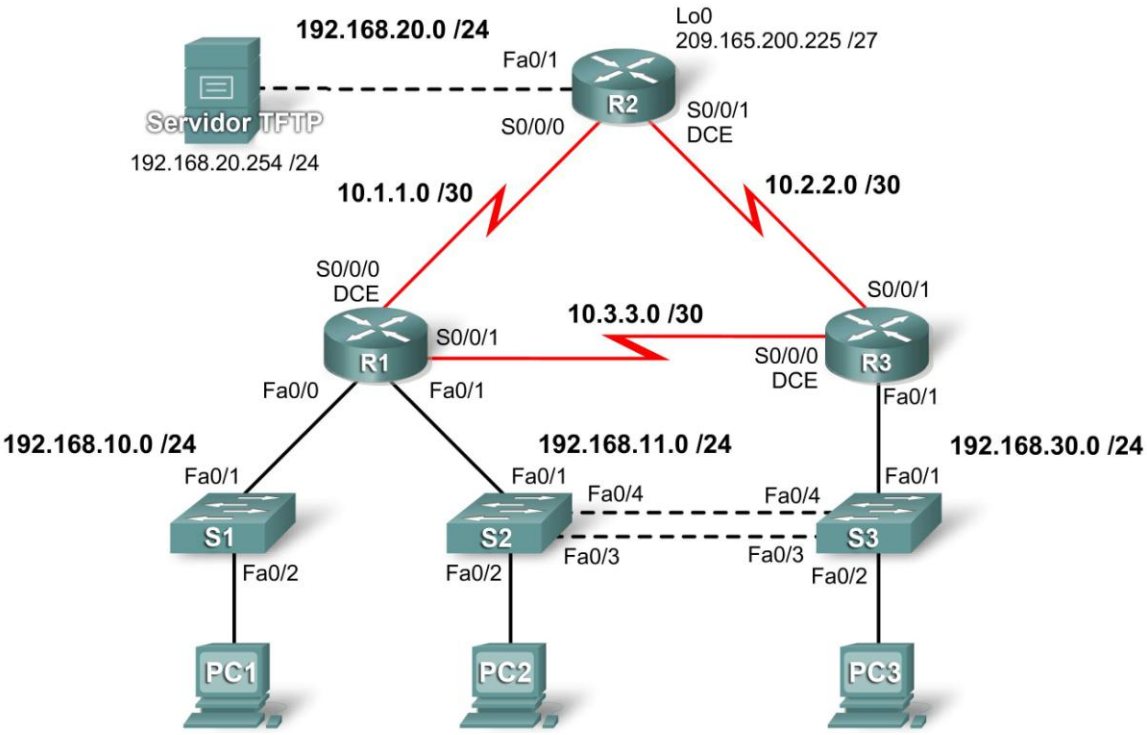


Tabla de direccionamiento

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		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**	DHCP		
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. Utilice **ciscoccna** para todas las contraseñas en esta práctica de laboratorio.

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 EIGRP.
- 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 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
frame-relay switching
!
username R2 password ciscoccna
username R3 password ciscoccna
! Un error tipográfico en el nombre de usuario impedirá que R3 se
! autentique con CHAP.
username ccna password ciscoccna
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip access-group Anti-spoofing out
 ip access-group Anti-spoofing in
! La lista de acceso se aplicó en la dirección incorrecta. Este error
! común impide el tráfico proveniente de la interfaz existente.
 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 10.3.3.1 255.255.255.0
 ip address 10.3.3.1 255.255.255.252
! La subred se configuró mal quizá debido al amplio uso de la subred
! /24.
 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 eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.255
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.255
 network 10.2.2.0 0.0.0.3
! Tal como se mencionó anteriormente, es fácil olvidarse de que no
! todas las subredes son /24.
 network 192.168.10.0 0.0.0.255
 network 192.168.11.0 0.0.0.255
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
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 209.165.200.225 255.255.255.224
 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 outside
 no shutdown
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 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
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
! Con frecuencia, una lista de acceso se crea pero sin aplicarse a una
! interfaz, lo que es necesario para que la ACL funcione.
 ip nat inside
 clockrate 128000
 no shutdown
!
!
```

```
router eigrp 100
router eigrp 10
! El número de AS se escribió incorrectamente, probablemente porque la
! tecla 0 se presionó demasiadas veces. Todos los comandos para este AS
! deben ingresarse nuevamente bajo el AS correcto para que EIGRP
! funcione.
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 no passive interface lo0
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.20.0 0.0.0.255
network 209.165.200.0 0.0.0.7
 no auto-summary
!
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 overload
!
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   172.16.0.0 0.15.255.255
 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
! El usuario olvidó que todas las ACL terminan con un comando deny
! implícito; por lo tanto,este comando es necesario para permitir el
! tráfico restante.
!
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
!
control-plane
!
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
! Un usuario olvidó ingresar la contraseña enable, lo cual no sólo es
! inseguro, sino que impedirá que la autenticación CHAP a través del
! enlace PPP funcione correctamente.
!
no aaa new-model
!
ip cef
!
no ip domain lookup
!
username R1 password ciscoccna
username ccna password ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 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-Spoofin in
 ip access-group Anti-spoofing in
! La lista de acceso se escribió incorrectamente. Ahora hace referencia
! a una ACL inexistente; por lo tanto, el tráfico se descarta debido al
! comando deny all implícito al final de cada ACL.
  no shutdown
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 encapsulation ppp
 clockrate 125000
! La frecuencia de reloj se omitió en la interfaz DCE.
 ppp authentication pap
```

```
 ppp authentication chap
! Por error, se configuró PAP en lugar de CHAP.
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 no shutdown
!
router eigrp 10
 passive-interface default

 no passive interface Fa0/0
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
! Estos comandos se omitieron; por lo que EIGRP se envía en todas las
interfaces.
 network 10.3.3.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.11.0 0.0.0.255
 network 192.168.30.0 0.0.0.255
 no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.2.1
! Se omitió la ruta por defecto a la gateway de Internet, lo que impide
! que este dispositivo pudiera acceder a ella.
!
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 out
 access-class VTY in
! Esta lista de acceso se aplicó en la dirección incorrecta. En este
! caso, no se descarta todo el tráfico. En cambio,
! se aceptan todas las conexiones.
 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 mst
spanning-tree mode rapid-pvst
! MST se configuró accidentalmente para spanning tree. Debería ser
! el mismo modo en todos los switches.
spanning-tree extend system-id
spanning-tree vlan 11 priority 4096
spanning-tree vlan 30 priority 4096
spanning-tree vlan 30 priority 8192
! Las raíces se colocaron incorrectamente debido a prioridades de
! colocación incorrectas.
!
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
!
control-plane
!
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 4096
spanning-tree vlan 11 priority 8192
! Este switch debe tener una mayor prioridad (peor) que el switch2 para
! esta VLAN. Esto ocurre cuando el usuario se olvida de que se prefiere
! la prioridad inferior para las elecciones de raíz.
spanning-tree vlan 30 priority 4096
! Se seleccionó la prioridad por defecto para esta VLAN. Debería
! establecerse como la más baja de los dos switches.
vlan internal allocation policy ascending
!
Vlan 11,30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 30
 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 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**).

Esta tarea es intencionalmente poco clara, ya que existen diversas maneras de verificar los requisitos. A continuación se muestra un ejemplo para el requisito 1.

1.
```
S2#show spanning-tree
VLAN0011
Spanning tree enabled protocol rstp
Root ID     Priority    24587
            Address     001c.57ec.2480
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15

 Bridge ID  Priority    24587  (priority 24576 sys-id-ext 11)
            Address     001c.57ec.2480
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
            Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0030
  Spanning tree enabled protocol rstp
  Root ID    Priority    24606
             Address     001c.57ec.1480
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15

  Bridge ID  Priority    28702  (priority 28672 sys-id-ext 30)
             Address     001c.57ec.2480
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

Tarea 4: Documentar la red corregida

```
!-----------------------------------------
!                  R1
!-----------------------------------------
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret 5 ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
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
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
!
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
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
!
router eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
```

```
network 10.3.3.0 0.0.0.3
 network 192.168.10.0 0.0.0.255
 network 192.168.11.0 0.0.0.255
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
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 outside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 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 inside
 clockrate 128000
!
interface Serial0/1/0
 no ip address
 shutdown
!
interface Serial0/1/1
 no ip address
 shutdown
 clockrate 2000000
!
router eigrp 10
 passive-interface default
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.20.0 0.0.0.255
 no auto-summary
!
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 overload
!
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
!
control-plane
!
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 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 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
 no snmp trap link-status
!
!
interface Serial0/0/0
 ip address 10.3.3.2 255.255.255.252
 encapsulation ppp
 clockrate 125000
 ppp authentication chap
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
!
router eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0.11
 no passive-interface FastEthernet0/0.30
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.3.3.0 0.0.0.3
 network 10.2.2.0 0.0.0.3
 network 192.168.11.0 0.0.0.255
 network 192.168.30.0 0.0.0.255
 no auto-summary
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!
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
!----------------------------------------
!
hostname S2
!
enable secret ciscoccna
!
vtp domain CCNA_Troubleshooting
vtp mode client
vtp password ciscoccna
!
no ip domain-lookup
!
!
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 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 Vlan11
 ip address 192.168.11.2 255.255.255.0
 no shutdown
!
ip http server
!
control-plane
!
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 11,30
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 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 shutdown
!
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 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.

Práctica de laboratorio 8.5.3: Resolución de problemas de redes empresariales 3 (Versión para el instructor)

Diagrama de topología

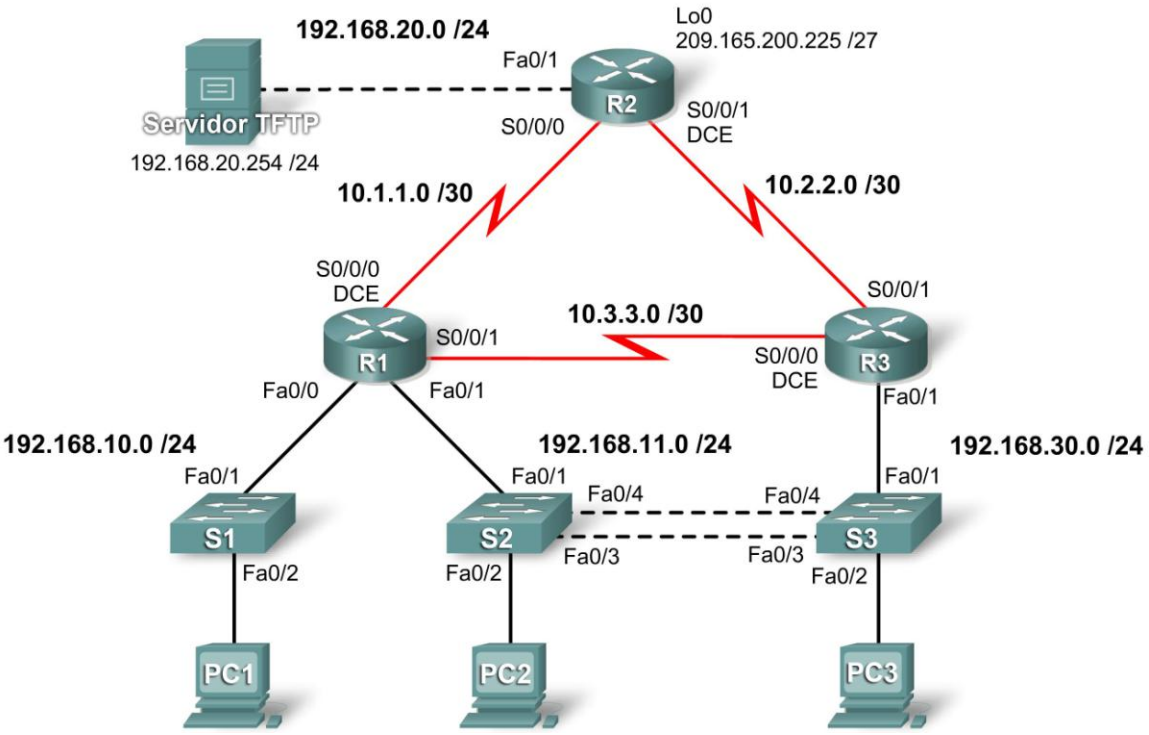


Tabla de direccionamiento

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
   network 192.168.10.0 255.255.255.0
! La red se escribió incorrectamente, lo que le impidió al pool
! alcanzar la subred correcta.
   default-router 192.168.10.1
!
no ip domain lookup
!
ip dhcp excluded-address 192.168.10.2 192.168.10.254
! Esta sentencia no corresponde, ya que excluye todo el espacio
! de direcciones disponible para DHCP.
!
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 10.1.1.0 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
! Se configuró la máscara wildcard incorrecta, ya que se utilizó la
! máscara /24 más común en lugar de la máscara /30 correcta.
 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
 ip nat outside
 duplex auto
 speed auto
 no shutdown
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat outside
 ip nat inside
 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
 no shutdown
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 no shutdown
! Este comando se omitió, lo que impide la conexión a R2.
 ip nat outside
 ip nat inside
```

```
! Las interfaces internas y externas se aplicaron al revés.
 clockrate 128000
! Un error común es omitir la frecuencia de reloj de una interfaz, lo
! que impide la activación del enlace.
!
!
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
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate

!
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 nat inside source list NAT interface FastEthernet0/0 overload
! La lista de acceso se escribió incorrectamente y se especificó que no
! se traducirá ninguna dirección IP. También se omitió la palabra clave
! overload. Esto impide que se realice más de una traducción a la vez.
!
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
 encapsulation dot1Q 11
! La VLAN se escribió incorrectamente, por lo que la subred se colocó
! en la VLAN incorrecta.
 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
 encapsulation hdlc
```

```
! La interfaz se configuró incorrectamente como un enlace 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
 network 10.2.2.0 0.0.0.3 area 0
 network 10.3.3.0 0.0.0.3 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
! Las redes se colocaron accidentalmente en el área incorrecta.
!
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 native vlan 99
 switchport trunk allowed vlan 11,30
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk native vlan 99
! La VLAN nativa se cambió en S3, pero luego se omitió. La falta de
! concordancia de la VLAN nativa generará errores durante el enlace
! troncal.
 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
vlan 11
! Debe existir la VLAN 11 para que se encuentre en el dominio de
! administración activo y para que el tráfico la atraviese.
!
```

```
interface FastEthernet0/1
 switchport trunk allowed vlan 11
 switchport trunk allowed vlan add 30
! La VLAN 30 se omitió en la designación de las VLAN permitidas en
! el enlace troncal a R3.
 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**).

Esta tarea es intencionalmente poco clara, ya que existen diversas maneras de verificar los requisitos. A continuación se muestra un ejemplo para el requisito 1.

1.
```
S2#show spanning-tree
VLAN0011
Spanning tree enabled protocol rstp
Root ID     Priority    24587
            Address     001c.57ec.2480
            This bridge is the root
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15

Bridge ID   Priority    24587  (priority 24576 sys-id-ext 11)
            Address     001c.57ec.2480
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
            Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/2            Desg FWD 19        128.2    P2p
Fa0/3            Desg FWD 19        128.3    P2p
Fa0/4            Desg FWD 19        128.4    P2p

VLAN0030
  Spanning tree enabled protocol rstp
  Root ID    Priority    24606
             Address     001c.57ec.1480
             Cost        19
             Port        3 (FastEthernet0/3)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15

  Bridge ID  Priority    28702  (priority 28672 sys-id-ext 30)
             Address     001c.57ec.2480
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15
             Aging Time 300

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------
Fa0/3            Root FWD 19        128.3    P2p
Fa0/4            Altn BLK 19        128.4    P2p
```

Tarea 4: Documentar la red corregida

```
!-----------------------------------------
!                  R1
!-----------------------------------------
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 6
enable secret 5 ciscoccna
!
ip cef
!
ip dhcp pool Access1
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
no ip domain lookup
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
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
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
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
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 0.0.0.3 area 0
 network 10.2.2.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate siempre
!
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 outside
 duplex auto
 speed auto
!
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 ip nat inside
 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 inside
 clockrate 128000
!
!
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
 network 192.168.20.0 0.0.0.255 area 0
 default-information originate
!
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 overload
!
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 0 ciscoccna
username ccna password 0 ciscoccna
!
interface FastEthernet0/1
 no shutdown
!
interface FastEthernet0/1.11
 encapsulation dot1Q 11
 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
!
interface Serial0/0/1
 ip address 10.2.2.2 255.255.255.252
!
router ospf 1
 passive-interface FastEthernet0/1.30
 network 10.2.2.0 0.0.0.3 area 0
 network 10.3.3.0 0.0.0.3 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
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
!
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
!
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 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 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
!
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 11,30
```

```
!
interface FastEthernet0/1
 switchport trunk allowed vlan 11,30
 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 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.