Miguel Palau Feliu Modelo CCNA

❎He resuelto esta Práctica de manera individual y bajo mi responsabilidad. Estoy al corriente de los requisitos para la cita de fuentes externas, y de las consecuencias académicas de la falta de originalidad en mis actividades evaluables

Ejercicio 1

SE ADJUNTAN DENTRO DEL .ZIP EL FICHERO PACKET TRACER Y EL DIAGRAMA DE RED

Dimensionado de equipos de comunicaciones y cableado

Para determinar cuántos switches de acceso se usan, éstos deberán permitir que se conecten los PCs o puntos de acceso. Los switches suelen ser de 24 o 48 puertos. Si se toman de 48 puertos, en la oficina principal, en cada planta, que tiene 200 usuarios, se usarán 5 switches. El resto de puertos sobrantes se usan para los puntos de acceso Wifi. Se puede ubicar un punto de acceso Wifi por cada 100 usuarios, que es la capacidad indicada en especificaciones de varios proveedores.

Podría suceder que no fueran capaces de cursar el tráfico de los 100 usuarios, y entonces habría que desplegar más puntos de acceso. Esto se asume que no sucederá. Entonces, para 200 usuarios por planta, se pondrán 2 puntos de acceso. Finalmente, los switches de acceso se conectarán con sus dos puertos troncales de mayor capacidad a los switches de agregación (también llamados de distribución). Los switches de acceso se ubicará en los racks de cada planta, y el de distribución en el sótano. El cableado irá con UTP categoría 6 (1 Gbps) para todas las sedes.

En el resto de sedes se seguirá un criterio similar, en función del número de usuarios. Se describe en más detalle en el diagrama de red anexo.

Definición de VLANs en switches

Los switches deben tener definidas sus VLANs para que pueda conmutar tráfico con 802.1q en sus cabeceras Ethernet. Se definen según:

vlan #número de la vlan#
exit

Asociación de puertos de acceso para conexión con PCs/Laptops/Servidores

Cada puerto conectado a PCs/Laptops/Servidores será asociado a una VLAN. Se configura según:

```
interface Gi#slot/puerto#
switchport access vlan #VLAN#
exit
```

Etherchannel troncales entre switches

Se usa el protocolo LACP para configurar los enlaces agregados (múltiples enlaces) entre switches. También se podría haber usado PAgP. Además, serán conexiones troncales (múltiples VLANs). En cada extremo del etherchannel se configura el agregado y los puertos según:

```
int Port-channel 1
switchport mode trunk
exit
int range Gi0/1-2
switchport mode trunk
channel-group 1 mode active
exit
```

Puertos entre switch de agregación y router

Los puertos entre switch de agregación y router: serán troncales (llevarán varias VLANs). Se configuran según:

```
int Gi#slot/puerto#
switchport mode trunk
exit
```

Puntos de acceso wifi:

Servirán su wifi con un SSID específico para cada sede.

Direccionamiento IP en routers y PCs/Laptops/servidores

Para el conjunto de IPs del enunciado, se reparte cada red en función del número de equipos a conectar. Por un lado estarán los PCs, laptops y servidores. Por otro lado los routers, que usarán una sola IP, salvo si usan HSRP, que necesitarán 3. En la red Wifi los usuarios que necesitan IPs son los equipos que se conectan, no el punto de acceso, que simplemente actúa de bridge (nivel 2).

Por ejemplo, para la red de usuarios de la oficina principal, hay 3 plantas con 200 empleados por planta, y además la IP del router. La máscara de red que cubre las 601 IPs necesitadas es una /22, que permite hasta 1022 IPs para hosts.

Se intenta asignar el uso del mayor al menor tamaño de red, para evitar que falten IPs y por tanto haya que configurar NAT dinámico con sobrecarga, por ejemplo.

Para las IPs de gestión, son necesarias en los switches y routers a gestionar.

Entre la oficina principal y el centro de investigación I+D 1 hay un enlace de nivel 2, que obliga a que compartan el direccionamiento en todas las VLANs. En centro de investigación consume un número de IPs menor que las IPs sobrantes en las redes reservadas para la oficina principal, así que no es necesario ampliarlo. El enlace se puede simular en Packet Tracer conectando los multilayer switches entre sí, para que las VLANs con mismo direccionamiento se comuniquen entre sí.

La IP de puerta de enlace en cada sede será distinta. Para los tráficos de vuelta, es posible que un router atraiga todo el tráfico de ambas sedes. Por ejemplo, con vuelta prioritaria por la oficina principal (se podría anunciar con menor coste OSPF por ahí, o mayor coste por la del centro de investigación). Para no atraer también el tráfico del centro de investigación se podría anunciar una estática a OSPF para el subrango del centro de investigación con un coste menor. Únicamente se ha implementado configurar un coste mayor en el router del centro de investigación 1 para cada subinterfaz:

```
int gi0/0/1.50
 ip ospf cost 1000
exit
int gi0/0/1.200
 ip ospf cost 1000
exit
int gi0/0/1.200
 ip ospf cost 1000
exit
```

Siguiendo este criterio, se obtiene:

CATALUÑA:

Oficina principal:
172.16.0.0/22 (usuarios, comenzando por las IPs más bajas)
172.16.4.0/22 (WiFi, comenzando por las IPs más bajas)
172.16.9.64/29 (servidores)
172.16.64.0/28 (gestión, comenzando por las IPs más bajas)

Centro de investigación 1:
172.16.0.0/22 (usuarios, comenzando por las IPs más altas. Necesita un /25: se toma 172.16.3.128/25)
172.16.4.0/22 (WiFi, comenzando por las IPs más altas. Necesita un /25: se toma 172.16.7.128/25)
172.16.64.0/28 (gestión, comenzando por las IPs más altas. Necesita un /29: se toma 172.16.64.8/29)

Almacén 1:

172.16.9.0/27 (usuarios)
172.16.9.32/27 (WiFi)
172.16.64.24/29 (gestión)

ESTADOS UNIDOS:

Centro de investigación 2:
10.0.0.0/21 (WiFi)
172.16.64.32/29 (gestión)

Almacén 2:
10.0.8.0/27 (usuarios)
10.0.8.32/27 (WiFi)
172.16.64.40/29 (gestión)

Direccionamiento en PCs, laptops y servidores:

Se asignan IPs del tramo más alto de cada subred.

Configuración IP LAN en los routers para cada subinterfaz:

En cada LAN, el router que actúa de gateway tendrá configurada su IP, con la encapsulación 802.1q correspondiente y compartida la subred en OSPF, según:

```
interface Gi0/0/1.#VLAN#
 no shutdown
 encapsulation dot1q #VLAN#
 ip ospf 1 area 0
 ip address #IP-router# #Máscara#
exit
```

Configuración de HSRP:

En Almacén 1 se proporcionan dos proveedores de servicio como gateways para salir a Internet. Con lo cual, deben comunicarse entre ellos en todas las subinterfaces para ofrecer una única IP de puerta de enlace. Esto se consigue con HSRP. Se tomará la primera IP como virtual en cada subred, y las dos siguientes para los routers que participan en HSRP. La prioridad por defecto es 100. Se pondrá en el de Telefónica 101 para preferenciar respecto al de Vodafone. Se configura según:

```
interface Gi0/0/1.#VLAN#
 standby #VLAN# ip #IP-virtual#
 standby #VLAN# priority #priority#
exit
```

Configuración de IP de gestión en switches

Cada switch podrá ser gestionado si se le asigna una IP asociada a la VLAN de gestión (50). Se configura según:

```
interface vlan 50
ip address #IP# #Máscara#
exit
```

Exportación de redes LAN a OSPF:

Se redistribuyen las redes directamente conectadas, que llegan a los PCs, laptops y servidores, a OSPF. Para eso, es necesario añadir lo siguiente en los routers gateway de dichas redes:

```
router ospf 1
redistribute connected subnets
exit
```

También cada subinterfaz deberá ser partícipe de conectarse a OSPF, según:

```
interface Gi0/0/1.#VLAN#
ip ospf 1 area 0
exit
```

Simulación de Internet:

Se conecta cada router del proveedor de servicios en cada sede con un switch que representa a Internet. Todos los routers de los proveedores se ven entre sí y usarán una IP del rango 9.0.0.0/8 (se ha elegido uno cualquiera disponible, dentro de los rangos de IPs públicas).

Estos routers se distribuirán las redes que conocen por OSPF, en el área 0.

Por ejemplo, en el router del proveedor de servicios de la oficina principal, se configura:

```
router ospf 1
redistribute connected subnets
exit
int gi0/0/0
ip address 9.0.0.1 255.0.0.0
ip ospf 1 area 0
exit
```

Conexiones WAN:

Los routers de salida de cada sede se conectan con los routers de su proveedor de servicios a través de las conexiones indicadas en el enunciado, y esas conexiones se comparten en OSPF.

Por ejemplo, en el router del proveedor de servicios de la oficina principal, se configura:

```
int gi0/0/1
no shut
ip add 88.37.32.41 255.255.255.248
ip ospf 1 area 0
exit
```

Configuración NAT:

Sólo la necesitan NAT (en este caso, estático) los servidores de la oficina principal, porque en el enunciado especifican que desde el Operador logístico se debe acceder por IPs públicas a los servidores.
El resto de elementos no necesitan NAT porque sobran direcciones IP privadas, y no se especifica que en Internet deban anunciarse otras posibles redes públicas.

El NAT estático de los servidores se configura en el router PRINCIPAL, con IPs públicas las siguientes disponibles del rango de salida hacia el proveedor de servicios:

```
interface gi0/0/1.150
ip nat inside
exit
interface gi0/0/0
ip nat outside
exit
ip nat inside source static 172.16.9.66 88.37.32.43
ip nat inside source static 172.16.9.67 88.37.32.44
```

Configuración de ACLs:

En el enunciado se obliga el operador logístico no pueda entrar a los servidores a través de su IP privada, sino sólo con la IP pública. El resto de sedes sí. Esto se consigue con una ACL de entrada en el router PRINCIPAL desde Internet.

```
int Gi0/0/0
ip access-group limita-servidores in
exit
ip access-list extended limita-servidores
deny ip 88.34.34.0 0.0.0.3 172.16.9.64 0.0.0.7
permit ip any any
exit
```

Se valida ejecutando pings desde el operador logístico hacia las IPs públicas y privadas de los servidores. Sólo las IPs públicas permitirán el acceso:

```
C:\>ping 172.16.9.66

Pinging 172.16.9.66 with 32 bytes of data:

Reply from 88.37.32.42: Destination host unreachable.
Reply from 88.37.32.42: Destination host unreachable.
Reply from 88.37.32.42: Destination host unreachable.
Reply from 88.37.32.42: Destination host unreachable.

Ping statistics for 172.16.9.66:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
C:\>ping 88.37.32.43

Pinging 88.37.32.43 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 88.37.32.43: bytes=32 time<1ms TTL=125
Reply from 88.37.32.43: bytes=32 time<1ms TTL=125

Ping statistics for 88.37.32.43:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

En el router PRINCIPAL se ven los contadores de la ACL, que muestran cómo se permiten o deniegan los pings:

```
Router#sh access-lists
Extended IP access list limita-servidores
    10 deny ip 88.34.34.0 0.0.0.3 172.16.9.64 0.0.0.7 (4 match(es))
    20 permit ip any any (18 match(es))
```

También se debe limitar que los servidores de Google Cloud sólo sean accesibles por las sedes propias, pero no por los operadores logísticos. Para cumplirlo, se debe poner una ACL de entrada desde Internet al router GOOGLE CLOUD, que permite el acceso a la red de Google Cloud sólo a las sedes propias.

```
int Gi0/0/0
ip access-group limita-cloud in
exit
ip access-list extended limita-cloud
permit ip 172.16.0.0 0.0.63.255 8.2.0.0 0.0.255.255
permit ip 172.16.64.0 0.0.15.255 8.2.0.0 0.0.255.255
permit ip 10.0.0.0 0.0.15.255 8.2.0.0 0.0.255.255
deny ip 88.34.34.0 0.0.0.3 8.2.0.0 0.0.255.255
permit ip any any
exit
```

Para probarlo, se lanzan pings a Google Cloud desde algún PC de las sedes y desde el operador logístico. Sólo en el primer caso se permite el tráfico.

Ping desde una sede:

C:\>ping 8.2.0.5

Pinging 8.2.0.5 with 32 bytes of data:

Request timed out.
Reply from 8.2.0.5: bytes=32 time<1ms TTL=125
Reply from 8.2.0.5: bytes=32 time<1ms TTL=125
Reply from 8.2.0.5: bytes=32 time=10ms TTL=125

Ping statistics for 8.2.0.5:
  Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
  Minimum = 0ms, Maximum = 10ms, Average = 3ms

Ping desde el operador:

C:\>ping 8.2.0.5

Pinging 8.2.0.5 with 32 bytes of data:

Reply from 88.34.34.1: Destination host unreachable.
Reply from 9.0.0.8: Destination host unreachable.
Reply from 9.0.0.8: Destination host unreachable.
Reply from 9.0.0.8: Destination host unreachable.

Ping statistics for 8.2.0.5:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

Muestra de los contadores de la ACL en el router GOOGLE CLOUD, donde se muestran en las entradas 10 y 40 los contadores de permitir o denegar el tráfico:

Router#sh access-lists
Extended IP access list limita-cloud
  10 permit ip 172.16.0.0 0.0.63.255 8.2.0.0 0.0.255.255 (3 match(es))

20 permit ip 172.16.64.0 0.0.15.255 8.2.0.0 0.0.255.255
30 permit ip 10.0.0.0 0.0.15.255 8.2.0.0 0.0.255.255
40 deny ip 88.34.34.0 0.0.0.3 8.2.0.0 0.0.255.255 (3 match(es))
50 permit ip any any (113 match(es))

EJERCICIO 2

Se adjunta el archivo de packet tracer dentro del ZIP con la configuración.

EJERCICIO 3

Capturas de los exámenes realizados en netacad.

Enterprise Networking, Security, and Automation (Versión 7.00) - Examen de optimización, monitoreo y solución de problemas de redes

Catálogo de la evaluación

Idioma de la evaluación	Descripción de la evaluación	Información de activación
English	This exam will cover material from Modules 9 - 12 of the CCNA3 - Enterprise Networking, Security, and Automation (ENSA) v7.0 curriculum. This exam will be scored using the Weighted Model where each MCSA (Multiple-Choice Single-Answer) is worth two points and each MCMA (Multiple-Choice Multiple-Answer) is worth one point for each correct option. Other tasks types such as drag and drop (matching) and Packet Tracer items may be included in this exam. For Packet Tracer tasks, you must have the latest version of Packet Tracer installed on your machine.	Puntaje: 95,7 % El instructor debe reactivar Historial de evaluaciones

Enterprise Networking, Security, and Automation (Versión 7.00) - Emerging Network Technologies Exam

Catálogo de la evaluación

Idioma de la evaluación	Descripción de la evaluación	Información de activación
English	This exam will cover material from Modules 13 and 14 of the CCNA3 - Enterprise Networking, Security, and Automation (ENSA) v7.0 curriculum. This exam will be scored using the Weighted Model where each MCSA (Multiple-Choice Single-Answer) is worth two points and each MCMA (Multiple-Choice Multiple-Answer) is worth one point for each correct option. Other tasks types such as drag and drop (matching) and Packet Tracer items may be included in this exam. For Packet Tracer tasks, you must have the latest version of Packet Tracer installed on your machine.	Puntaje: 100 % El instructor debe reactivar Historial de evaluaciones
	Este examen cubrirá material de los Módulos 13 y 14 del plan de estudios CCNA3 - Redes	

Catálogo de la evaluación

Enterprise Networking, Security, and Automation (Versión 7.00) - ENSA Final Exam

Catálogo de la evaluación

Idioma de la evaluación	Descripción de la evaluación	Información de activación
English	This final exam will cover material from all of the CCNA3 - Enterprise Networking, Security, and Automation (ENSA) curriculum. This exam will be scored using the Weighted Model where each MCSA (Multiple-Choice Single-Answer) is worth two points and each MCMA (Multiple-Choice Multiple-Answer) is worth one point for each correct option. Other task types such as drag and drop (matching) and Packet Tracer items may be included in this exam. For Packet Tracer tasks, you must have the latest version of Packet Tracer installed on your machine.	Puntaje: 100 % El instructor debe reactivar Historial de evaluaciones