Grado en Ingeniería Informática

Diseño de Redes de Computadores

Proyecto de Evaluación final

Jorge Antonio Sánchez Benítez

ÍNDICE

INTRODUCCIÓN

Proyecto para superar la evaluación mediante caso de estudio. 7 Hitos a resolver.

Una entidad dispone de 4 departamentos ubicados en 2 edificios de dos plantas e interconectados por una red local. Cada departamento tiene 15 empleados y todos los departamentos tienen empleados ubicados en todas las plantas.

Cada hito debe acompañarse de un estudio teórico esquematizado que incluya los conceptos y técnicas necesarios para solucionarlo. Además, se acompañará al escrito de la implementación del hito en Packet Tracer.

HITO 1

Enunciado

Se solicita que realices el diagrama de la topología lógica de la red en la que se diferencien las diferentes capas del diseño. Además ten en cuenta las siguientes consideraciones:

1. Justifica el tipo y la cantidad de switches que utilizarías para la empresa.
2. Se pretende que por encima de la capa de acceso se haga un diseño redundante a nivel de switch, a nivel de primer salto y del ISP.
3. Cada switch dispone de 24 puertos.
4. Los enlaces entre los switches se formarán por la agregación de los pares de interfaces gigabits más altas posibles.

Todos los switches deberán ser L3.

Planteamiento

En Packet Tracer he dividido la topología de lógica de red diferenciando las capas del diseño.

Existen dos edificios y dos plantas por cada edificio. En cada planta he colocado 15 PCs, ya que cada departamento tiene 15 trabajadores y ellos se encuentran trabajando en todas las plantas.

Capas de la arquitectura de red:

- En la capa de acceso hay 15 PCs más un switch L3 por cada planta.
- En la capa de distribución existe un switch L3 por cada planta.
- En la capa de núcleo hay un switch L3 en la planta 1 de cada edificio.
- Después existe el apartado de internet donde hay un router de borde nombre en la planta 1 de cada edificio.

Como tenemos que hacer la topología en packet tracer programa de cisco, voy a usar switches y routers estándares de Cisco.

He utilizado **10 switches Cisco Catalyst de la serie 3650 de L3 que disponen de 24 puertos cada uno.** Es el switch más estándar de L3 de Cisco y es el más adecuado para lo que se pide. Se les ha asignado un número del 0 al 9.

Los switches se han distribuido de la siguiente manera:

- Capa de acceso: Un switch por cada planta, total 4 switches.
  Encontramos 15 PCs conectados al switch de cada planta con cables de cobres directos y como disponemos de 24 puertos, es suficiente y nos sobran algunos puertos por si deja de funcionar alguno.
  Los PCs se conectan a las interfaces GigabitEthernet de la 0/1 a la 0/15 y cada switch conecta con los dos switches de su edificio de la capa de distribución por las interfaces GigabitEthernet 1/0/21-24 con cables de cobre cruzados.

- Capa de distribución: 2 switches por cada planta baja, total 4 switches.
  Se dispone de **redundancia a nivel de switch** ya que los dos switches de distribución de cada edificio están conectados con los dos switches de acceso de su edificio por enlaces GigabitEthernet 1/0/21-24.
  Los del edificio 1 están conectados con los 2 switches de núcleo por enlaces GigabitEthernet 1/0/17-20. Los del edificio 2 están conectados con los 2 switches de núcleo por enlaces GigabitEthernet fibra 1/1/1-4.

- Capa de núcleo: 2 switches en el edificio principal, el edificio 1.

Se dispone de **redundancia a nivel de switch** ya que cada switch de núcleo está conectado con los 2 switches de la capa de distribución del mismo edificio por enlace GigabitEthernet 1/0/21-24. Están conectados con los otros 2 switches de la capa de distribución del otro edificio por enlaces GigabitEthernet fibra 1/1/1-4. Además se conecta cada switch de núcleo con el otro núcleo por enlace GigabitEthernet 1/0/19-20. Se conectan a los routers por la interfaz GigabitEthernet 1/0/1-2.

Se dispone de **redundancia a nivel de primer salto** ya que ambos switches de núcleo están conectados a los dos routers de borde y también existe **redundancia a nivel de ISP** ya que se dispone de 2 proveedores de internet.

Se han utilizado **2 routers Cisco 2811** como routers de borde. Es un router estándar de Cisco y es el más adecuado para lo que se pide. Se les ha asignado un número del 0 al 1.

Cada router recibe internet de su proveedor y están conectados con los 2 switches de núcleo por conexiones FastEthernet 0/0-1. Además, están conectados entre ellos por una conexión FastEthernet en la interfaz fa1/0.

HITO 2

Enunciado

1. Justifica el uso o no de uno de los protocolos de negociación de la agregación de enlace.
2. Agrega los enlaces adecuados entre switches creando a su vez los troncales.
3. Justifica si utilizar VLANs de extremo a extremo o locales.
4. Genera las VLANs que consideres necesarias para una buena implementación de la red y siguiendo la justificación anterior. Crea una VLAN para la voz y otra para el Wifi.
5. Cada puesto de trabajo está formado por un PC y un teléfono, configura por tanto la VLAN de voz en los puertos donde vaya a conectarse un PC.
6. Establece un direccionamiento IP para cada VLAN utilizando la siguiente red 172.16.0.0/16.
7. Establece las puertas de enlaces para cada VLAN.
8. Establece puertos enrutados en switches conectados a dispositivos L3.
9. Establece la capacidad de enrutamiento donde lo consideres apropiado.

Sigue criterios de seguridad de red en todos los casos y recuerda que cada hito debe acompañarse de un estudio teórico esquematizado que incluya los conceptos y técnicas necesarios para solucionarlo. Además, se acompañará al escrito de la implementación del hito en Packet Tracer.

Planteamiento

He utilizado el protocolo de negociación estándar, **LACP**, de esta forma se puede negociar la creación de los **EtherChannel**.

Asegura que cuando se crea **EtherChannel**, todos los puertos tienen el mismo tipo de velocidad de configuración, configuración dúplex e información de VLAN.
Cualquier modificación de puerto después de la creación del canal también cambiará todos los otros puertos de canal.

LACP tiene 2 modos de operación, activo y pasivo. Yo he usado en ambos extremos el modo activo porque así el protocolo está habilitado y cada enlace tiene un número de enlace distinto.

He usado las **VLAN**s de extremo a extremo ya que, se puede agrupar usuarios, por seguridad por si se tiene la necesidad de confinar tráfico, por si queremos dar prioridad al tráfico aplicando QoS, para evitar el enrutamiento y para generar una **VLAN** de voz.

Se han colocado 60 teléfonos IP, 15 para cada planta y uno por cada puesto de trabajo. Un equipo está conectado al teléfono IP y este al Switch de acceso de la planta.

No se pueden usar más de 25 teléfonos IP en cada router en packet tracer, solo deja la opción de crear hasta 25. Una vez dado conectividad a los 25 teléfonos primeros, el resto saldrá error.

He establecido 2 puertos enrutados para cada switch de núcleo, ya que cada uno está conectado con los 2 routers y he activado la capacidad de enrutamiento con **ip routing** en todos los switches porque actúan como dispositivos de enrutamiento en la red.

He aplicado algunos criterios de seguridad en las Vlans como la BlackHole Vlan 1000 que tendrá los puertos caídos que no usarán cada Switch, la modificación de la Vlan nativa y la no negociación de la capacidad de enlace.

Además, he configurado la seguridad en los puertos de acceso de los Switches aplicando 3 reglas:

1. Máximo 45 MACs ya que existen 15 PCs y 15 teléfonos IP. Cada teléfono IP tiene 2 MACs, una de datos y otra de voz.
2. Cuando se produce una violación entra en modo error disable, por lo que se debe levantar con no shutdown para ponerlo operativo.
3. El tiempo que debe pasar para eliminar las MACs será de 120 minutos.

Configuración Hito 2

Switches de acceso:

Configuración del **Switch A1**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
```

```
 name VOZ
 exit
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.3 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.3 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.3 255.255.255.0
 no shutdown
 exit
interface range g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 switchport port-security
 switchport port-security maximum 45
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 2 mode active
 exit
interface range g1/0/21-22
 channel-group 3 mode active
 exit
interface port-channel 2
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 3
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Configuración del **Switch A2**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.4 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.4 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.4 255.255.255.0
 no shutdown
 exit
interface range g1/0/1-15
```

```
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 4 mode active
 exit
interface range g1/0/21-22
 channel-group 5 mode active
 exit
interface port-channel 4
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 5
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Configuración del **Switch A3**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A3 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
```

```
 name BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.5 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.5 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.5 255.255.255.0
 no shutdown
 exit
interface range g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 6 mode active
 exit
interface range g1/0/21-22
 channel-group 7 mode active
 exit
interface port-channel 6
 switchport mode trunk
 switchport nonegotiate
```

```
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 7
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Configuración del **Switch A4**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A4 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.6 255.255.255.0
 no shutdown
```

```
 exit
interface vlan 30
  ip address 172.16.30.6 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.6 255.255.255.0
 no shutdown
 exit
interface range  g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 8 mode active
 exit
interface range g1/0/21-22
 channel-group 9 mode active
 exit
interface port-channel 8
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 9
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Switches de distribución:

Configuración del **Switch D1**:

```
en
conf t
ip routing
```

```
no ip domain lookup
banner motd # D1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-16, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.7 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.7 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.7 255.255.255.0
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 2 mode active
 exit
interface range g1/0/21-22
 channel-group 4 mode active
 exit
interface range g1/0/19-20
```

```
 channel-group 10 mode active
 exit
interface range g1/0/17-18
 channel-group 11 mode active
 exit
interface port-channel 2
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 4
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 10
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 11
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Configuración del **Switch D2**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
```

```
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-16, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.8 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.8 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.8 255.255.255.0
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 3 mode active
 exit
interface range g1/0/21-22
 channel-group 5 mode active
 exit
interface range g1/0/19-20
 channel-group 12 mode active
 exit
interface range g1/0/17-18
 channel-group 13 mode active
 exit
interface port-channel 3
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 5
```

```
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 12
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 13
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Configuración del **Switch D3**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D3 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
```

```
interface range g1/0/1-20
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.9 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.9 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.9 255.255.255.0
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 6 mode active
 exit
interface range g1/0/21-22
 channel-group 8 mode active
 exit
interface range g1/1/3-4
 channel-group 14 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 15 mode active
 no shutdown
 exit
interface port-channel 6
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 8
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 14
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
```

```
 exit
interface port-channel 15
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Configuración del **Switch D4**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D4 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-20
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.10 255.255.255.0
 no shutdown
 exit
interface vlan 30
```

```
  ip address 172.16.30.10 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.10 255.255.255.0
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 7 mode active
 exit
interface range g1/0/21-22
 channel-group 9 mode active
 exit
interface range g1/1/3-4
 channel-group 16 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 17 mode active
 no shutdown
 exit
interface port-channel 7
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 9
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 16
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 17
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
ip default-gateway 192.168.1.3
```

Switches de núcleo:

Configuración del **Switch N1**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # N1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/3-18
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.11 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.11 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.11 255.255.255.0
 no shutdown
 exit
```

```
interface range g1/0/23-24
 channel-group 10 mode active
 no shutdown
 exit
interface range g1/0/21-22
 channel-group 12 mode active
 no shutdown
 exit
interface range g1/1/3-4
 channel-group 14 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 16 mode active
 no shutdown
 exit
interface range g1/0/19-20
 channel-group 18 mode active
 no shutdown
 exit
interface port-channel 10
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 12
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 14
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 16
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 18
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
```

```
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface g1/0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 exit
interface g1/0/2
 no switchport
 ip address 192.168.2.1 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 192.168.1.3
ip default-gateway 192.168.1.3
```

Configuración del **Switch N2**:

```
en
conf t
ip routing
no ip domain lookup
banner motd # N2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/3-18
 switchport mode access
 switchport access vlan 1000
 shutdown
```

```
 exit
interface vlan 20
 ip address 172.16.20.12 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.12 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.12 255.255.255.0
 no shutdown
 exit
interface range g1/0/23-24
 channel-group 11 mode active
 no shutdown
 exit
interface range g1/0/21-22
 channel-group 13 mode active
 no shutdown
 exit
interface range g1/1/3-4
 channel-group 15 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 17 mode active
 no shutdown
 exit
interface range g1/0/19-20
 channel-group 18 mode active
 no shutdown
 exit
interface port-channel 11
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 13
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30
 exit
interface port-channel 15
 switchport mode trunk
 switchport nonegotiate
```

```
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 17
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 18
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface g1/0/1
 no switchport
 ip address 192.168.1.2 255.255.255.0
 no shutdown
 exit
interface g1/0/2
 no switchport
 ip address 192.168.2.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 192.168.2.3
ip default-gateway 192.168.1.3
```

Routers:

Configuración del **Router R1**:

```
en
clock set 16:52:00 13 June 2023
conf t
hostname R1
no ip domain lookup
banner motd # This is R1 #
line con 0
 logging sync
 exec-time 0 0
 exit
interface fa0/0
 ip address 192.168.1.3 255.255.255.0
 no shutdown
 exit
interface fa0/1
```

```
 ip address 192.168.3.1 255.255.255.0
 no shutdown
 exit
interface fa1/0
 ip address 192.168.7.1 255.255.255.0
 no shutdown
 exit
interface se0/3/0
 ip address 192.168.5.1 255.255.255.0
 no shutdown
 exit
interface se0/3/1
 ip address 192.168.6.1 255.255.255.0
 no shutdown
 exit
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
 exit
telephony-service
 max-dn 30
 max-ephones 30
 ip source-address 192.168.30.1 port 2000
 auto assign 4 to 6
 exit
ephone-dn 1
number 501
ephone-dn 2
number 502
ephone-dn 3
number 503
ephone-dn 4
number 504
ephone-dn 5
number 505
ephone-dn 6
number 506
ephone-dn 7
number 507
ephone-dn 8
number 508
ephone-dn 9
number 509
ephone-dn 10
number 510
ephone-dn 11
number 511
```

```
ephone-dn 12
number 512
ephone-dn 13
number 513
ephone-dn 14
number 514
ephone-dn 15
number 515
ephone-dn 16
number 516
ephone-dn 17
number 517
ephone-dn 18
number 518
ephone-dn 19
number 519
ephone-dn 20
number 520
ephone-dn 21
number 521
ephone-dn 22
number 522
ephone-dn 23
number 523
ephone-dn 24
number 524
ephone-dn 25
number 525
ephone-dn 526
number 526
ephone-dn 527
number 527
ephone-dn 528
number 528
ephone-dn 529
number 529
ephone-dn 530
number 530
exit
```

Configuración del **Router R2**:

```
en
clock set 16:52:00 13 June 2023
conf t
hostname R2
no ip domain lookup
banner motd # This is R2 #
```

```
line con 0
 logging sync
 exec-time 0 0
 exit
interface fa0/0
 ip address 192.168.2.3 255.255.255.0
 no shutdown
 exit
interface fa0/1
 ip address 192.168.3.2 255.255.255.0
 no shutdown
 exit
interface fa1/0
 ip address 192.168.7.2 255.255.255.0
 no shutdown
 exit
interface se0/3/0
 ip address 192.168.5.2 255.255.255.0
 no shutdown
 exit
interface se0/3/1
 ip address 192.168.6.2 255.255.255.0
 no shutdown
exit
router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
 exit
telephony-service
 max-dn 60
 max-ephones 30
 ip source-address 192.168.30.2 port 2000
 auto assign 4 to 6
 exit
ephone-dn 31
number 531
ephone-dn 32
number 532
ephone-dn 33
number 533
ephone-dn 34
number 534
ephone-dn 35
number 535
ephone-dn 36
number 536
ephone-dn 37
```

```
number 537
ephone-dn 38
number 538
ephone-dn 39
number 539
ephone-dn 40
number 540
ephone-dn 41
number 541
ephone-dn 42
number 542
ephone-dn 43
number 543
ephone-dn 44
number 544
ephone-dn 45
number 545
ephone-dn 46
number 546
ephone-dn 47
number 547
ephone-dn 48
number 548
ephone-dn 49
number 549
ephone-dn 50
number 550
ephone-dn 51
number 551
ephone-dn 52
number 552
ephone-dn 53
number 553
ephone-dn 54
number 554
ephone-dn 55
number 555
ephone-dn 556
number 556
ephone-dn 557
number 557
ephone-dn 558
number 558
ephone-dn 559
number 559
ephone-dn 560
number 560
exit
```

Verificación:
show mac address-table dynamic
show ip cef
show adjacency
show adjacency detail
show interfaces trunk
show etherchannel summary

HITO 3

Enunciado

1. Justifica el uso del STP y haz un estudio teórico genérico de éste.
2. Analiza la versión de STP que sea estándar y más moderna.
3. Analiza los mecanismos de estabilidad del STP que consideres necesarios.
4. Crea un diagrama que muestre cómo deben quedar el rol de los puentes y los puertos por VLAN.
5. Configura el STP en su versión estándar y más moderna con redundancia del puente raíz y que ofrezca redundancia por VLAN.
6. Pon en marcha los mecanismos de estabilidad del STP.
7. Implementalo en packet tracert.

Sigue criterios de seguridad de red en todos los casos y recuerda que cada hito debe acompañarse de un estudio teórico esquematizado que incluya los conceptos y técnicas necesarios para solucionarlo. Además, se acompañará al escrito con la mejor implementación posible del hito en Packet Tracer.

Planteamiento

STP (Spanning Tree Protocol)

STP proporciona un mecanismo de evitación de bucles en topologías redundantes. Queda activa una única ruta en cada segmento bloqueando el resto de rutas. Los switches se envían BPDUs cada 2 segundos para mantener una topología libre de bucles en la que los enlaces redundantes están bloqueados.

Además, si la topología cambia por algún motivo, **STP** restablece la conectividad automáticamente.

Es necesario el uso de STP para protegernos de bucles en la topología.

Existen 5 versiones:

1. CST (Spanning Tree Protocol) o STP. Estándar 802.1D
2. PVST + (Protocolo de Spanning Tree Plus Por VLAN). Estándar Cisco
3. RSTP (STP Rápido). Estándar 802.1w
4. RPVST + (Rapid PVST +). Estándar Cisco
5. MST (Multiple Spanning Tree). Estándar 802.1s

Algunos de los términos de este protocolo son:

- **Puente raíz**: Puente/switch único y puente de referencia que hace de raíz del árbol de switches resultante del STP. Todo camino no necesario para llegar a él se bloqueará y todos sus puertos reenvían tráfico.
- **Puerto raíz**: Puerto de un switch no raíz que tiene el mejor camino (menor coste) al puente raíz y es único dentro del switch.
- **Puerto designado**: Puerto que envía y recibe tramas en dirección al puente raíz. En el puente raíz todos los puertos son designados y en el puente no raíz, el designado es el que pertenece al switch con mejor camino al puente raíz. Sólo existe uno en cada segmento.
- **Puerto no designado**: Puertos que no son raíz ni designados y que acaban bloqueados (no reenvían tramas).
- **Puerto deshabilitado**: puerto caído.
- **Coste del camino**: Valor que cuesta el paso de un switch a otro por un camino concreto. Este camino puede estar formado por varios segmentos y se formula en base a la velocidad.

La información de **STP** entre switches se intercambia en **BPDU**s.

Un switch envía tramas **BPDU**s por cada puerto a través de la dirección MAC multicast 0180:c200:0000.

Mecanismos de estabilidad en STP

Existen diferentes **mecanismos de estabilidad**, estos ayudan a STP a converger más rápido y aumentar el rendimiento:

- **UplinkFast**: permite una rápida convergencia cuando se produce un error en el enlace ascendente de un switch de acceso.
- **BackboneFast**: permite una rápida convergencia en la capa distribución o en la capa núcleo cuando se produce un cambio de STP.
- **PortFast**: configura el puerto de acceso para pasar directamente al estado de reenvío.

Otros, alteran la forma en que la red debería reaccionar en caso de un cambio no esperado en la topología de la red:

- **BPDU Guard**: desactiva el puerto habilitado para PortFast si se recibe una BPDU.
- **BPDU Filter**: suprime BPDUs en determinados puertos.
- **Root Guard**: evita que determinados switches se conviertan en raíz.
- **Loop Guard**: evita que un puerto alternativo se convierta en designado si no se reciben BPDUs.

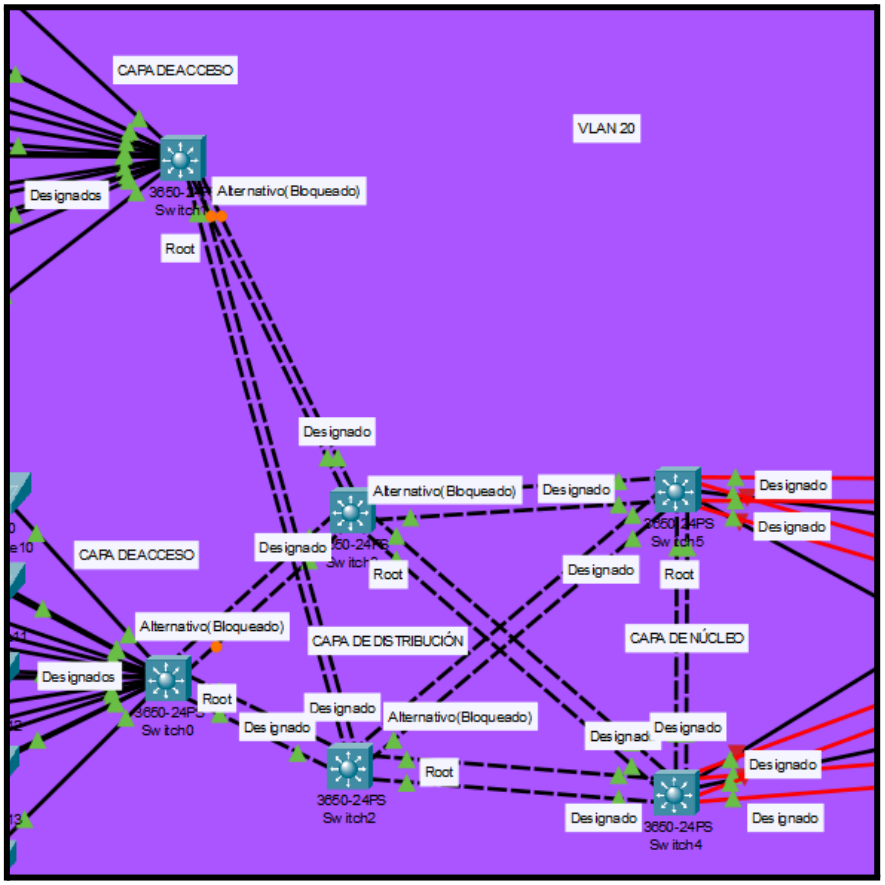
UDLD: complementa el funcionamiento detectando enlaces unidireccionales.
FlexLink: reemplaza STP por un sistema más simple.

Esta sería la descripción de mi **diseño** y pasos que seguiré en la configuración del rol de los puentes y los puertos para las VLAN 20 (Datos) y 30 (Voz)en el protocolo **RPVST+**.

- VLAN 20:
    - Selecciono un switch como el puente raíz para VLAN 20 estableciendo su prioridad de puente como la más baja entre los switches en la red.
    - Configuro los enlaces hacia otros switches como puertos troncales para permitir el paso de VLAN 20.
    - Cada switch debe tener uno o más puertos designados como puertos de acceso para conectar los dispositivos finales en VLAN 20.

- VLAN 30:
    - Selecciono el otro switch como el puente raíz para VLAN 30 estableciendo su prioridad de puente como la más baja entre los switches en la red.
    - Configura los enlaces hacia otros switches como puertos troncales para permitir el paso de VLAN 30.
    - Cada switch debe tener uno o más puertos designados como puertos de acceso para conectar los dispositivos finales en VLAN 30.

VLAN 20 | Edificio 1



Switches de Acceso:

- Switch 0 / A1:
    - Puerto raíz: Port-channel 2
    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 3
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

- Switch 1 / A2:
    - Puerto raíz: Port-channel 4
    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 5
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

Switches de Distribución:

- Switch 2 / D1:
    - Puerto raíz: Port-channel 10
    - Puertos designados: Port-channel 2 y 4
    - Puerto Alternativo: Port-channel 11
    - Puertos deshabilitados: g1/0/1-16, g1/1/1-4

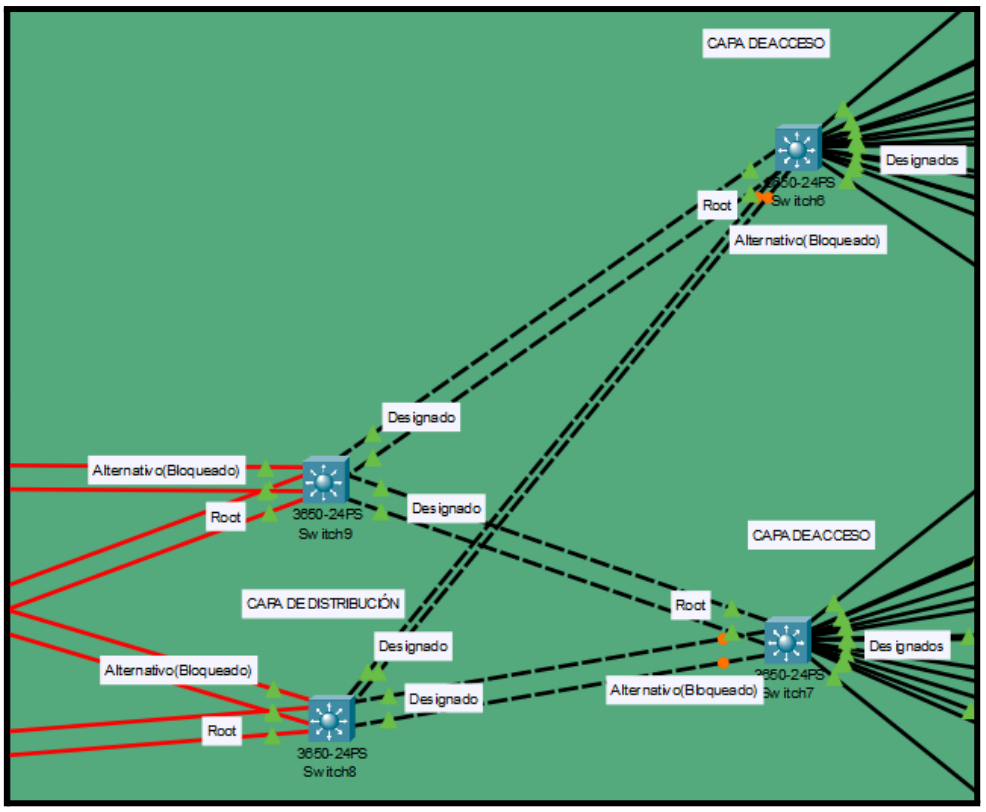
- Switch 3 / D3:
    - Puerto raíz: Port-channel 12
    - Puertos designados: Port-channel 3 y 5
    - Puerto Alternativo: Port-channel 13
    - Puertos deshabilitados: g1/0/1-16, g1/1/1-4

Switches de Núcleo:

- Switch 4 / N1 (**Puente Raíz**):
    - Puertos designados: Port-channel 10, 12, 14, 16 y 18
    - Puertos deshabilitados: g1/0/1-18

- Switch 5 / N2:
    - Puerto raíz: Port-channel 18
    - Puertos designados: Port-channel 11, 13, 15 y 17
    - Puertos deshabilitados: g1/0/1-18

VLAN 20 | Edificio 2



Switches de Acceso:

- Switch 6 / A4:
    - Puerto raíz: Port-channel 9
    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 8
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

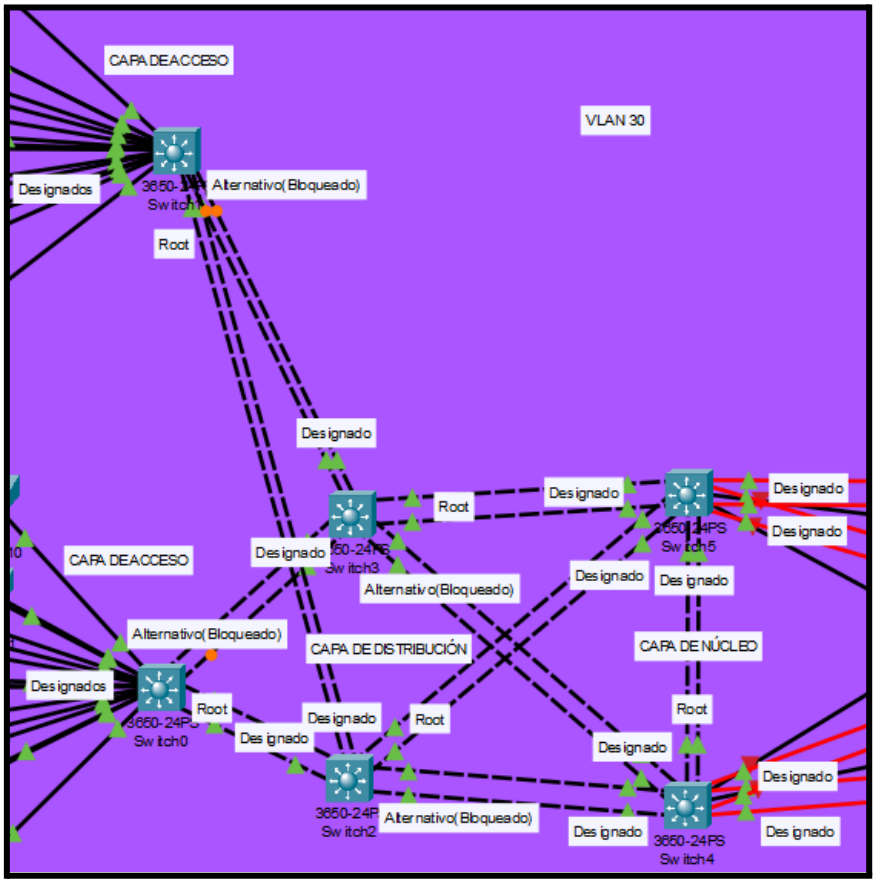
- Switch 7 / A3:
    - Puerto raíz: Port-channel 7
    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 6
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

Switches de Distribución:

- Switch 8 / D3:
    - Puerto raíz: Port-channel 14
    - Puertos designados: Port-channel 6 y 8
    - Puerto Alternativo: Port-channel 15
    - Puertos deshabilitados: g1/0/1-20

- Switch 9 / D4:
    - Puerto raíz: Port-channel 16
    - Puertos designados: Port-channel 7 y 9
    - Puerto Alternativo: Port-channel 17
    - Puertos deshabilitados: g1/0/1-20

VLAN 30 | Edificio 1



Switches de Acceso:

- Switch 0 / A1:
    - Puerto raíz: Port-channel 2
    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 3
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

- Switch 1 / A2:
    - Puerto raíz: Port-channel 4
    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 5
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

Switches de Distribución:

- Switch 2 / D1:
    - Puerto raíz: Port-channel 11
    - Puertos designados: Port-channel 2 y 4
    - Puerto Alternativo: Port-channel 10
    - Puertos deshabilitados: g1/0/1-16, g1/1/1-4

- Switch 3 / D2:

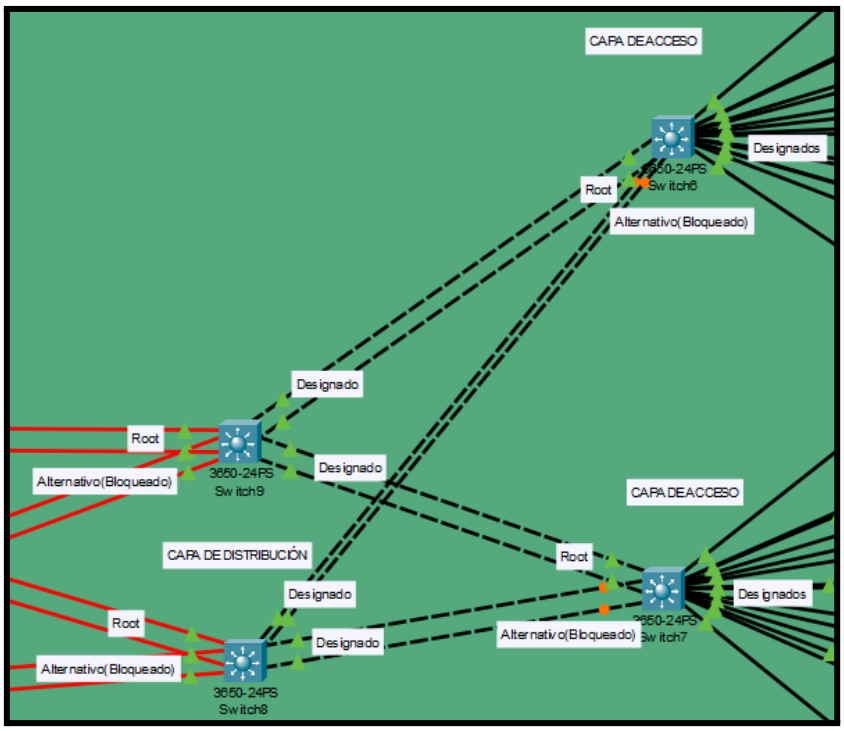
- Puerto raíz: Port-channel 13
- Puertos designados: Port-channel 3 y 5
- Puerto Alternativo: Port-channel 12
- Puertos deshabilitados: g1/0/1-16, g1/1/1-4

Switches de Núcleo:

- Switch 4 / N1:
  - Puerto raíz: Port-channel 18
  - Puertos designados: Port-channel 10, 12, 14 y 16
  - Puertos deshabilitados: g1/0/1-18

- Switch 5 / N2 (**Puente Raíz**):
  - Puertos designados: Port-channel 11, 13, 15, 17 y 18
  - Puertos deshabilitados: g1/0/1-18

VLAN 30 | Edificio 2



Switches de Acceso:

- Switch 6 / A4:
  - Puerto raíz: Port-channel 9
  - Puertos designados: g1/0/1-15
  - Puerto Alternativo: Port-channel 8
  - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

- Switch 7 / A3:
  - Puerto raíz: Port-channel 7

    - Puertos designados: g1/0/1-15
    - Puerto Alternativo: Port-channel 6
    - Puertos deshabilitados: g1/0/16-20, g1/1/1-4

Switches de Distribución:

- Switch 8 / D3:
    - Puerto raíz: Port-channel 15
    - Puertos designados: Port-channel 6 y 8
    - Puerto Alternativo: Port-channel 14
    - Puertos deshabilitados: g1/0/1-20

- Switch 9 / D4:
    - Puerto raíz: Port-channel 17
    - Puertos designados: Port-channel 7 y 9
    - Puerto Alternativo: Port-channel 16
    - Puertos deshabilitados: g1/0/1-20

Configuración Rapid-PVST+

RPVST+ es el protocolo más moderno y estándar que funciona en packet tracer, y por ello será el utilizado en las configuraciones en packet tracer.

Debería usar los siguientes mecanismos de seguridad: UplinkFast, BackboneFast, PortFast, BPDU Guard, Root Guard, Loop Guard y UDLD. Por limitaciones de packet tracer solo puedo configurar en los switches: **PortFast, BPDU Guard y Root Guard**.

Pero dejo la configuración de cómo deberían configurarse el resto de mecanismos que packet tracer no reconoce, y por tanto no funcionan. También se podría modificar las prioridades o los costes de los puertos para cambiar los puertos raíz de cada switch con **spanning-tree cost "x"** o **spanning-tree port-priority "x".**

Switches de acceso:

Configuración del **Switch A1**:

```
spanning-tree mode rapid-pvst
interface range g1/0/1-15
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree uplinkfast
 exit
interface port-channel 2
 spanning-tree uplinkfast
 exit
interface port-channel 3
 spanning-tree guard loop
```

```
 spanning-tree uplinkfast
 exit
```

Configuración del **Switch A2**:

```
spanning-tree mode rapid-pvst
interface range g1/0/1-15
 spanning-tree portfast
 spanning-tree bpduguard enable
 spanning-tree uplinkfast
 exit
interface port-channel 4
 spanning-tree uplinkfast
 exit
interface port-channel 5
 spanning-tree guard loop
 spanning-tree uplinkfast
 exit
```

Configuración del **Switch A3**:

```
spanning-tree mode rapid-pvst
interface range g1/0/1-15
 spanning-tree portfast
 spanning-tree bpduguard enable
  spanning-tree uplinkfast
 exit
interface port-channel 6
 spanning-tree guard loop
 spanning-tree uplinkfast
 exit
interface port-channel 7
 spanning-tree uplinkfast
 exit
```

Configuración del **Switch A4**:

```
spanning-tree mode rapid-pvst
interface range g1/0/1-15
 spanning-tree portfast
 spanning-tree bpduguard enable
  spanning-tree uplinkfast
 exit
interface port-channel 8
spanning-tree guard loop
 spanning-tree uplinkfast
 exit
interface port-channel 9
```

```
 spanning-tree uplinkfast
 exit
```

Switches de distribución:

Configuración del **Switch D1**:

```
spanning-tree mode rapid-pvst
interface port-channel 2
 spanning-tree guard root
 exit
interface port-channel 4
 spanning-tree guard root
 exit
interface port-channel 10
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 11
 spanning-tree backbonefast
 udld port agressive
 exit
```

Configuración del **Switch D2**:

```
spanning-tree mode rapid-pvst
interface port-channel 3
 spanning-tree guard root
 exit
interface port-channel 5
 spanning-tree guard root
 exit
interface port-channel 12
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 13
 spanning-tree backbonefast
 udld port agressive
 exit
```

Configuración del **Switch D3**:

```
spanning-tree mode rapid-pvst
interface port-channel 6
 spanning-tree guard root
 exit
```

```
interface port-channel 8
 spanning-tree guard root
 exit
interface port-channel 14
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 15
 spanning-tree backbonefast
 udld port agressive
 exit
```

Configuración del **Switch D4**:

```
spanning-tree mode rapid-pvst
interface port-channel 7
 spanning-tree guard root
 exit
interface port-channel 9
 spanning-tree guard root
 exit
interface port-channel 16
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 17
 spanning-tree backbonefast
 udld port agressive
 exit
```

Switches de núcleo:

Configuración del **Switch N1**:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 8192
spanning-tree vlan 999 priority 16384
spanning-tree vlan 1000 priority 32768
interface port-channel 10
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 12
 spanning-tree backbonefast
 udld port agressive
 exit
```

```
interface port-channel 14
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 16
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 18
 spanning-tree backbonefast
 udld port agressive
 exit
```

Configuración del **Switch N2**:

```
spanning-tree mode rapid-pvst
spanning-tree vlan 30 priority 4096
spanning-tree vlan 20 priority 8192
spanning-tree vlan 999 priority 16384
spanning-tree vlan 1000 priority 32768
interface port-channel 11
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 13
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 15
 spanning-tree backbonefast
  udld port agressive
 exit
interface port-channel 17
 spanning-tree backbonefast
 udld port agressive
 exit
interface port-channel 18
 spanning-tree backbonefast
 udld port agressive
 exit
```

Verificación:

```
show spanning-tree
show spanning-tree vlan20
show spanning-tree vlan30
show spanning-tree vlan1000
show spanning-tree blockedports
```

show spanning-tree root

MST(Árbol de expansión múltiple)

La versión estándar y más moderna para **STP** que hemos estudiado en este curso es el **MST**. Este protocolo no lo admite el simulador de packet tracer.

Está recogido en el estándar 802.1s como se mencionó anteriormente y extiende a RSTP a múltiples instancias.

Se basa en crear diferentes instancias **STP** para grupos de VLANs, cada instancia se utiliza en un conjunto de VLANs. Reduce la carga de la CPU al evitar una **instancia** por VLAN. Además, admite hasta 4096 VLANs.

Ofrece **balanceo de carga** ya que, cada **instancia** puede generar una topología distinta.

En redes grandes, para mejorar la administración, pueden existir conjuntos de switches que usen las VLANs de manera diferente y que difieran en las topologías del árbol de expansión. En cada grupo de switches puede existir un grupo de **instancias MST** distintas.

La **región MST** es el conjunto de switches interconectados con la misma configuración MST.

SPB(Shortest Path Bridging)

La versión estándar y más moderna para **STP** actual es el **SPB** y está recogido en el estándar 802.1aq.

Esta versión no está implementada en Packet Tracer pero como encontré un poco de información la voy a mostrar en esta memoria.

SPB permite el enrutamiento de rutas múltiples en una red de Ethernet mediante el uso de IS-IS como protocolo de control. La tecnología permite que todas las rutas estén activas, admite rutas de igual costo y proporciona el reenvío de la ruta más corta en una red de Ethernet.

Además, proporciona una convergencia más rápida, una mayor eficiencia de enlace y topologías de capa 2 más grandes que los protocolos de árbol de expansión convencionales, como MST.

Algunos de los términos de este protocolo son:

- **Área**: Subdominio de una red SPBM. El dispositivo solo admite un área.
- **BCB**: Los puentes centrales troncales son nodos centrales de una red SPBM. Los BCB reenvían tramas MAC-in-MAC basadas en B-MAC y B-VLAN.
- **BEB**: Los puentes de borde troncales son nodos de borde de la red SPB. Los BEB encapsulan tramas de clientes en tramas MAC-in-MAC antes de enviarlas a la red SPBM. Los BEB también desencapsulan tramas MAC-in-MAC antes de enviarlas al sitio de un cliente.

- **B-MAC**: Las direcciones MAC de red troncal son direcciones MAC de puente asociadas con puentes SPBM.

- **B-VLAN**: Las VLAN troncales son VLAN asignadas por el proveedor de servicios para transmitir tráfico de clientes en la red SPBM.

- **ISIS-SPB**: ISIS-SPB es el protocolo de control para una red SPB para calcular árboles de ruta más corta (SPT) y mantener adyacencias entre vecinos.

- **I-SID**: Un identificador de instancia de servicios de red troncal identifica de manera única una instancia de servicio MAC-in-MAC.

- **LSDB**: Una base de datos de estado de enlaces contiene los estados de todos los enlaces en una red SPB.

- **MAC-in-MAC**: SPB encapsula tramas Ethernet en tramas MAC-in-MAC mediante el uso de encapsulación PBB 802.1ah. Las tramas de los clientes se encapsulan en formato MAC-in-MAC en los bordes de la red SPBM antes de que se reenvíen de un sitio de cliente a otro.

- **SPB VSI**: Una instancia de servicio virtual SPB proporciona un servicio de túnel MAC-in-MAC para instancias de servicio Ethernet. Cada SPB VSI se identifica de forma única mediante un I-SID.

- **Tipos de paquetes SPB**: Existen dos tipos de paquetes, los de control y los de datos.

    - **Paquetes de control ISIS-SPB**:

        - **Hello**: Los vecinos de SPBM envían PDUs de saludo IS-IS para establecer y mantener adyacencias.

        - **LSP**: Los vecinos de SPB adyacentes envían PDUs de estado de enlace para anunciar datos de topología.

        - **SNP**: Los vecinos adyacentes de SPB intercambian PDU de número de secuencia (SNP) para la sincronización de LSDB. Los SNP incluyen SNP completo (CSNP) y SNP parcial (PSNP).

            - **CSNP**: contiene el resumen de cada LSP en LSDB. Los enrutadores adyacentes intercambian CSNP para mantener la sincronización de LSDB.

            - **PSNP**: contiene los números de secuencia de los LSP recibidos recientemente. Un nodo SPB usa un PSNP para reconocer los LSP o para solicitar los LSP necesarios de un vecino.

- **Paquetes de datos SPB**: Los paquetes de datos SPB utilizan el formato de trama MAC-in-MAC IEEE 802.1ah. En la siguiente foto se muestran todos los campos del encabezado de las tramas encapsuladas.

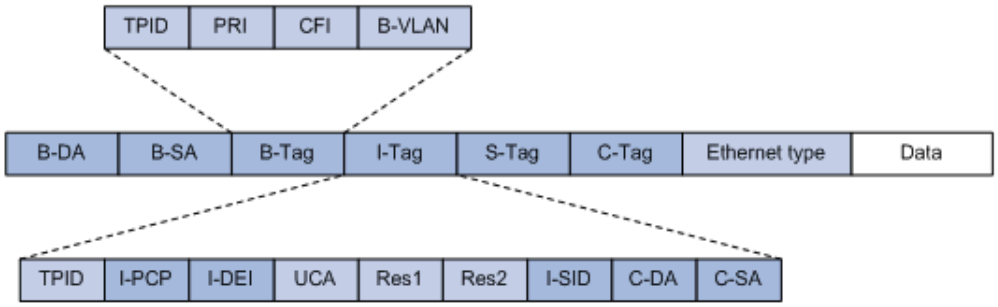


Tabla 1 Campos de encabezado de trama encapsulados IEEE 802.1ah

Campo	Descripción
BDA	B-MAC de destino que identifica el BEB de destino.
B-SA	Fuente B-MAC. Es una dirección MAC conocida del BEB que encapsula la trama MAC-in-MAC.
Etiqueta B	La etiqueta B-VLAN identifica el ID de VLAN y la prioridad de la trama en la red SPBM. El TPID en la etiqueta se fija en 0x8100.
I-etiqueta	La etiqueta de instancia de servicio de red troncal contiene los siguientes subcampos: • TPID : un valor fijado en 0x88E7 para identificar la trama como una trama encapsulada 802.1ah. • I-PCP — Prioridad de transmisión de la trama en el BEB. • I-DEI —Prioridad de caída de la trama en el BEB. • I-SID: identificador de instancia de servicio de red troncal. • C-DA : dirección MAC de destino del cliente. • C-SA : dirección MAC de origen del cliente.
Ciervo	Este campo contiene el ID y la prioridad de la VLAN del cliente externo.
Etiqueta C	Este campo contiene la prioridad y el ID de VLAN del cliente interno.

¿Cómo funciona y trabaja exactamente las redes SPB?

SPB utiliza ISIS-SPB en el plano de control para calcular árboles de ruta más corta. Utiliza la encapsulación PBB IEEE 802.1ah en el plano de datos para encapsular y reenviar el tráfico.

El siguiente proceso genérico es utilizado para calcular SPT y reenviar tráfico:

- BEBs y BCBs envían saludos ISIS-SPB P2P para establecer y mantener adyacencias.

- Los nodos adyacentes envían LSP para anunciar sus respectivos datos de topología. Eventualmente, los LSDB de todos los nodos se sincronizan.

- Cada nodo selecciona la ruta de reenvío:

    - Cada nodo ejecuta SPF para calcular la ruta más corta desde sí mismo hasta cada uno de los otros nodos.

    - Si hay rutas de igual costo disponibles, cada nodo ejecuta ECT para elegir la mejor ruta de reenvío.

    - Los nodos llenan sus respectivas tablas FDB y FIB con la ruta de reenvío.

- Los BEB establecen PW sobre la red SPBM para transmitir tráfico de clientes.

Además, existen dos modos de multidifusión:

- **Replicación de cabecera** : replica tramas en el BEB de ingreso para que las tramas ingresen a la red SPBM. Este método es adecuado para SPB que tienen un tráfico de multidifusión escaso.

- **Replicación en tándem** : replica tramas únicamente en el nodo donde se bifurca el árbol de la ruta más corta. Este método es adecuado para SPB que tienen un tráfico de multidifusión denso.

Configuración SPB

No he encontrado demasiada información acerca de configurar este protocolo, pero la que he encontrado no puedo comprobar si funciona, ya que packet tracer no soporta este protocolo.

A continuación, se mostrará la configuración de una red SPB formada por Switches BEB y BCB. Los switches de acceso y distribución son los BEB y los switches de núcleo son los BCB.

Fuente: **H3C S12508X-AF LSXM1SFH08C1 Card Manual-6PW102 - 01-SPBM configuration**

Configuración de los switches de acceso
Configuración de los identificadores de servicio (I-SIDs):
isid 100 vlan 20
isid 200 vlan 30

Configuración de enlaces físicos:
interface range g1/0/1-15
spbm link access
exit
interface range g1/0/21-24
spbm link routing

exit

Configuración de protocolos SPBM:
spbm enable
spbm protocol isis
spbm protocol rstp

Configuración de árboles multicast:
multicast tree isis
enable
exit
multicast tree igmp
enable
exit

Configuración de los switches de distribución
Configuración de los identificadores de servicio (I-SIDs):
isid 100 vlan 20
isid 200 vlan 30

Configuración de enlaces físicos:
interface range g1/0/17-24
spbm link routing
exit

Configuración de protocolos SPBM:
spbm enable
spbm protocol isis
spbm protocol rstp

Configuración de árboles multicast:
multicast tree isis
enable
exit
multicast tree igmp
enable
exit

Configuración de los switches de núcleo:
Configuración de los identificadores de servicio (I-SIDs):
isid 100 vlan 20
isid 200 vlan 30

Configuración de enlaces físicos:
interface range g1/0/17-24, g1/1/1-4
spbm link routing

exit

Configuración de protocolos SPBM:
spbm enable
spbm protocol isis
spbm protocol rstp

Configuración de árboles multicast:
multicast tree isis
enable
exit
multicast tree igmp
enable
exit

HITO 4

Enunciado

El hito 4 tiene tres partes y el enunciado es el siguiente:

NTP:

- Justifica y analiza el protocolo NTP.
- Diseña la implantación de NTP en tu red aplicando distintos modos de trabajo en función del tipo de switch.
- Configura un NTP en función del diseño anterior.
- Implementalo en PT.

FHRP:

- Justifica y analiza los diferentes protocolos de redundancia de primer salto.
- Estudia cuál de ellos utilizarías para implantarlo en tu red.
- Configura dicho protocolo incorporando las características de prioridad, preferencia, tracking y autentificación.
- Implementalo en PT.

NAT:

- Justifica y analiza el uso de NAT.
- Configura PAT en tu red.
- Implementalo en PT.

Incorpora este hito a los anteriores.

Sigue criterios de seguridad de red en todos los casos y recuerda que cada hito debe acompañarse de un estudio teórico esquematizado que incluya los conceptos y técnicas necesarios para solucionarlo. Además, se acompañará al escrito con la mejor implementación posible del hito en Packet Tracer.

Planteamiento

Protocolo NTP (Network Time Protocol)

El Protocolo de Tiempo de Red (**NTP**) es un protocolo utilizado para sincronizar los relojes de los sistemas en una red. Su función principal es asegurar que todos los dispositivos de la red tengan una referencia de tiempo precisa y consistente. Esto es imprescindible para muchas aplicaciones que dependen de la sincronización precisa, como el registro de eventos, la seguridad de red, la planificación y la coordinación de tareas.

Justificación y análisis de NTP:

- Sincronización precisa: El NTP permite la sincronización de relojes en toda la red, lo que garantiza que los dispositivos tengan la misma referencia de tiempo. Esto es crucial para evitar problemas de desincronización y asegurar que los eventos se registren correctamente en todos los dispositivos.

- Tolerancia a fallos: El NTP utiliza un algoritmo de selección de servidores y una arquitectura jerárquica para garantizar la disponibilidad y la redundancia. Si un servidor NTP falla, los dispositivos pueden seleccionar automáticamente otro servidor para mantener la sincronización.

- Escalabilidad: NTP puede manejar redes de cualquier tamaño, desde pequeñas redes locales hasta redes globales distribuidas. Su diseño permite una escalabilidad eficiente y una sincronización precisa incluso en entornos de red complejos.

- Seguridad: El NTP admite la autenticación y el cifrado para garantizar la integridad y la seguridad de la sincronización. Esto evita ataques maliciosos o falsificación de tiempo.

Diseño de la implantación de NTP en la red con diferentes modos de trabajo en función del tipo de switch:

Switches de capa de acceso:
Estos switches generalmente no requieren una configuración NTP compleja, ya que su principal función es proporcionar conectividad a los dispositivos finales. Pueden funcionar en modo cliente NTP, sincronizándose con los servidores NTP de nivel superior en la jerarquía de la red.

Switches de capa de distribución:
Estos switches pueden actuar tanto como clientes NTP, sincronizándose con los servidores NTP de nivel superior, como servidores NTP para los switches de capa de acceso. Esto permite que los switches de acceso se sincronicen con los de distribución.

Switches de capa de núcleo:
Estos switches pueden actuar como servidores NTP maestros en la red. Son los responsables de mantener una referencia de tiempo precisa y proporcionar sincronización a todos los dispositivos en la red. Estos switches deben estar configurados como servidores NTP y sincronizarse con fuentes de tiempo confiables, como relojes atómicos o servidores NTP públicos.

Configuración NTP

En packet tracer no se puede usar el comando ntp broadcast, no está implementado, por lo que es ntp pierde usabilidad.

Switches de acceso:

Configuración del **Switch A1**:
clock timezone EST -5
ntp server 172.16.20.11

Configuración del **Switch A2**:
clock timezone EST -5
ntp server 172.16.20.12

Configuración del **Switch A3**:
clock timezone EST -5
ntp server 172.16.20.11

Configuración del **Switch A4**:
clock timezone EST -5
ntp server 172.16.20.12

Switches de distribución:

Configuración del **Switch D1**:
clock timezone EST -5
ntp server 172.16.20.11

Configuración del **Switch D2**:
clock timezone EST -5
ntp server 172.16.20.12

Configuración del **Switch D3**:
clock timezone EST -5

ntp server 172.16.20.11

Configuración del **Switch D4**:
clock timezone EST -5
ntp server 172.16.20.12

Switches de núcleo:

Configuración del **Switch N1**:
clock timezone EST -5
ntp server 192.168.2.3

Configuración del **Switch N2**:
clock timezone EST -5
ntp server 192.168.1.3

Routers:

Configuración del **Router R1:**
ntp master 10
clock timezone EST -5

Configuración del **Router R2:**
ntp master 5
clock timezone EST -5

Verificación:
show clock detail
show ntp status
show ntp associations

Los protocolos de redundancia de primer salto (First Hop Redundancy Protocols, FHRP)

FHRP se utiliza para proporcionar redundancia y alta disponibilidad en la capa de red al permitir que varios routers actúen como un único gateway predeterminado para los hosts en una red. Estos protocolos permiten una conmutación rápida y automática del tráfico hacia un router de respaldo en caso de que el router principal falle.

Los protocolos de redundancia de primer salto que hemos estudiado son:

- **HSRP** (Hot Standby Router Protocol): HSRP es un protocolo propietario desarrollado por Cisco. Permite que varios routers compartan la misma dirección IP virtual como gateway predeterminado. Un router es designado como el router activo y los demás se mantienen en espera. Si el router activo falla, uno de los routers en espera asume el rol activo y continúa proporcionando conectividad a los hosts.

- **VRRP** (Virtual Router Redundancy Protocol): VRRP es un protocolo estándar definido en el RFC 5798. Es similar a HSRP y permite que varios routers compartan una dirección IP virtual. Un router es designado como el router maestro, mientras que los demás son routers de respaldo. El router maestro responde a las solicitudes ARP y enruta el tráfico hacia el gateway virtual. Si el router maestro falla, otro router de respaldo asume el rol de maestro.

- **GLBP** (Gateway Load Balancing Protocol): GLBP es otro protocolo propietario de Cisco. A diferencia de HSRP y VRRP, GLBP permite una distribución de carga activa entre los routers en lugar de tener un router activo y el resto en espera. Los hosts envían tráfico a través de diferentes routers, lo que permite una mejor utilización de los recursos disponibles.

La elección del protocolo de redundancia de primer salto depende de los requisitos y características de la red. Si se utilizan principalmente equipos de Cisco, HSRP o GLBP pueden ser opciones viables. Si se prefiere un protocolo estándar y compatible con múltiples fabricantes, VRRP es una buena opción.

Para la configuración del protocolo seleccionado, incorporando características como prioridad, preferencia, tracking y autenticación, proporcionaré un ejemplo de configuración para HSRP.

Configuración HSRP

Este protocolo solo es aplicable a los switches de la capa de núcleo, ya que están directamente conectados a los routers.

No se puede autenticar este protocolo en packet tracer, si se pudiera habría que añadir por ejemplo en la interfaz vlan 20, **standby 20 authentication md5 key-string cisco123,** en la interfaz vlan 30, **standby 30 authentication md5 key-string cisco123** y en la interfaz vlan 1000, **standby 1000 authentication md5 key-string cisco123**

Switches de núcleo:

Configuración del **Switch N1**:

```
interface vlan 20
 standby version 2
 standby 20 ip 172.16.20.254
 standby 20 priority 150
 standby 20 preempt
 exit
interface vlan 30
```

```
 standby version 2
 standby 30 ip 172.16.30.254
 standby 30 preempt
exit
interface vlan 1000
 standby version 2
 standby 1000 ip 172.16.100.254
 standby 1000 priority 90
 standby 1000 preempt
exit
```

Configuración del **Switch N2**:

```
interface vlan 20
 standby version 2
 standby 20 ip 172.16.20.254
 standby 20 preempt
 exit
interface vlan 30
 standby version 2
 standby 30 ip 172.16.30.254
 standby 30 priority 150
 standby 30 preempt
exit
interface vlan 1000
 standby version 2
 standby 1000 ip 172.16.100.254
 standby 1000 priority 90
 standby 1000 preempt
exit
```

Verificación:

```
show standby brief
show standby
```

Configuración VRRP

Este protocolo es el que hubiera usado si packet tracer lo permitiera, pero no es el caso. He usado el protocolo **HSRP**, aunque así sería como estaría la configuración para mi topología de **VRRP**.

Configuración del **Switch N1**:

```
fhrp version vrrp v3
interface vlan 20
 vrrp 20 address-family ipv4
 address 172.16.20.254
 priority 150
```

```
 exit
fhrp version vrrp v3
interface vlan 30
 vrrp 30 address-family ipv4
 address 172.16.30.254
 exit
interface vlan 1000
 vrrp 1000 address-family ipv4
 address 172.16.100.254
 priority 80
 exit
track 8 interface fa0/0 line-protocol
 exit
interface vlan 20
 vrrp 20 address-family ipv4
 track 8 decrement 60
 exit
```

Configuración del **Switch N2**:

```
fhrp version vrrp v3
interface vlan 20
 vrrp 20 address-family ipv4
 address 172.16.20.254
 exit
fhrp version vrrp v3
interface vlan 30
 vrrp 30 address-family ipv4
 address 172.16.30.254
 priority 150
 exit
interface vlan 1000
 vrrp 1000 address-family ipv4
 address 172.16.100.254
 priority 80
 exit
track 8 interface fa0/0 line-protocol
 exit
interface vlan 30
 vrrp 30 address-family ipv4
 track 8 decrement 60
 exit
```

Verificación:

```
show vrrp
show vrrp brief
```

La traducción de direcciones de red (NAT)

NAT es una técnica utilizada en redes para permitir la comunicación entre diferentes redes con direcciones IP incompatibles.

Aquí se presentan algunas justificaciones y análisis del uso de NAT:

- Escasez de direcciones IPv4: Con el agotamiento de las direcciones IPv4, NAT se convierte en una solución para utilizar una dirección IP pública única para múltiples dispositivos privados en una red. Esto ayuda a maximizar el uso de las direcciones IP disponibles y facilita la conexión a Internet para varias máquinas en una red interna.

- Seguridad y ocultamiento de la red interna: NAT proporciona un nivel adicional de seguridad al ocultar las direcciones IP privadas detrás de una dirección IP pública. Esto dificulta que los dispositivos externos accedan directamente a los dispositivos internos, lo que brinda una capa de protección contra ataques externos.

- Acceso a Internet compartido: Con NAT, varios dispositivos en una red interna pueden compartir una única dirección IP pública para acceder a Internet. Esto es especialmente útil en entornos domésticos o pequeñas oficinas donde se requiere conectividad a Internet para múltiples dispositivos, como computadoras, teléfonos inteligentes y tabletas.

- Flexibilidad en la reestructuración de la red: NAT permite cambios en la infraestructura de red sin afectar las direcciones IP públicas utilizadas para acceder a los servicios. Esto es beneficioso cuando se realiza una reorganización de la red o se cambia de proveedor de servicios de Internet, ya que no es necesario reconfigurar todas las direcciones IP en la red interna.

Configuración NAT

Este protocolo solo es aplicable a los routers.

Routers:

Configuración del **Router R1**:

```
access-list 1 permit 172.16.20.0 0.0.0.255
access-list 2 permit 172.16.30.0 0.0.0.255
interface serial0/3/0
 ip nat outside
 exit
interface serial0/3/1
 ip nat outside
 exit
interface range fa0/0-1
 ip nat inside
 exit
```

```
interface fa1/0
 ip nat inside
 exit
ip nat inside source list 1 interface serial0/3/0 overload
ip nat inside source list 1 interface serial0/3/1 overload
ip nat inside source list 2 interface serial0/3/0 overload
ip nat inside source list 2 interface serial0/3/1 overload
```

Configuración del **Router R2**:

```
access-list 3 permit 172.16.20.0 0.0.0.255
access-list 4 permit 172.16.30.0 0.0.0.255
interface serial0/3/0
 ip nat outside
 exit
interface serial0/3/1
 ip nat outside
 exit
interface range fa0/0-1
 ip nat inside
 exit
interface fa1/0
 ip nat inside
 exit
ip nat inside source list 3 interface serial0/3/0 overload
ip nat inside source list 3 interface serial0/3/1 overload
ip nat inside source list 4 interface serial0/3/0 overload
ip nat inside source list 4 interface serial0/3/1 overload
```

Verificación:

```
show ip nat translations
show tcp brief
```

HITO 5

Enunciado

Este hito abarca los temas de QoS y de gestión de red (Syslog, SNMP y Netflow)

Haz un resumen teórico de los temas y plantéate cómo implantarlos en la red que vienen diseñando. Proporciona la solución de la implantación paso a paso.

Implementa la QoS y un servidor Syslog, SNMP y Netflow en Packet Tracer de la manera que estimes oportuna.

Planteamiento

QoS (Quality of Service)

Es un conjunto de técnicas y mecanismos utilizados para gestionar y priorizar el tráfico de red con el fin de garantizar un rendimiento óptimo para aplicaciones y servicios específicos. El objetivo de QoS es proporcionar un ancho de banda adecuado, minimizar la latencia y asegurar una calidad de servicio consistente para aplicaciones críticas como voz sobre IP (VoIP) y videoconferencia.

Se utilizan las siguientes herramientas y mecanismos para lograr sus objetivos:

- Clasificación y marcado.
- Políticas y conformado de tráfico.
- Gestión y evitación de congestiones.

Causas principales de los problemas:

- Falta de ancho de banda:
    - Solución:
        - Incrementar el ancho de banda.
        - Implementar QoS para asignar un ancho de banda suficiente al tráfico importante y priorizarlo.

- Latencia y jitter:
    - Latencia: es el retardo unidireccional de extremo a extremo.
        - Tipos:
            - De propagación: tiempo fijo que tarda un paquete desde el origen al destino a la velocidad de la luz a través de un medio.
            - De serialización: tiempo fijo que se tarda en colocar los bits de un paquete en el enlace.
            - De procesamiento: tiempo fijo que tarda un paquete desde que entra hasta que sale de un dispositivo.
    - Variación del retardo o Jitter: es la diferencia del retardo de los paquetes.

- Pérdida de paquetes:
    - Se puede prevenir implementando una de las siguientes técnicas:
        - Incrementando la velocidad de la línea.
        - Implementando mecanismos de QoS para prevenir y gestionar la congestión.
        - Implementando políticas de tráfico que descarte el tráfico de baja prioridad.
        - Implementando conformado de tráfico que retrasen los paquetes en vez de descartarlos.

Flujo: conjunto de datagramas unidireccionales con el mismo origen y destino y con los mismos requisitos de QoS.

Clase: conjunto de flujos con los mismos requerimientos de QoS.

Existen 3 modelos:

- Mejor esfuerzo (o sin QoS): Usado con tráfico que no requiere tratamiento especial.
- Servicios Integrados (IntServ): Por cada flujo se solicita a cada router del camino hacer una reserva previa de recursos.
- Servicios Diferenciados (DiffServ): se marcan los paquetes en origen para que los dispositivos de red identifiquen las clases que requieren un tratamiento QoS especial.

Clasificación: se utilizan descriptores de tráfico para ubicar un paquete IP dentro de una clase específica.

Marcado: se usan descriptores de tráfico para ubicar un paquete IP dentro de una clase específica. Existen marcados a nivel de L2 y L3.

Comportamiento por salto (PHB): es el tratamiento que se da en un nodo DiffServ a una colección de paquetes con el mismo valor DSCP que cruzan un enlace en una dirección particular.

Pasos para implementar QoS:

- Identifica las aplicaciones y servicios críticos que requieren priorización en la red, como VoIP y videoconferencia.

- Configura la clasificación del tráfico utilizando ACLs (Listas de Control de Acceso) o marcado de paquetes con DSCP (Differentiated Services Code Point).

- Define las políticas de QoS en los routers y switches para asignar prioridad y limitar el ancho de banda según las necesidades de las aplicaciones.

- Realiza pruebas y ajustes para asegurar que la QoS está funcionando según lo esperado.

Syslog

Es un protocolo utilizado para la gestión de registros y eventos en los dispositivos de red. Permite la recopilación, el almacenamiento y el envío de mensajes de registro generados por los dispositivos a un servidor centralizado. Los mensajes de registro contienen información sobre eventos, errores y advertencias que pueden ayudar en la monitorización y solución de problemas de la red.

Un cliente Syslog se puede montar en casi cualquier dispositivo y puede enviar los logs a:

- Buffer de logs del propio dispositivo.
- Consola.
- Líneas terminales.
- Servidores Syslog.

Los mensajes se clasifican por niveles y usar un determinado nivel dependerá de los requisitos de seguridad.

Un sistema de SYSLOG está compuesto por:

- Servidor de Syslog (Log Host).
- Clientes de Syslog.

Pasos para implementar Syslog:

- Configura un servidor Syslog centralizado en la red, que puede ser un servidor dedicado o un dispositivo que admita esta funcionalidad.

- Configura los dispositivos de red (routers, switches, firewalls, etc.) para enviar los mensajes de registro al servidor Syslog.

- Establece niveles de severidad y filtros en el servidor Syslog para gestionar los mensajes de registro y generar alertas en caso de eventos críticos.

SNMP (Simple Network Management Protocol)

Es un protocolo utilizado para la gestión y monitorización de dispositivos de red. Permite la recopilación de información sobre el estado y el rendimiento de los dispositivos, así como la configuración remota y la generación de alarmas. SNMP utiliza un conjunto de comandos y mensajes para interactuar con los agentes SNMP en los dispositivos.

Existen tres versiones de SNMP:

- Los dos primeros basan la seguridad en el nombre de la comunidad, lo cual no es adecuado.
- Por flexibilidad, la v3 establece tres niveles de seguridad:
    - noAuthNoPriv
    - authNoPriv
    - authPriv (recomendado).

Para evitar vulnerabilidades de las versiones anteriores, SNMP v3 dispone de tres características concretas de seguridad:

- Integridad y autenticación.
- Encriptación.
- Control de acceso.

Pasos para implementar SNMP:

- Configura el servicio SNMP en los dispositivos de red, habilitando la capacidad de gestionar y monitorizar a través de SNMP.

- Define la comunidad SNMP, que actúa como una especie de contraseña para autenticar las solicitudes SNMP.

- Configura el servidor SNMP (puede ser el mismo servidor Syslog) para recibir y procesar las solicitudes SNMP de los dispositivos de red.

- Utiliza una herramienta de gestión de red compatible con SNMP para realizar la monitorización y gestión de los dispositivos de red.

Netflow

Es un protocolo utilizado para la monitorización y análisis del tráfico de red. Proporciona información detallada sobre el flujo de paquetes, incluyendo la dirección IP de origen y destino, el puerto, el protocolo, el tiempo de duración, entre otros datos. Netflow ayuda a identificar patrones de tráfico, detectar cuellos de botella y optimizar el rendimiento de la red.

Existen 2 componentes:
- Netflow Data Capture: captura el tráfico y realiza sobre él las estadísticas.
- Netflow Data Export: exporta los resultados a un recolector de NetFlow.

Un flujo es una secuencia unidireccional de paquetes entre un origen y un destino.

Flexible NetFlow permite hacer análisis de tráfico más complejos.

Existen 4 componentes de configuración que se pueden reutilizar:
- Registros de flujo (record): Declaración del tráfico a monitorizar por medio de campos clave y no clave de lo que se va a monitorizar.
- Exportadores de flujo (export): Declara el host remoto de destino de la exportación de datos.
- Monitores de flujo (monitor): Vincula la memoria caché al Record Flow y al Export Flow. Posteriormente el Monitor Flow se aplicará a una interfaz concreta para realizar la supervisión del tráfico de red.
- Muestreadores de flujo (samplers): Muestrea datos parciales de NetFlow en lugar de analizar todos los datos de NetFlow.

Pasos para implementar Netflow:

- Configura los dispositivos de red para exportar los registros de flujo Netflow a un colector Netflow.

- Establece la dirección IP del colector Netflow en los dispositivos de red para enviar los registros.

- Configura el colector Netflow para recibir y analizar los registros de flujo, proporcionando información detallada sobre el tráfico de red, como las principales fuentes y destinos, los protocolos utilizados y la cantidad de tráfico.

Configuración QoS

En Packet Tracer, la confianza en la clasificación del tráfico se configura automáticamente en las interfaces de acuerdo con el tipo de puerto configurado. Por ejemplo, los puertos de acceso se

configuran automáticamente para confiar en el campo CoS, mientras que los puertos troncales se configuran automáticamente para confiar en el campo DSCP.

Por ello en todos los switches solamente habrá que activar: mls qos

Configuración de todo los Switches:

```
mls qos
```

Configuración del Router R1:

```
class-map match-any VOICE_TRAFFIC
 match ip dscp ef
 exit
policy-map QOS_POLICY
 class VOICE_TRAFFIC
  priority percent 30
  exit
 class class-default
  fair-queue
  exit
interface range fa0/0-1
 service-policy output  QOS_POLICY
 exit
interface fa1/0
 service-policy output  QOS_POLICY
 exit
```

Configuración del Router R2:

```
class-map match-any VOICE_TRAFFIC
 match ip dscp ef
 exit
policy-map QOS_POLICY
 class VOICE_TRAFFIC
  priority percent 30
  exit
 class class-default
  fair-queue
  exit
interface range fa0/0-1
 service-policy output QOS_POLICY
 exit
interface fa1/0
 service-policy output  QOS_POLICY
 exit
```

Verificación:

show policy-map interface [interface]
show class-map [class-map]
show mls qos maps
show mls qos statistics
show mls qos interface [interface]

Configuración Syslog

La configuración de Syslog es igual para todos los Switches y Routers de la red.

Configuración de todos los dispositivos:

Modificación el registro almacenado en búfer:
logging buffered 16384

Modificación del nivel del registro(sólo está disponible en packet el nivel 7, Debug):
logging trap debugging

Configuración del servidor Syslog:
logging host 172.16.125.2

Habilitar protocolo:
logging on

Verificación:
show run all | include logging
show logging

Configuración SNMP

La configuración del protocolo SNMP es igual para todos los Switches y Routers de la red.

Configuración de todos los dispositivos:
snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

Verificación:
debug snmp packets

Configuración Netflow

Configuración del Router R1:
Habilitar Netflow:

ip flow-export version 9
ip flow-export destination 172.16.125.4 9999

Configurar interfaces para Netflow:
interface range fa0/0-1, fa1/0
 ip flow ingress
 ip flow egress
 exit

Configuración del Router R2:
Habilitar Netflow:
ip flow-export version 9
ip flow-export destination 172.16.125.4 9999

Configurar interfaces para Netflow:
interface range fa0/0-1, fa1/0
 ip flow ingress
 ip flow egress
 exit

Verificación:
show ip flow interface
show ip flow export

HITO 6

Enunciado

Este hito abarca el tema 9 sobre Protocolos de descubrimiento, POE, puertos espejo e IP SLA.

Haz un resumen en pdf de las transparencias y plantéate cómo implantarlo en la red que vienen diseñando. Justifica todas tus decisiones.

Implementa un puerto espejo y protocolos de descubrimiento en Packet Tracer de la manera que estimes oportuna.

Planteamiento

Protocolos de descubrimiento

Estos protocolos de capa 2 son usados por los dispositivos para publicar su identidad y capacidades a los vecinos. Se emplean para la construcción de las topologías, la administración de la red y la solución de problemas.

Ejemplos:

- **CDP**: Protocolo de Descubrimiento de Cisco (en desuso).
- **LLDP**: Protocolo de Descubrimiento de Capa de Enlace.
    - Es estándar: 802.1AB
    - También llamado “Station and Media Access Control Connectivity Discovery”.

LLDP trabaja enviando y recibiendo atributos en formato **TLV** (Tipo/Longitud/Valor) y se limita a publicitarlos unidireccionalmente y de manera periódica (30s por defecto).

LLDP recibirá y registrará toda la información que reciba sobre sus vecinos. La información obtenida se procesa a nivel local y no se reenvía.

Tipos de TLV:

- Valor 0 (Final del LLDPDU) Obligatorio.
- Valor 1 (ID del chasis) Obligatorio.
- Valor 2 (ID del puerto) Obligatorio.
- Valor 3 (Tiempo de vida) Obligatorio.
- Valor 4 (Descripción del puerto) Opcional.
- Valor 5 (Nombre del sistema) Opcional.
- Valor 6 (Descripción del sistema) Opcional.
- Valor 7 (Capacidades del sistema) Opcional.
- Valor 8 (Dirección de gestión) Opcional.
- Valor 9-126 (Reservado) Indefinido.
- Valor 127 (Organización específica de los TLVs) Opcional.

Los TLVs se envían a las direcciones de destino multicast: 01:80:c2:00:00:00, 01:80:c2:00:00:03 y 01:80:c2:00:00:0e.

Llevan información de:

- Configuración.
- Capacidades del dispositivo.
- Dirección IP.
- Nombre de host.
- Identificador del dispositivo

Destacar que existen 2 más ejemplos de protocolos de descubrimientos que son **ARP** y **NDP**.

Address Resolution Protocol (**ARP**): Es un protocolo utilizado en redes IP para asociar direcciones IP con direcciones MAC. ARP permite que los dispositivos descubran las direcciones físicas de los dispositivos en la misma red local.

Neighbor Discovery Protocol (**NDP**): Es un protocolo utilizado en redes IPv6 para el descubrimiento y la configuración automática de nodos en una red. NDP realiza funciones similares a ARP en IPv4, como la resolución de direcciones y el descubrimiento de vecinos.

Configuración LLDP

Para activar LLDP hay que configurarlo con el comando **lldp run.**

También, podremos modificar el modo de LLDP con el comando **lldp {med-tlv-select tlv | receive | transmit }**.

Mi configuración de LLDP para todos los switches y routers de mi red es la siguiente:

lldp run
lldp med-tlv-select tlv receive transmit (No funciona en packet tracer)

Con la configuración anterior, además de habilitar LLDP en cada dispositivo, se permite la recepción y transmisión de las TLVs de LLDP-MED. Esto permitirá el descubrimiento y la comunicación de información adicional relacionada con la capacidad de los dispositivos para admitir características de telefonía IP, como Power over Ethernet (PoE) y VLANs de voz.

Como no funciona el segundo comando en packet tracer, si se habilita el comando "lldp run" en la configuración, el modo de operación por defecto de LLDP es el modo "TX and RX" (transmitir y recibir). Esto significa que el dispositivo enviará y recibirá información de descubrimiento de enlace a través del protocolo LLDP.

Verificación:
show lldp neighbors
show lldp neighbors detail
show lldp statistics
show lldp traffic

Power over Ethernet (PoE)

PoE es una tecnología que permite suministrar energía a un dispositivo a través del cable de datos. Es muy útil porque se consigue una mayor flexibilidad ya que evita la instalación eléctrica hasta el dispositivo.

Dispositivos que pueden usar **PoE**:

- Puntos de acceso.
- Teléfonos inalámbricos.
- Clientes ligeros.
- Cámaras de seguridad.
- Sensores.
- Relojes.
- Antenas.
- Decodificadores.

- Switches y routers.

Elementos de la arquitectura:
- PSE (Power Sourcing Equipment).
- PD (Powered Device).
- Cables.

Posibilidades:
- Switch sin **PoE** más inyector por puerto:
    - Usado con un número pequeño de dispositivos PoE.
    - Además del switch, se debe alimentar al inyector.

- Switch **PoE**:
    - Sólo es necesario alimentar al switch.
    - Proporciona la posibilidad de administración remota de la energía.
    - Se configura a nivel de puerto.
    - Tras configuración, el puerto con PoE ofrece directamente alimentación.
    - Un dispositivo que no requiere PoE se puede conectar a un puerto con PoE habilitado.
    - Se recomienda el uso de UPS (Uninterruptible Power Supply).
    - Es caro.

Estándares:
- El estándar más comúnmente utilizado para PoE es el **802.3af** (2003), que proporciona hasta 15.4 vatios de potencia a través del cable Ethernet.

- También existe el estándar **802.3at** (2009), conocido como PoE + o PoE Plus, que puede suministrar hasta 30 vatios de potencia. Con implementaciones no estándares se puede aumentar a 50 vatios.

- El estándar **802.3bt** (2018) tiene 2 tipos, Tipo 3 de hasta 55 vatios de potencia y el Tipo 4 de hasta 100 vatios de potencia. Además, soporta nuevas tecnologías Ethernet sobre pares, 2.5GBASE-T, 5GBASE-T y 10GBASE-T.

PoE se pone en funcionamiento de la siguiente manera:
- El PSE envía un pequeño voltaje al puerto con objeto de detectar una resistencia de 25K aproximada. Si la detecta significa que en el otro extremo hay un PD.
- El PD envía información sobre el nivel de potencia que requiere. Existen dos alternativas para ajustar la potencia:
    - PSE envía voltaje para detección de la resistencia del PD que indica el rango de potencia.
    - Por medio de LLDP.
- El PSE asigna al PD la potencia adecuada y lo alimenta.

Niveles de potencia:
- Niveles de potencia en 802.3af
    - 0. No implementada
    - 1. 4 vatios
    - 2. 7 vatios

    - 3. 15.4 vatios

- Niveles de potencia en 802.3at
    - 4. 30 vatios

- Niveles de potencia en 802.3bt
    - 5. 45 vatios (dispositivos tipo 3)
    - 6. 60 vatios (dispositivos tipo 3)
    - 7. 75 vatios (dispositivos tipo 4)
    - 8. 99 vatios (dispositivos tipo 4)

Configuración PoE

Para implementar PoE en un switch hay que seguir los siguientes pasos en la configuración:

- **Verificar la compatibilidad**: Asegúrate de que el switch sea compatible con PoE y cuente con los puertos habilitados para PoE.

- **Conectar dispositivos compatibles con PoE**: Conecta los dispositivos compatibles con PoE, como cámaras IP, teléfonos IP o puntos de acceso inalámbricos, a los puertos PoE del switch. Utiliza cables Ethernet estándar para la conexión.

- **Accede a la interfaz del switch** que le quieras aplicar PoE.

- **Habilita la funcionalidad de PoE** en el switch con el comando **power inline {auto | static}**. La opción "**auto**" permite que el switch ajuste automáticamente la potencia según los requisitos del dispositivo, mientras que "**static**" establece una potencia fija para todos los puertos PoE.

- **Configura la potencia máxima** que se puede suministrar a través de los puertos PoE con el comando **power inline max {milliwatts | watts}.** Por ejemplo, puedes establecer la potencia máxima en 15.4 watts con **power inline max 15400**.

En mi configuración de packet tracer como son todos switches de capa 3 ya viene implementado PoE, por lo que no he tenido que configurar nada.

Puertos espejos

Es una función que permite a un conmutador hacer una copia duplicada de una trama entrante para enviarla a un puerto en el que hay conectado un analizador de paquetes o un sensor.

Cisco permite hacerlo de tres maneras:
- **SPAN**: el tráfico se envía a un puerto del propio switch que lo captura.
- **RSPAN**: el tráfico se envía a otro switch de la LAN mediante enlaces L2.
- **ERSPAN**: el tráfico atraviesa routers (L3) para analizarse en otra red.

SPAN (Switched Port ANalyzer)

Cómo funciona:

- La monitorización se produce sobre los puertos fuente.
- Una copia del tráfico del puerto fuente se envía al puerto de destino.
- Una sesión SPAN asocia uno o varios puertos fuentes con uno o varios puertos de destino.
- En vez de sobre puertos, la sesión también se puede establecer sobre una VLAN fuente.

El origen puede ser:

- Uno o varios puertos (incluido un puerto troncal).
- Una agregación de puertos (Etherchannel).
- Una VLAN.

Consideraciones:

- Conmutadores antiguos admiten hasta dos sesiones SPAN, los nuevos admiten más.
- El origen y destino no puede formar parte de dos sesiones SPAN distintas.
- Los puertos de origen pueden ser L2 y L3.

RSPAN (Remote Switched Port ANalyzer)
Acerca de RSPAN:

- Se utiliza cuando se desea capturar paquetes que pasan por puertos de switches distintos al switch al que se conecta el sensor.
- Se usa en un entorno de redes grande.
- Una VLAN especial transporta el tráfico entre switches.

ERSPAN (Encapsulated Remote Switched Port ANalyzer)

Acerca de ERSPAN:

- Se utiliza cuando se desea capturar paquetes que se analizarán en una red diferente del switch al que se conecta el sensor.
- Existen routers entre el origen de los paquetes y el sensor.
- Usado para hacer monitorización remota.
- Utiliza el túnel GRE entre origen y destino para transportar tráfico a monitorizar.
- Es posible configurar valores específicos de TTL y de TOS para los paquetes del túnel.

Configuración SPAN

He configurado un puerto espejo del puerto GigabitEthernet 1/0/1 del Switch A1 en la interfaz GigabitEthernet 1/0/2.

Switch de acceso:

Configuración del **Switch A1**:
monitor session 1 source interface g1/0/1
monitor session 1 destination interface g1/0/2

Verificación:
show monitor
show monitor session local

Configuración RSPAN

He configurado un puerto espejo del puerto GigabitEthernet 1/0/3 del Switch A1 en la interfaz GigabitEthernet 1/0/16 del Switch D1.

Switch de acceso:

Configuración del **Switch A1**:
vlan 200
 name RSPAN-VLAN
 remote-span
 exit
monitor session 2 source vlan 20
monitor session 2 destination remote vlan 200

Switch de distribución:

Configuración del **Switch D1**:
vlan 200
 name RSPAN-VLAN
 remote-span
 exit
monitor session 2 source remote vlan 200
monitor session 2 destination interface g1/0/16

#Luego si se quiere comprobar el tráfico en ese pc, hay que levantar esa interfaz ya que estaba caída y colocar un pc en esa interfaz del packet tracer.
interface g1/0/16
 no shutdown
 exit

Verificación:
show monitor
show monitor session local

IP SLA

SLA (Acuerdo del niveL de Servicio) es un contrato entre proveedor y usuario que garantiza el buen funcionamiento de la red y el nivel de experiencia del usuario. Con ello se garantiza que no ocurran problemas de inactividad o de degradación de las redes.

Contiene:

- Detalles de conectividad.
- Acuerdos de rendimiento para un servicio.

Parámetros técnicos de un SLA:

- Nivel garantizado de disponibilidad de la red, medido en minutos consecutivos de no disponibilidad. También, puede ser medido como el porcentaje mensual del tiempo de actividad:
    - 99.5% de tiempo de actividad = 216 minutos de tiempo de inactividad en un mes.
    - 99.8% de tiempo de inactividad = 86.4 minutos de tiempo de inactividad en un mes.
    - 99.9% de tiempo de inactividad = 43.2 minutos de tiempo de inactividad en un mes.
    - 99.99% de tiempo de inactividad = 4.32 minutos de tiempo de inactividad en un mes.
    - 99.999% de tiempo de actividad = 0.432 minutos (26 segundos) en un mes.

- El rendimiento de la red en términos de tiempo de ida y vuelta (**RTT**) es medido como una media mensual del tiempo de tránsito de ida y vuelta de los paquetes.

- La respuesta de la red en términos de latencia es medida en milisegundos de media mensual.

- Fluctuación del retardo o jitter es medido como valor medio mensual medido en ms.

- Pérdida de paquetes es medido en porcentaje de la media mensual de paquetes perdidos.

IP SLA de Cisco permite hacer pruebas para asegurar el funcionamiento correcto de la red, estas pruebas consisten en monitorizar el tráfico enviado entre dos dispositivos.

Este acuerdo de nivel de servicio está formado por 2 elementos, la fuente y el respondedor (opcional en función del test).

Usos de los test:

- Evaluar la accesibilidad a un dispositivo.
- Asegurar el soporte de la red de aplicaciones en tiempo real y de sistemas críticos.
- Monitorizar la disponibilidad borde a borde entre redes, el rendimiento de la red, el correcto funcionamiento de las VPN, la calidad de la VoIP o del vídeo, el SLA contratado y la red MPLS.
- Establecer el nivel de salud de los servicios IP.
- Solucionar problemas de red.

La fuente de IP SLA:

- Dispositivo que realiza el análisis de las mediciones.
- De él parte el flujo de tráfico de sondeo.
- El destino del tráfico es cualquier host IP específico.

El destino puede ser un respondedor de IP SLA:

- Éste contiene un Cisco IOS configurado para responder a los paquetes de IP SLA.
- Aumenta la precisión de la medida.
- Es de uso obligatorio en determinados test.

Para aplicar IP SLA hay que seguir una serie de pasos:
- Habilitar el respondedor de IP SLA si fuese necesario.
- Configurar el test a realizar.
- Configurar opciones concretas del test.
- Configurar el umbral de las condiciones si fuese necesario.
- Programar la ejecución del test para ejecutar el test durante el periodo de tiempo necesario para recopilar estadísticas.
- Visualizar los resultados desde el CLI o desde la línea de comandos.

La operación con respondedor tiene 2 fases:
- Fase de control:
    - Envía un mensaje de control IP SLA al puerto 1967 UDP con información de autenticación y con información para establecer la segunda fase (puerto, protocolo y duración).
    - Si todo está correcto, el respondedor envía un OK y se pone a escuchar el puerto con el protocolo concreto y durante el tiempo determinado.

- Fase de prueba:
    - La fuente envía los paquetes de prueba al respondedor para cálculos de tiempos.
    - El respondedor acepta los paquetes de prueba y responde añadiendo marcas de tiempo.

Las **marcas de tiempo** permiten calcular el tiempo de ida y vuelta sin incorporar a éste el delay de los dispositivos IP SLA fuente y respondedor. Se introducen en los paquetes para determinados cálculos.

Configuración IP SLA

Dejo un ejemplo de cómo se configuraría IP SLA en un Switch para los test ICMP-echo, HTTP y Jitter UDP. No los configuro en mi red ya que no lo pide el enunciado del hito y no funciona en packet tracer

Además, se puede activar la autenticación IP SLA.

ICMP-echo:
```
ip sla 1
 icmp-echo 192.168.20.1
  frequency 30
  exit
ip sla schedule 1 start-time now live forever
end
```

HTTP:

```
ip sla 2
 http get http://192.168.14.100
  frequency 90
  exit
ip sla schedule 2 start-time now live forever
end
```

Jitter UDP:

```
ip sla 3
 udp-jitter 192.168.1.1 65000 num-packets 20
 request-data-size 160
 frequency 30
 exit
ip sla schedule 3 start-time after 00:10:00
ip sla responder
```

Para autenticar se usan las keychain:

```
key chain Jorge
 key 1
  key-string Secret
ip sla key-chain Jorge
```

Verificación:

```
show ip sla configuration
show ip sla statistics
show ip sla responder
show ip sla schedule
```

HITO 7

Enunciado

Este hito abarca la temática sobre AAA, 802.1X y seguridad de L2.

Haz un resumen en pdf de las transparencias y plantéate cómo implantarlo en la red que vienes diseñando. Justifica todas tus decisiones.

Implementa en Packet Tracert todos los protocolos que te sean posible en relación con la temática del hito.

Planteamiento

AAA(Authentication, Authorization and Accounting)

Los servicios de seguridad de red proporcionados por AAA controlan:

- Quién tiene permiso para acceder a una red (autenticar).
- Qué se puede hacer mientras se está en la red (autorizar).
- Auditar qué acciones se realizan en el acceso a la red (contabilizar).

Autentificación:

- Consiste en una prueba que se hace al usuario para demostrar que es quien dice que es.
- Métodos:
    - Nombre de usuario y contraseña.
    - Preguntas de desafío y respuesta.
    - Tarjetas de coordenadas.
    - Mensajes a dispositivos personales.
    - Otros métodos.

Métodos de autenticación:

- Contraseña simple (enable): se configura en interfaces de consola, vty y auxiliares.
- BD de usuarios local: se configura en cada dispositivo.
- BD de usuarios en servidor usando protocolo RADIUS (Remote Authentication Dial-In User Service) o TACACS + (Terminal Access Controller Access Control System).

La autenticación local del acceso administrativo está pensada para redes pequeñas. Contiene nombres de usuario y contraseñas que se almacenan en el router.

Tipos de algoritmos de clave secreta:

- Tipo 0: sin encriptación.
- Tipo 5: md5 hashed (vulnerable).
- Tipo 7: Cifrado de Vigenère (es una sustitución de caracteres).
- Tipo 8: PBKDF2 con sha256.
- Tipo 9: scrypt (el más fuerte).

Autorización: es una concesión de privilegios que se hace al usuario una vez autentificado. Puede ser local (basada en niveles o roles) o basada en servidor.

La autorización utiliza un conjunto creado de atributos que describe el acceso del usuario a la red. Estos atributos se envían al servidor AAA para que sean comparados con la BD.

Contabilización/Auditoría: es un seguimiento del uso de recursos que hace el usuario.

Es una recopilación de datos de:

- Usuario, IPs y/o tiempos de inicio/finalización de sesión.
- Comandos ejecutados.
- Número de paquetes y bytes generados.
- Encendido, apagado y reinicios de sistemas.

La contabilización se considera técnica incluida en el ámbito de:

- La gestión de red: control de la red para detectar que no se degraden sus prestaciones y trazabilidad de los cambios.
- La gestión financiera: los ISP lo utilizan para cuantificar el uso de los servicios que ofrecen y a partir de ahí cobrar al cliente.
- Seguridad: controlando accesos inapropiados o a destiempo.

La comunicación AAA contra servidor se realiza por medio de uno de estos protocolos:

- **TACACS**: sistema de Control de Acceso del Controlador de Acceso a Terminales.
- **TACACS+**: versión mejorada del anterior e incompatible con ésta.
- **RADIUS**: servicio de autenticación remota de llamadas de usuarios.
- **DIAMETER:** Protocolo que viene a sustituir a Radius. Utiliza TCP o SCTP (Stream Control Transmission Protocol).

TACACS+:

- Usa el puerto 49 de TCP.
- Soporta múltiples protocolos L3.
- Encripta toda la comunicación.
- Separa la autentificación de autorización.

RADIUS:

- Uso de puertos:
  - Para autenticación: 1645 ó 1812 de UDP.
  - Para contabilización: 1646 ó 1813 de UDP.
- Encripta sólo la contraseña.
- La autentificación y la autorización forman un solo proceso: el usuario se autentica y es autorizado a la vez.

Configuración AAA

Configuración de la autenticación local

- Creación de la BD usuarios: **username “nombre” algorithm-type scrypt secret “contraseña”**
- Habilitación del uso de la BD de usuarios: **aaa new-model**
- Habilitación del logueo mediante AAA para CON, AUX y VTYs: **aaa authentication login {default | nombre} “método”**
- **Configuración de todos los switches y routers en packet tracer:**
  - **username admin privilege 15 password cisco123**
  - **aaa new-model**
  - **aaa authentication login default local-case enable**
  - **aaa authentication login SSH-LOGIN local-case**
  - **line vty 0 4**
    - **login authentication SSH-LOGIN**
    - **exit**
  - **Verificación:**

        - **show aaa sessions**
        - **show aaa local user lockout**

Configurar TACACS+:

- Habilitar AAA: **AAA new-model**
- Habilitar protocolo TACACS+: **tacacs server "nombre_servidor"**
- Configurar la IP del servidor: **address ipv4 "nº_IP"**
- Configurar una conexión estable para mejorar el rendimiento TCP**: single_connection**
- Configurar la contraseña: **key "contraseña"**
- **No funciona en packet tracer, pero la configuración sería así:**
    - **Configuración de todos los switches y routers:**
        - **aaa new-model**
        - **tacacs server TACACS**
            - **address ipv4 192.168.1.5**
            - **single_connection**
            - **key cisco12345**
            - **exit**
        - **aaa group server tacacs+ TACACS-GP**
            - **server name TACACS**
            - **exit**
    - **Verificación:**
        - **debug tacacs**

Configurar Radius:

- Habilitar AAA: **AAA new-model**
- Habilitar protocolo RADIUS: **radius server "nombre_servidor"**
- Configurar la IP del servidor: **address ipv4 "nº_IP" auth-port 1812 acct-port 1813**
- Si se desean usar los puertos del RFC se debe indicar expresamente ya que por defecto Cisco usa los puertos 1645 y 1646
- Configurar la contraseña: **key "contraseña"**
- **Configuración de todos los switches y routers en packet tracer:**
    - **aaa new-model**
    - **radius server RADIUS**
        - **address ipv4 192.168.1.5 auth-port 1812**, no existe acct-port en packet tracer
        - **key cisco12345**
        - **exit**
    - Los grupos no funcionan en packet tracer:
        - **aaa group server radius RADIUS-GP**
            - **server name RADIUS-GP**
            - **exit**
        - **Verificación:**
            - **debug radius**

Configuración de la autenticación:

- Para usar la autenticación basada en servidor: **aaa authentication login default group [ldap|radius|tacacs+]**
- **Configuración de todos los switches y routers:**
    - Entorno real (no funciona en packet tracer):
        - **aaa authentication login default group TACACS-GP group RADIUS-GP local-case**
    - Packet tracer, solo está disponible para local:
        - **aaa authentication login default local-case**

Configuración de la autorización:

- Para habilitarla: **aaa authorization {network| exec |commands level} {default | nombre} group [ldap|radius|tacacs+]**
- Se debe especificar el tipo de servicio a autorizar:
    - network: servicios como el PPP
    - exec: para iniciar el modo privilegiado
    - commands level: para ejecutar comandos concretos.
- **Configuración de todos los switches y routers en packet tracer:**
    - Entorno real (no funciona en packet tracer):
        - **aaa authorization exec default group TACACS-GP group RADIUS-GP local-case**
        - **aaa authorization network default group TACACS-GP group RADIUS-GP local-case**
    - Packet tracer, solo está disponible para local:
        - **aaa authorization exec default local**
        - **aaa authorization network default local**

Configuración de la contabilización:

- Para activar la contabilización: **aaa accounting {network| exec | connection} {default | nombre} {start-stop | stop-only | none} {broadcast} group [radius|tacacs+]**
- **Configuración de todos los switches y routers en packet tracer:**
    - Entorno real (no funciona en packet tracer):
        - **aaa accounting exec default start-stop group TACACS-GP group RADIUS-GP local-case**
        - **aaa accounting network default start-stop group TACACS-GP group RADIUS-GP local-case**
    - Packet tracer, solo está disponible para grupos de servidor, y estos no se pueden crear:
        - **aaa accounting exec default start-stop group RADIUS**

802.1X

802.1X: Es un mecanismo control de acceso de los host a la LAN basada en los puertos de switch.

3 roles en 802.1X:

- Suplicante (host):
    - Dispositivo que solicita el acceso a la red al switch.
    - Debe tener implementado un cliente 802.1X
    - Si el host tiene configurado 802.1X y trata de iniciar sesión y el switch no le responde, el host trabajará normalmente.

- Autentificador (switch):
    - Actúa como proxy entre host y el servidor..
    - Los puertos del switch pueden estar en estado autorizado o no autorizado.
    - Encapsula y desencapsula paquetes EAP (RFC 4187) que transportan parámetros de autenticación:
        - EAPoL (Extensible Authentication Protocol over LAN) del lado del suplicante.
        - EAP sobre Radius del lado del Servidor.
    - No conoce detalles de EAP: la autenticación le es transparente.
    - Mientras el suplicante no esté autentificado, sólo permitirá el paso de paquetes EAPOL.
    - Si el switch tiene configurado 802.1X y el host no, el switch no permitirá el tráfico de éste.

- Servidor de autentificación: Radius con extensión EAP que realiza la autenticación.

Intercambios de mensajes de 802.1X:

- 2 formas de iniciar el proceso de autenticación:
    - Por parte del autentificador: cuando nota que se le conectan a un puerto envía por éste tramas periódicas EAP-request/identify.
    - Por parte del suplicante: enviando tramas EAPoL-start al autenticador.

- Posteriormente, se selecciona un método EAP:
    - El autenticador retransmite los mensajes EAP entre el solicitante y el servidor de autenticación.
    - Lo hace copiando el mensaje EAP de la trama EAPoL a un paquete RADIUS y viceversa.

- Luego, la autenticación se lleva a cabo utilizando el método EAP seleccionado.

- Si la autenticación tiene éxito:
    - El servidor envía un mensaje de aceptación (RADIUS access-accept) al autenticador que lleva:
    - Un mensaje EAP-success encapsulado.
    - Alguna opción de autorización.

- Finalmente, el autenticador abre el puerto.

Métodos EAP:

- EAP-MD5: autenticación basada en desafío.

- EAP-TLS: autenticación mediante certificado.

- Métodos EAP que crean túneles TLS (también llamados externos):
    - PEAP:
        - Sólo el servidor requiere certificado.
        - Crea un túnel TLS con el que autentica al suplicante a través de uno de estos métodos de autenticación internos.
    - EAP-FAST: como PEAP pero con la capacidad de reautenticar más rápido por el uso de Credenciales de Acceso Protegidas (PAC) que es una especie de cookie.
    - EAP-TTLS: similar a PEAP pero admite otros métodos internos de autenticación no PEAP.

Los métodos de autenticación EAP externos o tunelados se emplean en combinación con los internos y crean túneles TLS para negociar las credenciales de autenticación del cliente mediante un método interno de EAP.

Configuración 802.1X

No está disponible en packet tracer.

- Habilitación de **AAA: aaa new-model**
- Habilitación del método de autenticación 802.1X: **aaa authentication dot1x {default | nombre} método1 [… método4]**
- Habilitación de la autenticación 802.1X de manera global en switch: **dot1x system-auth-control**
- Habilitación de autenticación basada en puerto 802.1X en interfaz concreta de switch: **authentication port-control {auto|force-authorized|force-unauthorized}**
    - **auto**: habilita 802.1X
    - **force-authorized** (por defecto si 802.1X no está habilitado): switch permite cualquier tráfico.
    - **force-unauthorized**: el switch bloquea el puerto.
- Establece el tipo de Port Access Entity (PAE) del puerto concreto de switch como autentificador 802.1X: **dot1x pae authenticator**
- **Verificación:**
    - **debug authentication**
    - **show dot1x interface type slot/port details**
    - **show authentication registrations**
    - **show authentication sessions**

Seguridad L2

Si hay éxito en un ataque de capa 2 el resto de capas quedan comprometidas. Los ataques de capa 2 requieren acceso desde el interior, es importante proteger la red de ataques internos.

Se debe establecer una política de seguridad y, en función de ella, se deben configurar las funciones apropiadas para protegerlos.

Ataques:

- **Desbordamiento de la tabla de direcciones MAC**:
    - Un ataque de desbordamiento de la tabla de direcciones MAC (MAC address flooding) consiste en el envío de multitud de tramas con direcciones MACs de origen distintas con objeto de colapsar la tabla.
    - Tras el colapso, el switch puede empezar a trabajar como un hub y/o disminuir su rendimiento.
    - Los intrusos utilizan herramientas como macof o yersinia para realizar este ataque.

- **Suplantación de direcciones**: Ataque en el que un host se hace pasar por otro para recibir datos destinados a la víctima y/o eludir las configuraciones de seguridad. Existen 2 suplantaciones:

    - **Suplantación MAC (MAC Spoofing)**: Los switches presentan una vulnerabilidad en el aprendizaje MAC al rellenar la tabla de direcciones MACs pues no se garantiza la procedencia de las tramas. Se produce cuando un atacante utiliza la MAC de su víctima:
        - Al enviar una trama, sobreescribirá la tabla de direcciones MACs del switch asignándole a la MAC de la víctima el puerto del atacante.
        - Como consecuencia, los paquetes destinados a la víctima van a parar al atacante.
        - Esto sucederá hasta que la víctima genere tráfico, momento en el que el switch retorna la tabla de direcciones MAC a su estado correcto.
        - Para revertir la situación, el atacante suele crear un script que envían tramas constantemente para que el switch mantenga su asignación MAC-Puerto.

    - **Suplantación de IPs**: Se produce cuando un atacante utiliza la IP válida de un vecino o una IP aleatoria. La suplantación de direcciones IP es difícil de mitigar, especialmente cuando se usa dentro de una subred a la que pertenece la IP.

- **Ataques mediante ARP**: ARP es el protocolo que traduce direcciones IP en direcciones MACs. Mitigar estos ataques supone asegurar que sólo se envían paquetes ARP válidos.

    - **Suplantación ARP (ARP Spoofing)**: El atacante se apropia de cualquier IP/MAC que elija tras el envío de ARP Reply gratuito con la MAC falsificada a un switch el cual actualizará su tabla CAM en consecuencia.

    - **Ataque de envenenamiento ARP (ARP Poisoning)**: envío de ARP Reply a otro host con la dirección MAC del atacante y la IP de la puerta de enlace consiguiendo un Man-in-the-middle.

- **Abuso de VLAN**: Existen 2 posibles ataques:.

    - **Ataque VLAN hopping**: Consiste en pasar el tráfico de una VLAN a otra sin router. El ataque se consigue una vez que el intruso obtiene un enlace trunk con un switch bien por negociar DTP u otro método.

    - **Ataque VLAN de doble etiquetado**: Es unidireccional (no recibe respuesta). Sólo puede realizarse si el atacante se encuentra en la misma VLAN nativa que el puerto trunk.

- **Manipulación de STP**: Como la prioridad es configurable en STP, un atacante puede crear un falso switch y enviar BPDUs con prioridad 0. La topología STP se recalcularía estableciendo al falso switch como raíz, y el tráfico pasaría a través de él.

- **Ataques al DHCP**: Existen 2 posibles ataques DHCP:

    - **Suplantación DHCP**: El ataque DHCP spoofing se produce cuando un intruso coloca un servidor DHCP en la red y ofrece una configuración falsa a los clientes. La respuesta DHCP del intruso llega antes por estar más cerca. El intruso podría ofrecer:
        - Una puerta de enlace falsa, consiguiendo un ataque man-in-the-middle.
        - Un servidor DNS falso, que envía al cliente a servicios falsos.
        - Una IP falsa, para crear un ataque DoS.

    - **Inanición DHCP**: El ataque DHCP starvation se produce cuando un intruso hace peticiones con MACs distintas a un servidor DHCP hasta que a éste se le agotan las posibles direcciones a ofrecer. Para realizar el ataque se utiliza una herramienta externa como puede ser Goobler o Yersinia.

Técnicas para mitigar estos ataques L2:

- **Realizar una serie de buenas prácticas** para proteger el software de la red. Cómo aplicar contraseñas endurecidas y encriptadas, contraseñas para el acceso por consola y líneas VTY con AAA, deshabilitar servicios, puertos y protocolos de descubrimiento no usados, y no usar mecanismos de estabilidad en STP, que entre ellos, puedan incurrir en bucles.

- **Seguridad de puertos**: Se utiliza para filtrar las tramas de entrada a un puerto de un switch en función de la dirección MAC de origen de dicha trama. Si se produce una violación se realizará una acción que, al menos, no permitirá el paso de la trama que ha producido la violación. Previene de los ataques a MACs.

    - Se habilita en los puertos de acceso con el comando **switchport port-security**.
    - Se pueden establecer las MACs que se van a permitir en el puerto, **switchport port-security mac-address "MAC"**.
    - Para que el switch aprenda las MACs se utiliza, **switchport port-security mac-address sticky**.
    - Una violación genera una de las siguientes acciones:
        - Shutdown: acción por defecto que cae el puerto (err-disable) y que se debe levantar con no shutdown para ponerlo operativo. Envía un trap SNMP si éste está configurado.
        - Protect: el puerto sigue activo, pero se descartan las tramas que la han producido.
        - Restrict: Idéntico al anterior, pero envía un trap SNMP.

        - La acción a configurar después de una violación será, **switchport port-security violation {protect | restrict | shutdown}**.
    - Se pueden configurar los minutos que deben pasar para eliminar las MACs configuradas estática o dinámicamente. Dos tipos de envejecimiento (aging):
        - Absoluto: las MACs se eliminan después del tiempo de envejecimiento especificado.
        - Inactivo: las MACs se eliminan solo si están inactivas durante el tiempo de envejecimiento especificado.
        - **switchport port-security aging {static|time min.|type {absolute|inactive}}**.
    - Verificación: **show port-security**.

- **Notificación de MACs**: Es posible monitorizar cualquier cambio de la tabla de direcciones MACs mediante SNMP. Un switch puede enviar traps al Gestor SNMP cuando aprende una nueva MAC o cuando estas caducan y se eliminan. Para habilitar este tipo de traps se usa el siguiente comando, **mac address-table notification**.

- **Evitar ataques a VLANs**: Existen distintas acciones para evitar estos ataques:
    - Deshabilitar la negociación DTP en puertos de acceso y en los trunk, **switchport nonegotiate**.
    - Asignar una VLAN que no se utilice como VLAN nativa, evitando la nativa por defecto (VLAN 1), **switchport trunk native vlan "nº"**.
    - Deshabilitar los puertos no utilizados, **shutdown**.
    - Colocar dichos puertos en una VLAN que no se utilice (VLAN BlackHole).
    - Protección de puertos (PVLAN Edge): Los puertos protegidos están aislados completamente del resto de puertos protegidos dentro del mismo switch.
        - Configuración: **switchport protected**.
        - Verificación: **show interfaces "interfaz" switchport**.

- **DHCP Snooping**: Establece por qué puertos pueden entrar los mensajes de un servidor DHCP y limitar el número de paquetes DHCP Discovery que puede enviar un cliente.
    - Los puertos se clasifican como:
        - Confiables: son los puertos por donde entran los mensajes DHCP del servidor.
        - No confiables: es la opción por defecto y donde se conectan los host que no deberían enviar mensajes de servidor DHCP.
    - Construye una tabla con la siguiente información de los clientes conectados a puertos no confiables: MAC, IP, tiempo de concesión, interfaz y VLAN.
    - **Configuración**:
        - Habilitación del DHCP snooping, **ip dhcp snooping**.
        - Configurar puertos confiables, **ip dhcp snooping trust**.
        - Habilitarlo por VLAN, **ip dhcp snooping vlan "nº"**.
        - Limitar el número de peticiones, **ip dhcp snooping limit rate "nº"**.

- **Dynamic ARP Inspection (DAI)**: mitiga ataques ARP Spoofing y ARP Poisoning:
    - Bloquea y/o loguea los ARP Reply inválidos o gratuitos dirigidos a otros puertos en la misma VLAN.
    - Limita la cantidad de paquetes ARP de una interfaz, pudiendo colocar la interfaz en estado de error-disabled.

    - Para cada trama se verifica que la dupla IP-MAC es válida.
    - Para ello DAI funciona junto con DHCP Snooping, por lo que para cada trama verifica que la dupla IP-MAC existe en la tabla construida en DHCP Snooping.
    - **Configuración**:
        - Habilitar DHCP Snooping globalmente.
        - Habilitar DHCP Snooping en las VLANs concretas.
        - Habilitar DAI en dichas VLANs, **ip arp inspection vlan "nº"**.
        - Configurar las interfaces confiables tanto en DHCP Snooping como en DAI, **ip arp inspection trust**.
        - Bloquear paquetes que no superen una prueba de verificación/validación de las direcciones MACs e IPs, **ip arp inspection validate {[src-mac][dst-mac][ip]}**.

- **IP Source Guard**: Funcionalidad para mitigación de ataque de suplantación de direcciones. Analiza cada paquete que llega al switch verificando que sus direcciones son válidas al compararlas con la tabla de DHCP Snooping.
    - Requiere que DHCP Snooping esté habilitado.
    - Funcionamiento:
        - En principio sólo el tráfico DHCP se permite por la interfaz.
        - Tras la recepción de una IP desde un servidor DHCP por parte del host conectado a la interfaz, se configura dinámicamente en la interfaz una ACLs por VLANs (PVACLs) que filtra paquetes con IPs de origen diferentes a la recibida.
        - La PVACL se adapta a los cambios de IPs procedentes del servidor DHCP.
    - **Configuración**:
        - Se accede a la interfaz.
        - **ip verify source.**
        - **ip verify source port-security**.

- **Mecanismos de estabilidad STP**: Para mitigar ataques lo mejor es usar estos 4 mecanismos:
    - **Portfast**: permite que un host se conecte de forma inmediata sin esperar a la convergencia STP. No se debe usar cuando el puerto se conecta a otro switch.
        - Configuración general de todos los puertos, **spanning-tree portfast default**.
        - Configuración en una interfaz concreta, **spanning-tree portfast**.
    - **BPDU Guard**: deshabilita un puerto al que le llega una BPDU. Se aplica sólo a los puertos donde se conecta un host. Se utiliza habitualmente junto con portfast.
        - Configuración general de todos los puertos portfast, **spanning-tree portfast bpduguard default**.
        - Configuración en una interfaz concreta, **spanning-tree bpduguard enable**.
    - **Root Guard**: hace que un puerto sólo envíe BPDUs y no la reciba. Se aplica a puertos conectados a switches que nunca deberían ser raíz. Si recibe una BPDU se quedará en estado err-disable.
        - Configuración en una interfaz, **spanning-tree guard root**.
    - **Loop guard**: Los puertos bloqueados pasan a estado forwarding por error y se produce un bucle. Se puede evitar eso activando esta característica en el puerto.
        - Configuración general de todos los puertos, **spanning-tree loopguard default**.

        - Configuración en una interfaz concreta, **spanning-tree guard loop**.

- **Err-disabled:** es el estado de bloqueo en el que se queda un puerto tras producirse algunas de las siguientes condiciones:
    - Infracción de la seguridad del puerto.
    - Infracción de BPDU Guard en STP.
    - Infracción de Root Guard en STP.
    - Configuración incorrecta de EtherChannel.
    - Desajuste duplex.
    - Condición de UDLD.
    - Agitación del enlace.
    - Infracción DHCP Snooping.
    - Infracción de DAI.
    - Otras
    - **Configuración**:
        - Para crear una causa**: errdisable detect cause [all | "cause-name"]**.
        - Para reactivar un puerto en err-disable, tras la desaparición de la condición de error, **shutdown/no shutdown**.
        - Se puede programar automáticamente tras un tiempo de espera, **errdisable recovery cause "psecure-violation"** y **errdisable recovery interval "60"**.

Configuración Seguridad L2

La mayoría de las configuraciones de Seguridad de los dispositivos los he aplicado en cada Hito correspondiente según el ataque.

- Se han realizado la mayoría de las **buenas prácticas** para proteger el software de la red nombradas en Seguridad L2.

- La **seguridad de los puertos** está aplicada en los puertos de acceso de los switches de acceso en el Hito 2. Lo único que se ha añadido, en todos los puertos de acceso, es la acción tras producirse una violación, **switchport port-security violation shutdown.**

- Se debería activar la **notificación de MACs** en todos los switches con **mac address-table notification**, pero no funciona en packet tracer.

- Toda la configuración para evitar ataques a **VLANs** están aplicadas en las interfaces aplicables de todos los switches en el Hito 2.

- Se ha habilitado **DHCP Snooping**, **Dynamic ARP Inspection** y **IP Source Guard** para los switches de acceso y se aplican en los puertos de acceso. **IP Source Guard** no funciona en packet tracer
    - En cada Switch de acceso, y luego en los puertos de acceso:
        - **ip dhcp snooping**
        - **ip dhcp snooping vlan 20,30,1000**
        - **ip arp inspection vlan 20,30,1000**

        - **ip arp inspection validate src-mac dst-mac ip**
        - **interface range g1/0/1-15**
            - **ip dhcp snooping trust**
            - **ip arp inspection trust**
            - **ip verify source**, no funciona en packet tracer.
            - **ip verify source port-security**, no funciona en packet tracer.
            - **exit**

- Se han aplicado los **4 mecanismos de estabilidad** mencionados anteriormente, Seguridad L2, dentro del Hito 3 en el protocolo **RPVST+**. Cada mecanismo se ha establecido en los puertos que les corresponde en los Switches. El único no aplicable en packet tracer es Loop Guard, este programa no lo tiene aplicado.

- Se ha aplicado la configuración de **Err-Disabled** para todos los Switches y que se reactiven después de 60 segundos. Se han creado causas adicionales como la violación de un puerto de seguridad, error en BPDU guard y error en UDLD. El problema es que tampoco funciona para packet tracer errdisable.

    - Configuración entorno real:
        - **errdisable detect cause all**
        - **errdisable detect cause security-violation**
        - **errdisable detect cause bpduguard**
        - **errdisable detect cause udld**
        - **errdisable recovery cause all**
        - **errdisable recovery interval 60**
        - **errdisable recovery cause security-violation**
        - **errdisable recovery cause bpduguard**
        - **errdisable recovery cause udld**

BIBLIOGRAFÍA

Hito 2: Contenidos del campus virtual..
Hito 3: Contenidos del campus virtual y H3C S12500X-AF series CE DoC-6W104 - 01-SPBM configuration.
Hito 4: Contenido del campus virtual y NTP » CCNA desde Cero
Hito 5: Contenido del campus virtual y Ejemplo de Configuración de QoS en los Puertos de Acceso Catalyst 6800ia - Cisco
Hito 6: Contenido del campus virtual y ¿Qué es un Switch PoE y cómo funciona? | Comunidad FS
Hito 7: Contenido del campus virtual.

CONCLUSIÓN

Creo que en la elaboración de este proyecto se aprende más que si tuviéramos un examen, ya que hay muchas cosas que nos la estudiamos de memoria, hecho que está mal, pero lo hacemos. En mi opinión me ha gustado más hacer este proyecto que realizar un examen. Lo único malo ha sido el programa de packet tracer porque está un poco desactualizado del entorno real y protocolos más modernos.

Después de haber implementado todos los protocolos en packet tracer, quiero destacar que el programa no ha ayudado mucho debido a que bastantes protocolos o no funcionaban correctamente o sus comandos de configuración no están implementados en el programa.

Así que he tenido que usar o versiones más antiguas de algunos protocolos o usar otros comandos para poder realizar la implementación de todo lo que se pedía.

Además, me he encontrado con numerosos fallos en el programa, no se si es debido a los numerosos protocolos implementados en cada switch, pero de un día a otro me cambia el esquema de RPVST+ inicial que había hecho de todos los puertos.

Creo que también podría ser que al introducir todos los protocolos a la vez, el programa no funcione del todo bien.

CONFIGURACIÓN FINAL DE LOS EQUIPOS

Switches de acceso:

Switch A1:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
ip dhcp snooping
ip dhcp snooping vlan 20,30,1000
ip arp inspection vlan 20,30,1000
ip arp inspection validate src-mac dst-mac ip
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
```

```
 exit
interface range g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping trust
 ip arp inspection trust
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface vlan 20
 ip address 172.16.20.3 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.3 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.3 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 2 mode active
 exit
interface range g1/0/21-22
 channel-group 3 mode active
 exit
interface port-channel 2
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 3
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
```

```
mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

monitor session 1 source interface g1/0/1
monitor session 1 destination interface g1/0/2

vlan 200
 name RSPAN-VLAN
 remote-span
 exit
monitor session 2 source vlan 20
monitor session 2 destination remote vlan 200

clock timezone EST -5
ntp server 172.16.20.11

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch A2:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A2 #
line con 0
```

```
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
ip dhcp snooping
ip dhcp snooping vlan 20,30,1000
ip arp inspection vlan 20,30,1000
ip arp inspection validate src-mac dst-mac ip
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface range g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping trust
 ip arp inspection trust
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface vlan 20
 ip address 172.16.20.4 255.255.255.0
```

```
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.4 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.4 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 4 mode active
 exit
interface range g1/0/21-22
 channel-group 5 mode active
 exit
interface port-channel 4
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 5
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 172.16.20.12

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
```

```
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch A3:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A3 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
ip dhcp snooping
ip dhcp snooping vlan 20,30,1000
ip arp inspection vlan 20,30,1000
ip arp inspection validate src-mac dst-mac ip
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
```

```
 switchport access vlan 1000
 shutdown
 exit
interface range g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping trust
 ip arp inspection trust
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface vlan 20
 ip address 172.16.20.5 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.5 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.5 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 6 mode active
 exit
interface range g1/0/21-22
 channel-group 7 mode active
 exit
interface port-channel 6
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 7
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
```

```
 exit

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 172.16.20.11

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch A4:

```
en
conf t
ip routing
no ip domain lookup
banner motd # A4 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
```

```
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
ip dhcp snooping
ip dhcp snooping vlan 20,30,1000
ip arp inspection vlan 20,30,1000
ip arp inspection validate src-mac dst-mac ip
interface range g1/0/16-20, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface range  g1/0/1-15
 switchport mode access
 switchport access vlan 20
 switchport voice vlan 30
 spanning-tree portfast
 spanning-tree bpduguard enable
 ip dhcp snooping trust
 ip arp inspection trust
 switchport port-security
 switchport port-security maximum 45
 switchport port-security violation shutdown
 switchport port-security aging time 120
 switchport protected
 no shutdown
 exit
interface vlan 20
 ip address 172.16.20.6 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.6 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.6 255.255.255.0
```

```
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 8 mode active
 exit
interface range g1/0/21-22
 channel-group 9 mode active
 exit
interface port-channel 8
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 9
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 172.16.20.12

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
```

```
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switches de distribución:

Switch D1:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-16, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.7 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.7 255.255.255.0
```

```
 no shutdown
 exit
interface vlan 1000
 ip address 172.16.100.7 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 2 mode active
 exit
interface range g1/0/21-22
 channel-group 4 mode active
 exit
interface range g1/0/19-20
 channel-group 10 mode active
 exit
interface range g1/0/17-18
 channel-group 11 mode active
 exit
interface port-channel 2
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 4
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 10
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 11
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit

mls qos
```

```
logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

vlan 200
 name RSPAN-VLAN
 remote-span
 exit
monitor session 2 source remote vlan 200
monitor session 2 destination interface g1/0/16

clock timezone EST -5
ntp server 172.16.20.11

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch D2:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
```

```
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-16, g1/1/1-4
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.8 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.8 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.8 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 3 mode active
 exit
interface range g1/0/21-22
 channel-group 5 mode active
 exit
interface range g1/0/19-20
 channel-group 12 mode active
 exit
interface range g1/0/17-18
 channel-group 13 mode active
 exit
interface port-channel 3
```

```
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 5
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 12
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 13
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 172.16.20.12

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
```

```
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch D3:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D3 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-20
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.9 255.255.255.0
 no shutdown
 exit
interface vlan 30
```

```
  ip address 172.16.30.9 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.9 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 6 mode active
 exit
interface range g1/0/21-22
 channel-group 8 mode active
 exit
interface range g1/1/3-4
 channel-group 14 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 15 mode active
 no shutdown
 exit
interface port-channel 6
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 8
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 14
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 15
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
```

```
mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 172.16.20.11

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch D4:

```
en
conf t
ip routing
no ip domain lookup
banner motd # D4 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
```

```
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/1-20
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.10 255.255.255.0
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.10 255.255.255.0
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.10 255.255.255.0
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 7 mode active
 exit
interface range g1/0/21-22
 channel-group 9 mode active
 exit
interface range g1/1/3-4
 channel-group 16 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 17 mode active
 no shutdown
 exit
interface port-channel 7
 switchport mode trunk
 switchport nonegotiate
```

```
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 9
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 spanning-tree guard root
 exit
interface port-channel 16
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 17
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 172.16.20.12

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
```

```
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switches de núcleo:

Switch N1:

```
en
conf t
ip routing
no ip domain lookup
banner motd # N1 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
vlan 30
 name VOZ
 exit
interface range g1/0/3-18
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.11 255.255.255.0
 standby version 2
 standby 20 ip 172.16.20.254
```

```
 standby 20 priority 150
 standby 20 preempt
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.11 255.255.255.0
 standby version 2
 standby 30 ip 172.16.30.254
 standby 30 preempt
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.11 255.255.255.0
standby version 2
 standby 1000 ip 172.16.100.254
 standby 1000 priority 90
 standby 1000 preempt
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 10 mode active
 no shutdown
 exit
interface range g1/0/21-22
 channel-group 12 mode active
 no shutdown
 exit
interface range g1/1/3-4
 channel-group 14 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 16 mode active
 no shutdown
 exit
interface range g1/0/19-20
 channel-group 18 mode active
 no shutdown
 exit
interface port-channel 10
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 12
 switchport mode trunk
```

```
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 14
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 16
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 18
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface g1/0/1
 no switchport
 ip address 192.168.1.1 255.255.255.0
 no shutdown
 exit
interface g1/0/2
 no switchport
 ip address 192.168.2.1 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 192.168.1.3

spanning-tree vlan 20 priority 4096
spanning-tree vlan 30 priority 8192
spanning-tree vlan 999 priority 16384
spanning-tree vlan 1000 priority 32768

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw
```

```
lldp run

clock timezone EST -5
ntp server 192.168.2.3

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Switch N2:

```
en
conf t
ip routing
no ip domain lookup
banner motd # N2 #
line con 0
 exec-timeout 0 0
 logging synchronous
 exit
line vty 0 4
 privilege level 15
 password cisco123
 exec-timeout 0 0
 login
 exit
spanning-tree mode rapid-pvst
vlan 1000
 name  BLACKHOLE
 exit
vlan 999
 name NATIVA
 exit
vlan 20
 name DATOS
 exit
```

```
vlan 30
 name VOZ
 exit
interface range g1/0/3-18
 switchport mode access
 switchport access vlan 1000
 shutdown
 exit
interface vlan 20
 ip address 172.16.20.12 255.255.255.0
 standby version 2
 standby 20 ip 172.16.20.254
 standby 20 preempt
 no shutdown
 exit
interface vlan 30
  ip address 172.16.30.12 255.255.255.0
 standby version 2
 standby 30 ip 172.16.30.254
 standby 30 priority 150
 standby 30 preempt
  no shutdown
  exit
interface vlan 1000
 ip address 172.16.100.12 255.255.255.0
standby version 2
 standby 1000 ip 172.16.100.254
 standby 1000 priority 90
 standby 1000 preempt
 no shutdown
 exit
ip default-gateway 192.168.1.3
interface range g1/0/23-24
 channel-group 11 mode active
 no shutdown
 exit
interface range g1/0/21-22
 channel-group 13 mode active
 no shutdown
 exit
interface range g1/1/3-4
 channel-group 15 mode active
 no shutdown
 exit
interface range g1/1/1-2
 channel-group 17 mode active
 no shutdown
 exit
```

```
interface range g1/0/19-20
 channel-group 18 mode active
 no shutdown
 exit
interface port-channel 11
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 13
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30
 exit
interface port-channel 15
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 17
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface port-channel 18
 switchport mode trunk
 switchport nonegotiate
 switchport trunk native vlan 999
 switchport trunk allowed vlan 20,30,999,1000
 exit
interface g1/0/1
 no switchport
 ip address 192.168.1.2 255.255.255.0
 no shutdown
 exit
interface g1/0/2
 no switchport
 ip address 192.168.2.2 255.255.255.0
 no shutdown
 exit
ip route 0.0.0.0 0.0.0.0 192.168.2.3

spanning-tree vlan 30 priority 4096
spanning-tree vlan 20 priority 8192
```

```
spanning-tree vlan 999 priority 16384
spanning-tree vlan 1000 priority 32768

mls qos

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

clock timezone EST -5
ntp server 192.168.1.3

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Routers:

Router R1:

```
en
clock set 16:52:00 13 June 2023
conf t
hostname R1
no ip domain lookup
banner motd # This is R1 #
line con 0
 logging sync
 exec-time 0 0
 exit
```

```
access-list 1 permit 172.16.20.0 0.0.0.255
access-list 2 permit 172.16.30.0 0.0.0.255

class-map match-any VOICE_TRAFFIC
 match ip dscp ef
 exit
policy-map QOS_POLICY
 class VOICE_TRAFFIC
  priority percent 30
  exit
 class class-default
  fair-queue
  exit

ip flow-export version 9
ip flow-export destination 172.16.125.4 9999

interface fa0/0
 ip address 192.168.1.3 255.255.255.0
 ip nat inside
 service-policy output  QOS_POLICY
 ip flow ingress
 ip flow egress
 no shutdown
 exit
interface fa0/1
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
 service-policy output  QOS_POLICY
 ip flow ingress
 ip flow egress
 no shutdown
 exit
interface fa1/0
ip address 192.168.7.1 255.255.255.0
 ip nat inside
 service-policy output  QOS_POLICY
 ip flow ingress
 ip flow egress
 no shutdown
 exit
interface se0/3/0
 ip address 192.168.5.1 255.255.255.0
 ip nat outside
 no shutdown
 exit
interface se0/3/1
```

```
 ip address 192.168.6.1 255.255.255.0
 ip nat outside
 no shutdown
 exit

ip nat inside source list 1 interface serial0/3/0 overload
ip nat inside source list 1 interface serial0/3/1 overload
ip nat inside source list 2 interface serial0/3/0 overload
ip nat inside source list 2 interface serial0/3/1 overload

router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
 exit

telephony-service
 max-dn 30
 max-ephones 30
 ip source-address 192.168.30.1 port 2000
 auto assign 4 to 6
 exit
ephone-dn 1
number 501
ephone-dn 2
number 502
ephone-dn 3
number 503
ephone-dn 4
number 504
ephone-dn 5
number 505
ephone-dn 6
number 506
ephone-dn 7
number 507
ephone-dn 8
number 508
ephone-dn 9
number 509
ephone-dn 10
number 510
ephone-dn 11
number 511
ephone-dn 12
number 512
ephone-dn 13
number 513
```

```
ephone-dn 14
number 514
ephone-dn 15
number 515
ephone-dn 16
number 516
ephone-dn 17
number 517
ephone-dn 18
number 518
ephone-dn 19
number 519
ephone-dn 20
number 520
ephone-dn 21
number 521
ephone-dn 22
number 522
ephone-dn 23
number 523
ephone-dn 24
number 524
ephone-dn 25
number 525
ephone-dn 526
number 526
ephone-dn 527
number 527
ephone-dn 528
number 528
ephone-dn 529
number 529
ephone-dn 530
number 530
exit

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

ntp master 10
clock timezone EST -5
```

```
username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```

Router R2:

```
en
clock set 16:52:00 13 June 2023
conf t
hostname R2
no ip domain lookup
banner motd # This is R2 #
line con 0
 logging sync
 exec-time 0 0
 exit

access-list 3 permit 172.16.20.0 0.0.0.255
access-list 4 permit 172.16.30.0 0.0.0.255

class-map match-any VOICE_TRAFFIC
 match ip dscp ef
 exit
policy-map QOS_POLICY
 class VOICE_TRAFFIC
  priority percent 30
  exit
 class class-default
  fair-queue
  exit

ip flow-export version 9
ip flow-export destination 172.16.125.4 9999

interface fa0/0
 ip address 192.168.2.3 255.255.255.0
```

```
 ip nat inside
 service-policy output  QOS_POLICY
 ip flow ingress
 ip flow egress
 no shutdown
 exit
interface fa0/1
 ip address 192.168.3.2 255.255.255.0
 ip nat inside
 service-policy output  QOS_POLICY
 ip flow ingress
 ip flow egress
 no shutdown
 exit
interface fa1/0
 ip address 192.168.7.2 255.255.255.0
 ip nat inside
 service-policy output  QOS_POLICY
 ip flow ingress
 ip flow egress
 no shutdown
 exit
interface se0/3/0
 ip address 192.168.5.2 255.255.255.0
 ip nat outside
 no shutdown
 exit
interface se0/3/1
 ip address 192.168.6.2 255.255.255.0
 ip nat outside
 no shutdown
 exit

ip nat inside source list 3 interface serial0/3/0 overload
ip nat inside source list 3 interface serial0/3/1 overload
ip nat inside source list 4 interface serial0/3/0 overload
ip nat inside source list 4 interface serial0/3/1 overload

router ospf 1
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.7.0 0.0.0.255 area 0
 exit

telephony-service
 max-dn 60
 max-ephones 30
 ip source-address 192.168.30.2 port 2000
```

```
 auto assign 4 to 6
 exit
ephone-dn 31
number 531
ephone-dn 32
number 532
ephone-dn 33
number 533
ephone-dn 34
number 534
ephone-dn 35
number 535
ephone-dn 36
number 536
ephone-dn 37
number 537
ephone-dn 38
number 538
ephone-dn 39
number 539
ephone-dn 40
number 540
ephone-dn 41
number 541
ephone-dn 42
number 542
ephone-dn 43
number 543
ephone-dn 44
number 544
ephone-dn 45
number 545
ephone-dn 46
number 546
ephone-dn 47
number 547
ephone-dn 48
number 548
ephone-dn 49
number 549
ephone-dn 50
number 550
ephone-dn 51
number 551
ephone-dn 52
number 552
ephone-dn 53
number 553
```

```
ephone-dn 54
number 554
ephone-dn 55
number 555
ephone-dn 556
number 556
ephone-dn 557
number 557
ephone-dn 558
number 558
ephone-dn 559
number 559
ephone-dn 560
number 560
exit

logging buffered 16384
logging trap debugging
logging host 172.16.125.2
logging on

snmp-server community CCNPv8 ro
snmp-server community CCNPv8-rw rw

lldp run

ntp master 5
clock timezone EST -5

username admin privilege 15 password cisco123
aaa new-model
aaa authentication login default  local-case enable
aaa authentication login SSH-LOGIN local-case
line vty 0 4
 login authentication SSH-LOGIN
 exit
radius server RADIUS
 address ipv4 192.168.1.5 auth-port 1812
 key cisco12345
 exit
aaa authentication login default local-case
aaa authorization exec default local
aaa authorization network default local
```