

1.- Poner nombre:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)#hostname R1
```

```
R1(config)#
```

2.- Quitar traducción Automática de Dominios:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z

```
R1(config)#no ip domain lookup
```

```
R1(config)#
```

3.- Poner que los mensajes de sistema de sincronicen:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z

```
R1(config)#line console 0
```

```
R1(config-line)#logging synchronous
```

```
R1(config-line)#
```

4.- Poner contraseña "enable" encriptada:

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z

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

```
R1(config)#
```

5.- Poner contraseña "Consola"

```
Router>enable
```

```
Router#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z

```
R1(config)#line console 0
```

```
R1(config-line)#password troya
```

```
R1(config-line)#login
```

```
R1(config-line)#
```

6.- Contraseñas "terminales virtuales VTY"

```
Router>enable
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
R1(config)#line vty 0 4
```

```
R1(config-line)#password hector
```

```
R1(config-line)#login
```

```
R1(config-line)#
```

7.- Poner un mensaje MOTD para advertir de delitos

```
Router>enable
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z
```

```
R1(config)#banner motd #AVISO LEGAL: ENTRADA PROHIBIDA#
```

```
R1(config)#
```

8.- Revisar contraseñas para ver si nos hemos equivocado antes de encriptarlas

```
R1#
```

```
R1#show running-config
```

```
hostname R1
```

```
enable secret 5 $1$mERr$hX5rVt7rPNoS4wqbXKX7m0
```

```
banner motd ^CAVISO LEGAL: ENTRADA PROHIBIDA^C
```

```
line con 0
```

```
password troya
```

```
logging synchronous
```

```
login
```

```
line vty 0 4
```

```
password hector
```

```
login
```

9.- Encriptar todas las contraseñas:

```
R1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

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

```
R1(config)#
```

```
Contraseñas Encriptadas
```

```
hostname R1
```

```
enable secret 5 $1$mERr$hX5rVt7rPNoS4wqbXKX7m0
```

```
banner motd ^CAVISO LEGAL: ENTRADA PROHIBIDA^C
```

```
line con 0
```

```
password 7 08355E411018
```

```
logging synchronous
```

```
login
```

```
line vty 0 4
```

```
password 7 0829494D1D1617
```

```
login
```

10.- Configurar Interfaces fa0/0

```
R1#
```

```
R1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#interface fa0/0
```

```
R1(config-if)#ip address 192.168.1.1 255.255.255.0
```

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

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
R1(config-if)#
```

11.- Configurar Interfaces seriales se2/0

```
R1#
```

```
R1#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)#interface se2/0
```

```
R1(config-if)#ip address 192.168.2.1 255.255.255.0
```

```
R1(config-if)#clock rate 64000
```

R1(config-if)#description La anterior instrucción sólo se utiliza en los cables serial en el lado del reloj

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

```
%LINK-5-CHANGED: Interface Serial2/0, changed state to down
```

```
R1(config-if)#
```

12.- Agregar descripciones al código de configuración del router

```
R1(config-if)#description TEXTO
```

13.- Rutas Estáticas



```
R1#
```

```
R1#configure terminal
```

```
R1(config)#ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

```
R1(config-if)#description Se escribe especificando la IP o el nombre de la Interfaz
```

```
R1(config)#ip route 192.168.3.0 255.255.255.0 se2/0
```

```
R1(config)#
```

14.- Eliminar Rutas Estáticas Erroneas

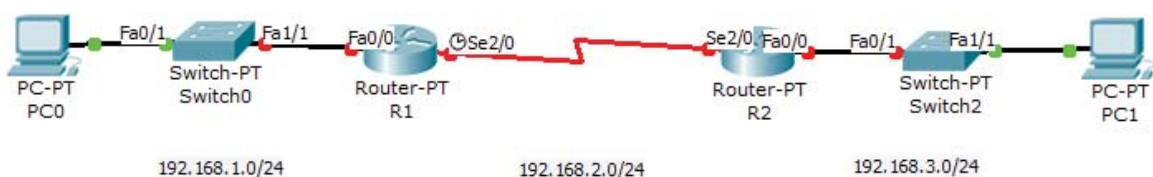
```
R1#
```

```
R1#configure terminal
```

```
R1(config)#no ip route 192.168.3.0 255.255.255.0 192.168.2.2
```

```
R1(config)#
```

15.- Activar el servicio DHCP en el router



R1#

R1#configure terminal

R1(config)#ip dhcp pool red1

R1(dhcp-config)#network 192.168.1.0 255.255.255.0 (Rango de direcciones IP)

R1(dhcp-config)#default-router 192.168.1.1 (Gateway)

R1(dhcp-config)#exit

R1(config)#ip dhcp excluded-address 192.168.1.2 192.168.1.19 (Si queremos excluir alguna IP)

R1(config)#

16.- RIP en el router



R1#

R1#configure terminal

R1(config)#router rip

R1(config-router)#network 192.168.1.0

R1(config-router)#network 192.168.2.0

R1(config-router)#

R2#

R2#configure terminal

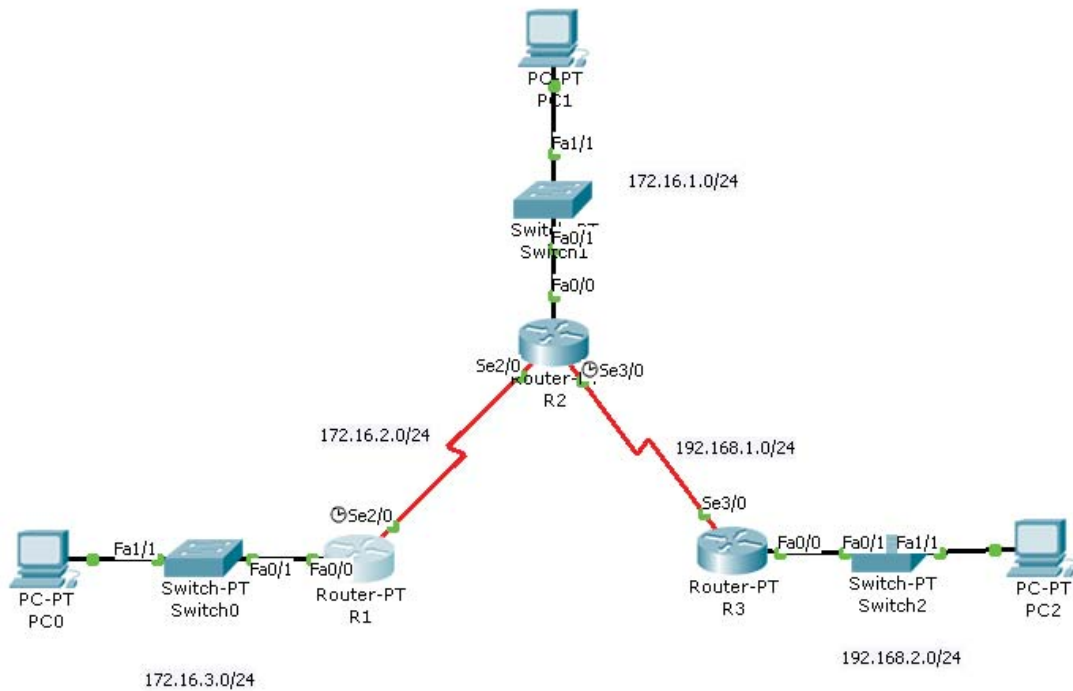
R2(config)#router rip

R2(config-router)#network 192.168.2.0

R2(config-router)#network 192.168.3.0

R2(config-router)#

EJERCICIO5 – RIPv1 SUMARIZACIÓN AUTOMÁTICA



R1

R1#show ip route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

R 172.16.1.0 [120/1] via 172.16.2.2, 00:00:08, Serial2/0

C 172.16.2.0 is directly connected, Serial2/0

C 172.16.3.0 is directly connected, FastEthernet0/0

R 192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:08, Serial2/0

R 192.168.2.0/24 [120/2] via 172.16.2.2, 00:00:08, Serial2/0

R1#

R2

R2#show ip route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

C 172.16.1.0 is directly connected, FastEthernet0/0

C 172.16.2.0 is directly connected, Serial2/0

R 172.16.3.0 [120/1] via 172.16.2.1, 00:00:24, Serial2/0

C 192.168.1.0/24 is directly connected, Serial3/0

R 192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:20, Serial3/0

R2#

R3

R3#show ip route

Gateway of last resort is not set

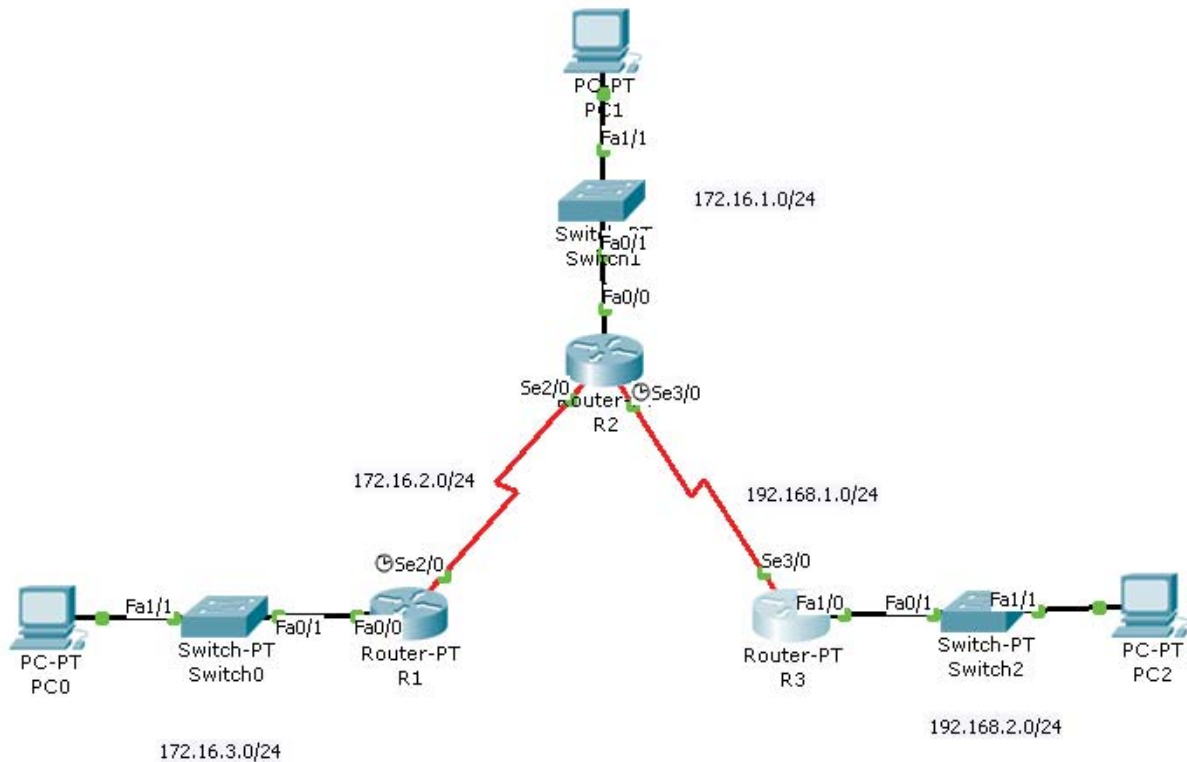
R 172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:04, Serial3/0

C 192.168.1.0/24 is directly connected, Serial3/0

C 192.168.2.0/24 is directly connected, FastEthernet0/0

R3#

EJERCICIO6 – RIPv2



R1

R1#show ip route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

R 172.16.1.0 [120/1] via 172.16.2.2, 00:00:09, Serial2/0

C 172.16.2.0 is directly connected, Serial2/0

C 172.16.3.0 is directly connected, FastEthernet0/0

R 192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:09, Serial2/0

R 192.168.2.0/24 [120/2] via 172.16.2.2, 00:00:09, Serial2/0

R1#

R2

R2#show ip route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

C 172.16.1.0 is directly connected, FastEthernet0/0

C 172.16.2.0 is directly connected, Serial2/0

R 172.16.3.0 [120/1] via 172.16.2.1, 00:00:16, Serial2/0

C 192.168.1.0/24 is directly connected, Serial3/0

R 192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:14, Serial3/0

R2#

R3

R3#show ip route

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

R 172.16.1.0 [120/1] via 192.168.1.1, 00:00:02, Serial3/0

R 172.16.2.0 [120/1] via 192.168.1.1, 00:00:02, Serial3/0

R 172.16.3.0 [120/2] via 192.168.1.1, 00:00:02, Serial3/0

C 192.168.1.0/24 is directly connected, Serial3/0

C 192.168.2.0/24 is directly connected, FastEthernet1/0

R3#

17.-EIGRP en el router

Router>enable

Router#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

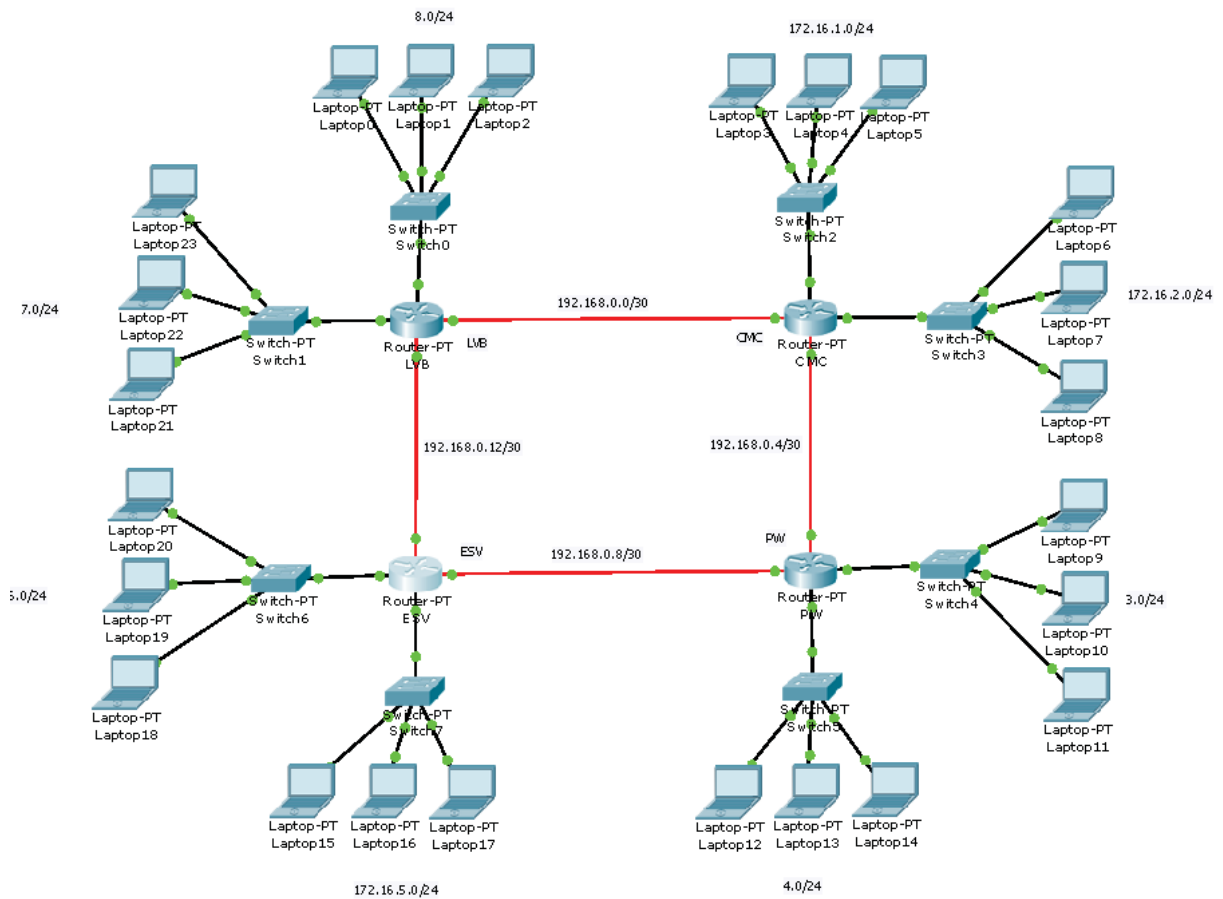
Router(config)#router eigrp 1

Router(config)# #no auto-summary (se pone cuando hay subredes para que no se solapen entre ellas)

Router(config-router)#network 192.168.10.0 (las directamente conectadas a él)

Router(config-router)#

18.- OSPF en el router



ROUTER-ID

Router>enable

Router#configure terminal

Router(config)#router ospf 1

Router(config-router)#router-id 8.8.8.8

```
Router(config-router)#exit
```

```
Router(config)#
```

LOOPBACK

```
PW>enable
```

```
PW#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
PW(config)#interface loopback 0
```

```
%LINK-5-CHANGED: Interface Loopback0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

```
PW(config-if)#ip address 55.55.55.55 255.255.255.255
```

```
PW(config-if)#
```

```
PW(config)#interface loopback 1
```

```
%LINK-5-CHANGED: Interface Loopback1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up
```

```
PW(config-if)#ip address 44.44.44.44 255.255.255.255
```

```
PW(config-if)#
```

NETWORK

```
Router>enable
```

```
Router#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)#router ospf 1
```

```
Router(config-router)#network 172.16.7.0 0.0.0.255 area 0
```

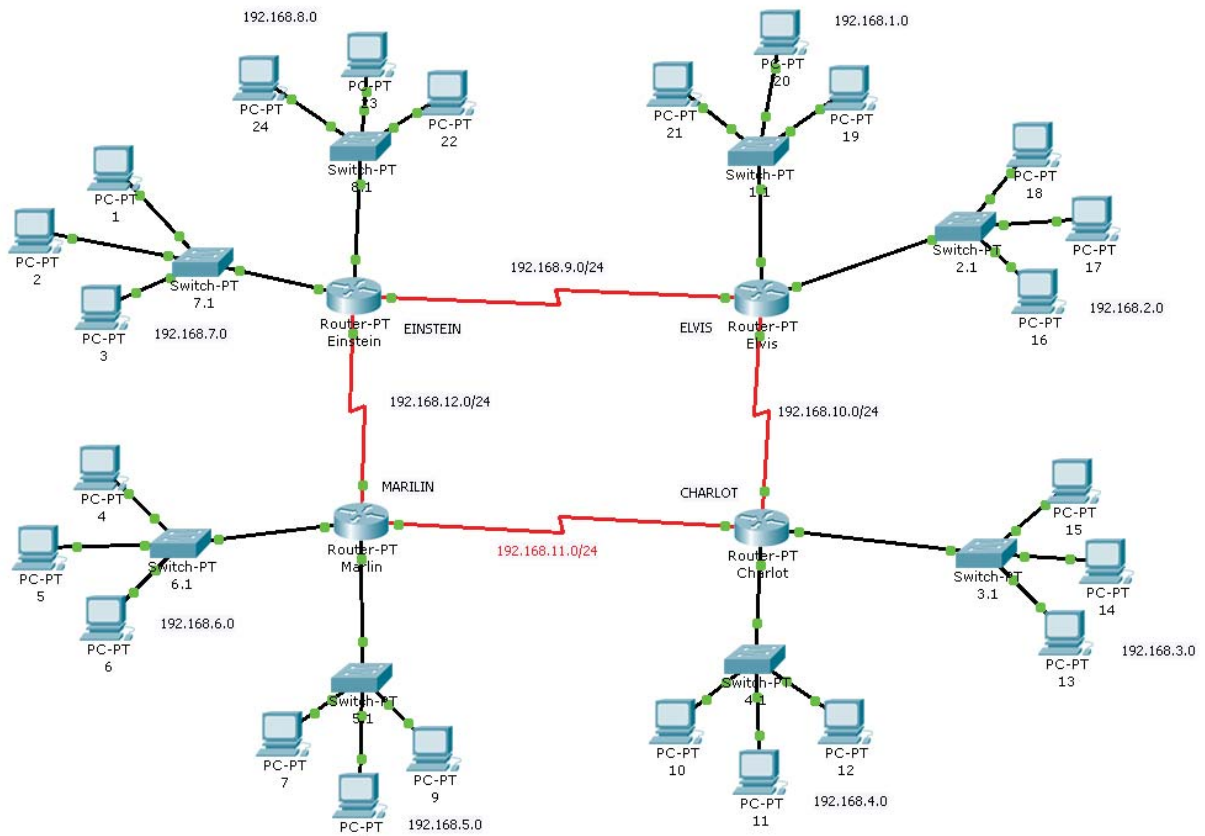
```
Router(config-router)#network 172.16.8.0 0.0.0.255 area 0
```

```
Router(config-router)#network 192.168.0.0 0.0.0.3 area 0
```

```
Router(config-router)#network 192.168.0.12 0.0.0.3 area 0
```

```
Router(config-router)#
```

19.- ACL ESTANDAR en el router (Se asocia en la interfaz más cercana al destino en sentido out = salida)



DECLARACIÓN DE ACL

```
Einstein#
```

```
Einstein#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Einstein(config)#access-list 1 deny host 192.168.1.88
```

```
Einstein(config)#access-list 1 deny host 192.168.2.88
```

```
Einstein(config)#access-list 1 deny host 192.168.3.88
```

```
Einstein(config)#access-list 1 deny 192.168.4.0 0.0.0.255
```

```
Einstein(config)#access-list 1 deny 192.168.5.0 0.0.0.255
```

```
Einstein(config)#access-list 1 deny 192.168.6.0 0.0.0.255
```

```
Einstein(config)#access-list 1 permit any
```

ASOCIACIÓN DE INTERFAZ

```
Einstein(config)#interface fa0/0
```

```
Einstein(config-if)#ip acces-group 1 out
```

```
Einstein(config-if)#
```

DECLARACIÓN DE ACL

```
Marilin>enable
```

```
Marilin#
```

```
Marilin#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Marilin(config)#access-list 1 deny 192.168.1.0 0.0.0.255
```

```
Marilin(config)#access-list 1 deny 192.168.2.0 0.0.0.255
```

```
Marilin(config)#access-list 1 deny 192.168.3.0 0.0.0.255
```

```
Marilin(config)#access-list 1 deny 192.168.4.0 0.0.0.255
```

```
Marilin(config)#access-list 1 deny 192.168.7.0 0.0.0.255
```

```
Marilin(config)#access-list 1 deny 192.168.8.0 0.0.0.255
```

```
Marilin(config)#access-list 1 permit any
```

```
Marilin(config-if)#
```

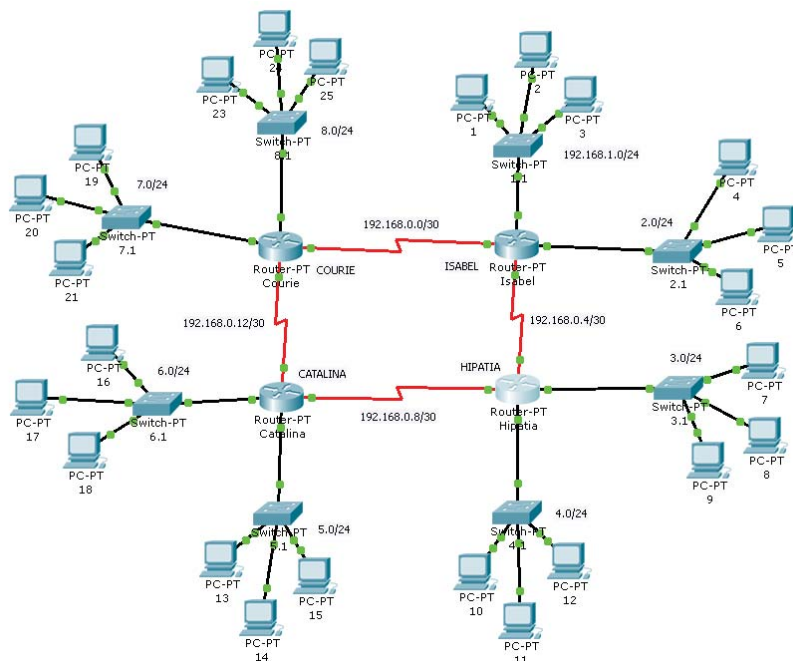
ASOCIACIÓN DE INTERFAZ

```
Marilin(config)#interface fa0/0
```

```
Marilin(config-if)#ip access-group 1 out
```

```
Marilin(config-if)#
```

20.- ACL EXTENDIDAS en el router (Se asocia en la interfaz más cercana al origen en sentido in = entrada)



1.- DECLARACIÓN DE ACL:

Se denegará el tráfico SMTP, FTP, TELNET con origen el equipo 192.168.3.2 y destino los equipos impares de las redes pares. Así mismo se denegará el tráfico TFTP con origen la red 192.168.3.0 y destino las redes del router Catalina. Se permitirá todo lo demás.

```
hipatia>enable
```

```
hipatia#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.2.3 eq 21
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.2.3 eq 23
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.2.3 eq 25
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.4.3 eq 21
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.4.3 eq 23
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.4.3 eq 25
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.6.3 eq 21
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.6.3 eq 23
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.6.3 eq 25
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.8.3 eq 21
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.8.3 eq 23
```

```
hipatia(config)#access-list 101 deny tcp host 192.168.3.2 host 192.168.8.3 eq 25
```

```
hipatia(config)#access-list 101 deny udp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 69
```

```
hipatia(config)#access-list 101 deny udp 192.168.3.0 0.0.0.255 192.168.6.0 0.0.0.255 eq 69
```

```
hipatia(config)#access-list 101 permit ip any any
```

```
hipatia(config)#
```

1.- ASOCIACIÓN DE INTERFAZ

```
hipatia(config)#interface fa0/0
```

```
hipatia(config-if)#ip access-group 101 in
```

```
hipatia(config-if)#
```

2.- DECLARACIÓN DE ACL

Se denegarán todos los protocolos TCP con origen la red 192.168.1.0/24 y destino los equipos acabados en x.x.x.3 y x.x.x.4 de las redes de los routers Courie e Hipatia. Se permitirá todo lo demás.

```
Isabel>enable
```



```
Isabel(config)#access-list 102 deny tcp 192.168.1.0 0.0.0.255 host 192.168.8.4 eq 23
```

```
Isabel(config)#access-list 102 deny tcp 192.168.1.0 0.0.0.255 host 192.168.8.4 eq 25
```

```
Isabel(config)#access-list 102 deny tcp 192.168.1.0 0.0.0.255 host 192.168.8.4 eq 53
```

```
Isabel(config)#access-list 102 permit ip any any
```

2.- ASOCIACIÓN DE INTERFAZ

```
Isabel(config)#interface fa0/0
```

```
Isabel(config-if)#ip access-group 102 in
```

```
Isabel(config-if)#
```

3.- DECLARACIÓN DE ACL

Se permitirán todos los protocolos UDP con origen el equipo 192.168.8.2 y destino los equipos pares de las redes impares. Se denegará todo lo demás.

```
Courie>enable
```

```
Courie#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.2 eq 53
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.2 eq 69
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.2 eq 161
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.2 eq 520
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.4 eq 53
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.4 eq 69
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.4 eq 161
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.1.4 eq 520
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.2 eq 53
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.2 eq 69
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.2 eq 161
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.2 eq 520
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.4 eq 53
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.4 eq 69
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.4 eq 161
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.3.4 eq 520
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.2 eq 53
```

```
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.2 eq 69
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.2 eq 161
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.2 eq 520
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.4 eq 53
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.4 eq 69
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.4 eq 161
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.5.4 eq 520
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.2 eq 53
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.2 eq 69
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.2 eq 161
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.2 eq 520
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.4 eq 53
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.4 eq 69
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.4 eq 161
Courie(config)#access-list 103 permit udp host 192.168.8.2 host 192.168.7.4 eq 520
Courie(config)#access-list 103 deny ip any any
```

3.- ASOCIACIÓN DE INTERFAZ

```
Courie(config)#interface fa0/0
Courie(config-if)#ip access-group 103 in
Courie(config-if)#
```

BORRAR LISTA DE ACCESO

```
Courie(config)#no access-list 103
```

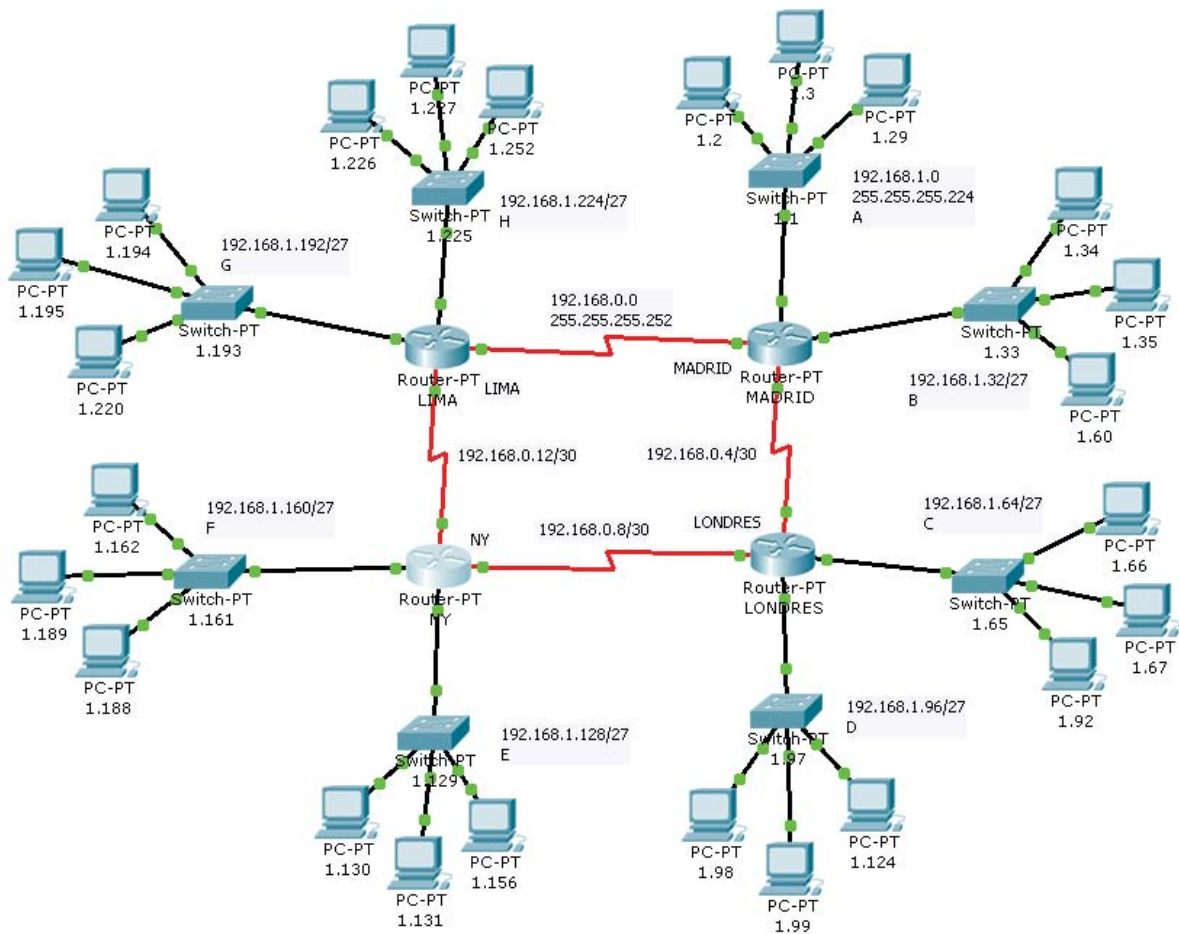
BORRAR ASOCIACIÓN DE LISTA DE ACCESO CON INTERFAZ

```
Courie(config-if)#no ip access-group 103 in
```

COMANDOS VERIFICACIÓN

Para ver el contenido de la ACL configurada de un router **SHOW IP ACCESS-LIST**

Para ver a que interfaz está asignada la lista de acceso **SHOW RUNNING-CONFIG**



1.- DECLARACIÓN DE ACL

Se denegará el tráfico FTP, SNMTP, TELNET, TFTP con origen el primer equipo de la red C del router Londres con destino el primer equipo de la red F,G,H. Se permitirá el resto.

```
LONDRES>enable
```

```
LONDRES#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
LONDRES(config)#access-list 101 deny tcp host 192.168.1.66 host 192.168.1.226 eq 21
```

```
LONDRES(config)#access-list 101 deny tcp host 192.168.1.66 host 192.168.1.226 eq 23
```

```
LONDRES(config)#access-list 101 deny udp host 192.168.1.66 host 192.168.1.226 eq 69
```

```
LONDRES(config)#access-list 101 deny udp host 192.168.1.66 host 192.168.1.226 eq 161
```

```
LONDRES(config)#access-list 101 deny tcp host 192.168.1.66 host 192.168.1.194 eq 21
```

```
LONDRES(config)#access-list 101 deny tcp host 192.168.1.66 host 192.168.1.194 eq 23
```

```
LONDRES(config)#access-list 101 deny udp host 192.168.1.66 host 192.168.1.194 eq 69
```

```
LONDRES(config)#access-list 101 deny udp host 192.168.1.66 host 192.168.1.194 eq 161
```

```
LONDRES(config)#access-list 101 deny tcp host 192.168.1.66 host 192.168.1.162 eq 21
LONDRES(config)#access-list 101 deny tcp host 192.168.1.66 host 192.168.1.162 eq 23
LONDRES(config)#access-list 101 deny udp host 192.168.1.66 host 192.168.1.162 eq 69
LONDRES(config)#access-list 101 deny udp host 192.168.1.66 host 192.168.1.162 eq 161
LONDRES(config)#access-list 101 permit ip any any
LONDRES(config)#
```

1.- ASOCIACIÓN DE INTERFAZ

```
LONDRES(config)#interface fa0/0
LONDRES(config-if)#ip access-group 101 in
LONDRES(config-if)#
```

2.- DECLARACIÓN DE ACL

Al penúltimo equipo de la red F se le permitirá hacer TFTP al antepenúltimo equipo de las redes del router Madrid. Se denegará el resto.

```
NY>enable
NY#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NY(config)#access-list 102 permit udp host 192.168.1.189 host 192.168.1.29 eq 69
NY(config)#access-list 102 permit udp host 192.168.1.189 host 192.168.1.60 eq 69
NY(config)#access-list 102 deny ip any any
NY(config-if)#
```

2.- ASOCIACIÓN DE INTERFAZ

```
NY(config)#interface fa1/0
NY(config-if)#ip access-group 102 in
NY(config-if)#
```

3.- DECLARACIÓN DE ACL

El tráfico TFTP y el PING (ICMP) con origen el segundo equipo de la red E y destino las redes de los routers Lima y Madrid se denegará. Se permitirá todo lo demás.

```
NY>enable
NY#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
NY(config)#access-list 103 deny icmp host 192.168.1.131 192.168.1.1 0.0.0.31
```

```
NY(config)#access-list 103 deny icmp host 192.168.1.131 192.168.1.32 0.0.0.31
```

```
NY(config)#access-list 103 deny icmp host 192.168.1.131 192.168.1.192 0.0.0.31
```

```
NY(config)#access-list 103 deny icmp host 192.168.1.131 192.168.1.224 0.0.0.31
```

```
NY(config)#access-list 103 deny udp host 192.168.1.131 192.168.1.1 0.0.0.31 eq 69
```

```
NY(config)#access-list 103 deny udp host 192.168.1.131 192.168.1.32 0.0.0.31 eq 69
```

```
NY(config)#access-list 103 deny udp host 192.168.1.131 192.168.1.192 0.0.0.31 eq 69
```

```
NY(config)#access-list 103 deny udp host 192.168.1.131 192.168.1.224 0.0.0.31 eq 69
```

```
NY(config)#access-list 103 permit ip any any
```

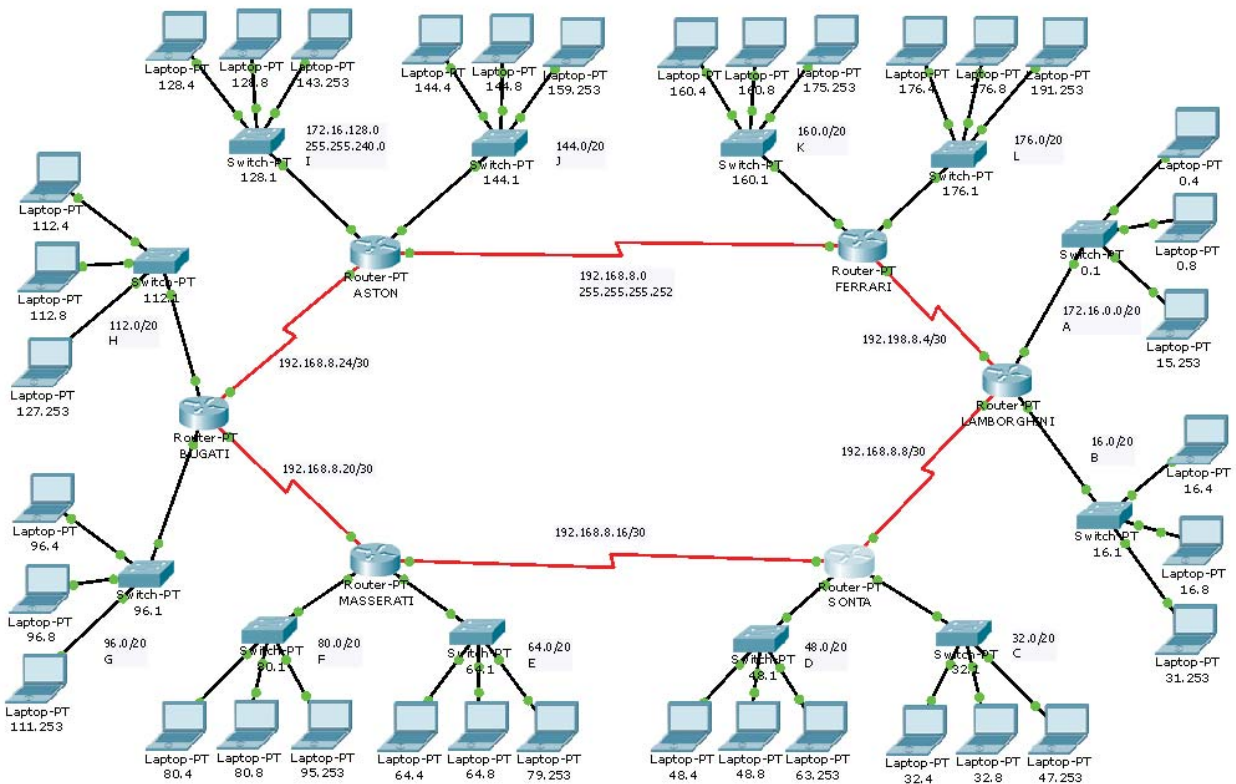
```
NY(config-if)#
```

3.- ASOCIACIÓN DE INTERFAZ

```
NY(config)#interface fa0/0
```

```
NY(config-if)#ip access-group 103 in
```

```
NY(config-if)#
```



1.- DECLARACIÓN DE ACL

Se denegará el tráfico HTTP, TFTP, FTP y SNMP con origen el penúltimo equipo de la red H y destino los equipos X.X.0.4 de las redes de los routers SONTA, MASERATI, FERRARI. Se permite el resto.

```
BUGATI>enable
```

```
BUGATI# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.0.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.16.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.32.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.64.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.80.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.96.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.112.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.128.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.144.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.160.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.176.4 eq ftp
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.0.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.16.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.32.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.64.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.80.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.96.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.112.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.128.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.144.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.160.4 eq www
```

```
BUGATI# access-list 101 deny tcp host 172.16.127.253 host 172.16.176.4 eq www
```

```
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.0.4 eq tftp
```

```
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.16.4 eq tftp
```

```
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.32.4 eq tftp
```

```
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.64.4 eq tftp
```

```
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.80.4 eq tftp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.96.4 eq tftp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.112.4 eq tftp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.144.4 eq tftp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.160.4 eq tftp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.176.4 eq tftp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.0.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.16.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.32.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.64.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.80.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.96.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.112.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.144.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.160.4 eq snmp
BUGATI# access-list 101 deny udp host 172.16.127.253 host 172.16.176.4 eq snmp
BUGATI# access-list 101 permit ip any any
```

1.- ASOCIACIÓN DE INTERFAZ

```
BUGATI (config)#interface fa0/0
BUGATI (config-if)#ip access-group 101 in
BUGATI (config-if)#
```

2.- DECLARACIÓN DE ACL

Se denegará todo el tráfico proveniente de la redes BUGATI, ASTON y FERRARI y destino la red D. Se permitirá todo lo demás.

```
SONTA#
SONTA#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SONTA(config)#access-list 1 deny 172.16.96.0 0.0.15.255
SONTA(config)#access-list 1 deny 172.16.112.0 0.0.15.255
SONTA(config)#access-list 1 deny 172.16.128.0 0.0.15.255
SONTA(config)#access-list 1 deny 172.16.144.0 0.0.15.255
```

```
SONTA(config)#access-list 1 deny 172.16.160.0 0.0.15.255
```

```
SONTA(config)#access-list 1 deny 172.16.176.0 0.0.15.255
```

```
SONTA(config)#access-list 1 permit any
```

2.- ASOCIACIÓN DE INTERFAZ

```
SONTA(config)#interface fa0/0
```

```
SONTA(config-if)#ip access-group 1 out
```

```
SONTA(config-if)#
```

3.- DECLARACIÓN DE ACL

Se permitirá todo el tráfico UDP con origen el primer equipo de la red E y destino los equipos X.X.0.8 de las redes de los routers BUGATTI, SONTA y MASERATI.

```
MASSERATI>enable
```

```
MASSERATI#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
MASSERATI(config)#access-list 102 permit udp host 172.16.64.4 host 172.16.32.8
```

```
MASSERATI(config)#access-list 102 permit udp host 172.16.64.4 host 172.16.48.8
```

```
MASSERATI(config)#access-list 102 permit udp host 172.16.64.4 host 172.16.64.8
```

```
MASSERATI(config)#access-list 102 permit udp host 172.16.64.4 host 172.16.80.8
```

```
MASSERATI(config)#access-list 102 permit udp host 172.16.64.4 host 172.16.96.8
```

```
MASSERATI(config)#access-list 102 permit udp host 172.16.64.4 host 172.16.112.8
```

```
MASSERATI(config)#
```

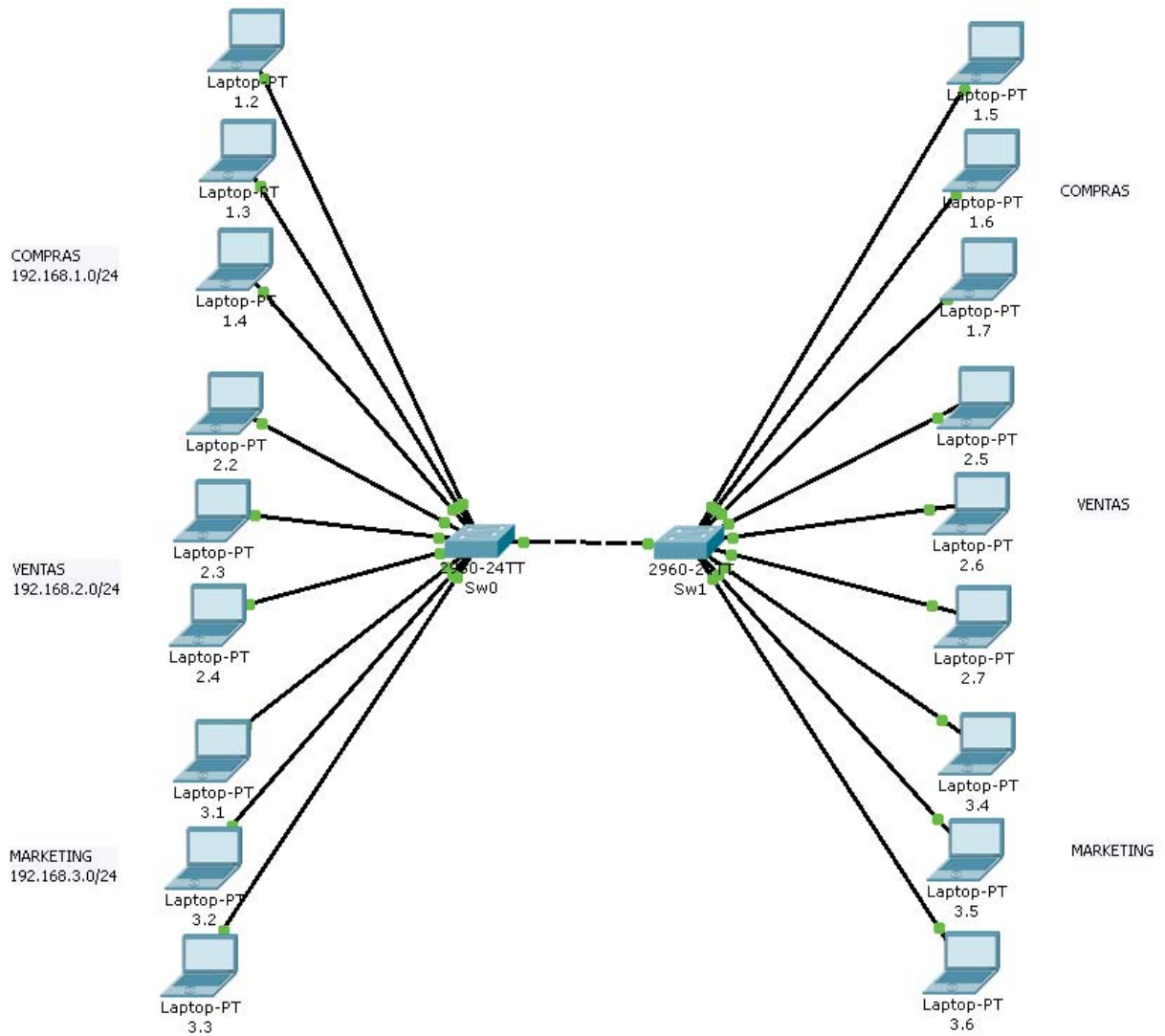
3.- ASOCIACIÓN DE INTERFAZ

```
MASSERATI(config)#interface fa1/0
```

```
MASSERATI(config-if)#ip access-group 102 in
```

```
MASSERATI(config-if)#
```

21.- VLAN



Asociar Vlan a los interfaces

SW0

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Sw0

Sw0(config)#interface fa0/1

Sw0(config-if)#switchport mode access

Sw0(config-if)#switchport access vlan 2

% Access VLAN does not exist. Creating vlan 2

Sw0(config-if)#interface fa0/2

Sw0(config-if)#switchport mode access

Sw0(config-if)#switchport access vlan 2

```
Sw0(config-if)#interface fa0/3
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 2
Sw0(config-if)#interface fa0/4
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
Sw0(config-if)#interface fa0/5
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 3
Sw0(config-if)#interface fa0/6
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 3
Sw0(config-if)#interface fa0/7
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 4
% Access VLAN does not exist. Creating vlan 4
Sw0(config-if)#interface fa0/8
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 4
Sw0(config-if)#interface fa0/9
Sw0(config-if)#switchport mode access
Sw0(config-if)#switchport access vlan 4
Sw0(config-if)#exit
Sw0(config)#
```

Renombrar las VLAN

```
Sw0#
```

```
Sw0# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```



```
Sw0(config)#vlan 2
Sw0(config-vlan)#name COMPRAS
Sw0(config-vlan)#exit
Sw0(config)#vlan 3
Sw0(config-vlan)#name VENTAS
Sw0(config-vlan)#exit
Sw0(config)#vlan 4
Sw0(config-vlan)#name MARKETING
Sw0(config-vlan)#exit
Sw0(config)#exit
Sw0#
```

SW1

```
Switch>enable
Switch#hostname Sw1
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw1
Sw1(config)#interface fa0/1
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 2
% Access VLAN does not exist. Creating vlan 2
Sw1(config-if)#interface fa0/2
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 2
Sw1(config-if)#interface fa0/3
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 2
Sw1(config-if)#interface fa0/4
Sw1(config-if)#switchport mode access
```

```
Sw1(config-if)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
Sw1(config-if)#interface fa0/5
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 3
Sw1(config-if)#interface fa0/6
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 3
Sw1(config-if)#interface fa0/7
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 4
% Access VLAN does not exist. Creating vlan 4
Sw1(config-if)#interface fa0/8
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 4
Sw1(config-if)#interface fa0/9
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 4
Sw1(config-if)#exit
Sw1(config)#
```

Renombrar las VLAN

```
Sw1(config)#vlan 2
Sw1(config-vlan)#name COMPRAS
Sw1(config-vlan)#exit
Sw1(config)#vlan 3
Sw1(config-vlan)#name VENTAS
Sw1(config-vlan)#exit
Sw1(config)#vlan 4
Sw1(config-vlan)#name MARKETING
```

```
Sw1(config-vlan)#exit
```

```
Sw1(config)#exit
```

```
Sw1#
```

Configurar Enlace Troncal SW0

```
Sw0>enable
```

```
Sw0# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Sw0(config)#interface fa0/10
```

```
Sw0(config-if)#switchport mode trunk
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up
```

```
Sw0(config-if)#switchport trunk allowed vlan all
```

```
Sw0(config-if)#exit
```

```
Sw0(config)#exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Sw0#
```

Configurar Enlace Troncal SW1

```
Sw1>enable
```

```
Sw1# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Sw1(config)#interface fa0/10
```

```
Sw1(config-if)#switchport mode trunk
```

```
Sw1(config-if)#switchport trunk allowed vlan all
```

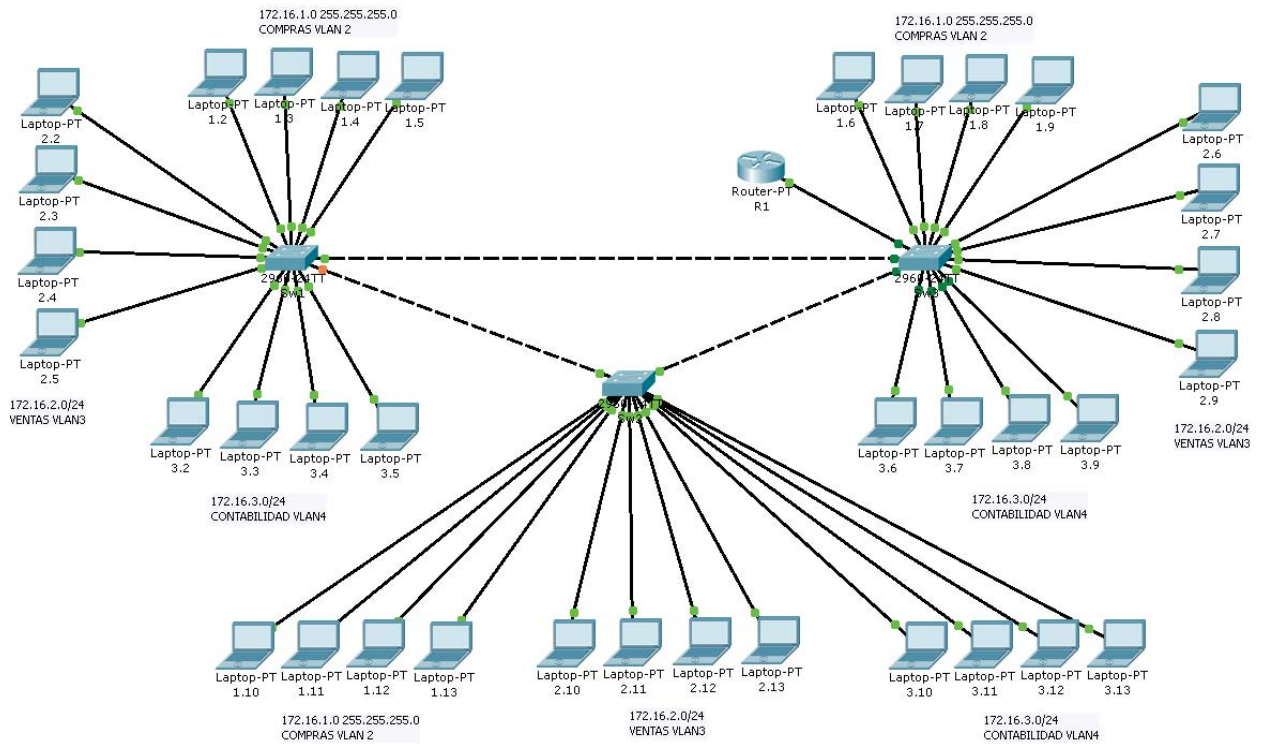
```
Sw1(config-if)#exit
```

```
Sw1(config)#exit
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
Sw1#
```

22.- Enrutamiento Inter VLAN



Sw1 (igual para el Sw2 y Sw3)

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Sw1

Sw1(config)#interface fa0/1

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2

% Access VLAN does not exist. Creating vlan 2

Sw1(config-if)#interface fa0/2

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2

Sw1(config-if)#interface fa0/3

Sw1(config-if)#switchport mode access

Sw1(config-if)#switchport access vlan 2

Sw1(config-if)#interface fa0/4

Sw1(config-if)#switchport mode access

```
Sw1(config-if)#switchport access vlan 2
Sw1(config-if)#interface fa0/5
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 3
% Access VLAN does not exist. Creating vlan 3
Sw1(config-if)#interface fa0/6
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 3
Sw1(config-if)#interface fa0/7
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 3
Sw1(config-if)#interface fa0/8
Sw1(config-if)#switchport mode access
Sw1(config-if)#switchport access vlan 3
Sw1(config-if)#exit
Sw1(config)#
```

Renombrar las VLAN

```
Sw1(config-if)#vlan 2
Sw1(config-vlan)#name COMPRAS
Sw1(config-vlan)#vlan 3
Sw1(config-vlan)#name VENTAS
Sw1(config-vlan)#vlan 4
Sw1(config-vlan)#name CONTABILIDAD
Sw1(config-vlan)#exit
Sw1(config)#exit
```

Configurar Enlace Troncal Sw1 (igual al Sw2 y Sw3)

```
Sw1>enable
Sw1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw1(config)#interface fa0/13
```

```
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state to up
Sw1(config-if)#switchport trunk allowed vlan all
Sw1(config-if)#interface fa0/14
Sw1(config-if)#switchport mode trunk
Sw1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14, changed state to up
Sw1(config-if)#switchport trunk allowed vlan all
Sw1(config-if)#
%SYS-5-CONFIG_I: Configured from console by console
Sw1#
```

Configurar el router para enrutamiento Inter VLAN

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface fa0/0.2
R1(config-subif)#encapsulation dot1q 2
R1(config-subif)#ip address 172.16.1.1 255.255.255.0
R1(config-subif)#interface fa0/0.3
R1(config-subif)#encapsulation dot1q 3
R1(config-subif)#ip address 172.16.2.1 255.255.255.0
R1(config-subif)#interface fa0/0.4
R1(config-subif)#encapsulation dot1q 4
R1(config-subif)#ip address 172.16.3.1 255.255.255.0
R1(config-subif)#exit
R1(config)#interface fa0/0
```

R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.2, changed state to up

R1(config-if)#

%LINK-5-CHANGED: Interface FastEthernet0/0.3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state to up

Configurar VLAN Nativa 99 (igual para los switch Sw2 y Sw3)

Sw1#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Sw1(config)#interface fa0/13

Sw1(config-if)#switchport trunk native vlan 99

Sw1(config-if)#interface fa0/14

Sw1(config-if)#switchport trunk native vlan 99

Sw1(config-if)#exit

Sw1(config-if)#

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/14 (99), with Sw3 FastEthernet0/13 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/13 (99), with Sw2 FastEthernet0/13 (1).

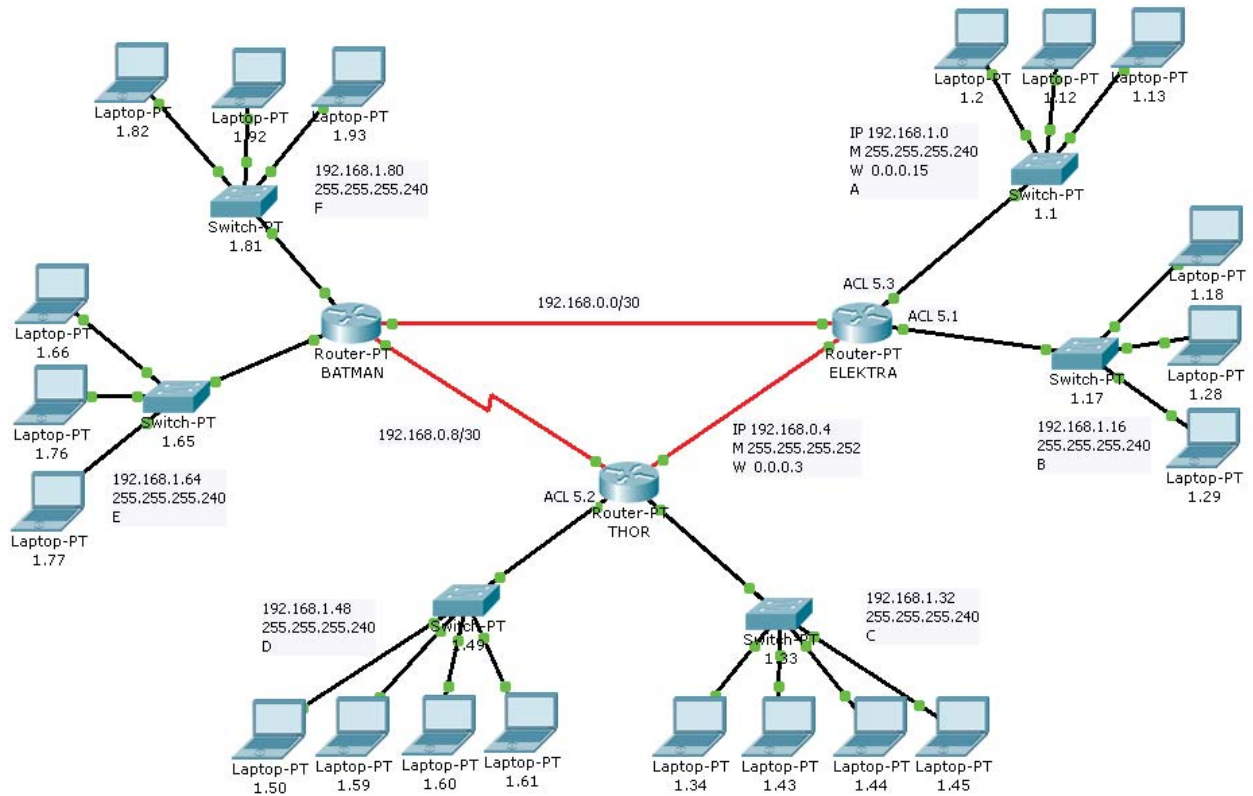
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/14 (99), with Sw3 FastEthernet0/13 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/13 (99), with Sw2 FastEthernet0/13 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/14 (99), with Sw3 FastEthernet0/13 (1).

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/13 (99), with Sw2 FastEthernet0/13 (1).

23.- Repaso EIGRP y ACL



Configuración EIGRP (igual en los routers THOR y ELEKTRA)

```
BATMAN>enable
```

```
BATMAN#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
BATMAN(config)#router eigrp 1
```

```
BATMAN(config-router)#no auto-summary
```

```
BATMAN(config-router)#network 192.168.1.80
```

```
BATMAN(config-router)#network 192.168.1.64
```

```
BATMAN(config-router)#network 192.168.0.0
```

```
BATMAN(config-router)#network 192.168.0.8
```

```
BATMAN(config-router)#exit
```

```
BATMAN(config)#
```

1.- DECLARACIÓN DE ACL

Se denegará todo el tráfico con origen los primeros equipos de las redes D,E,F y destino la red B. Se permitirá todo lo demás.

```
ELEKTRA>enable
```



```
ELEKTRA#configure terminal  
ELEKTRA(config)#access-list 1 deny host 192.168.1.50  
ELEKTRA(config)#access-list 1 deny host 192.168.1.66  
ELEKTRA(config)#access-list 1 deny host 192.168.1.82  
ELEKTRA(config)#access-list 1 permit any
```

1.- ASOCIACIÓN DE INTERFAZ

```
ELEKTRA(config)#interface fa1/0  
ELEKTRA(config-if)#ip access-group 1 out  
ELEKTRA(config-if)#exit  
ELEKTRA(config)#exit
```

2.- DECLARACIÓN DE ACL

Se denegará el tráfico telnet, icmp, tftp, ftp con origen el penúltimo equipo de la red D y destino las redes de los routers BATMAN y ELEKTRA. Se permitirá todo lo demás.

```
THOR>enable  
THOR#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.0 0.0.0.15 eq 21  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.0 0.0.0.15 eq 23  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.16 0.0.0.15 eq 21  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.16 0.0.0.15 eq 23  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.64 0.0.0.15 eq 21  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.64 0.0.0.15 eq 23  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.80 0.0.0.15 eq 21  
THOR(config)#access-list 101 deny tcp host 192.168.1.60 192.168.1.80 0.0.0.15 eq 23  
THOR(config)#access-list 101 deny udp host 192.168.1.60 192.168.1.0 0.0.0.15 eq 69  
THOR(config)#access-list 101 deny udp host 192.168.1.60 192.168.1.16 0.0.0.15 eq 69  
THOR(config)#access-list 101 deny udp host 192.168.1.60 192.168.1.64 0.0.0.15 eq 69  
THOR(config)#access-list 101 deny udp host 192.168.1.60 192.168.1.80 0.0.0.15 eq 69  
THOR(config)#access-list 101 deny icmp host 192.168.1.60 192.168.1.0 0.0.0.15  
THOR(config)#access-list 101 deny icmp host 192.168.1.60 192.168.1.16 0.0.0.15  
THOR(config)#access-list 101 deny icmp host 192.168.1.60 192.168.1.64 0.0.0.15
```

```
THOR(config)#access-list 101 deny icmp host 192.168.1.60 192.168.1.80 0.0.0.15
```

```
THOR(config)#access-list 101 permit ip any any
```

2.- ASOCIACIÓN DE INTERFAZ

```
THOR(config)#interface fa0/0
```

```
THOR(config-if)#ip access-group 101 in
```

```
THOR(config-if)#exit
```

```
THOR(config)#exit
```

```
THOR#
```

3.- DECLARACIÓN DE ACL

Se permitirá el tráfico UDP con origen la red A y destino los antepenúltimos equipos de las redes de THOR. Se denegará todo lo demás.

```
ELEKTRA >enable
```

```
ELEKTRA #configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
ELEKTRA(config)#access-list 102 permit udp 192.168.1.0 0.0.0.15 host 192.168.1.43
```

```
ELEKTRA(config)#access-list 102 permit udp 192.168.1.0 0.0.0.15 host 192.168.1.59
```

```
ELEKTRA(config)#access-list 102 deny ip any any
```

3.- ASOCIACIÓN DE INTERFAZ

```
ELEKTRA(config)#interface fa0/0
```

```
ELEKTRA(config-if)#ip access-group 102 in
```

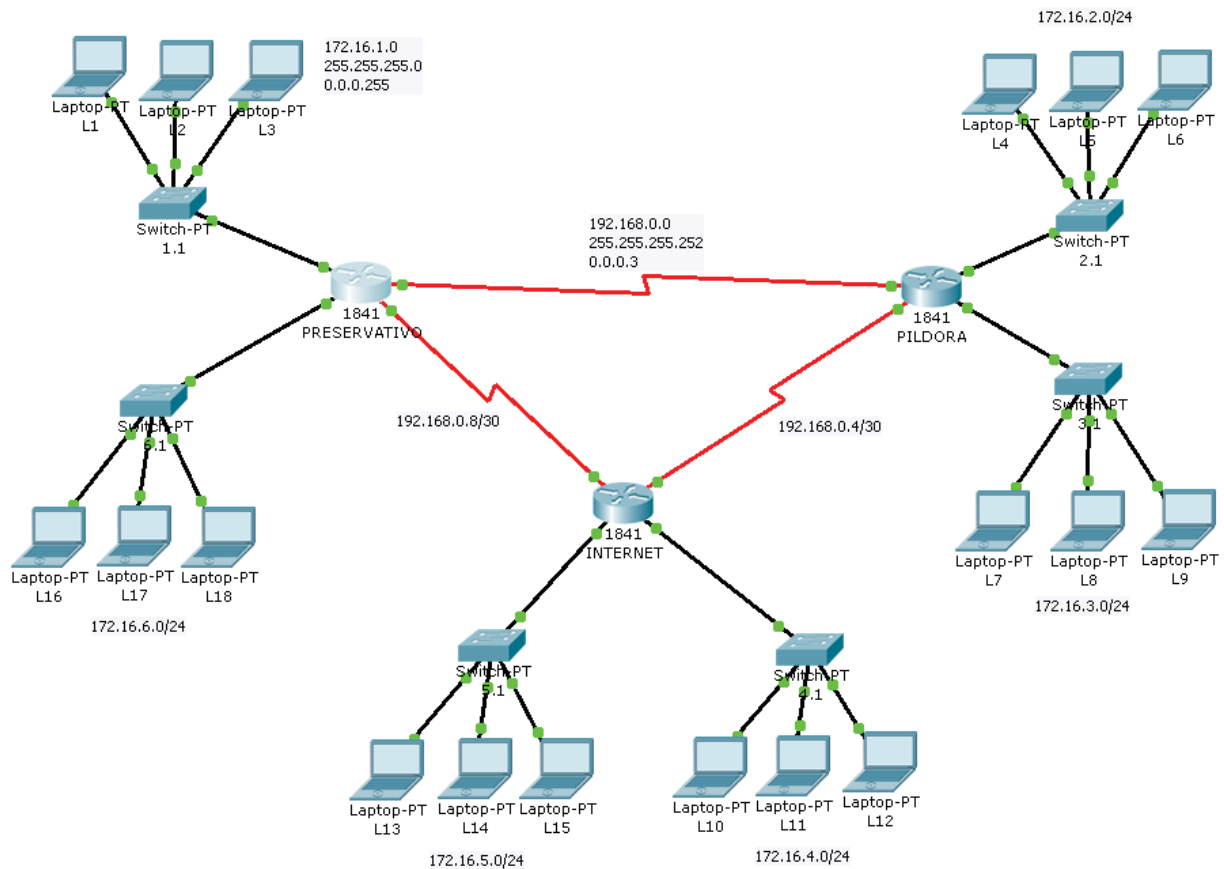
```
ELEKTRA(config-if)#exit
```

```
ELEKTRA(config)#exit
```

```
ELEKTRA#
```

SEGURIDAD EN LOS ROUTERS. MÓDULO 2

24.- Seguridad en los routers



1.- Configuración Básica (Ip por DHCP)

2.- Contraseña mínima de 10 caracteres

```
PILDORA(config)#security passwords min-length 10
```

3.- Deshabilitar conexiones desatendidas cuando pasen 10 min

```
PILDORA(config)#line console 0
```

```
PILDORA(config-line)#exec-timeout 10 00
```

```
PILDORA(config-line)#
```

4.- Configurar contraseña enable secret

```
PILDORA(config)#enable secret cisco12345
```

5.- Conigurar OSPF

6.- Añadir usuarios a la base local del router

```
PILDORA(config)#username pepe password pepe123456
```

```
PILDORA(config)#
```

7.- Habilitar el logado local para las líneas VTY y consola

```
PILDORA(config)#line console 0
```

```
PILDORA(config)#login local
```

PILDORA(config)#line vty 0 4

PILDORA(config)#login local

PILDORA(config)#

8.- Bloquear la línea VTY durante 15 minutos cuando se detecta 3 intentos fallidos durante 60 segundos

PILDORA(config)#login block-for 150 attempts 3 within 60

PILDORA(config)#

9.- Asociar una lista de acceso que permita a los dispositivos de administración (redes del router preservativo) acceder al router por línea VTY aunque el acceso esté bloqueado

PRESERVATIVO#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

PRESERVATIVO(config)#ip access-list standard PERMIT-ADMIN

PRESERVATIVO(config-std-nacl)#permit 172.16.1.0

PRESERVATIVO(config-std-nacl)#permit 172.16.6.0

PRESERVATIVO(config-std-nacl)#exit

PRESERVATIVO(config)#line vty 0 4

PRESERVATIVO(config-line)#access-class PERMIT-ADMIN in

PRESERVATIVO(config-line)#exit

PRESERVATIVO(config)#

10.- Cambiar el tiempo por defecto para login sucesivos a 5 segundos

PILDORA(config)#login delay 5 (no funciona el comando en el simulador)

PILDORA(config)#

11.- Registro de login fallidos y con éxito

PILDORA(config)#login on-success log

PILDORA(config)#login on-failure log

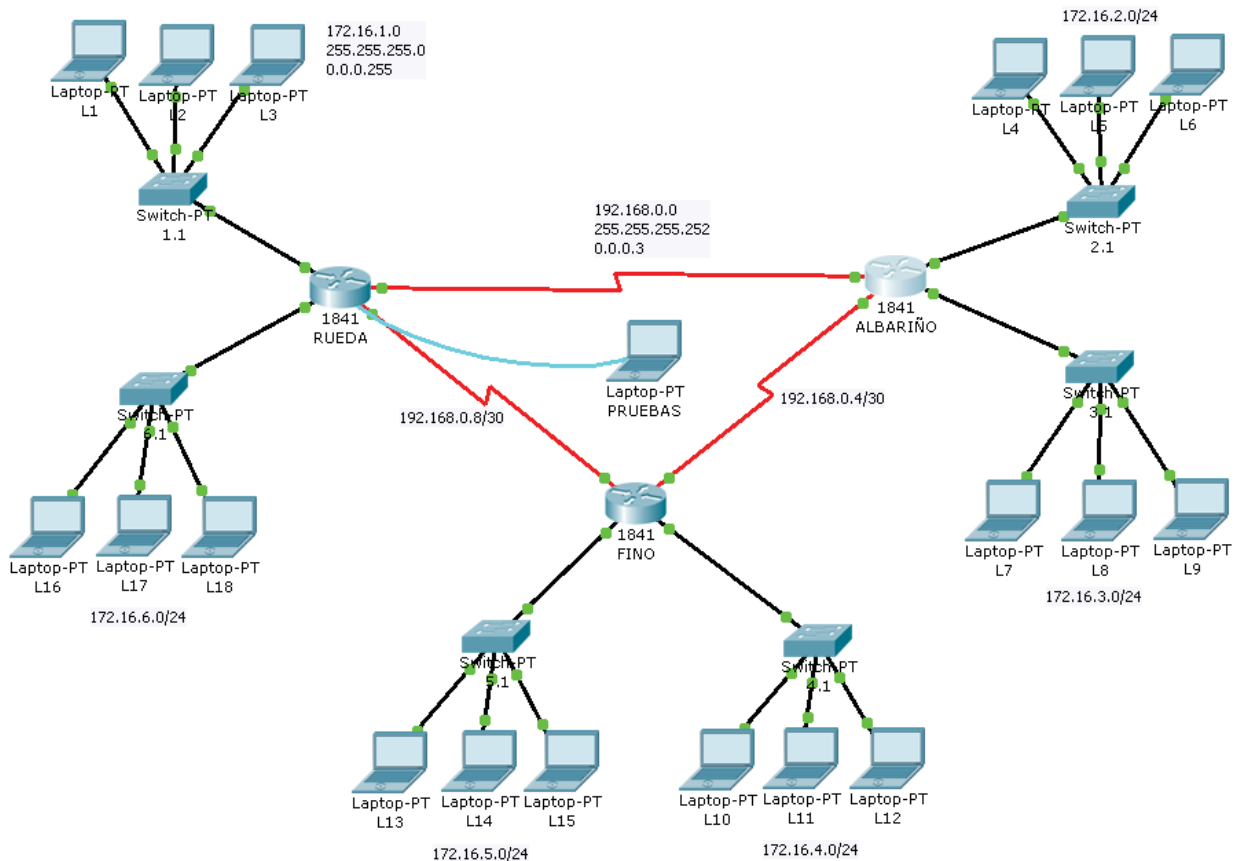
PILDORA(config)#

12.- Activar conexiones Telnet en los routers

PILDORA(config)#line vty 0 4

PILDORA(config-line)#transport input telnet

25.- Recuperación de contraseñas



1.- Configuración Básica (Ip por DHCP)

2.- Contraseña mínima de 10 caracteres

RUEDA(config)#security passwords min-length 10

3.- Configurar contraseña enable secret

RUEDA(config)#enable secret cisco12345

4.- Proceso Recuperación de Contraseña

Paso 1: conectar al puerto consola

Paso 2: reiniciar el router

Paso 3: emitir la secuencia de escape Ctrl+break (pausa) para entrar al modo ROMmon

Paso 4: escribir el comando **confreg 0x2142**

Paso 5: escribir el comando **reset** y el router se reinicia

Paso 6: responder no a la pregunta de acceso a setup

Paso 7: escribir **enable** para acceder a modo privilegiado

Paso 8: escribir **copy startup-config running-config**

Paso 9: escribir **show running**, las contraseñas descriptadas pueden seguir utilizandose, las encriptadas necesitan ser reconfiguradas

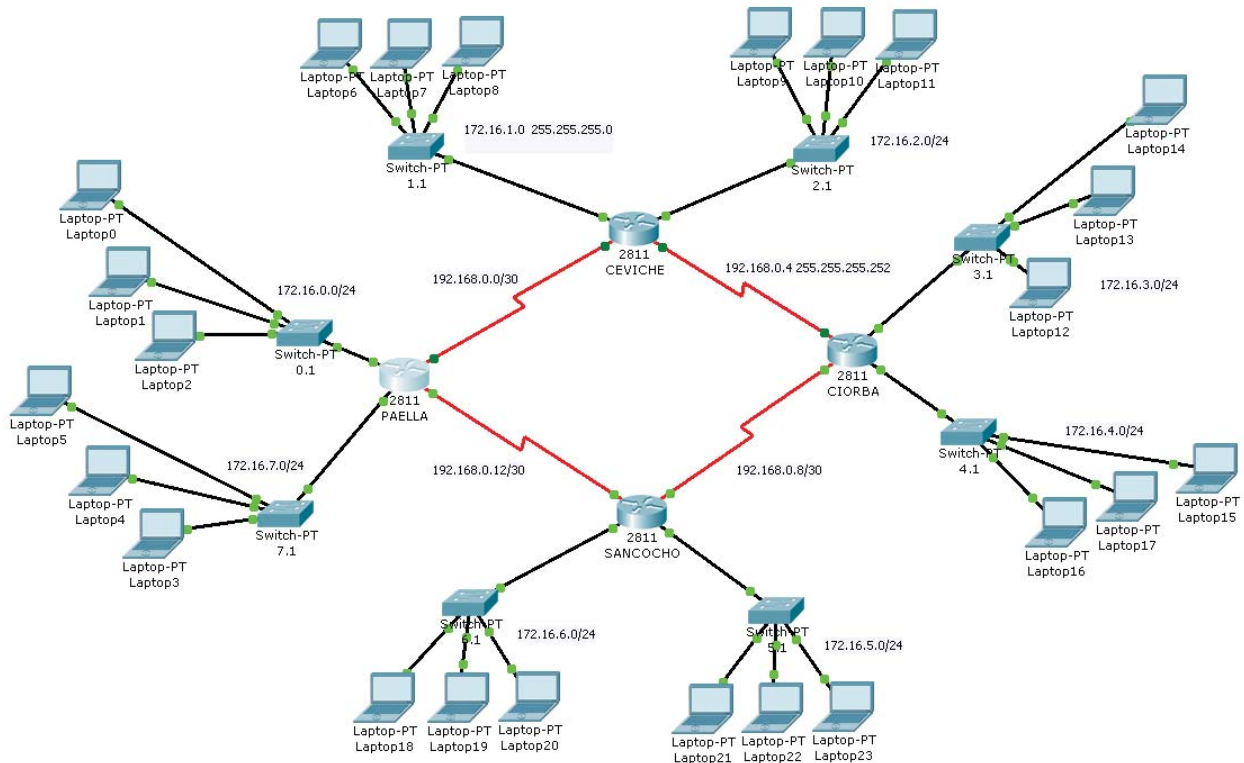
Paso 10: entra en el modo de configuración y configura una nueva enable secret

Paso 11: emite el comando **no shutdown** en las interfaces

Paso 12: escribe **config-register 0x2102**

Paso 13: guarda la configuración con el comando **copy running startup**

26.- Nivel de Privilegios



- 1.- Configuración Básica
- 2.- Protocolo de Enrutamiento EIGRP
- 3.- Crear 3 niveles de privilegios en cada router:
 - BASIC sólo puede utilizar el comando Ping
 - ADMIN-JUNIOR sólo puede utilizar el comando show running-config
 - ADMIN sólo puede utilizar los comandos reload, show ip route, show ip protocols, show ip interface brief
- 4.- Crear usuarios asociados a cada nivel de privilegios

EJEMPLO

```
R1# conf t
R1(config)# username USER privilege 1 secret cisco
R1(config)#
R1(config)# privilege exec level 5 ping
R1(config)# enable secret level 5 cisco5
R1(config)# username SUPPORT privilege 5 secret cisco5
R1(config)#
R1(config)# privilege exec level 10 reload
R1(config)# enable secret level 10 cisco10
R1(config)# username JR-ADMIN privilege 10 secret cisco10
R1(config)#
R1(config)# username ADMIN privilege 15 secret cisco123
R1(config)#
```

Creación de usuarios

```
PAELLA(config)#username basic password cisco12345
```

```
PAELLA(config)#username admin-junior password cisco12345
```

```
PAELLA(config)#username admin password cisco12345
```

Creación de usuarios desde la creación de privilegios

```
PAELLA(config)#enable secret level 2 ciscocisco
```

Creación de 3 niveles de privilegios

```
PAELLA>enable
```

```
PAELLA#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
PAELLA(config)#privilege exec level 2 ping
```

```
PAELLA(config)#username basic privilege 2
```

```
PAELLA(config)#privilege exec level 3 show running-config
```

```
PAELLA(config)#username admin-junior privilege 3
```

```
PAELLA(config)#privilege exec level 4 reload
```

```
PAELLA(config)#privilege exec level 4 show ip route
```

```
PAELLA(config)#privilege exec level 4 show ip protocols
```

```
PAELLA(config)#privilege exec level 4 show ip interface brief
```

```
PAELLA(config)#username admin privilege 4
```

```
PAELLA(config)#exit
```

```
PAELLA#
```

SHOW RUNNING-CONFIG

```
PAELLA#show running-config
```

```
Building configuration...
```

```
Current configuration : 1682 bytes
```

```
version 12.4
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
no service password-encryption
```

```
hostname PAELLA
```

```
!
```

```
enable secret level 2 5 $1$mERr$2kSZR9DN2ofxL11bGij.S1
```

```
enable secret level 3 5 $1$mERr$2kSZR9DN2ofxLllbGij.S1
enable secret level 4 5 $1$mERr$2kSZR9DN2ofxLllbGij.S1
enable secret 5 $1$mERr$2kSZR9DN2ofxLllbGij.S1
!
ip dhcp pool red1
    network 172.16.0.0 255.255.255.0
    default-router 172.16.0.1
ip dhcp pool red2
    network 172.16.7.0 255.255.255.0
    default-router 172.16.7.1
!
username admin privilege 4 password 0 cisco12345
username admin-junior privilege 3 password 0 cisco12345
username administrador password 0 ciscociscocisco
username basic privilege 2 password 0 cisco12345
!
interface FastEthernet0/0
    ip address 172.16.0.1 255.255.255.0
    duplex auto
    speed auto
!
interface FastEthernet0/1
    ip address 172.16.7.1 255.255.255.0
    duplex auto
    speed auto
!
interface Serial0/3/0
    ip address 192.168.0.1 255.255.255.252
    clock rate 64000
!
interface Serial0/3/1
```



```
ip address 192.168.0.13 255.255.255.252

!

interface Vlan1

  no ip address

  shutdown

!

router eigrp 1

  network 172.16.0.0

  network 192.168.0.0

  no auto-summary

!

ip classless

!

privilege exec level 2 ping
privilege exec level 4 reload
privilege exec level 4 show
privilege exec level 4 show ip
privilege exec level 4 show ip interface
privilege exec level 4 show ip protocols
privilege exec level 4 show ip route
privilege exec level 4 show ipv6
privilege exec level 4 show ipv6 interface
privilege exec level 4 show ipv6 protocols
privilege exec level 4 show ipv6 route
privilege exec level 3 show running-config

!

line con 0

  login local

line vty 0 4

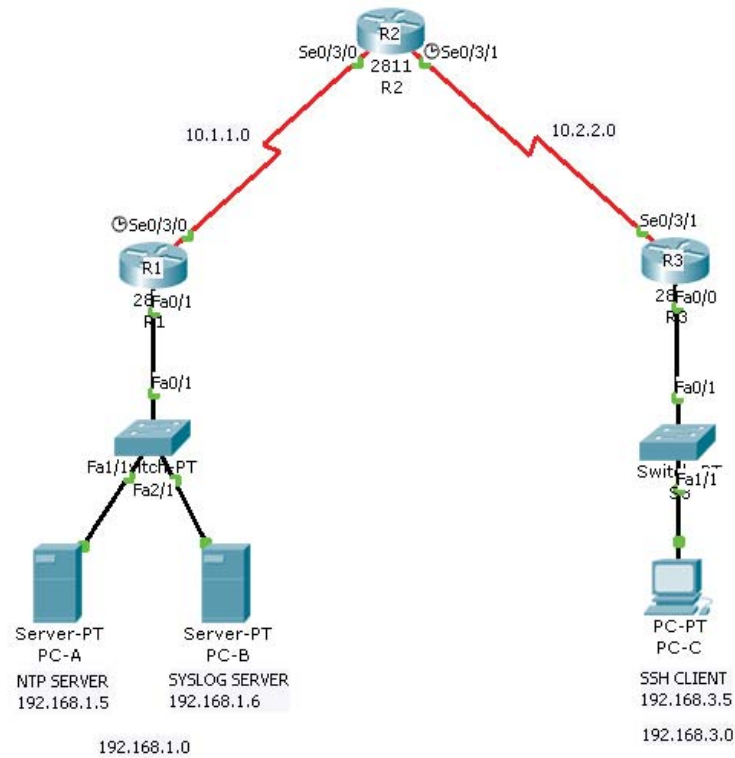
  login local

!
```

end

PAELLA#

LABORATORIO 2 (NTP-SSH)



- Contraseña Enable **ciscoenpa55**
- Contraseña para línea VTY **ciscovtypa55**
- Contraseña para línea SSH **ciscosshpa55**
- Enrutamineto Estático

```
R1>enable
```

```
R1#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R1(config)#ip route 192.168.3.0 255.255.255.0 10.1.1.2
```

```
R1(config)#
```

```
R3> enable
```

```
R3# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R3(config)#ip route 192.168.1.0 255.255.255.0 10.2.2.2
```

```
R3(config)#
```

```
R2> enable
```

```
R2# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
R2(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

```
R2(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
```

```
R2(config)#
```

Activar conexiones Telnet en los routers

```
R1(config)#line vty 0 4
```

```
R1(config-line)#transport input telnet
```

Seguidamente tenemos que crear los usuarios telnet para probar las conexiones telnet

Para encriptar los datos en la comunicación

```
R3(config)#crypto key generate rsa
```

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

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R3(config)#
```

1.- Configure routers as NTP Clients

Configurar R1, R2 y R3 como clientes NTP

```
R1(config)# ntp server 192.168.1.5
```

```
R2(config)# ntp server 192.168.1.5
```

```
R3(config)# ntp server 192.168.1.5
```

Comando de verificación **show ntp status**

Configurar los routers para actualizar el reloj de hardware

```
R1(config)# ntp update-calendar
```

```
R2(config)# ntp update-calendar
```

```
R3(config)# ntp update-calendar
```

Comando de verificación `show clock`

Configurar routers de mensajes de registro de fecha y hora

```
R1(config)# service timestamps log datetime msec
R2(config)# service timestamps log datetime msec
R3(config)# service timestamps log datetime msec
```

2.- Configure routers to log messages to the Syslog Server

Configurar los routers para identificar el host remoto (servidor syslog) que recibirá los mensajes de registro

```
R1(config)# logging host 192.168.1.6
R2(config)# logging host 192.168.1.6
R3(config)# logging host 192.168.1.6
```

Comando de verificación `show logging`

3.- Configure R3 to support SSH connections

Configure el nombre de dominio `ccnasecurity.com` en el router R3

```
R3(config)# ip domain-name ccnasecurity.com
```

Configurar los usuarios de inicio de sesión desde el cliente de SSH en R3.

Crear un ID de usuario de SSHadmin con el nivel de privilegio más alto posible y una contraseña secreta de `ciscosshpa55`

```
R3(config)# username SSHadmin privilege 15 secret ciscosshpa55
```

Configure las líneas vty entrantes en R3

Utilizar las cuentas de usuario locales para el acceso y validación obligatoria. Aceptar sólo las conexiones SSH

```
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

Para encriptar los datos en la comunicación

```
R3(config)#crypto key generate rsa
```

```
The name for the keys will be: R3.ccnasecurity.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512]: 1024
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

```
R3(config)#
```

Configurar tiempos de espera y los parámetros de autenticación SSH

Los tiempos de espera por defecto SSH y parámetros de autenticación puede ser alterado para ser más restrictivos. Establezca el tiempo de espera a 90 segundos, el número de reintentos de autenticación a 2, y la versión a 1

```
R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
R3(config)# ip ssh version 1
```

Comando de verificación **show ip ssh**

VERIFICACIÓN

Abra el escritorio de la PC-C. Seleccione el icono del símbolo del sistema. Desde el PC-C, escriba el comando para conectarse a R3 a través de Telnet

```
PC> telnet 192.168.3.1
```

Esta conexión falla, ya que R3 se ha configurado para aceptar sólo las conexiones SSH en las líneas de terminal virtual.

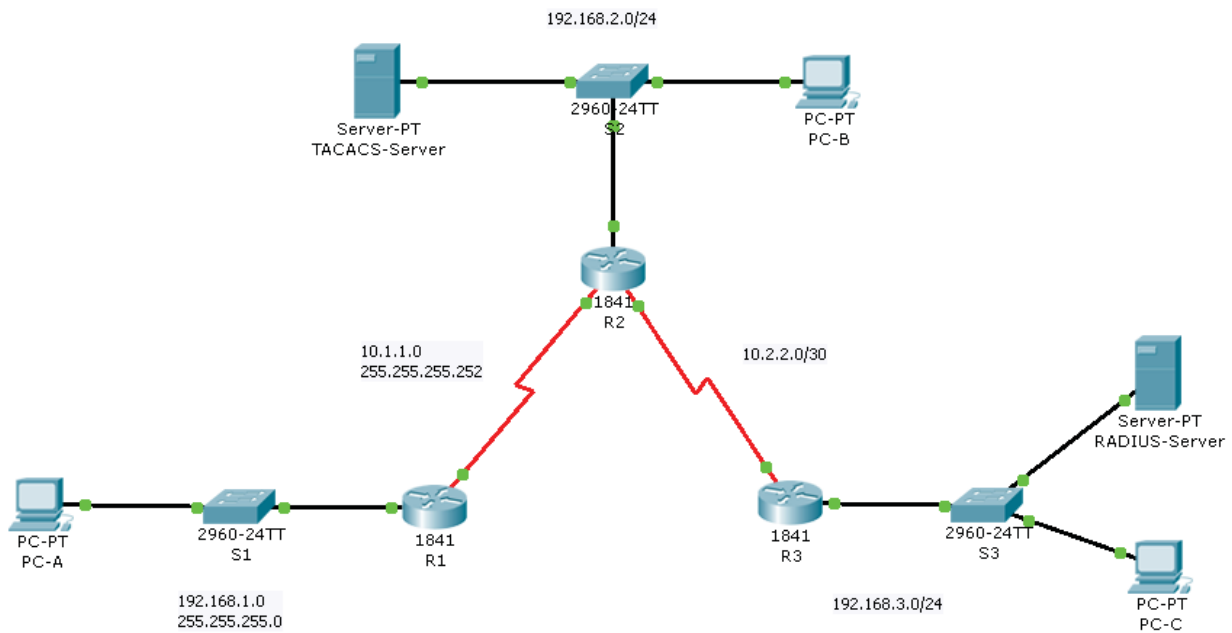
Abra el escritorio de la PC-C. Seleccione el icono del símbolo del sistema. Desde el PC-C, escriba el comando para conectarse a R3 a través de SSH. Cuando se le pida la contraseña, introduzca la contraseña configurada para el administrador: **ciscosshpa55**

```
PC> ssh -l SSHadmin 192.168.3.1
```

Con el fin de solucionar problemas y mantener el router R3, el administrador en el ISP debe utilizar SSH para acceder a la CLI del router. Desde el CLI de R2, escriba el comando para conectarse a través de R3 versión 1 de SSH utilizando la cuenta de usuario SSHadmin. Cuando se le pida la contraseña, introduzca la contraseña configurada para el administrador: **ciscosshpa55**

```
R2# ssh -v 1 -l SSHadmin 10.2.2.1
```

LABORATORIO 3 (AAA)



La topología de red muestra los routers R1, R2 y R3. En la actualidad toda la seguridad administrativa se basa en el conocimiento de la contraseña secreta de activación. Su tarea consiste en configurar y probar las soluciones de AAA local y basado en el servidor.

Va a crear una cuenta de usuario local y configurar AAA local en el router R1 para probar la consola y los inicios de sesión VTY.

- Cuenta de usuario: **Admin1** Contraseña: **admin1pa55**

A continuación, configurar el router R2 para apoyar la autenticación basada en servidor utilizando el protocolo TACACS +. El servidor TACACS + se ha pre-configurado con lo siguiente:

- Cliente: **R2** utilizando la clave: **tacacspa55**
- Cuenta de usuario: **Admin2** Contraseña: **admin2pa55**

Por último, va a configurar el router R3 para apoyar la autenticación basada en servidor utilizando el protocolo RADIUS. El servidor RADIUS se ha pre-configurado con lo siguiente:

- Cliente: **R3** utilizando la clave: **radiuspa55**
- Cuenta de usuario: **Admin3** Contraseña: **admin3pa55**

Los routers también han sido pre-configurado con los siguientes:

- Habilitar contraseña encriptada: **ciscoenpa55**
- RIP versión 2

Configure un usuario local:Admin1 y una contraseña: admin1pa55.

```
R1(config)# username Admin1 password admin1pa55
```

Activar AAA en R1 y configurar la autenticación AAA para la consola de acceso para utilizar la base de datos local.

```
R1(config)# aaa new-model  
R1(config)# aaa authentication login default local
```

Configuración de la línea de consola a utilizar el método de autenticación definido AAA.

```
R1(config)# line console 0
R1(config-line)# login authentication default
```

Verifique el método de autenticación AAA

```
R1(config-line)# end

%SYS-5-CONFIG_I: Configured from console by console
R1# exit

R1 con0 is now available
Press RETURN to get started.

***** AUTHORIZED ACCESS ONLY *****
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification
Username: Admin1
Password: admin1pa55
R1>
```

Configuración de la autenticación local AAA para las líneas vty en el R1

Configurar una lista con nombre denominado TELNET LOGIN para autenticar inicios de sesión con AAA local.

```
R1(config)# aaa authentication login TELNET-LOGIN local
```

Configure las líneas vty a utilizar el método denominado AAA.

```
R1(config)# line vty 0 4

R1(config-line)# login authentication TELNET-LOGIN

R1(config-line)# end
```

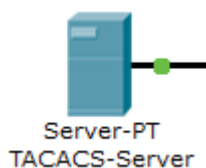
Verifique la configuración Telnet. Desde el símbolo del sistema del PC-A, Telnet a R1.

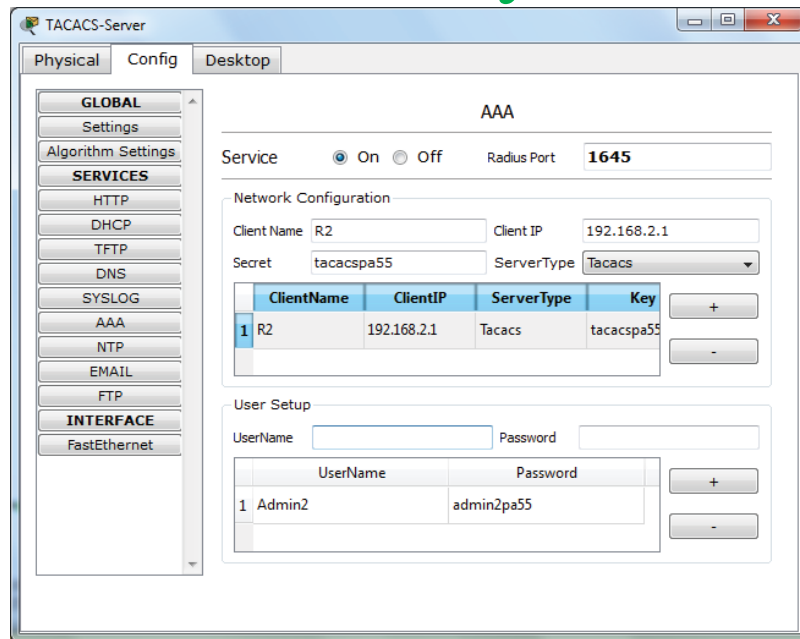
```
PC> telnet 192.168.1.1

***** AUTHORIZED ACCESS ONLY *****
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

User Access Verification
Username: Admin1
Password:
```

Configurar el servidor de autenticación basada en AAA utilizando TACACS + en R2





A los efectos de copia de seguridad, configurar un nombre de usuario local de contraseña de administrador y el secreto de adminpa55

```
R2(config)# username Admin password adminpa55
```

Configurar el servidor AAA TACACS dirección IP y la clave secreta en R2

```
R2(config)# tacacs-server host 192.168.2.2
R2(config)# tacacs-server key tacacspa55
```

Activar AAA en el R2 y configurar todos los inicios de sesión para autenticar en el servidor TACACS y si no está disponible, a continuación, utilizar la base de datos local

```
R2(config)# aaa new-model
R2(config)# aaa authentication login default group tacacs+ local
```

Configurar la autenticación AAA para los accesos de la línea de consola y utilizar el método de acceso predeterminado el de autenticación AAA

```
R2(config)# line console 0
R2(config-line)# login authentication default
```

Compruebe la conexión del usuario EXEC con la AAA servidor TACACS +

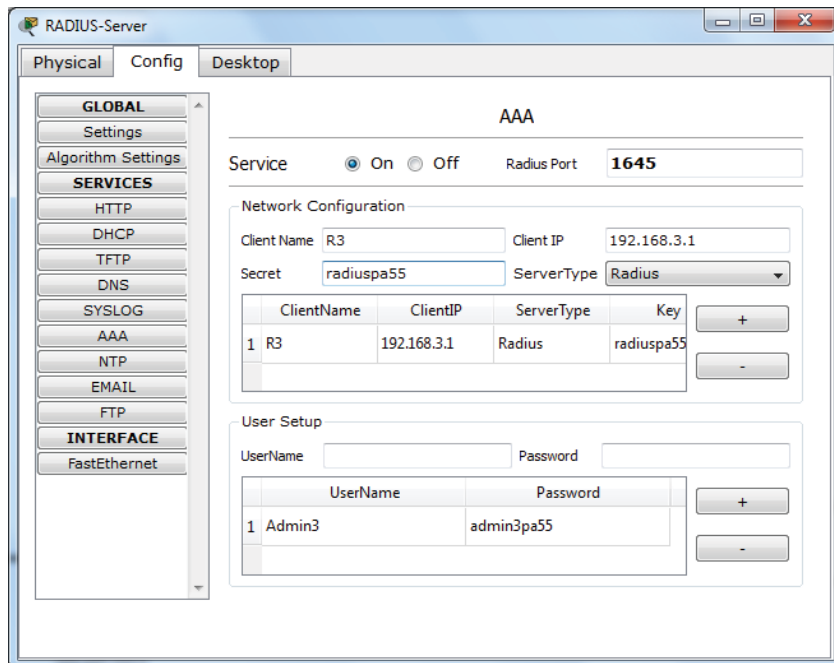
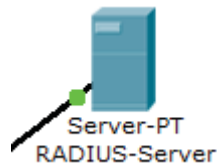
```
R2(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R2# exit
R2 con0 is now available
```

Press RETURN to get started.

```
***** AUTHORIZED ACCESS ONLY *****
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
```

```
User Access Verification
Username: Admin2
Password: admin2pa55
R2>
```


Configurar el servidor de autenticación basada en AAA Usar RADIUS en R3



A los efectos de copia de seguridad, configurar un nombre de usuario local de contraseña de administrador y el secreto de adminpa55

```
R3(config)# username Admin password adminpa55
```

Configurar el servidor RADIUS AAA dirección IP y la clave secreta en R3

```
R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55
```

Activar AAA en R3 y configurar todos los inicios de sesión para autenticar con el servidor RADIUS AAA y si no está disponible, a continuación, utilizar la base de datos local

```
R3(config)# aaa new-model
R3(config)# aaa authentication login default group radius local
```

Configurar la autenticación AAA para la consola de acceso para utilizar el método predeterminado de autenticación AAA

```
R3(config)# line console 0
R3(config-line)# login authentication default
```

Compruebe la conexión del usuario EXEC con la AAA servidor RADIUS +

```
R3(config-line)# end
%SYS-5-CONFIG_I: Configured from console by console
R3# exit
R3 con0 is now available
```

Press RETURN to get started.

***** AUTHORIZED ACCESS ONLY *****
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.

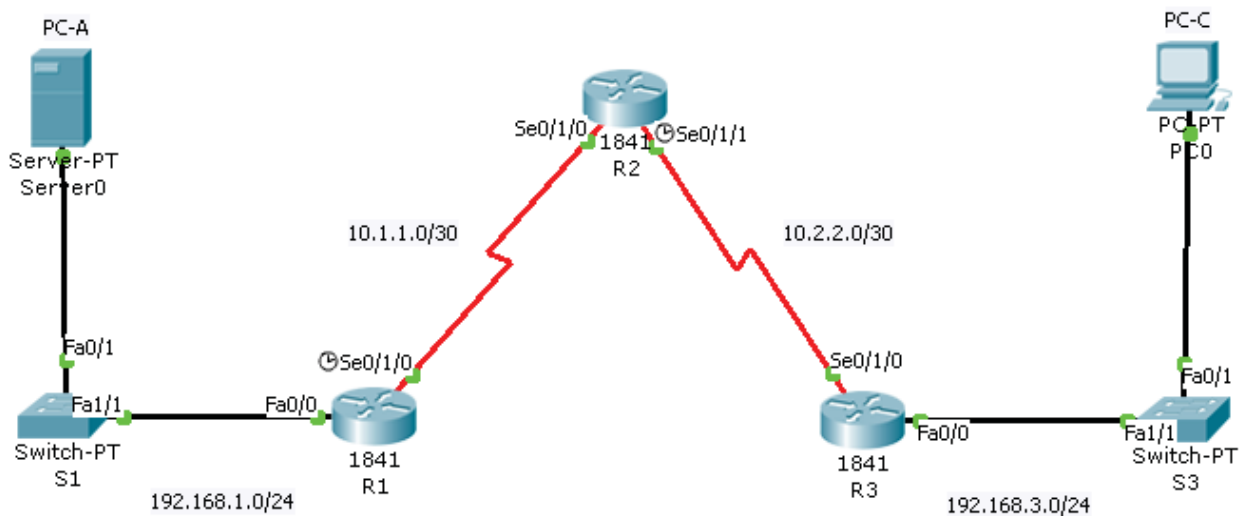
User Access Verification

Username: **Admin3**

Password: **admin3pa55**

R3>

LABORATORIO 4 (ACL)



- Contraseña enable: **ciscoenpa55**
- Contraseña línea de consola: **ciscoconpa55**
- Usuario para la línea VTY: **SSHadmin**
- Contraseña para la línea VTY: **ciscosshpa55**
- Enrutamiento estático

Desde el PC-C mandar una conexión SSH hasta la interfaz Loopback 0 del R2. Salir de la sesión SSH

Configuración de SSH en el R2

Configurar un nombre de dominio:

```
R3(config)# ip domain-name ccnasecurity.com
```

Configurar los usuarios de inicio de sesión desde el cliente de SSH en R 3

```
R3(config)# username SSHadmin privilege 15 secret ciscosshpa55
```

Utilizar las cuentas de usuario locales para el acceso y validación obligatoria. Aceptar sólo las conexiones SSH

```
R3(config)# line vty 0 4  
R3(config-line)# login local  
R3(config-line)# transport input ssh
```

Generar las claves para encriptar el tráfico SSH utilizando el algoritmo RSA. Tamaño de módulo mínimo recomendado de 1024

```
R3(config)#crypto key generate rsa
```

Si no existen claves, es posible que reciba este mensaje: % No Signature RSA Keys found in configuration.

El router utiliza el par de claves RSA para la autenticación y el cifrado de los datos transmitidos por SSH. Configure las llaves RSA con un módulo de 1024. El valor por defecto es 512, y el rango es de 360 a 2048

```
R3(config)# crypto key generate rsa [Enter]
```

```
The name for the keys will be: R3.ccnasecurity.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Los tiempos de espera por defecto SSH y parámetros de autenticación puede ser alterado para ser más restrictivos. Establezca el tiempo de espera a 90 segundos, el número de reintentos de autenticación a 2, y la versión la 1

```
R3(config)# ip ssh time-out 90
R3(config)# ip ssh authentication-retries 2
R3(config)# ip ssh version 1
```

Configuración de una ACL para bloquear todo el acceso remoto a los routers excepto el de PC-C

```
R1(config)# access-list 10 permit 192.168.3.3 0.0.0.0
R2(config)# access-list 10 permit 192.168.3.3 0.0.0.0
R3(config)# access-list 10 permit 192.168.3.3 0.0.0.0
```

Utilice el comando access-class para aplicar la lista de acceso para el tráfico entrante en las líneas vty

```
R1(config-line)# access-class 10 in
R2(config-line)# access-class 10 in
R3(config-line)# access-class 10 in
```

SSH a 192.168.2.1 desde el PC-C (en caso de tener éxito). SSH a 192.168.2.1 desde el PC-A (falla)

```
PC> ssh -l SSHadmin 192.168.2.1
```

Configurar ACL 100 para bloquear todo el tráfico específico de la red de salidas

```
R3(config)# access-list 100 deny ip 10.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 172.16.0.0 0.15.255.255 any
R3(config)# access-list 100 deny ip 192.168.0.0 0.0.255.255 any
R3(config)# access-list 100 deny ip 127.0.0.0 0.255.255.255 any
R3(config)# access-list 100 deny ip 224.0.0.0 15.255.255.255 any
R3(config)# access-list 100 permit ip any any
```

Asociar la lista de acceso a la interfaz serial del R3

```
R3(config)# interface s0/1/0
R3(config-if)# ip access-group 100 in
```

Elimine la ACL. De lo contrario, todo el tráfico desde la red externa (siendo abordado con direcciones IP de origen privado) se negó durante el resto de la actividad

```
R3(config)# interface s0/0/1
R3(config-if)# no ip access-group 100 in
```

Denegar todos los paquetes de salida con dirección de origen fuera del rango de direcciones IP internas.
Configurar la ACL 110 para permitir sólo el tráfico de la red 192.168.3.0

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 any
```

Asociar la lista de acceso a la interfaz Fa0/0

```
R3(config)# interface fa0/0  
R3(config-if)# ip access-group 110 in
```

Permitirá que cualquier host externo para acceder al DNS, SMTP y FTP en el servidor de PC-A, negará cualquier acceso a los servicios de HTTPS en el PC-A, y permitirá que PC-C para acceder a R1 a través de SSH

```
R1(config)# access-list 120 permit udp any host 192.168.1.3 eq domain  
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq smtp  
R1(config)# access-list 120 permit tcp any host 192.168.1.3 eq ftp  
R1(config)# access-list 120 deny tcp any host 192.168.1.3 eq 443  
R1(config)# access-list 120 permit tcp host 192.168.3.3 host 10.1.1.1 eq
```

22

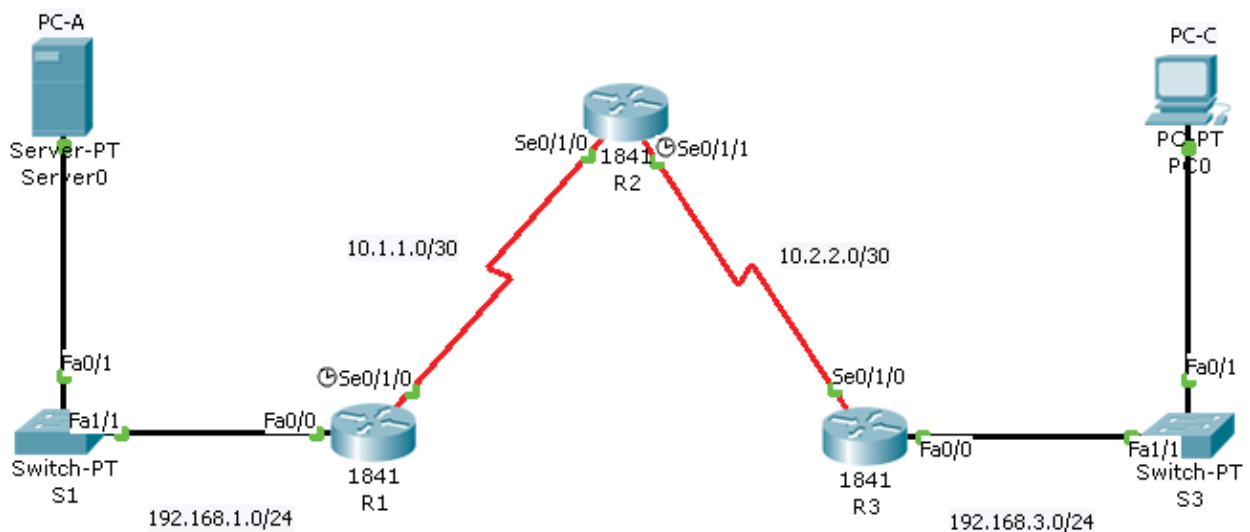
Asociar la lista de acceso a la interfaz serial 0/1/0

```
R1(config)# interface s0/0/0  
R1(config-if)# ip access-group 120 in
```

Permiso de respuestas de eco ICMP y mensajes de destino inaccesible desde la red externa (en relación con R1); negará todos los otros paquetes ICMP entrantes

```
R1(config)# access-list 120 permit icmp any any echo-reply  
R1(config)# access-list 120 permit icmp any any unreachable  
R1(config)# access-list 120 deny icmp any any  
R1(config)# access-list 120 permit ip any any
```

LABORATORIO 4 (CBAC)



- Contraseña de enable: **ciscoenpa55**
- Contraseña para las línea de consola: **ciscoconpa55**
- Contraseña para las líneas VTY: **ciscovtypa55**

- Enrutamiento estático

Hacer Telnet en el Router R2 en la interfaz S0/1/0 con al dirección IP 10.1.1.2. Salir de la sesión Telnet.

Lista de acceso extendida

```
R3 (config) # ip access-list extended OUT-IN
R3 (config-ext-nacl) # deny ip any any
R3 (config-ext-nacl) # exit
```

Aplicar la ACL a la interfaz S 0/1/0

```
R3 (config) # interfaz S0/1/0
R3 (config-if) # ip access-group-OUT IN in
```

Crear una regla de inspección

```
R3(config)# ip inspect name IN-OUT-IN icmp
R3(config)# ip inspect name IN-OUT-IN telnet
R3(config)# ip inspect name IN-OUT-IN http
```

Utilice una regla de inspección para activar los mensajes de auditoría CBAC para proporcionar un registro de acceso a la red a través del firewall, incluyendo los intentos de acceso ilegítimo. Habilitar el registro en el servidor syslog, 192.168.1.3. Asegúrese de que los mensajes registrados son de su fecha.

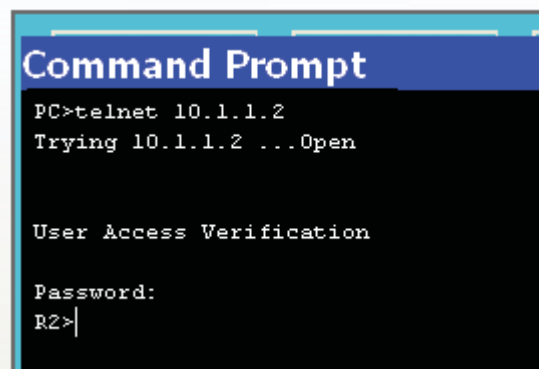
```
R3(config)# ip inspect audit-trail
R3(config)# service timestamps debug datetime msec
R3(config)# logging host 192.168.1.3
```

Aplica la regla de inspección para visualizar el tráfico en la interfaz se0/1/0

```
R3(config)#interface se0/1/0
R3(config-if)# ip inspect IN-OUT-IN out
```

Verificar la funcionalidad del Firewall

Abre una sesión Telnet desde el PC-C a el router R2



```
Command Prompt
PC>telnet 10.1.1.2
Trying 10.1.1.2 ...Open

User Access Verification

Password:
R2>
```

Comando Show de verificación de sesiones

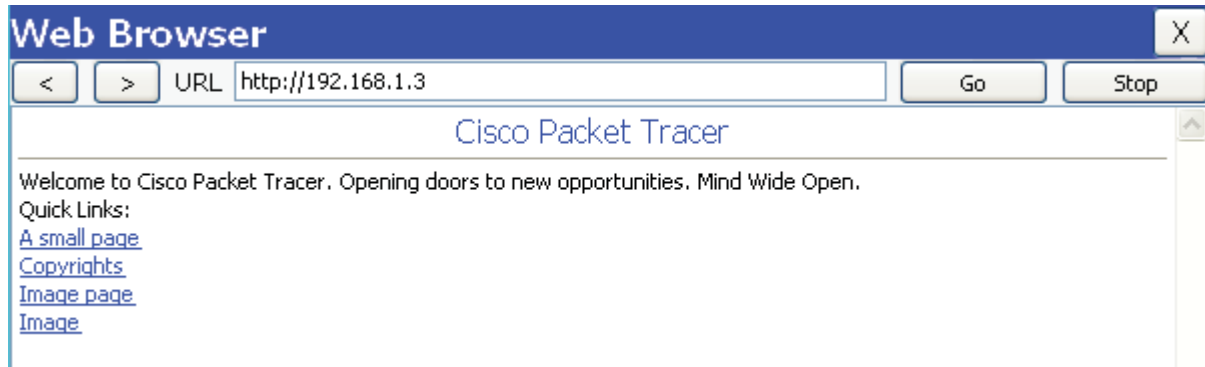
```
R3# show ip inspect sessions
```

```
Established Sessions
Session 100424296 (192.168.3.3:1031)=>(10.1.1.2:23) telnet SIS_OPEN
```

¿Cuál es la dirección IP de origen y número de puerto? 192.168.3.3:1031 (port 1031 is random)

¿Cuál es la dirección IP de destino y número de puerto? 10.1.1.2:23 (Telnet = port 23)

Abre un navegador web desde el PC-C con la dirección Ip del servidor PC-A (192.168.1.3)



R3# show ip inspect sessions

```
Established Sessions
Session 104637440 (192.168.3.3:1032)=>(192.168.1.3:http SIS_OPEN
```

¿Cuál es la dirección IP de origen y número de puerto? 192.168.3.3:1027 (port 1032 israndom)

¿Cuál es la dirección IP de destino y número de puerto? 192.168.1.3:80 (HTTP web = port 80)

Comando show ip inspect en la interfaz R3

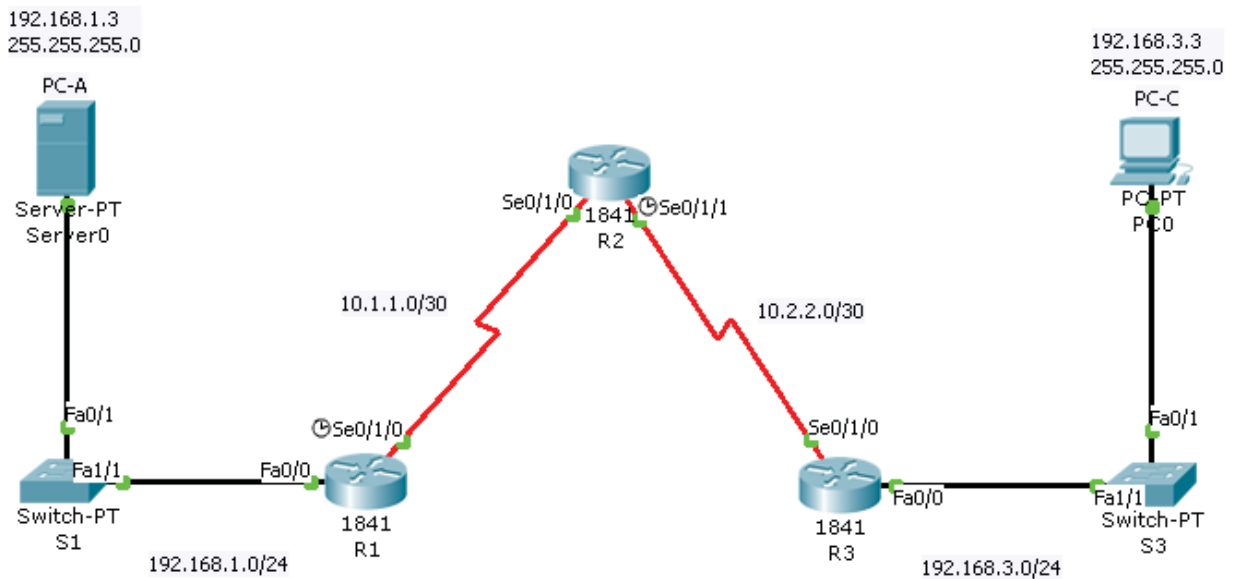
R3# show ip inspect interfaces

```
Interface Configuration
Interface Serial0/1/0
Inbound inspection rule is not set
Outgoing inspection rule is IN-OUT-IN
icmp alert is on audit-trail is on timeout 10
telnet alert is on audit-trail is on timeout 3600
http alert is on audit-trail is on timeout 3600
Inbound access list is OUT-IN
Outgoing access list is not set
```

R3# show ip inspect config

```
Session audit trail isenabled
Session alert is enabled
one-minute (sampling period) thresholds are [unlimited : unlimited]
connections
max-incomplete sessions thresholds are [unlimited : unlimited]
max-incomplete tcp connections per host is unlimited. Block-time 0
minute
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
tcp reassembly queue length 16; timeout 5 sec; memory-limit 1024 kilo
bytes
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name IN-OUT-IN
icmp alert is on audit-trail is off timeout 10
telnet alert is on audit-trail is off timeout 3600
http alert is on audit-trail is off timeout 3600
```

LABORATORIO 4 (ZPB)



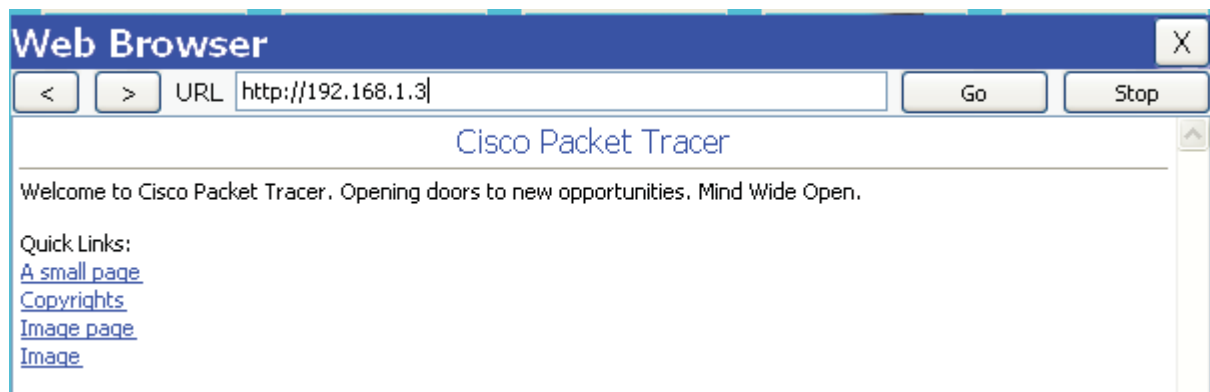
- Contraseña de consola: **ciscoconpa55**
- Contraseña de línea VTY: **ciscovtypa55**
- Contraseña de enable: **ciscoenpa55**
- Enrutamiento estático

Désde el símbolo de sistema del PC-C hacer Telnet a el R2 (10.2.2.2). Salir de la sesión de Telnet

```
R2(config)#line vty 0 4
```

```
R2(config-line)#transport input telnet
```

Haga clic en la ficha Escritorio y haga clic en la aplicación de navegador Web. Introduzca el PC una dirección IP 192.168.1.3 en la dirección URL. El Packet Tracer mostrará la página web de bienvenida del servidor Web



Crear las zonas de firewall en el router R3

Zona Interna

```
R3(config)# zone security IN-ZONE
```

Zona Externa

```
R3(config)# zone security OUT-ZONE
```

Definir la lista de acceso para definir el tráfico

Utilice el comando access-list para crear ACL extendida 101 para permitir todos los protocolos IP de la red de origen 192.168.3.0/24 hacia cualquier destino

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

Crear un Mapa de Clase llamado IN-NETCLASS-MAP

```
R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP
R3(config-cmap)# match access-group 101
R3(config-cmap)# exit
```

Especificar las Políticas Firewall

Crear un mapa de la política llamado EN-2-OUT-PMAP

```
R3(config)# policy-map type inspect IN-2-OUT-PMAP
```

Especifique la acción de la inspección de este mapa de la política

```
R3(config-pmap-c)# inspect
%No specific protocol configured in class IN-NET-CLASS-MAP for
inspection.
All protocols will be inspected
```

Aplicar las Políticas Firewall

Usando el comando de seguridad crear un par de zona denominada EN-2-OUT-ZPAIR. Especificar el origen y las zonas de destino que se crearon en la Tarea 1

```
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination
OUT-ZONE
```

Adjuntar un mapa de la formulación de políticas y sus acciones asociadas a la par de la zona utilizando el tipo de política-servicio inspeccione el mando y hacer referencia al mapa de la política ha creado anteriormente, EN-2-OUT-PMAP

```
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
R3(config-sec-zone-pair)# exit
R3(config)#
```

Utilice el comando de zona de seguridad-miembro en el modo de interfaz de configuración para asignar Fa0/0 de IN-ZONE y Se0/1/0 en OUT-ZONE

```
R3(config)# interface fa0/0
R3(config-if)# zone-member security IN-ZONE
R3(config-if)# exit
R3(config)# interface se0/1/0
R3(config-if)# zone-member security OUT-ZONE
R3(config-if)# exit
```

Prueba de funcionalidad de firewall de IN-ZONE en OUT-ZONE

Desde el PC-C Símbolo del sistema, telnet a R2 en 10.2.2.2 y proporcionar la contraseña de vty ciscovtpa55

El telnet debe tener éxito. Mientras que la sesión de Telnet está activo, ejecute el comando show políticas de tipo de mapa inspeccionar la zona par de sesiones en R3 para ver las sesiones establecidas


```
R3# show policy-map type inspect zone-pair sessions
```

```
Zone-pair: IN-ZONE-OUT-ZONE
```

```
Service-policy inspect : IN-2-OUT-PMAP
```

```
Class-map: IN-NET-CLASS-MAP (match-all)
```

```
Match: access-group 101
```

```
Inspect
```

```
Established Sessions
```

```
Session 139644744 (192.168.3.3:1025)=>(10.2.2.2:23) telnet:tcp
```

```
SIS_OPEN
```

```
Created 00:00:02, Last heard 00:00:00
```

```
Bytes sent (initiator:responder) [0:0]
```

¿Cuál es la dirección IP de origen y número de puerto? 192.168.3.3:1025 (port 1025 is random)

¿Cuál es la dirección IP de destino y número de puerto? 10.2.2.2:23 (Telnet = port 23)

Introduzca la dirección IP del servidor 192.168.1.3 en el campo de URL del navegador y haga clic en Go. La sesión de HTTP debe tener éxito. Si bien la sesión HTTP está activo, ejecute el comando show políticas de tipo de mapa inspeccionar la zona par de sesiones en R3 para ver las sesiones establecidas

```
R3# show policy-map type inspect zone-pair sessions
```

```
Zone-pair: IN-ZONE-OUT-ZONE
```

```
Service-policy inspect : IN-2-OUT-PMAP
```

```
Class-map: IN-NET-CLASS-MAP (match-all)
```

```
Match: access-group 101
```

```
Inspect
```

```
Established Sessions
```

```
Session 139142400 (192.168.3.3:1027)=>(192.168.1.3:80)
```

```
http:tcp SIS_OPEN
```

```
CCNA Security
```

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information. Page 5 of 5

```
Created 00:00:02, Last heard 00:00:00
```

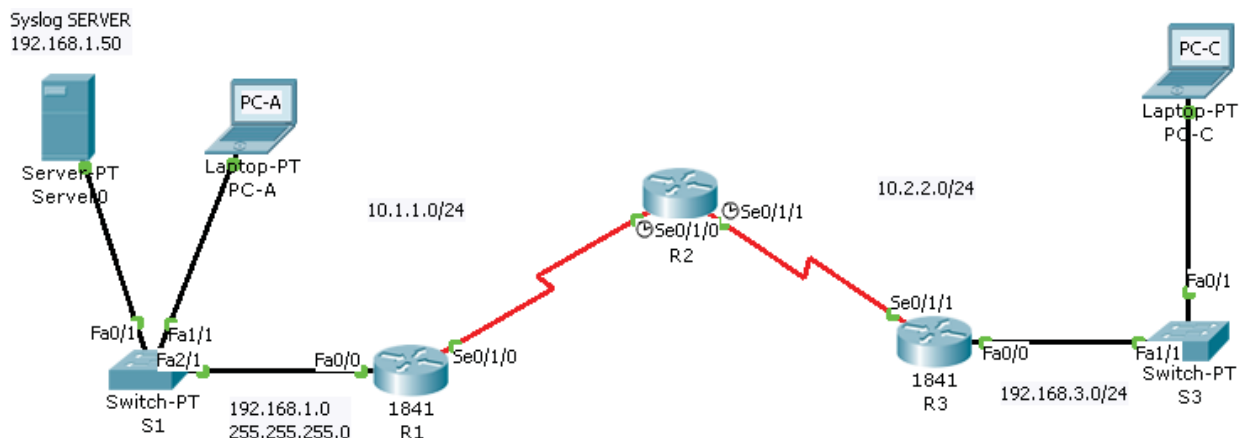
```
Bytes sent (initiator:responder) [0:0]
```

¿Cuál es la dirección IP de origen y número de puerto? 192.168.3.3:1027 (port 1027 is random)

¿Cuál es la dirección IP de destino y número de puerto? 192.168.1.3:80 (HTTP web = port 80)

Prueba de funcionalidad de firewall de IN-ZONE / OUT-ZONE

LABORATORIO 5 (CONFIGURACIÓN IOS)



Cree un directorio de configuración de IOS IPS en flash

```
R1#mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir
```

Para verificar que hemos creado bien el directorio, hacemos:

```
R1#dir flash:
Directory of flash:/

   3  -rw-     33591768      <no date>  c1841-advipservicesk9-mz.124-
15.T1.bin
   4  drw-         0      <no date>  ipsdir
   2  -rw-     28282      <no date>  sigdef-category.xml
   1  -rw-     227537      <no date>  sigdef-default.xml

64016384 bytes total (30168797 bytes free)
```

En el router R1, configurar la firma IPS ubicación de almacenamiento para ser el directorio que acaba de crear

```
R1(config)#ip ips config location flash:ipsdir
```

En el router R1, crear un nombre de regla de IPS con el nombre de comando ip ips nombre en el modo de configuración global. El nombre de las reglas IPS es iosips

```
R1(config)# ip ips name iosips
```

IOS IPS apoya el uso de syslog para enviar la notificación de eventos. Syslog notificación está activada por defecto. Si se habilita el registro de la consola, ver los mensajes de syslog IPS. Habilitar syslog si no está habilitado

```
R1(config)# ip ips notify log
```

Utilice el comando de ajuste del reloj del modo EXEC privilegiado para reajustar el reloj si es necesario

```
R1# clock set 01:20:00 6 january 2009
```

Compruebe que el servicio de marca de hora para el registro está habilitado en el router mediante el comando show run. Habilitar el servicio de marca de tiempo si no está habilitado

```
R1(config)# service timestamps log datetime msec
```

Enviar mensajes de registro al servidor Syslog en la dirección IP 192.168.1.50

```
R1(config)# logging host 192.168.1.50
```

Configurar IPS IOS para utilizar las categorías de la firma

```
R1(config)#ip ips signature-category
R1(config-ips-category)#category all
R1(config-ips-category-action)#retired true
R1(config-ips-category-action)#exit
R1(config-ips-category)#category ios_ips basic
R1(config-ips-category-action)#retired false
R1(config-ips-category-action)#exit
R1(config-ips-category)#exit

Do you want to accept these changes? [confirm] ENTER
```

```
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this
engine will be scanned
```

```
R1(config)#
```

Aplicar la regla a IPS en una interfaz

Aplicar la regla a IPS que una interfaz con el comando de dirección ip ips nombre en el modo de configuración de interfaz. Aplique la regla de salida en la interfaz Fa0/0 del R1. Después de habilitar IPS, algunos mensajes de registro serán enviado a la línea de la consola que indica que los motores IPS se está inicializando

```
R1(config)#interface fa0/0
R1(config-if)#ip ips iosips out
R1(config-if)#

*ene 06, 01:45:44.4545: %IPS-6-ENGINE_BUILDS_STARTED: 01:45:44 UTC ene 06 2009
*ene 06, 01:45:44.4545: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
*ene 06, 01:45:44.4545: %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this
engine will be scanned
*ene 06, 01:45:44.4545: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms
```

```
R1(config-if)#exit
R1(config)#
```

Modificación de la firma

Cambiar el evento de acción de una firma

```
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 2004 0
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired false
R1(config-sigdef-sig-status)# enabled true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit

Do you want to accept these changes? [confirm] <Enter>

%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this
engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

R1(config)#
```

Usar los comandos show para verificar IPS

```
R1#show ip ips all
IPS Signature File Configuration Status
Configured Config Locations: flash:ipsdir
Last signature default load time:
```

```
Last signature delta load time:  
Last event action (SEAP) load time: -none-
```

```
General SEAP Config:  
Global Deny Timeout: 3600 seconds  
Global Overrides Status: Enabled  
Global Filters Status: Enabled
```

```
IPS Auto Update is not currently configured
```

```
IPS Syslog and SDEE Notification Status  
Event notification through syslog is enabled  
Event notification through SDEE is enabled
```

```
IPS Signature Status  
Total Active Signatures: 1  
Total Inactive Signatures: 0
```

```
IPS Packet Scanning and Interface Status  
IPS Rule Configuration  
  IPS name iosips  
  IPS fail closed is disabled  
  IPS deny-action ips-interface is false  
  Fastpath ips is enabled  
  Quick run mode is enabled  
Interface Configuration  
  Interface FastEthernet0/0  
    Inbound IPS rule is not set  
    Outgoing IPS rule is iosips
```

```
IPS Category CLI Configuration:  
Category all  
  Retire: True  
Category ios_ips basic  
  Retire: False
```

```
R1#
```

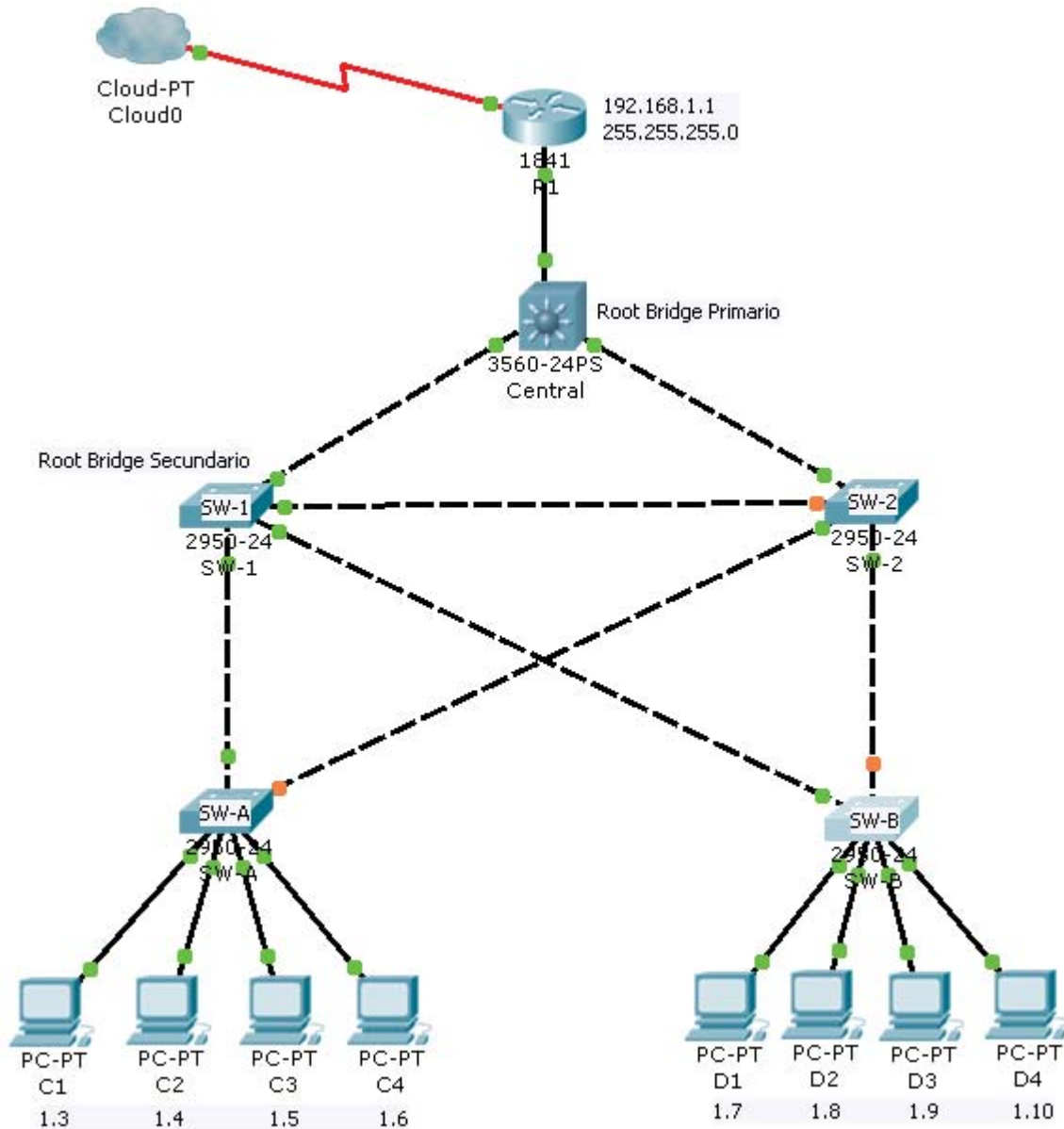
Desde el PC-C, intente hacer ping a PC-A. ¿Los pings son exitosos? ¿Por qué o por qué no?

Los pings deberían fallar. Esto se debe a la regla de IPS para el evento-acción de una solicitud de eco se ajusta a "negar-packet-inline".

Desde el PC-A, intente hacer ping a PC-C. Los pings son exitosos? ¿Por qué o por qué no?

El ping debe tener éxito. Esto es debido a la regla IPS no cubre respuesta de eco. Cuando PC-A PCC pings, PC-C responde con una respuesta de eco.

LABORATORIO 6 (NIVEL 2 DE SEGURIDAD)



Introducción

Ha habido una serie de ataques en la red recientemente. Por esta razón, el administrador de la red le ha asignado la tarea de configurar la seguridad de capa 2.

Para un rendimiento óptimo y la seguridad, el administrador le gustaría asegurarse de que el puente raíz es el conmutador central 3560. Para prevenir contra el spanning-tree ataques de manipulación, el administrador quiere asegurarse de que los parámetros de STP son seguras. Además, el administrador de red desea activar el control de tormentas para evitar las tormentas de broadcast. Por último, para evitar los ataques de desbordamiento de tabla de direcciones MAC, el administrador de red ha decidido configurar la seguridad del puerto para limitar el número de direcciones MAC que pueden ser aprendidas por cada puerto del conmutador. Si el número de direcciones MAC supera el límite establecido, el administrador le gustaría para el puerto que se cierre.

Contraseñas

- Enable password: **ciscoenpa55**
- Console password: **ciscoconpa55**

- VTY line password: **ciscovtpa55**

Configurar el puente raíz

Desde el switch Central, utilizará el comando show spanning-tree para determinar el puente raíz actual y para ver los puertos en uso y su estado.

Cuál de los switches es la raíz del actual puente? Asignar Central como el puente raíz primario.

Asignar Central como Root Bridge Primario

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

Asignar SW-1 como Root Bridge Secundario

```
SW-1(config)# spanning-tree vlan 1 root secondary
```

Proteger contra los ataques de STP

Habilitar PortFast en todos los puertos de acceso

PortFast se ha configurado en los puertos de acceso que se conectan a una estación de trabajo o servidor a fin de que se active con mayor rapidez. En los puertos de acceso conectados de los interruptores SW-A y SW-B, utilice el comando portfast spanning-tree

```
SW-A(config)# interface range fa0/4 - 7
SW-A(config-if-range)# spanning-tree portfast
SW-B(config)# interface range fa0/4 - 7
SW-B(config-if-range)# spanning-tree portfast
```

Habilitar BPDU en todos los puertos de acceso

BPDU Guard es una característica que puede ayudar a evitar estos cambios no autorizados y suplantación de identidad en los puertos de acceso. Habilitar BPDU guardia en SW-A y SW-B puertos de acceso

```
SW-A(config)# interface range fa0/4 - 7
SW-A(config-if-range)# spanning-tree bpduguard enable
SW-B(config)# interface range fa0/4 - 7
SW-B(config-if-range)# spanning-tree bpduguard enable
```

Habilitar protección de raíz

Root Guard se puede habilitar en todos los puertos en un switch que no son puertos raíz.

En el switch SW-1, habilitar root guard en los puertos Fa0/3 y Fa0/4.

En el switch SW-2, habilitar root guard en los puertos Fa0/3 y Fa0/4.

```
SW-1(config)# interface fa0/3
SW-1(config-if)# spanning-tree guard root
SW-1(config-if)# interface fa0/4
SW-1(config-if)# spanning-tree guard root
SW-2(config)# interface fa0/3
SW-2(config-if)# spanning-tree guard root
SW-2(config-if)# interface fa0/4
SW-2(config-if)# spanning-tree guard root
```

Habilitar el control de tormentas

Habilitar el control de tormentas para las emisiones en todos los puertos de conexión de los switch (puertos troncales). Establezca un 50 por ciento el aumento del nivel de supresión con el comando de

control de tormentas de difusión. Habilitar el control de la tormenta en las interfaces de conexión central, SW-1 y SW-2

```
SW-1(config)# interface fa0/1
SW-1(config-if)# storm-control broadcast level 50
SW-1(config-if)# interface fa0/2
SW-1(config-if)# storm-control broadcast level 50
SW-1(config-if)# interface fa0/3
SW-1(config-if)# storm-control broadcast level 50
SW-1(config-if)# interface fa0/4
SW-1(config-if)# storm-control broadcast level 50

SW-2(config)# interface fa0/1
SW-2(config-if)# storm-control broadcast level 50
SW-2(config-if)# interface fa0/2
SW-2(config-if)# storm-control broadcast level 50
SW-2(config-if)# interface fa0/3
SW-2(config-if)# storm-control broadcast level 50
SW-2(config-if)# interface fa0/4
SW-2(config-if)# storm-control broadcast level 50

Central(config)# interface fa0/1
Central(config-if)# storm-control broadcast level 50
Central(config-if)# interface fa0/2
Central(config-if)# storm-control broadcast level 50
Central(config-if)# interface fa0/3
Central(config-if)# storm-control broadcast level 50
```

SHOW STORM-CONTROL BROADCAST

Central

Central#show storm-control broadcast

Interface	Filter State	Upper	Lower	Current
Fa0/1	Link Up	50.00%	50.00%	0.32%
Fa0/2	Link Up	50.00%	50.00%	2.56%
Fa0/3	Link Up	50.00%	50.00%	0.00%

Central#

SW-1

SW-1#show storm-control broadcast

Interface	Filter State	Upper	Lower	Current
Fa0/1	Link Up	50.00%	50.00%	0.32%
Fa0/2	Link Up	50.00%	50.00%	1.28%
Fa0/3	Link Up	50.00%	50.00%	1.28%
Fa0/4	Link Up	50.00%	50.00%	0.00%

SW-1#

SW-2

SW-2#show storm-control broadcast

Interface	Filter State	Upper	Lower	Current
Fa0/1	Link Up	50.00%	50.00%	2.88%

Fa0/2	Link Up	50.00%	50.00%	0.00%
Fa0/3	Link Up	50.00%	50.00%	0.00%
Fa0/4	Link Up	50.00%	50.00%	0.00%

SW-2#

Configurar la seguridad del puerto y deshabilitar los puertos no utilizados

Este procedimiento debe realizarse en todos los puertos de acceso en SW-A y SW-B. Establecer el número máximo de direcciones MAC aprendidas a 2, permitir que la dirección MAC que hay que aprender de forma dinámica y si después de dos intentos erróneos de conexión tira el puerto

```
SW-A(config)# interface FastEthernet 0/4 -7
SW-A(config-if)# switchport mode access
SW-A(config-if)# switchport port-security
SW-A(config-if)# switchport port-security maximum 2
SW-A(config-if)# switchport port-security violation shutdown
SW-A(config-if)# switchport port-security mac-address sticky
```

```
SW-B(config)# interface FastEthernet 0/4 - 7
SW-B(config-if)# switchport mode access
SW-B(config-if)# switchport port-security
SW-B(config-if)# switchport port-security maximum 2
SW-B(config-if)# switchport port-security violation shutdown
SW-B(config-if)# switchport port-security mac-address sticky
```

** Repita el procedimiento en otros puertos de SW-A y SW-B

¿Por qué no desea habilitar el puerto de seguridad en los puertos conectados a otros switches o routers?

Verifique la seguridad del puerto

Puertos conectados a otros dispositivos de conmutación y los enrutadores pueden y deben tener una multitud de direcciones MAC aprendidas para ese único puerto. Limitar el número de direcciones MAC que pueden ser aprendidas en estos escaneos de puertos de manera significativa la funcionalidad de la red de impacto

Verificación con el comando Show

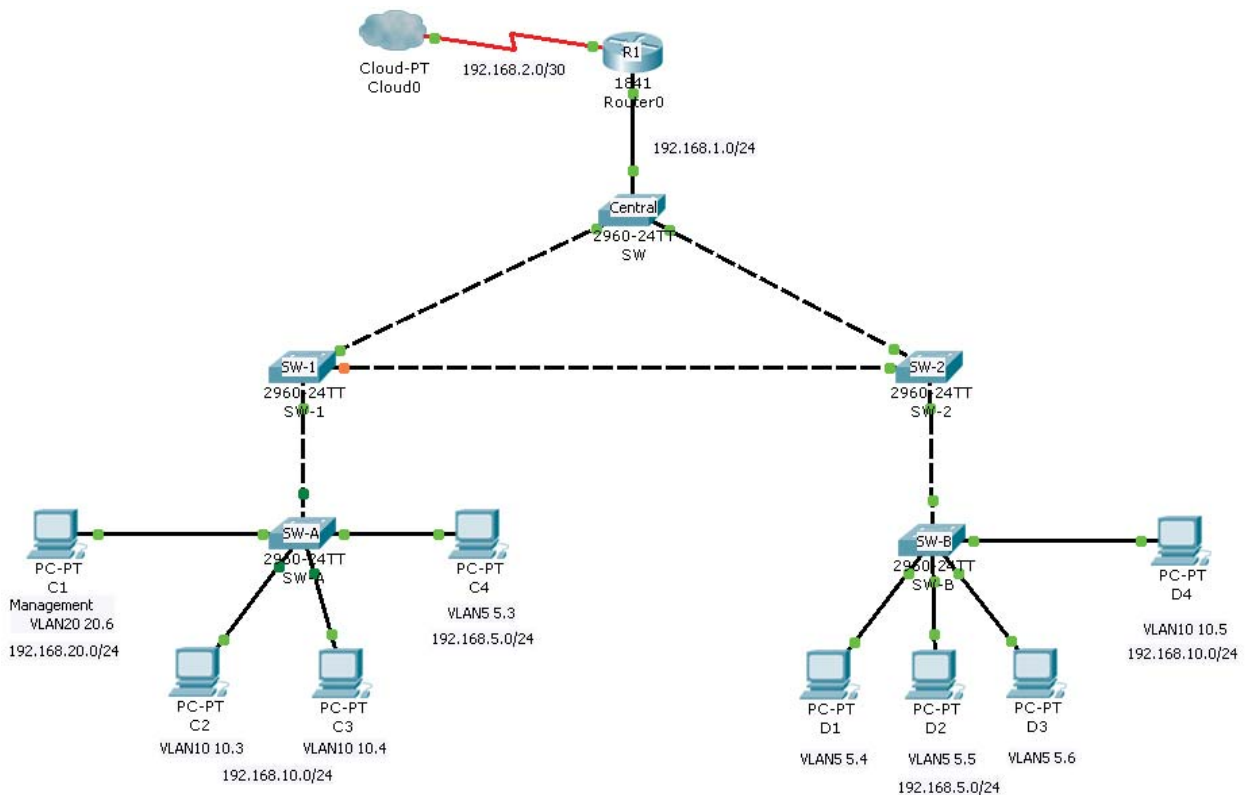
```
show port-security interface fa0/4 - 7
```

Deshabilitar los puertos no utilizados

Desactivar todos los puertos que se encuentran actualmente sin uso.

```
SW-A(config)# interface FastEthernet 0/2
SW-A(config-if)# shutdown
** Repita el procedimiento en otros puertos de SW-A y SW-B
```


LABORATORIO 6 (NIVEL 2 DE SEGURIDAD VLAN)



La red de una compañía está actualmente configurada con dos VLAN: VLAN separadas 5 y VLAN 10. Además, todos los puertos troncales se configuran con VLAN nativa 15. Un administrador de red quiere añadir un enlace redundante entre conmutador SW-1 y SW 2-. El enlace debe haber concentración de enlaces habilitada y con todos los requisitos de seguridad debe estar en su lugar. Además, el administrador de red desea conectar un PC para cambiar la gestión de SW-A. El administrador desea permitir que el PC de gestión para poder conectar con todos los switches y el router, pero no quiere cualquier otro dispositivo para poder conectar con el PC de gestión o de los interruptores.

El administrador le gustaría crear una nueva VLAN 20 con fines de gestión

- Enable secret password: **ciscoenpa55**
- Console password: **ciscoconpa55**
- VTY line password: **ciscovtypa55**

Conecte SW-1 y SW-2

Con un cable cruzado conecte el puerto Fa0/23 en SW-1 al puerto Fa0/23 en SW-2

El modo troncal se ha configurado en todas las interfaces troncales ya existentes. El nuevo enlace debe estar configurado en modo troncal. En el SW-1 y SW-2 establecer el puerto en el troncal en las interfaz fa0/23, asignar VLAN nativa 15 modo troncal, y desactivar la auto-negociación.

Activar todos los troncales de los switch SW-1, SW-2, SW-A, SW-B y Central

```
SW-1(config)# interface fa0/23
SW-1(config-if)# no shutdown
SW-1(config-if)# switchport mode trunk
```

```
SW-1(config-if)# switchport trunk native vlan 15
SW-1(config-if)# switchport nonegotiate

SW-1(config)# interface fa0/1
SW-1(config-if)# no shutdown
SW-1(config-if)# switchport mode trunk
SW-1(config-if)# switchport trunk allowed vlan all

SW-1(config)# interface gig1/1
SW-1(config-if)# no shutdown
SW-1(config-if)# switchport mode trunk
SW-1(config-if)# switchport trunk allowed vlan all

SW-2(config)# interface fa0/23
SW-2(config-if)# no shutdown
SW-2(config-if)# switchport mode trunk
SW-2(config-if)# switchport trunk native vlan 15
SW-2(config-if)# switchport nonegotiate

SW-2(config)# interface fa0/1
SW-2(config-if)# no shutdown
SW-2(config-if)# switchport mode trunk
SW-2(config-if)# switchport trunk allowed vlan all

SW-2(config)# interface gig1/1
SW-2(config-if)# no shutdown
SW-2(config-if)# switchport mode trunk
SW-2(config-if)# switchport trunk allowed vlan all

Central(config)# interface gig1/1
Central(config-if)# no shutdown
Central(config-if)# switchport mode trunk
Central(config-if)# switchport trunk allowed vlan all

Central(config)# interface gig1/2
Central(config-if)# no shutdown
Central(config-if)# switchport mode trunk
Central(config-if)# switchport trunk allowed vlan all

SW-A(config)# interface fa0/5
SW-A(config-if)# no shutdown
SW-A(config-if)# switchport mode trunk
SW-A(config-if)# switchport trunk allowed vlan all

SW-B(config)# interface fa0/5
SW-B(config-if)# no shutdown
SW-B(config-if)# switchport mode trunk
SW-B(config-if)# switchport trunk allowed vlan all
```

El administrador de red desea acceder a todos los conmutadores y dispositivos de enrutamiento que utilizan un PC de gestión.

Para mayor seguridad, el administrador quiere asegurar que todos los dispositivos administrados estén en una VLAN separadas (VLAN 5, 10 y 20)

Habilitar VLAN 20 en SW-A

```
SW-A(config)# vlan 20
SW-A(config-vlan)# exit
```

Crear una interfaz VLAN 20 y asignar una dirección IP dentro de la red 192.168.20.0/24

```
SW-A(config)# interface vlan 20
SW-A(config-if)# ip address 192.168.20.1 255.255.255.0
```

Habilitar la misma VLAN de gestión en todos los otros switches

Asegúrese de crear la VLAN en todos los switches: SW-B, SW-1, SW-2 y Central

```
SW-B(config)# vlan 20
SW-B(config-vlan)# exit
SW-B(config)# interface vlan 20
SW-B(config-if)# ip address 192.168.20.2 255.255.255.0
```

```
SW-1(config)# vlan 20
SW-1(config-vlan)# exit
SW-1(config)# interface vlan 20
SW-1(config-if)# ip address 192.168.20.3 255.255.255.0
```

```
SW-2(config)# vlan 20
SW-2(config-vlan)# exit
SW-2(config)# interface vlan 20
SW-2(config-if)# ip address 192.168.20.4 255.255.255.0
```

```
Central(config)# vlan 20
Central(config-vlan)# exit
Central(config)# interface vlan 20
Central(config-if)# ip address 192.168.20.5 255.255.255.0
```

```
SW-A(config)# vlan 5
SW-A(config-vlan)# exit
SW-A(config)# interface vlan 5
SW-A(config-if)# ip address 192.168.5.1 255.255.255.0
```

```
SW-A(config)# vlan 10
SW-A(config-vlan)# exit
SW-A(config)# interface vlan 10
SW-A(config-if)# ip address 192.168.10.1 255.255.255.0
```

```
SW-B(config)# vlan 5
SW-B(config-vlan)# exit
SW-B(config)# interface vlan 5
SW-B(config-if)# ip address 192.168.5.2 255.255.255.0
```

```
SW-B(config)# vlan 10
SW-B(config-vlan)# exit
SW-B(config)# interface vlan 10
SW-B(config-if)# ip address 192.168.10.2 255.255.255.0
```

Asegúrese de que el equipo de gestión se le asigna una dirección IP dentro de la red 192.168.20.0/24.
Conecte el PC a la gestión de SW-A a un puerto Fa0/4

Asignar la interfaz Fa0/4 debe ser parte de la VLAN 20

```
SW-A(config)# interface fa0/4
SW-A(config-if)# switchport mode access
SW-A(config-if)# switchport access vlan 20
SW-A(config-if)# no shutdown
```

Seguir asignando las Vlan a las interfaz de los switch

```
SW-A(config)# interface fa0/3
SW-A(config-if)# switchport mode access
```

```
SW-A(config-if) # switchport access vlan 10  
SW-A(config-if) # no shutdown
```

```
SW-A(config) # interface fa0/2  
SW-A(config-if) # switchport mode access  
SW-A(config-if) # switchport access vlan 10  
SW-A(config-if) # no shutdown
```

```
SW-A(config) # interface fa0/1  
SW-A(config-if) # switchport mode access  
SW-A(config-if) # switchport access vlan 5  
SW-A(config-if) # no shutdown
```

```
SW-B(config) # interface fa0/1  
SW-A(config-if) # switchport mode access  
SW-B(config-if) # switchport access vlan 5  
SW-B(config-if) # no shutdown
```

```
SW-B(config) # interface fa0/2  
SW-A(config-if) # switchport mode access  
SW-B(config-if) # switchport access vlan 5  
SW-B(config-if) # no shutdown
```

```
SW-B(config) # interface fa0/3  
SW-A(config-if) # switchport mode access  
SW-B(config-if) # switchport access vlan 5  
SW-B(config-if) # no shutdown
```

```
SW-B(config) # interface fa0/4  
SW-A(config-if) # switchport mode access  
SW-B(config-if) # switchport access vlan 10  
SW-B(config-if) # no shutdown
```

Asegúrese de que el equipo de gestión se le asigna una dirección IP dentro de la red 192.168.20.0/24 y Conecte el PC a la gestión de SW-A a un puerto Fa0/4

Habilitar el PC de gestión de acceso del router R1

Crear subinterfaz Fa0/0.20 y asignar una dirección IP dentro de la red 192.168.20.0/24. Asegúrese de ajustar la encapsulación para dot1q 20 para tener en cuenta para la VLAN 20

```
R1(config) # interface fa0/0.20  
R1(config-subif) # encapsulation dot1q 20  
R1(config-subif) # ip address 192.168.20.100 255.255.255.0
```

```
R1(config) # interface fa0/0.10  
R1(config-subif) # encapsulation dot1q 10  
R1(config-subif) # ip address 192.168.10.100 255.255.255.0
```

```
R1(config) # interface fa0/0.5  
R1(config-subif) # encapsulation dot1q 5  
R1(config-subif) # ip address 192.168.5.100 255.255.255.0
```

Activar la Seguridad

Mientras que el PC de gestión debe ser capaz de acceder al router, ninguna otra PC debe ser capaz de acceder a la VLAN de administración

Crear una ACL que niega cualquier red de acceso a la red 192.168.20.0/24, pero permite que todas las otras redes para acceder a unos de otros

```
R1(config)# access-list 101 deny ip any 192.168.20.0 0.0.0.255
R1(config)# access-list 101 permit ip any any
```

Aplicar la ACL a las interfaz

```
R1(config)# interface fa0/0.5
R1(config-subif)# ip access-group 101 in

R1(config-subif)# interface fa0/0.10
R1(config-subif)# ip access-group 101 in
```

Hay varias formas en las que una ACL se pueden crear para lograr la seguridad necesaria. Por esta razón, la clasificación en esta porción de la actividad se basa en los requisitos de conectividad correcta. El equipo de gestión debe ser capaz de conectarse a todos los interruptores y el router. Todos los otros equipos no debe ser capaz de conectarse a cualquier dispositivo dentro de la VLAN de administración

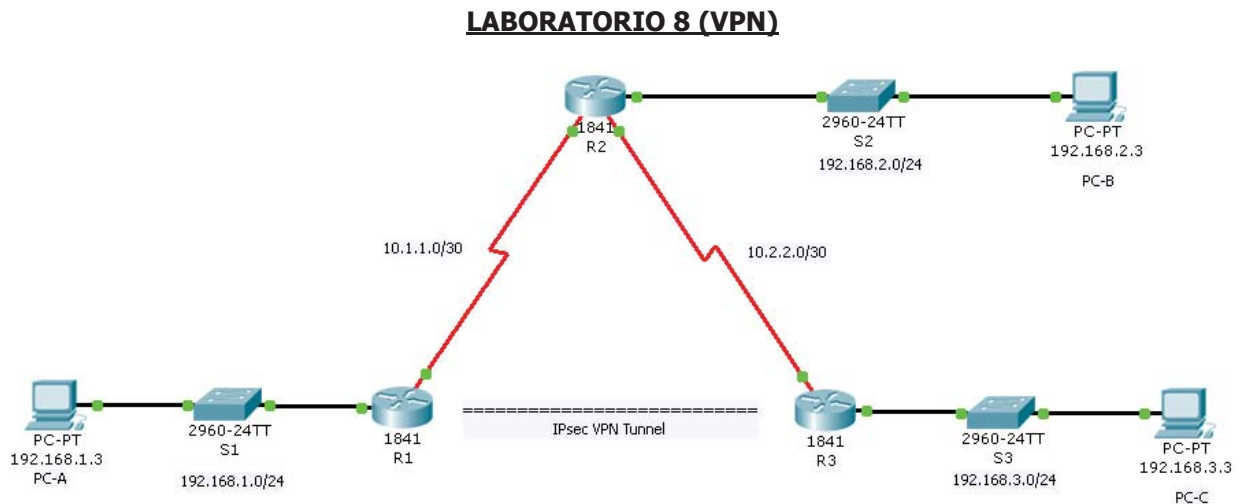


Tabla de Direcciomnes

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	192.168.1.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
R2	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.2.1	255.255.255.0
R3	S0/0/1	10.2.2.1	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
	Fa0/0	192.168.3.1	255.255.255.0
PC-A	NIC	192.168.1.3	255.255.255.0
PC-B	NIC	192.168.2.3	255.255.255.0
PC-C	NIC	192.168.3.3	255.255.255.0

La topología de la red muestra tres routers. Su tarea consiste en configurar los routers R1 y R3 para apoyar a un sitio a sitio VPN IPsec cuando el tráfico fluye de sus respectivas redes de área local. El túnel VPN IPsec es desde el router R1 a R3 a través del router R2. R2 actúa como un paso a través y no tiene conocimiento de la VPN. IPsec proporciona una transmisión segura de información confidencial a través de redes desprotegidas como Internet. IPsec actúa en la capa de red.

ISAKMP(Internet Security Association and Key management protocol) Fase 1 parámetros de la política

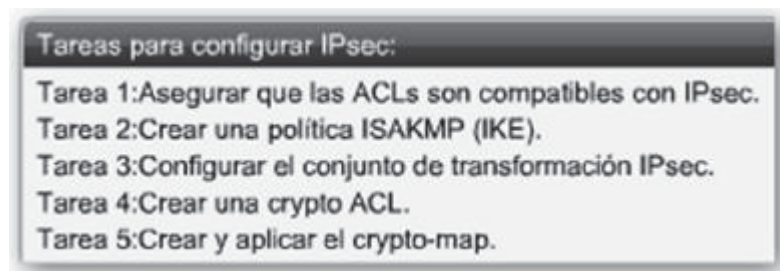
PARÁMETROS		R1	R2
Método de intercambio de claves	Manual o ISAKMP	ISAKMP	ISAKMP
Algoritmo de cifrado	DES, 3DES O AES	AES	AES
Integridad	MD5 O SHA-1	SHA-1	SHA-1
Autenticación al par	Pre-shared keys o RSA	Pre-share	Pre-share
Intercambio de clave DH	Diffie-Hellman Grupo 1,2 o 5	DH2	DH2
Tiempo de Vida de SA IKE	86400 segundos o menos	86400	86400
Clave ISAKMP	Clave	Vpnpa55	Vpnpa55

Parameters		R1	R3
Key distribution method	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption algorithm	DES, 3DES, or AES	AES	AES
Hash algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication method	Pre-shared keys or RSA	pre-share	pre-share
Key exchange	DH Group 1, 2, or 5	DH 2	DH 2
IKE SA Lifetime	86400 seconds or less	86400	86400
ISAKMP Key		vpnpa55	vpnpa55

IPsec Fase 2 parámetros de la política

Parameters	R1	R3
Transform Set	VPN-SET	VPN-SET
Peer Hostname	R3	R1
Peer IP Address	10.2.2.2	10.1.1.2
Network to be encrypted	192.168.1.0/24	192.168.3.0/24
Crypto Map name	VPN-MAP	VPN-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

Configuración Ipsec



Contraseñas y Enrutamiento

- Password for console line: **ciscoconpa55**
- Password for vty lines: **ciscovtypa55**
- Enable password: **ciscoenpa55**
- RIP version 2

Configuración de los parámetros Ipsec en el R1

Identificar el tráfico interesante R1

Configurar la ACL 110 para identificar el tráfico de la LAN de R1 a la LAN de R3 como interesante. Este tráfico interesante se disparará la VPN IPsec para implementar cada vez que hay tráfico entre R1 a R3 LAN. Todos los demás el tráfico procedente de las LAN no se cifrará

Recuerde que debido a la implícita negar todo, no hay necesidad de configurar un negar cualquier declaración alguna (deny any any)

```
R1(config)# access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```

Configuración de la Fase 1 de ISAKMP propiedades en el router R1

Configure las propiedades de cifrado ISAKMP **10** en el R1, junto con la clave de cifrado precompartida **vpnpa55**. Consulte la tabla de la Fase 1 de ISAKMP para ver los parámetros específicos a configurar. Los valores por defecto no tienen que ser configurados, por lo tanto, sólo el algoritmo de cifrado, el método de intercambio de claves, y el método de DH debe estar configurado

```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# encryption aes
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 2
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnpa55 address 10.2.2.2
```

Configuración de la Fase 2 de ISAKMP propiedades en el router R1

Crear el conjunto de transformación **VPN-SET** para el uso de **esp-3des** y **esp-sha-hmac**. A continuación, cree el cryptomapa **VPN-MAP** que une a todos los de la Fase 2 parámetros juntos. Utilice el número de secuencia de **10** y lo identifican como un mapa de **ipsec-isakmp**

```
R1(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R1(config)# crypto map VPN-MAP 10 ipsec-isakmp
R1(config-crypto-map)# description VPN connection to R3
R1(config-crypto-map)# set peer 10.2.2.2
R1(config-crypto-map)# set transform-set VPN-SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit
```

Configurar el mapa criptográfico en el interfaz de salida Serial0/0/0

Por último, asociar el crypto mapa VPN-MAP a la salida de interfaz Serial0/0/0

```
R1(config)# interface S0/0/0
R1(config-if)# crypto map VPN-MAP
```

Configurar los parámetros de IPsec en el R3

Configurar el router R3 para apoyar a una VPN de sitio a sitio con R1. Ahora configurar los parámetros de movimiento alternativos en R3. Configurar ACL 110 identificar el tráfico de la LAN de R3 a la LAN en R1 como interesante

```
R3(config)# access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
```

Configuración de la Fase 1 de ISAKMP propiedades en el router R3

Configure el cifrado ISAKMP 10 en las propiedades del R3, junto con la criptografía de clave precompartida **vpnpa55**

```
R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 2
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnpa55 address 10.1.1.2
```

Configuración de la Fase 2 de ISAKMP propiedades en el router R3

Así como lo hizo en R1, crear el conjunto de transformación llamado **VPN-SET** para el uso de **esp-3des** y **esp-sha-hmac**. A continuación, crear el mapa de cifrado **VPN-MAP** que une a todos los de la Fase 2 parámetros juntos. Utilice el número de secuencia de **10** y lo identifican como un mapa de **ipsec-isakmp**

```
R3(config)# crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
R3(config)# crypto map VPN-MAP 10 ipsec-isakmp
R3(config-crypto-map)# description VPN connection to R1
R3(config-crypto-map)# set peer 10.1.1.2
R3(config-crypto-map)# set transform-set VPN-SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

Configurar el mapa criptográfico en el interfaz de salida Serial0/0/1

Por último, asociar el crypto mapa VPN-MAP a la salida de interfaz Serial0/0/1

```
R3(config)# interface S0/0/1
R3(config-if)# crypto map VPN-MAP
```

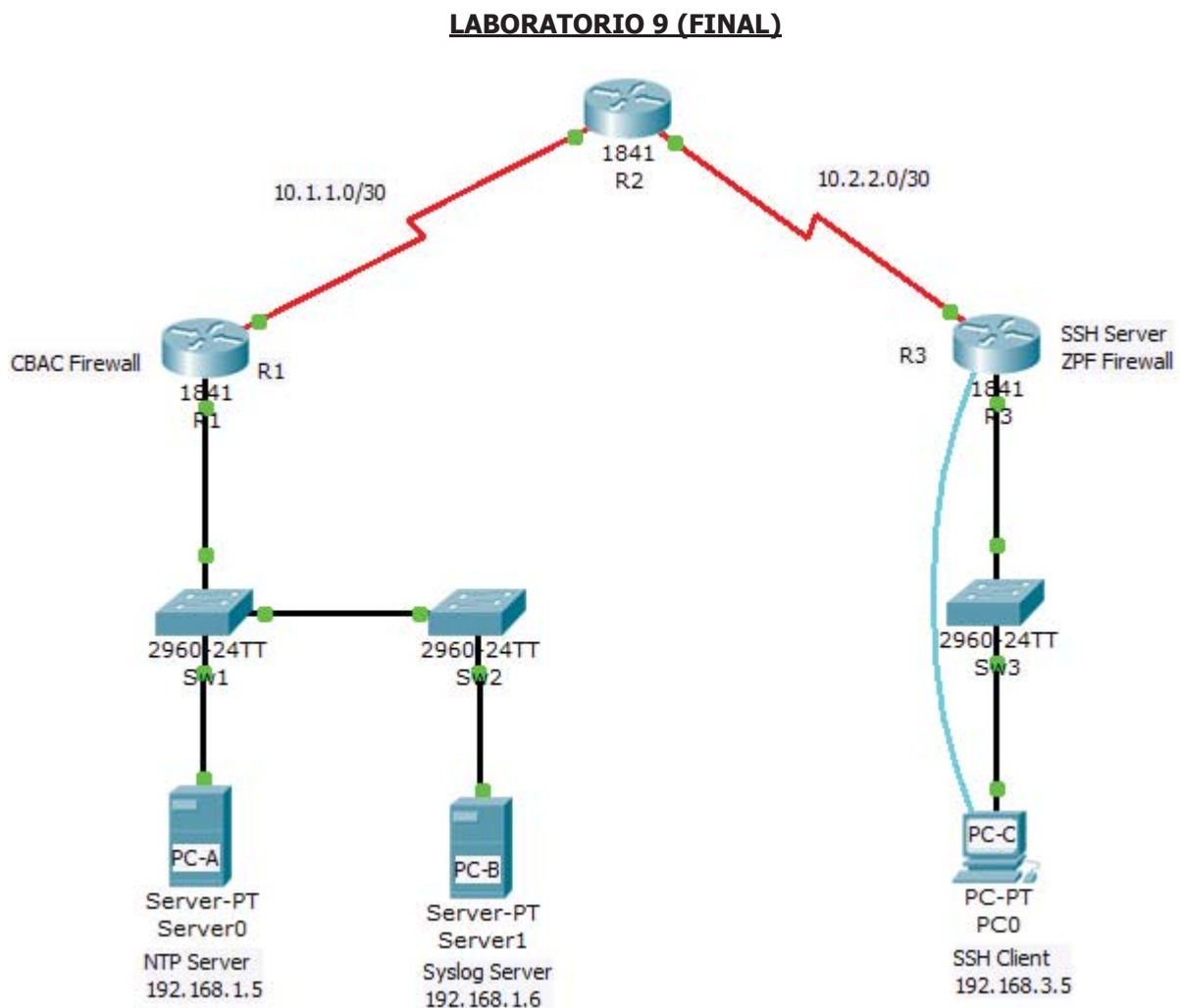


Tabla de Direcciones

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	FA0/1	192.168.1.1	255.255.255.0	N/A	S1 FA0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A	N/A
R2	S0/0/0	10.1.1.2	255.255.255.252	N/A	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3	FA0/1	192.168.3.1	255.255.255.0	N/A	S3 FA0/5
	S0/0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 FA0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 FA0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 FA0/6

Introducción

En esta actividad, la práctica integral, que se aplicará una combinación de medidas de seguridad que se introdujeron en el curso. Estas medidas figuran en los objetivos.

En la topología, R1 es el borde exterior de la empresa A, mientras que R3 es el router de borde de la compañía B. Estas redes están interconectadas a través del router R2 que representa el ISP. Va a configurar varias características de seguridad en los routers y switches para la empresa A y B. de la compañía no todas las características de seguridad se pueden configurar en R1 y R3

Objetivos de Aprendizaje:

- Asegure los routers con contraseñas seguras, encriptación de la contraseña y un cuadro de inicio de sesión
- Asegure la consola y las líneas vty con contraseñas
- Configurar la autenticación AAA local
- Configurar el servidor SSH
- Configurar router para syslog
- Configurar router para el NTP
- Asegure el router de los ataques de inicio de sesión
- Configurar CBAC y firewalls ZPF
- Los switches de red seguros

Las configuraciones previas siguientes se han realizado:

- Los nombres de hosts en todos los dispositivos
- Las direcciones IP de todos los dispositivos
- Contraseña de consola del R2: ciscoconpa55
- Contraseña en líneas vty del R2: ciscovtypa55
- Contraseña de Enable en el R2: ciscoenpa55
- El enrutamiento estático
- Servicios de Syslog en el PC-B
- búsqueda de DNS ha sido deshabilitado
- Las puertas de enlace IP por defecto para todos los conmutadores

Enrutamiento Estático

```
R1(config)# ip route 10.2.2.0 255.255.255.252 10.1.1.2
R1(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
R2(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
R2(config)# ip route 192.168.3.0 255.255.255.0 10.2.2.1
R3(config)# ip route 10.1.1.0 255.255.255.252 10.2.2.2
R3(config)# ip route 192.168.1.0 255.255.255.0 10.1.1.1
```

Prueba de conectividad y verificar las configuraciones

```
*R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	10.1.1.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
R1#
```

```
*R1#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
```

```
       i - IS-IS, 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
```

```
10.0.0.0/30 is subnetted, 2 subnets
```

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

```
S      10.2.2.0 [1/0] via 10.1.1.2
```

```
C     192.168.1.0/24 is directly connected, FastEthernet0/1
```

```
S     192.168.3.0/24 [1/0] via 10.2.2.1
```

```
R1#
```

Seguridad en los routers

Establecer una longitud de contraseña mínima de 10 caracteres en el router R 1 y R 3

```
R1(config)# security passwords min-length 10
```

```
R3(config)# security passwords min-length 10
```

Configuramos una contraseña de enable encriptada en los router R1 y R3 que sea ciscoenpa55.

```
R1(config)# enable secret ciscoenpa55
```

```
R3(config)# enable secret ciscoenpa55
```

Cifrar contraseñas en texto plano

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

```
R3(config)# service password-encryption
```

Configurar las líneas de consola del router R1 y R3

Configurar una contraseña de la consola de ciscoconpa55 y permitir inicio de sesión. Ajuste el exec-timeout para cerrar la sesión después de 5 minutos de inactividad. Evitar mensajes de la consola de interrumpir la entrada de comandos

```
R1(config)# line console 0
R1(config-line)# password ciscoconpa55
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

```
R3(config)# line console 0
R3(config-line)# password ciscoconpa55
R3(config-line)# exec-timeout 5 0
R3(config-line)# login
R3(config-line)# logging synchronous
```

Configurar las líneas VTY en el router R1

Configurar una contraseña de la línea vty de **ciscovtypa55** y permitir inicio de sesión. Ajuste el exec-timeout para cerrar la sesión después de 5 minutos de inactividad. Configurar la autenticación de inicio de sesión para usar la lista por defecto AAA que se definirá más adelante

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypa55
R1(config-line)# exec-timeout 5 0
R1(config-line)# login authentication default
```

Nota: Las líneas vty en R3 será configurado para SSH en una tarea posterior

Configuración del aviso de seguridad en el Router R1 y R3

```
R1(config)# banner motd #ENTRADA PROHIBIDA!#
R3(config)# banner motd #ENTRADA PROHIBIDA!#
```

Configuración de la autenticación local en R1 y R3

Configurar la base de datos local de usuarios

Crear una cuenta de usuario local llamada **Admin01** con una contraseña secreta que sea **Admin01pa55**

```
R1(config)# username Admin01 privilege 15 secret Admin01pa55
R3(config)# username Admin01 privilege 15 secret Admin01pa55
```

Activar los Servicios AAA

```
R1(config)# aaa new-model
R3(config)# aaa new-model
```

Implementar servicios de AAA que utilizan la base de datos local

Cree el inicio de sesión predeterminado de autenticación lista de métodos de uso de la autenticación local con un método de copia de seguridad

```
R1(config)# aaa authentication login default local none
R3(config)# aaa authentication login default local none
```

Configuración NTP

Habilitar la autenticación NTP en el PC-A

El PC-A, seleccione la ficha Configuración, y luego el botón de NTP. Seleccione On para el servicio NTP. Habilitar la autenticación e introduzca una clave de 1 y una contraseña de **ciscontppa55**

Configurar R1 como un cliente NTP

Configuración de NTP autenticación de clave 1 con una contraseña de **ciscontpa55**. Configurar el R1 para sincronizar con el servidor NTP y la autenticación mediante la clave 1

```
R1(config)# ntp authenticate
R1(config)# ntp authentication-key 1 md5 ciscontppa55
R1(config)# ntp trusted-key 1
R1(config)# ntp server 192.168.1.5 key 1
```

Configurar routers para actualizar el reloj de hardware

Configurar routers para actualizar periódicamente el reloj del hardware con el tiempo aprendido de NTP

```
R1(config)# ntp update-calendar
```

Configuración del roter R1 como un Cliente Syslog

Configurar el R1 para los mensajes de registro de fecha y hora

```
R1(config)# service timestamps log datetime msec
```

Configurar el R1 para registrar los mensajes en el servidor syslog

Configurar los routers para identificar el host remoto (servidor syslog) que recibirá los mensajes de registro

```
R1(config)# logging 192.168.1.6
```

Usted debe ver un mensaje en la consola similar a lo siguiente:

```
SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.1.6 port 514
started - CLI initiated
```

Compruebe si hay mensajes de syslog en el PC-B

En el router R1, salir del modo de configuración para generar un mensaje de syslog. Abra el servidor syslog en la PC-B para ver el mensaje enviado desde R1. Usted debe ver un mensaje similar al siguiente en el servidor syslog:

```
%SYS-5-CONFIG_I: Configured from console by console
```

Asegurar el Router R1 contra ataques

Log de intentos fallidos de inicio de sesión en R 1

```
R1(config)# login on-failure log
```

Telnet a R1 desde el PC-A

Hacer un Telnet desde el PC-A a R1 y proporcionar el nombre de usuario y contraseña **Admin01Admin01pa55**. El Telnet debe tener éxito.

Telnet a R1 desde el PC-A y revisar los mensajes del syslog en el servidor syslog

Salir de la sesión de Telnet y hacer Telnet otra vez a R1 mediante el nombre de usuario y la contraseña de cualquier usuario de la base de datos
Compruebe el servidor syslog en la PC-B. Usted debe ver un mensaje de error similar al siguiente que se genera por el intento fallido de login

```
SEC_LOGIN-4-LOGIN_FAILED:Login failed [user:baduser]  
[Source:192.168.1.5][localport:23] [Reason:Invalid login] at 15:01:23 UTC Wed  
June 17 2009
```

Configurar SSH en el router R3

Crear un ID de usuario de SSHadmin con el nivel de privilegio más alto posible y una contraseña secreta de ciscosshpa55

```
R3(config)# username SSHadmin privilege 15 secret ciscosshpa55
```

Configure un nombre de dominio de ccnasecurity.com en el router R3

```
R3(config)# ip domain-name ccnasecurity.com
```

Configure las líneas vty entrantes en R 3

Utilizar las cuentas de usuario locales para el acceso obligatorio y la validación y aceptar sólo conexiones SSH

```
R3(config)# line vty 0 4  
R3(config-line)# exec-timeout 5 0  
R3(config-line)# login local  
R3(config-line)# transport input ssh
```

Configurar el par de claves RSA de cifrado para R3

Todos los pares de claves RSA existentes deben borrarse en el router. Si no hay claves configuradas actualmente aparecerá un mensaje indicando esto. Configure las llaves RSA con un módulo de 1024

```
R3(config)# crypto key zeroize rsa  
% No Signature RSA Keys found in configuration.
```

```
R3(config)# crypto key generate rsa [Enter]  
The name for the keys will be: R3.ccnasecurity.com  
Choose the size of the key modulus in the range of 360 to 2048 for your  
General Purpose Keys. Choosing a key modulus greater than 512 may take a  
few minutes.
```

```
How many bits in the modulus [512]:1024  
% Generating 1024 bit RSA keys, keys will be non-exportable... [OK]
```

Configurar tiempos de espera y los parámetros de autenticación SSH.

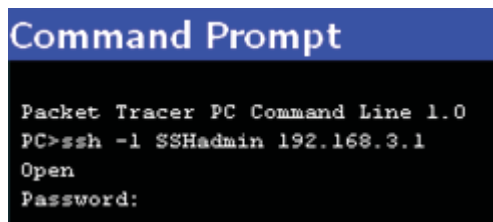
Establezca el tiempo de espera de SSH a 90 segundos, el número de reintentos de autenticación a 2, y la versión a 1

```
R3(config)# ip ssh time-out 90  
R3(config)# ip ssh authentication-retries 2  
R3(config)# ip ssh version 1
```

VERIFICACIÓN

Abra el escritorio del PC-C. Seleccione el icono del símbolo del sistema. Desde el PC-C, escriba el comando para conectarse a R3 a través de SSH. Cuando se le pida la contraseña, introduzca la contraseña configurada para el administrador: **ciscosshpa55**

```
PC> ssh -l SSHadmin 192.168.3.1
```



```
Command Prompt  
Packet Tracer PC Command Line 1.0  
PC>ssh -l SSHadmin 192.168.3.1  
Open  
Password:
```

Configuración de un Firewall CBAC en el R1

Configuración de la ACL

Crear una ACL IP llamado OUT-IN para bloquear todo el tráfico procedente de la red exterior

```
R1(config)# ip access-list extended OUT-IN  
R1(config-ext-nacl)# deny ip any any  
R1(config-ext-nacl)# exit
```

Aplicar la lista de acceso para el tráfico entrante en la interfaz Serial0/0/0

```
R1(config)# interface s0/0/0  
R1(config-if)# ip access-group OUT-IN in
```

Confirme que la interfaz Serial0/0/0 el tráfico de netrada está caído

Desde el símbolo del sistema del PC-A, hacer un ping PC-C. Las respuestas de ehco ICMP son bloqueados por la ACL

Crear una regla de inspección para inspeccionar el tráfico ICMP, Telnet y HTTP

Crear una regla de inspección denominada IN-OUT-IN para inspeccionar Telnet ICMP, y el tráfico HTTP

```
R1(config)# ip inspect name IN-OUT-IN icmp  
R1(config)# ip inspect name IN-OUT-IN telnet
```

```
R1(config)# ip inspect name IN-OUT-IN http
```

Aplicar la regla de inspección a la interfaz con sentido salida

Aplicar el IN-OUT-IN regla de inspección a la interfaz de donde sale el tráfico a las redes externas

```
R1(config)# interface s0/0/0  
R1(config-if)# ip inspect IN-OUT-IN out
```

Prueba de funcionamiento de la regla de inspección

Desde el PC-Un símbolo del sistema, mesa de ping PC-C. Las respuestas de eco ICMP deben ser inspeccionados y autorizados por medio

Configuración de un Firewall ZPF en el R3

Prueba de conectividad:

- A partir de PC-C, para probar la conectividad con ping y Telnet a R2, todo debe tener éxito
- A partir de ping R2 para PC-C. Los pings se debe permitir

Crear el firewall basado en zonas (ZPF)

Crear una zona interna llamada **IN-ZONE**.

```
R3(config)# zone security IN-ZONE
```

Crear una zona externa llamada **OUT-ZONE**.

```
R3(config)# zone security OUT-ZONE
```

Crear una ACL que define el tráfico interno

Crear una extendida, con el número ACL que permite que todos los protocolos IP de la red de origen 192.168.3.0/24 hacia cualquier destino. Utilice 101 para el número de ACL

```
R3(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 any
```

Crear un mapa de clase que hace referencia al tráfico interno de ACL

Crear un mapa de clase llamado EN-NET-CLASE-MAP para que coincida con ACL 101

```
R3(config)# class-map type inspect match-all IN-NET-CLASS-MAP  
R3(config-cmap)# match access-group 101  
R3(config-cmap)# exit
```

Especificar las políticas del firewall

Crear un mapa de la política llamado EN-2-OUT-PMAP para determinar qué hacer con el tráfico coincidente

```
R3(config)# policy-map type inspect IN-2-OUT-PMAP
```

Especifique un tipo de clase de inspeccionar y hacer referencia a mapa de clase IN-NET-CLASE-MAP

```
R3(config-pmap)# class type inspect IN-NET-CLASS-MAP
```

Especifique la acción de la inspección de este mapa de la política

```
R3(config-pmap-c)# inspect
```


Usted debe ver el mensaje en la consola lo siguiente:

```
%No specific protocol configured in class IN-NET-CLASS-MAP for inspection.All protocols will be inspected."
```

Aplicar las políticas del firewall

Crear un par de zona denominada EN-2-OUT-PAR. Especificar el origen y las zonas de destino que se creó anteriormente

```
R3(config)# zone-pair security IN-2-OUT-ZPAIR source IN-ZONE destination OUT-ZONE
```

Adjuntar un mapa de la política y las acciones a la par de la zona que hace referencia al mapa de la política ha creado anteriormente, IN-2-OUT MAP

```
R3(config-sec-zone-pair)# service-policy type inspect IN-2-OUT-PMAP
```

Salida a la configuración global del sistema y asignar las interfaces internas y externas a las zonas de seguridad

```
R3(config)# interface fa0/1
R3(config-if)# zone-member security IN-ZONE
R3(config-if)# interface s0/0/1
R3(config-if)# zone-member security OUT-ZONE
```

Seguridad en los switches

Configuración de una contraseña secreta en todos los switches

Utilice una contraseña secreta que sea **ciscoenpa55**

```
S1(config)# enable secret ciscoenpa55
```

Encriptar las contraseñas en texto plano

```
S1(config)# service password-encryption
```

Configurar las líneas de consola en todos los switches

Configurar una contraseña de la consola de ciscoconpa55 y permitir inicio de sesión. Ajuste el exec-timeout para cerrar la sesión después de 5 minutos de inactividad. Evitar mensajes de la consola de interrumpir la entrada de comandos

```
S1(config)# line console 0
S1(config-line)# password ciscoconpa55
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
S1(config-line)# logging synchronous
```

Configuración de las líneas VTY en los switches

Configurar una contraseña de la línea vty de cisco **vtypa55** y habilitar el registro. Ajuste el exec-timeout para cerrar la sesión después de 5 minutos de inactividad. Establezca el parámetro de inicio de sesión

```
S1(config)# line vty 0 4
S1(config-line)# password ciscovtypa55
S1(config-line)# exec-timeout 5 0
S1(config-line)# login
```

Puertos seguros troncales en el SW 1 y SW 2

Configure el puerto Fa0/1 en el SW1 como un puerto troncal

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode trunk
```

Configure el puerto Fa0/1 en el SW2 como un puerto troncal

```
S2(config)# interface FastEthernet 0/1
S2(config-if)# switchport mode trunk
```

Compruebe que el puerto Fa0 /1 del SW1 está en modo de enlace troncal

```
S1# show interfaces trunk
```

Compruebe que el puerto Fa0 /1 del SW2 está en modo de enlace troncal

```
S2# show interfaces trunk
```

Configurar la VLAN nativa en S1 y S2 puertos troncales para un sin utilizar la VLAN 99

```
S1(config)# interface Fa0/1
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
```

```
S2(config)# interface Fa0/1
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# end
```

Establecer los puertos troncales en S1 y S2 de manera que no negocian apagando la generación de marcos de DTP (Dynamic Trunking Protocol)

```
S1(config)# interface Fa0/1
S1(config-if)# switchport nonegotiate
```

```
S2(config)# interface Fa0/1
S2(config-if)# switchport nonegotiate
```

Habilitar el control de tormentas para las emisiones en los puertos de enlace troncal SW1 y SW2 con un nivel de supresión de 50 por ciento de aumento

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# storm-control broadcast level 50
```

```
S2(config)# interface FastEthernet 0/1
S2(config-if)# storm-control broadcast level 50
```

Asegure los puertos de acceso

Desactivar el enlace troncal en los puertos de acceso SW1, SW2 y SW3

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# switchport mode access
S1(config-if)# interface FastEthernet 0/6
S1(config-if)# switchport mode access
```

```
S2(config)# interface FastEthernet 0/18
S2(config-if)# switchport mode access
```

```
S3(config)# interface FastEthernet 0/5
S3(config-if)# switchport mode access
S3(config-if)# interface FastEthernet 0/6
S3(config-if)# switchport mode access
```

Habilitar PortFast en SW1, SW2, SW3 y los puertos de acceso

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# spanning-tree portfast
S1(config-if)# interface FastEthernet 0/6
S1(config-if)# spanning-tree portfast

S2(config)# interface FastEthernet 0/18
S2(config-if)# spanning-tree portfast

S3(config)# interface FastEthernet 0/5
S3(config-if)# spanning-tree portfast
S3(config-if)# interface FastEthernet 0/6
S3(config-if)# spanning-tree portfast
```

Habilitar BPDU guard en los puertos del switch configurados previamente como único acceso

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# interface FastEthernet 0/6
S1(config-if)# spanning-tree bpduguard enable

S2(config)# interface FastEthernet 0/18
S2(config-if)# spanning-tree bpduguard enable

S3(config)# interface FastEthernet 0/5
S3(config-if)# spanning-tree bpduguard enable
S3(config-if)# interface FastEthernet 0/6
S3(config-if)# spanning-tree bpduguard enable
```

Habilitar la seguridad básica de puerto por defecto en todos los puertos de acceso de los usuarios finales que están en uso

```
S1(config)# interface FastEthernet 0/5
S1(config-if)# shutdown
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# no shutdown
S1(config-if)# interface FastEthernet 0/6
S1(config-if)# shutdown
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# no shutdown

S2(config)# interface FastEthernet 0/18
S2(config-if)# shutdown
S2(config-if)# switchport port-security
S2(config-if)# switchport port-security mac-address sticky
S2(config-if)# no shutdown

S3(config)# interface FastEthernet 0/5
S3(config-if)# shutdown
S3(config-if)# switchport port-security
S3(config-if)# switchport port-security mac-address sticky
S3(config-if)# no shutdown
S3(config-if)# interface FastEthernet 0/6
```

```
S3(config-if)# shutdown
S3(config-if)# switchport port-security
S3(config-if)# switchport port-security mac-address sticky
S3(config-if)# no shutdown
```

Deshabilite todos los puertos que no son utilizados en cada switch

```
S1(config)# interface range Fa0/2 - 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range Fa0/7 - 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range gigabitethernet1/1 - 2
S1(config-if-range)# shutdown

S2(config)# interface range Fa0/2 - 17
S2(config-if-range)# shutdown
S2(config-if-range)# interface range Fa0/19 - 24
S2(config-if-range)# shutdown
S2(config-if-range)# interface range gigabitethernet1/1 - 2
S2(config-if-range)# shutdown

S3(config)# interface range Fa0/1 - 4
S3(config-if-range)# shutdown
S3(config-if-range)# interface range Fa0/7 - 24
S3(config-if-range)# shutdown
S3(config-if-range)# interface range gigabitethernet1/1 - 2
S3(config-if-range)# shutdown
```

Verificación

Configuración de prueba SSH

Intente conectarse a R3 a través de Telnet desde el PC-C

Desde el PC-C, escriba el comando para conectarse a R3 a través de Telnet una dirección IP 192.168.3.1

Esta conexión falla, ya que R3 se ha configurado para aceptar sólo las conexiones SSH en las líneas de terminal virtual.

Desde el PC-C, entre el ssh-l 192.168.3.1 Admin01 de comandos para conectarse a R3 a través de SSH

Cuando se le pida la contraseña, introduzca la contraseña configurada para Admin01pa55 el administrador local

Utilice el comando **show ip ssh** para ver las opciones de configuración

```
R3# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
```

Verificar fecha y hora, estado de NTP para R1 y un PC

```
R1# show clock
*17:28:49.898 UTC Tue May 19 2009

R1# show ntp status
```

```
Clock is synchronized, stratum 2, reference is 192.168.1.5
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is
2**19 reference time is CD99AF95.0000011B (15:00:37.283 UTC Tue May 19
2009)
clock offset is 0.00 msec, root delay is 0.00 msec root dispersion is
0.02 msec, peer dispersion is 0.02 msec
```

Prueba firewall CBAC en R 1

- Realice un ping desde el PC-A-R2 en 10.2.2.2 (en caso de éxito)
- Telnet desde el PC-A a R2 10.2.2.2 (en caso de éxito)
- Haga ping desde R2 a la PC-A en 192.168.1.3 (falla)

Prueba de firewall ZPF en R3

- Realice un ping desde el PC-C para R2 en 10.2.2.2 (en caso de éxito)
- Telnet desde el PC-C para R2 en 10.2.2.2 (en caso de éxito)
- Haga ping desde R2 a PC-C en 192.168.3.5 (falla)
- Telnet de R2 a R3 en 10.2.2.1 (en caso de no - sólo se permite SSH)

Verificación del port security

```
S2#show run
```

```
Building configuration...
<output omitted>
interface FastEthernet0/18
switchport mode access
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0001.435D.3057
spanning-tree portfast
spanning-tree bpduguard enable
<output omitted>
```

Este comando sirve para ver el estado de la interfaz: **show interface Fa0/18**

```
S2#show int fa0/18
```

```
FastEthernet0/18 is down, line protocol is down (err-disabled)
<output omitted>
```

```
S2#show port-security
```

```
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
          (Count)          (Count)          (Count)
-----
Fa0/18          1              1              1              Shutdown
-----
```

En el modo de interfaz de configuración del switch SW2 interface Fa0/18, utilice el **no switchport port-security mac-address sticky address** para eliminar la dirección aprendida del PC-B

```
S2(config)# int fa0/18
S2(config-if)# no switchport port-security mac-address sticky
0001.435D.3057
```

Tirar y volver a habilitar la interfaz Fa0/18

```
S2(config)# int fa0/18
S2(config-if)# shutdown
```

```
S2(config-if)# no shutdown
```

En el SW2, utilice el comando **show run** para saber la configuración del puerto y la nueva dirección MAC que se ha aprendido

```
S2#show run
```

```
Building configuration...  
<output omitted>  
interface FastEthernet0/18  
switchport mode access  
switchport port-security  
switchport port-security mac-address sticky  
switchport port-security mac-address sticky 0001.435D.BBBB  
spanning-tree portfast  
spanning-tree bpduguard enable  
<output omitted>
```

Nota: Si se desea volver a conectar el PC con la dirección MAC original, simplemente puede cambiar la dirección MAC de la PC de nuevo a la original y emitir el cierre y no cierre los comandos en el puerto Fa0/18. Si el PC o una tarjeta de red está siendo sustituido y tendrá una nueva dirección MAC, primero debe eliminar la antigua dirección aprendido

Fin.