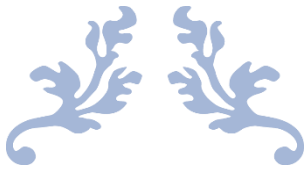

DISEÑO Y CONSTRUCCIÓN DE REDES CORPORATIVAS

Práctica Evaluable

ALUMNO: Adrián Bennasar Polzin

PROFESOR: Antonio Sola Venteo

ASIGNATURA: Redes Avanzadas

CURSO: 2021-2022

Introducción

En esta práctica final de la asignatura, realizada con el software Cisco Packet Tracer, se diseña e implementa la red indicada en el enunciado, que consiste en una red corporativa (XYZ) que obtiene conectividad y servicios de un operador (ABC) que a su vez está conectado a 2 operadores nacionales.

He intentado implementar en CPT todo lo que he podido, y las cosas que no he conseguido implementar o que no funcionan del todo, las explicaré lo mejor que pueda de manera teórica en esta memoria de la práctica.

Esquema de direccionamiento

El operador ABC ha solicitado un bloque de direcciones, así como un número de sistema autónomo a RIPE NCC, entidad con la capacidad de proporcionar estos servicios.

El número de sistema autónomo asignado al operador ABC es el 300. Por otra parte, el bloque de direcciones que RIPE le ha proporcionado a la red ABC, es el bloque 172.16.0.0 de clase B. Como el enunciado especifica, la red corporativa XYZ obtiene su direccionamiento IP de la red ABC. La red ABC ha utilizado el bloque de clase B obtenido por RIPE y lo ha dividido para asignar direcciones de clase C a la red XYZ. Con esta asignación de direcciones, podemos asignar direcciones a todos los dispositivos que especifica el enunciado y además dejar un margen de direcciones libres para posibles futuras expansiones.

Los operadores nacionales también han obtenido su bloque de direcciones y sus sistemas autónomos (AS 100 y AS 200) de RIPE. El direccionamiento de toda la red ha quedado de la siguiente manera:

Red XYZ:

VLAN 10: 172.16.10.0/24 - VLAN 20: 172.16.20.0/24 - VLAN 30: 172.16.30.0/24 - VLAN 40: 172.16.40.0/24 - VLAN 60: 172.16.60.0/24 - VLAN 70: 172.16.70.0/24 - VLAN 90: 172.16.90.0/24 – Servidores Públicos: 172.16.80.0/24 – Enlace con router FronteraXYZ: 172.16.100.0/30.

Operadores:

- ABC: 192.10.2.0/24, sistema autónomo 300.
- Enlace fibra con FronteraXYZ: 10.1.4.0/30.
- OperadorNacional1: 192.10.3.0/24, sistema autónomo 100.
- OperadorNacional2: 192.10.1.0/24, sistema autónomo 200.
- Enlaces serial: 10.1.1.0/30, 10.1.2.0/30 y 10.1.3.0/30.

Topología física

Red XYZ:

Es la red de una organización compuesta por 2 edificios. Se ha utilizado un modelo de 2 capas:

- Capa núcleo: compuesta por 2 MLS (Multilayer Switch).

- Capa de acceso: Compuesta por 3 conmutadores a los que van conectados los equipos finales de los edificios.

En una red más compleja se podría incluir la capa de distribución, pero para esta práctica se ha decidido prescindir de ella.

Como los edificios están separados a una distancia de 3 km, el enlace trunk que une ambos MLS debería estar implementado con fibra, ya que con Copper Straight Through o Copper Cross-over no podemos abarcar más de 100 m de distancia. La conexión consiste en una VPN implementada en capa 2 (VLAN) contratada al operador ABC.

No he encontrado un módulo de fibra para los MLS en el CPT, así que he dejado indicado que el enlace debería ser fibra, con un texto colocado bajo el enlace.

En la capa de acceso, he colocado un conmutador para el edificio 1, y 2 conmutadores para el edificio 2, uno para cada planta. En la planta 1 del edificio 2 se encuentran los servidores privados y los servidores públicos, en la parte que representaría un CPD, pero los servidores públicos están protegidos detrás de un router que actúa como Firewall.

Red ABC:

La red ABC consiste en un triángulo, es decir 3 conmutadores conectados entre ellos. El enlace entre los conmutadores debería consistir en 2 enlaces Gigabit ethernet implementados con Link Aggregation(EtherChannel), pero como a veces uno de los Port Channels que he creado me da problemas, he dejado 1 solo enlace entre los conmutadores y en un cluster justo debajo de la Red ABC he colocado una versión simplificada de la red (En lugar de los servidores y la configuración SNMP, contiene simplemente 3 PCs) con Link Aggregation implementado, haciendo uso del protocolo LACP, en que se han creado 3 Port Channels. El enlace entre los conmutadores es de fibra, ya que el enunciado especifica que están separados por una distancia de 2km y la fibra permite cubrir esta distancia.

La red tiene un único router frontera, que está conectado a los routers frontera de los 2 operadores nacionales y a su vez al router frontera de la red XYZ. Una mejora que se podría hacer es colocar otro router frontera en la red ABC dedicado específicamente a la conexión con el router frontera de la red XYZ, y el router que tengo colocado estaría entonces conectado solo a los operadores nacionales.

El enlace entre el router frontera de la red ABC y el router frontera de la red XYZ está implementado con fibra, ya que necesitamos esta para cubrir la distancia que separa a las 2 redes.

Los operadores nacionales están conectados entre ellos y a la red ABC mediante enlaces serial. Los enlaces de cobre no serían viables, ya que se supone que la distancia entre estos routers frontera es superior a los 100 metros. Se podría optar por fibra si se necesitara mas ancho de banda, ya que los enlaces serial tienen un bajo ancho de banda.

Plan de virtualización de las redes(VLANs)

En la red XYZ se ha creado una VLAN para cada perfil (ventas, contabilidad, dirección, operaciones e invitados). De esta manera se consigue que cada perfil tenga un dominio de difusión distinto. También se ha creado una VLAN para los servidores privados, pero no para los públicos ya que estos cuelgan de un router extra que actúa de firewall y por tanto ya tienen su propia subred y dominio de difusión. Finalmente, se ha creado una VLAN para la interfaz fa0/0 del router RouterSPublicos.

Por lo tanto el plan queda de la siguiente manera:

Ventas(**Vlan10**),Contabilidad(**Vlan20**),Operaciones(**Vlan30**), Direccion(**Vlan40**), Invitados(**Vlan60**),ServidoresPrivados(**Vlan70**), InterfazFa0/0RouterSPublicos(**Vlan90**).

Plan de encaminamiento

Primeramente, se ha activado el enrutamiento de los multilayer switch de la red XYZ introduciendo el comando "ip routing". Tras esto y haber creado las VLANs que utilizo, he configurado OSPF en ambos MLS y en el RouterSPublicos, introduciendo los comandos "network ip mask" correspondientes para que se anuncien las redes a las que están conectados estos equipos. De esta manera se han creado en ambos MLS y el RouterSPublicos las entradas adecuadas que han permitido que exista conectividad entre ambos edificios de la red XYZ.

Tras esto, me he centrado en los 3 operadores. Como los operadores tienen distinto número de sistema autónomo, se necesita la utilización de un protocolo de encaminamiento EGP(Exterior Gateway Protocol) y concretamente he utilizado BGP(Border Gateway Protocol) ya que es el que hemos estudiado en esta asignatura. Configurando BGP en los routers frontera de los 3 operadores con los comandos correspondientes, he conseguido conectividad entre los 3 operadores.

Finalmente, he configurado OSPF en los routers frontera para conseguir el último objetivo de conectividad, es decir, conectividad entre los operadores y la red XYZ, en ambos sentidos. No he utilizado ninguna entrada estática, todas las entradas que se pueden encontrar en las tablas de encaminamiento de los routers han sido generadas a través de BGP(B) y OSPF(O) a parte de las que se generan siempre por conectividad directa a través de interfaces.

Plan de seguridad

El plan de seguridad consiste en utilizar medidas de seguridad en las distintas capas. En esta práctica me he centrado en la capa 3. Para implementar seguridad de capa 3 he pensado en utilizar Access Lists (ACL) para conseguir los distintos objetivos relacionados con control de acceso:

- Para que solo tengan acceso a los servidores privados los usuarios internos de la red XYZ: implementar ACL en el router frontera XYZ que bloquee el tráfico que proviene de internet con intención de llegar a los servidores privados. He intentado implementar esta ACL con una política en que se permite exactamente el tráfico que se sabe que se debe permitir y se bloquea el resto por defecto, pero no me acaba de funcionar. En concreto he probado de poner 2 ACL en este router, probando varias combinaciones (in/out) en sus interfaces:
  access-list 100 permit ip any 172.16.10.0 0.0.0.255
  access-list 100 permit ip any 172.16.20.0 0.0.0.255
  access-list 100 permit ip any 172.16.30.0 0.0.0.255
  access-list 100 permit ip any 172.16.40.0 0.0.0.255
  access-list 100 permit ip any 172.16.60.0 0.0.0.255
  access-list 100 permit ip any 172.16.80.0 0.0.0.255
  access-list 100 permit ip any 172.16.90.0 0.0.0.255
  access-list 101 permit ip 172.16.10.0 0.0.0.255 any
  access-list 101 permit ip 172.16.20.0 0.0.0.255 any
  access-list 101 permit ip 172.16.30.0 0.0.0.255 any
  access-list 101 permit ip 172.16.40.0 0.0.0.255 any
  access-list 101 permit ip 172.16.60.0 0.0.0.255 any

access-list 101 permit ip 172.16.80.0 0.0.0.255 any
access-list 101 permit ip 172.16.90.0 0.0.0.255 any

La idea con estas ACL era permitir que el tráfico que proviene de internet se pueda dirigir a todas las VLAN configuradas excepto a la VLAN 70, que es la de los servidores privados.

- Para que el tráfico permitido relacionado con los servidores públicos sea solo tráfico que es coherente con el protocolo utilizado: implementar ACL en el router RouterSPublicos. La idea de esta ACL es que por ejemplo si el destino del tráfico es el servidor web, solo se permita tráfico que está utilizando el protocolo HTTPS. De igual manera, permitir solo tráfico del protocolo 53 si se dirige al servidor DNS. He implementado una ACL con unas entradas que pretenden conseguir esto, pero no me acaba de funcionar tampoco, pero este sería el razonamiento. La ACL se puede consultar con el comando "show run" en el router RouterSPublicos, pero como digo no me funciona y con esta ACL activada se pierde toda la conectividad con los servidores públicos, si se desactiva la ACL entonces sí hay conectividad pero evidentemente se permitiría pasar todo el tráfico por lo que no sería del todo correcto en cuanto a este aspecto.
- Para que del conjunto de usuarios internos de la red XYZ, solo los del perfil de operaciones y dirección tengan acceso al servidor MedidasSensores colocado en la zona de los servidores privados: para esto la idea sería crear una ACL en el MLS del que cuelga el edificio 2, y asignarla a la VLAN 70, que es la de los servidores privados. De nuevo he probado varias cosas y no consigo cuadrarlo.

Justificación del cumplimiento de los requisitos

- Requisito **Ancho de banda mínimo de 2 Gbps entre los conmutadores de la red ABC**: Esto se consigue utilizando 3 switches generic y añadirles 4 puertos Gigabit Ethernet de fibra (Modulo PT-SWITCH-NM-1FGE) desde la interfaz Physical. Entre cada par de switches se hacen 2 enlaces Gigabit ethernet. Como GigEthernet = 1 Gbps, si se agregan los 2 enlaces GigEthernet entre cada switch mediante Link Aggregation, que en Cisco se conoce como EtherChannel y hace uso de los protocolos LACP/PAgP. La idea es crear 3 port channels. Lo he hecho en un cluster que he colocado debajo del operador ABC, porque como he mencionado anteriormente, cuando se cierra y vuelve a abrir el fichero, uno de los canales falla unas cuantas veces pero si se insiste llega a funcionar, y entonces lo he dejado en un clúster a parte para que no distorsione el funcionamiento de la red en general. Se pueden hacer pings entre los PCs con direcciones 192.168.0.1, 192.168.0.2 y 192.168.0.3 para comprobar el funcionamiento.
- Requisito **Tiempo de recuperación mínimo (menor a 1 segundo) ante caídas**: como hay 2 enlaces entre cada switch, aunque estén agregados y simulen ser solo uno con el ancho de banda agregado, si cae uno de los 2 enlaces, inmediatamente se puede utilizar el otro, que ya se encuentra activo, por lo tanto sería tiempo de recuperación menor a 1 segundo, simplemente imagino que se perdería el ancho de banda del enlace que ha caído. Si cayeran ambos enlaces entre un mismo par de routers, habría que redireccionar el tráfico.
- Requisito **Los equipos han de monitorizarse a través de SNMP:** se ha activado SNMP en los encaminadores correspondientes con el comando "snmp-server community Comm11Zx RO". Se puede comprobar el funcionamiento desde un equipo final de la red XYZ o red ABC, si se entra en la aplicación "Mib Browser" y se introduce la dirección ip de la interfaz del router y la contraseña de Read (En este caso es Comm11Zx). Si

navegamos por el arbol MIB podemos ver por ejemplo el tiempo que el router lleva activo.

- Requisito **Se requiere un servidor syslog que recibe los mensajes de registro de todos los sistemas intermedios de la red:** se puede comprobar que tanto el servidor syslog de la red XYZ como el de la red ABC reciben mensajes de diagnóstico. Esto se puede ver en la pestaña servicios de los servidores Syslog. Si no aparece ningún mensaje, se pueden provocar nuevos mensajes mediante la desactivación/activación de interfaces de los sistemas intermedios que están configurados con el comando "logging host".
- Requisito **Se requiere un servidor Netflow para monitorizar el tráfico ip de interconexión**: se puede comprobar que tanto el servidor Netflow de la red XYZ como el servidor Netflow de la red ABC monitorizan el tráfico de interconexión. Se puede ver en la aplicación "Netflow Collector" en la pestaña Desktop de los servidores. Si hacemos cualquier ping entre la red XYZ y la red ABC, queda registrado en el servidor Netflow y se muestra el tráfico en un gráfico de tarta.
- Requisito **El operador ABC ofrece servicio de internet a la red XYZ**: se puede comprobar realizando pings desde cualquier usuario final de la red XYZ a los PC o Servidores colocados en el cluster de los operadores, que representa internet. También se puede comprobar que existe conectividad con el servidor web a través de la aplicación "Web Browser" de un usuario final de la red XYZ, si introducimos en la URL la dirección ip de uno de los servidores, por ejemplo 192.10.3.3, que es el servidor web del operador nacional con sistema autónomo 100.
- Requisito **La red XYZ conecta los 2 edificios con una VPN privada contratada al operador ABC**: se puede comprobar que existe conectividad entre ambos edificios mediante pings entre equipos finales.
- Requisito **Control de acceso a los servidores privados, servidores públicos y servidor MedidasSensores**: Desafortunadamente no se puede comprobar, ya que no me acaba de funcionar.

Conclusiones

Esta ha sido una práctica densa que me ha permitido aprender mucho más de lo que hubiera aprendido mediante la realización de un examen. Aunque me ha llevado muchas horas y a cada paso que daba me salian muchas dudas, ha valido la pena.

Me ha gustado la práctica porque está relacionada con todos los aspectos que hemos estudiado durante esta asignatura y también está relacionado con otras cosas extra que he aprendido, por ejemplo nunca había usado Multilayer switches ni había hecho una práctica de redes de esta dimensión donde se gestionan tantas cosas y hay varias maneras de hacer las cosas.

En la primera etapa he dedicado varios días a analizar el enunciado y resolver dudas mediante el envío de correos y realización de tutorías online. Una vez ya tenía bastante "descifrado" el enunciado, he pasado a hacer ya la implementación en Cisco Packet Tracer. Al empezar a implementar la red en Cisco Packet Tracer me han surgido muchas más dudas y he ido resolviendo estas poco a poco consultando documentación, haciendo razonamientos y mediante la realización de más tutorías y el envío de muchos correos.

Estoy contento con todo lo que he aprendido, aunque me sabe mal no haber podido completar al 100% los objetivos, por ejemplo las ACL no me han acabado de funcionar y las he tenido que explicar en la memoria de manera teórica, pero en general diría que estoy satisfecho con lo que he conseguido, el esfuerzo que he invertido y todo lo que he aprendido.