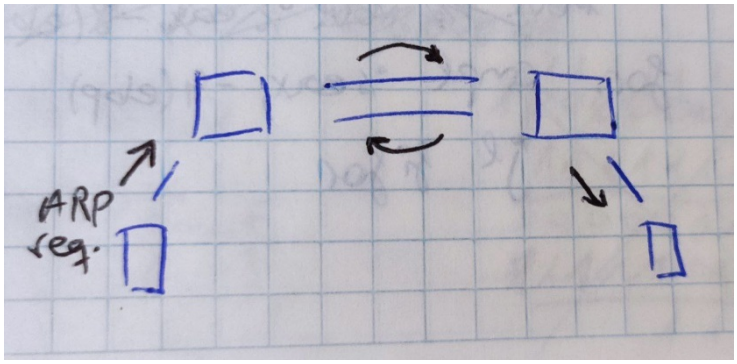
TOPIC 2: Red Corporativa

1- Explica porqué es necesario el Spanning Tree Protocol en una red conmutada.

El Spanning Tree Protocol es un protocolo de red que se encarga de detectar bucles en la topología de la red debido a la redundancia de enlaces, que hacen que los paquetes se queden circulando eternamente saturando la red, así, los dispositivos pueden activar y desactivar puertos para eliminar estos bucles de la topología.

2- Explica qué es una tormenta broadcast y pon un ejemplo donde se vea dicha tormenta. ¿Cómo se puede evitar las tormentas broadcasts?

Una tormenta broadcast ocurre cuando existe un bucle en la topología y un paquete se queda circulando eternamente saturando la red, por ejemplo, cuando se envía una ARP request entre dos conmutadores conectados mediante dos enlaces. Para evitarlo podemos utilizar el protocolo STP, que bloquea uno de los puertos de manera que solo queda un enlace por el que mandar el paquete y que no vuelva.



3- Explica cómo se integra STP con el protocolo IEEE802.3ad (agregación) y con las VLANs en sus varias vertientes (PVST, IEEE802.1Q, IEEE802.1s también llamado MSTP).

STP con agregación:
El enlace de agregación es tratado como un único enlace por lo que no se generan bucles.

STP con VLANS:

- ➔ PVST: el protocolo de etiquetado de VLANs propio de CISCO. Definen una instancia de STP para cada VLAN.
- ➔ MSTP: Tenemos una instancia STP por VLAN, pero pueden modificarse las prioridades de los puertos de manera que se puede generar distintas topologías para cada VLAN, balanceando las cargas entre los dos enlaces, por lo que si por ejemplo tenemos dos enlaces, uno se bloquea para una VLAN y el otro no y viceversa.
- ➔ IEEE802.1Q: Usaban PVST, luego pasaron a MSTP.

TOPIC 2: Red Corporativa

4- Da una corta descripción de cómo funciona el STP.

El STP se utiliza para evitar bucles en una red conmutada. Para enviar mensajes utiliza un protocolo llamado BPDU. Primero se define el Root Bridge (el switch cabeza de la topología), luego se siguen unos criterios para establecer los root ports (puertos conectados al RB) y los designated ports (los que reciben las tramas). Estos criterios son:

- Menor Root BID
- Menor Root Path Cost
- Menor Sender BID
- Menor Port ID

Los puertos que no son ni root ni designated son bloqueados para evitar bucles. Una vez hecho esto, hay que esperar a que se obtengan las tablas MAC y ya tendremos conectividad.

Según el protocolo de VLANs, el protocolo STP funciona de distinta manera, alguno permite balancear las cargas de los enlaces hasta incluso permitir doble enlazado si somos capaces de manejar las prioridades para bloquear el paso de más de una VLAN.

5- Explica qué es un "root bridge", un "root port" y un "designated port" en STP.

➔ Root Bridge: El conmutador que encabeza la topología.

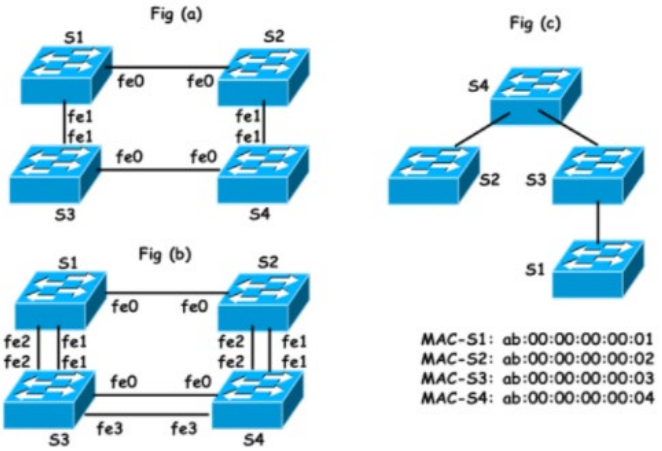
➔ Root Port: Cada conmutador tiene un puerto que dirige el tráfico hacia el RB. No puede ser designated. Se encarga de transmitir tramas, cada switch que no es RB escoge el root port, como todos los paquetes tienen el mismo RB hay que basarse en otros aspectos. El root path sería el mismo si hubiese dos enlaces por lo que se comparan el sender BID y ya por último el puerto más bajo.

➔ Designated Port: Están conectados a un host. Por cada segmento tenemos al menos un puerto que transmite tramas Ethernet. Para el RB todos son designated. Para el resto, se escogen de manera que se evita crear bucles. Se basa en los mismos criterios que para el RP, y el resto se bloquean.

Los puertos que no son ni RP ni Designated son puertos bloqueados.

TOPIC 2: Red Corporativa

6- Sabiendo que la prioridad de un switch es el valor 8000(hex):MAC-Sw, qué la menor prioridad de un switch tiene preferencia, que todos los enlaces de los Sw de la figura son de igual coste y que la prioridad de los puertos es de 128 :ID (a menor valor mayor prioridad) y el ID es el número de interface (e.g. interface fe1 tendría prioridad 128:1):



(a) Indica cómo conseguir tener una topología STP como la de la Fig (c) partiendo de la red de la Fig (a). Los enlaces bloqueados no aparecen en la Fig (c).

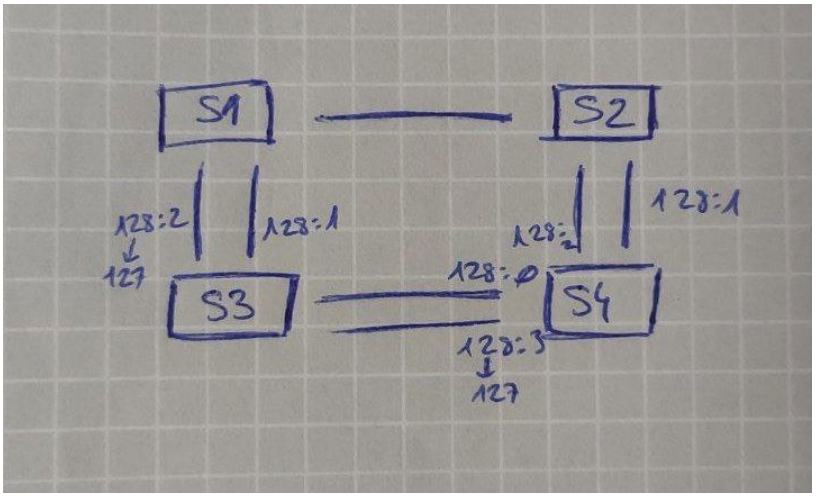
El Root Bridge ha de ser S4, por lo que es quien tiene el senderBID más pequeño. Luego, S3 y S2 serán los posibles sender a S1, que escogerá el que tenga el BID más pequeño, como queremos que sea S3 le ponemos menor BID que a S2. Por último, entre S2 y S1 nos da igual el BID.

$$senderBID_4 < senderBID_3 < senderBID_2 < senderBID_1$$
$$senderBID_2 > senderBID_1$$

(b) Indica cómo conseguir tener una topología STP como la de la Fig (c) partiendo de la red de la Fig (b), pero ahora los enlaces activos de la Fig (c) son: de S4 a S2, fe1-fe1; de S4 a S3 fe3-fe3 y de S3 a S1, fe2-fe2. Los enlaces bloqueados no aparecen en la Fig (c).

Para la topología: $senderBID_4 < senderBID_3 < senderBID_2 <> senderBID_1$

Para los dobles enlaces: modificamos el port priority a un número random porque el num.port no se puede cambiar-> 128:x (port priority:num.port)



TOPIC 2: Red Corporativa

Entre S2-S4, 128:1 < 128:2 por lo que no hay que cambiarlo.
Como en S3-S4 queremos que pille fe3, y 128:0<128:3, bajamos a 127:3.
Y de S3 a S1, 128:2 > 128:1 bajamos a 127:2 para que coja fe2.

(c) Si tenemos 2 VLANs (VLAN=2 y VLAN=3), indica cómo podríamos modificar la respuesta del apartado (b) para que entre el switch S1 y S3 el tráfico de la VLAN=2 vaya por el enlace fe2-fe2 y el de la VLAN=3 por el enlace fe1-fe1.

STP1: $BID_4 < BID_3 < BID_2 <> BID_1$ SW4= 127:3
SW3= 127:2

STP2: $BID_4 < BID_3 < BID_2 <> BID_1$ SW4= 127:3

7- Sabemos qué la prioridad de un switch es el valor 8000(hex):MAC-Sw, qué la menor prioridad de un switch tiene preferencia, que todos los enlaces de los Sw de la figura son de igual coste y qué la prioridad de los puertos es de 128:ID (a menor valor mayor prioridad) y el ID es el número de interface (e.g. interface fe1 tendría prioridad 128:1). Se crean 2 VLANs (VLAN=2 y VLAN=3). Todos los puertos son trunk.

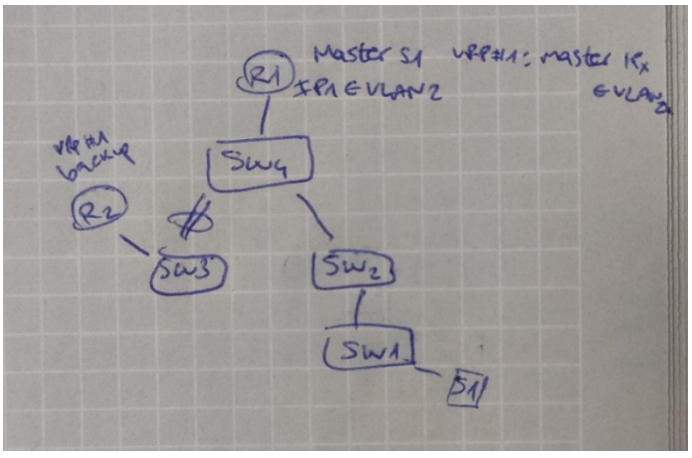
(a) Indica cómo conseguir tener una topología STP como la de la Fig (b) partiendo de la red de la Fig (a) para la VLAN=2. Los enlaces bloqueados no aparecen en la Fig (b).

senderBID4 < senderBID2 < senderBID3 <> senderBID1
SW4 = 128:2 -> 127:2
SW2 = 128:3 -> 127:3

(b) Indica cómo conseguir tener una topología STP como la de la Fig (c) partiendo de la red de la Fig (a) para la VLAN=3. Los enlaces bloqueados no aparecen en la Fig

SenderBID3 < senderBID1 < senderBID4 <> senderBID2
SW3 = 128:2 -> 127:2
SW1 = 128:3 -> 127:3

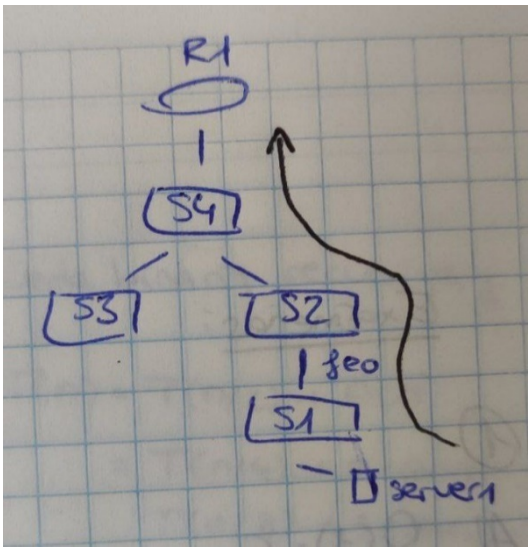
Creamos 2 instancias VRRP, una para la VLAN=2 (la llamamos VRRP-2) y otra para la VLAN=3 (la llamamos VRRP-3). R1 es master para VLAN=2 y backup para VLAN=3 y R2 es master para VLAN=3y backup para VLAN=2. Asumimos que tenemos un servidor "Server 1" conectado al conmutadorS1 y pertenece a la VLAN=2. Asumimos las topologías de los apartados a) y b) (Fig(b) y Fig(c)).



TOPIC 2: Red Corporativa

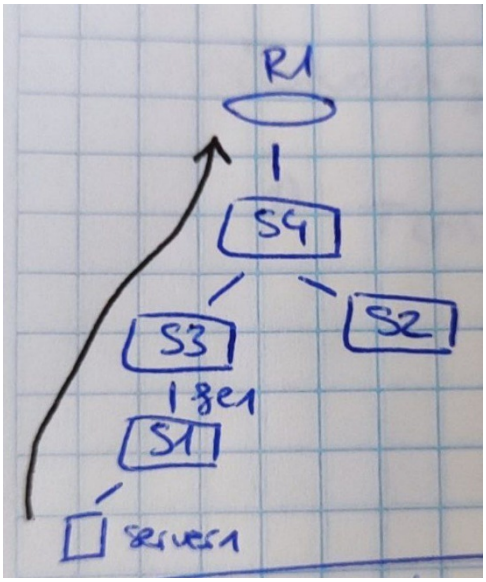
(c) Indica qué ocurre y que topología se configura si cae el enlace fe3 del conmutador S1 y que camino seguiría el tráfico desde el Server 1 hasta su router de salida.

Al caer fe3, el S1 ahora coge el puerto fe0 y se enlazan. El master R1 sigue activo por lo que va hacia él.



(d) Recuperamos el enlace fe3. Indica qué ocurre y qué topología se configura si caen los enlaces fe0 y fe3 del conmutador S1 y qué camino seguiría el tráfico desde el Server 1 hasta su router de salida.

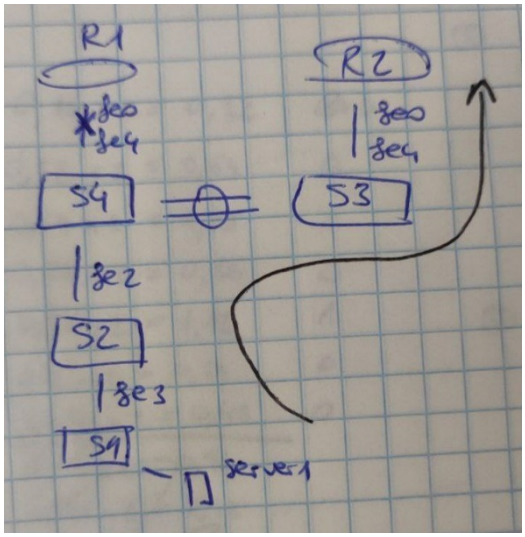
Al caer S2-S1, el S1 ahora coge el puerto hacia S3 y se enlazan por fe1 para VLAN2 (teníamos fe2 en VLAN3). El master R1 sigue activo por lo que va hacia él.



TOPIC 2: Red Corporativa

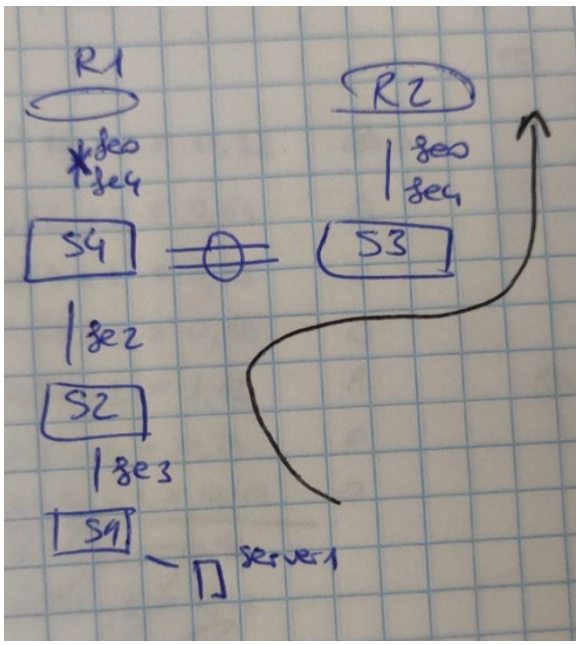
(e) Recuperamos los enlaces caídos. Indica qué ocurre y qué topología se configura si perdemos el enlace fe0 del R1 y por dónde va el tráfico del Server 1.

Ahora el router master de Server1 ha caído, por lo que R2 se convierte en el sustituto.



(f) Recuperamos los enlaces caídos. Indica qué ocurre y que topología se configura si perdemos el enlace fe0 del R1 los enlaces fe1 y fe2 de S2 y por dónde va el tráfico del Server 1.

Al perder la conexión con el RB, el S1 cambia de sender a S3 por la fe1, y al haber caído también el router master, R2 se convierte en el sustituto.



TOPIC 2: Red Corporativa

8- ¿Cuál es la limitación en el número de instancias STP que puede haber en un conmutador?

Inicialmente la limitación de VLANs vendría por el tamaño de la etiqueta del protocolo VLAN, n bits -> 2^n VLANs. Pero realmente el límite de VLANs depende del límite de instancias STP de un conmutador, ya que en MSTP hay una instancia STP por VLAN. Tenemos dos métricas para este límite:

- El número de puertos virtuales por tarjeta/módulo: se calcula sumando las VLANs que pasan por todos los enlaces trunk de un módulo y no debe superar el límite del fabricante.
- El número de puertos lógicos STP: se suman todos los enlaces trunk de todos los módulos del conmutador y no puede superar el límite del fabricante.

9- Explica el funcionamiento básico de un conmutador de nivel 3 (Multi-layered switch -MLS) y qué lo diferencia de un switch y de un router convencional.

Un switch multilayer puede asignar una IP a una interfície física igual que un router, pero también puede asignar una IP a una interfície lógica (SVI) que representa una VLAN entera. La IP que se configura se convierte en el Gateway por defecto para cualquier servidor que esté conectado a la VLAN, con lo cual el servidor usará la interfície de capa 3 para comunicarse con el exterior de su dominio de broadcast. El MLS crea una tabla de hash de IPs similar a la tabla de MAC donde aparece a qué VLAN se corresponden, el primer paquete consulta la tabla de encaminamiento para rellenar la caché, y los demás paquetes consultan la caché directamente. A diferencia de un switch convencional, este trabaja solamente en el nivel 2 de enlace.

10- Explica qué es la tolerancia a fallos en el L3 respecto a los Hosts (clientes y servidores) y explica el funcionamiento básico del protocolo/mecanismo qué puede usarse para evitar dichos fallos.

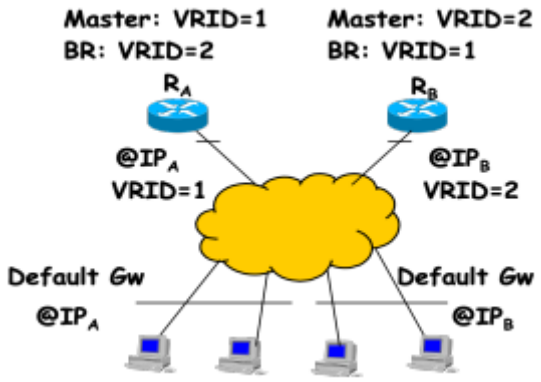
Todos los hosts tienen por defecto un Gateway, si pierde conectividad con este, el host ha de encontrar otro. Esta tolerancia existe gracias al mecanismo VRRP, que se encarga de sustituir la dirección de Gateway de forma automática para mantener el funcionamiento. Para ello, tenemos dos routers y se asigna una prioridad para definir cuál es el master y cuál el backup. Si el master cae, el backup lo detecta y envía un ARP request broadcast que los hosts reciben, y la tabla MAC del switch sustituye su IP Gateway con la IP del router que les contesta, el de backup.

TOPIC 2: Red Corporativa

11- Explica cómo funciona un ARP gratuito y para qué lo usa el protocolo VRRP.

El ARP gratuito consiste en un ARP request broadcast que se envía para resolver su propia dirección MAC, poniendo la misma IP origen y destino. En el caso de VRRP se utiliza para actualizar la tabla caché del conmutador, y sustituir la dirección MAC del que antes era el master, por la del backup.

12- Explica el funcionamiento general de VRRP y explica para qué es necesario usar VRRP en un bloque de conmutación. Ayúdate de la figura.

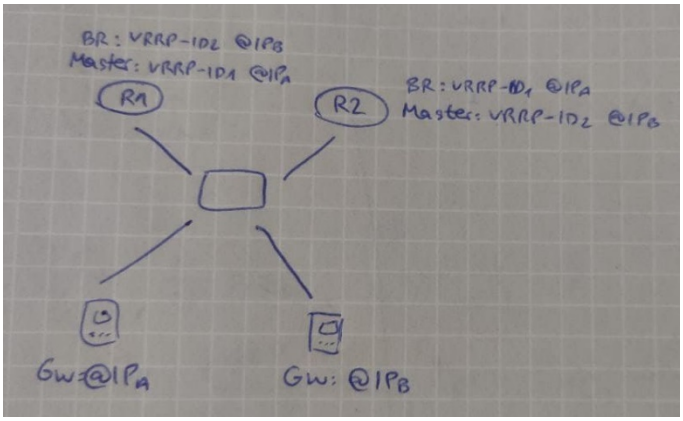


VRRP es un protocolo destinado a la tolerancia de fallos L3, en concreto a la caída de un Gateway. Para ello disponemos de más de un router en la topología, uno que será el master (ppal) y otro que será el backup. Ambos utilizan la misma @IPvirtual, la que usan los hosts como gw. También usan distintas MAC virtuales. Cuando uno de ellos cae, por ejemplo RA, el RB deja de recibir señal y envía un ARP request gratuito con su @IPvirtual como IP origen y destino, y MAC de origen la suya virtual, y destino broadcast. Ahora, el switch y los hosts que lo reciben borran sus ARP caché, y cuando quieran conectarse al Gateway, RB pondrá su MACvirtual para esa IP y se convertirá en su nuevo Gateway y la tabla caché del switch dirigirá el tráfico hacia él. Si el RA vuelve a funcionar, debe mandar un ARP request gratuito para volver a limpiar las cachés, y el tráfico de los hosts de la izquierda volverán a apuntar hacia él.

TOPIC 2: Red Corporativa

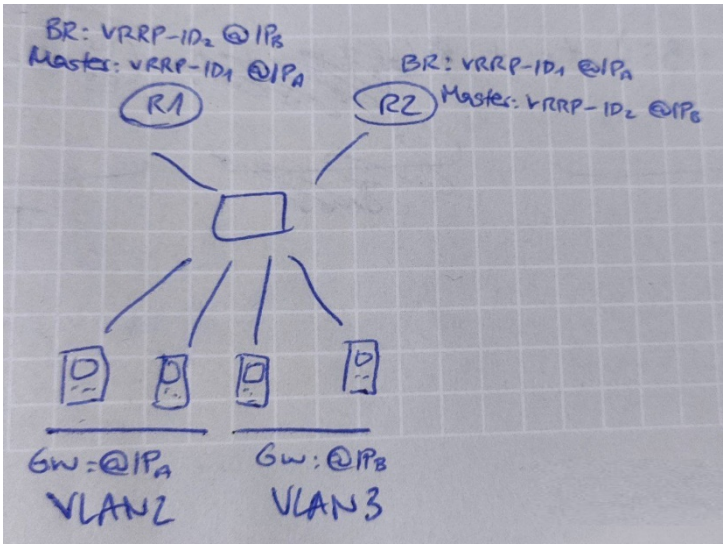
13- Pon un ejemplo de funcionamiento de VRRP con dos routers y dos Hosts con balanceo de cargas. Los dos Host en la misma VLAN.

Para balancear las cargas con dos routers y dos hosts de la misma VLAN, ponemos como Gateway de uno de los hosts a R1, y al otro R2, de manera que el R1 sea master de un host y backup del otro, y lo mismo para R2.



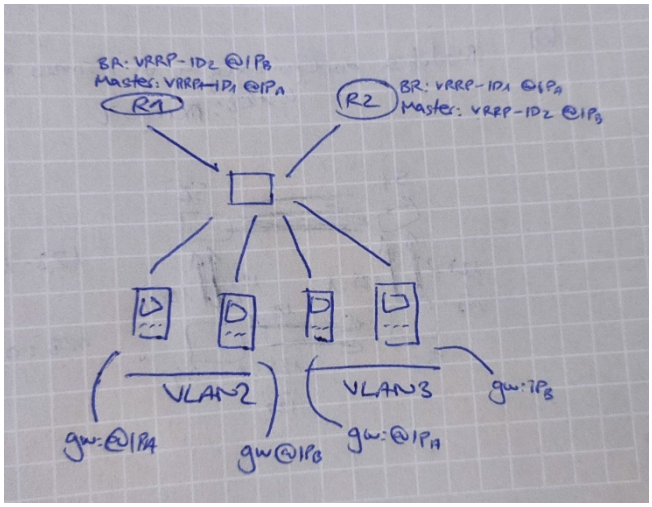
14- Pon un ejemplo de funcionamiento con dos routers y cuatro Hosts (dos en VLAN=2 y 2 en VLAN=3) con balanceo de cargas de tal manera que tráfico de VLAN=2 salga por el router R1(backup el R2) y tráfico de VLAN=3 salga por el router R2 (backup el R1).

Para balancear las cargas con cuatro routers y dos hosts en cada VLAN, ponemos como Gateway de los hosts de VLAN2 a R1, y en el otro router, los de VLAN3, de manera que el R1 sea master de una VLAN y backup de la otra, y lo mismo para R2.



TOPIC 2: Red Corporativa

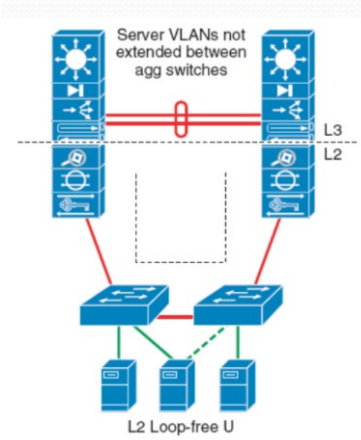
15- Pon un ejemplo de funcionamiento con dos routers y cuatro Hosts (dos en VLAN=2 y 2 en VLAN=3) con balanceo de cargas de tal manera que H1 de VLAN=2 y H3 de VLAN=3 salga por el router R1 (backup el R2) y H2 de VLAN=2 y H4 de VLAN=3 salga por el router R2 (backup el R1).



Para balancear las cargas con cuatro routers y dos hosts en cada VLAN, ponemos como Gateway de un host de cada VLAN a R1, y en el otro router, los otros hosts, de manera que el R1 sea master de un host de cada VLAN y backup de los otros, y lo mismo para R2.

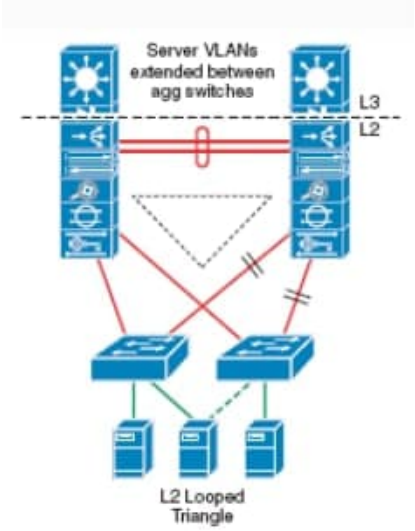
16- Explica la diferencia entre una topología que usa STP con U y una en triángulo en el diseño de un CPD multi-tier. Usa un dibujo en donde se vea dicha diferencia y comenta las ventajas y desventajas de una y otra. Explica por qué y una de ellas escala las VLANs entre conmutadores y la otra no.

<u>En la topología en U:</u> todos los links están activados, es sencillo. Está limitado al uso de sólo dos switches, por lo que no es escalable. En caso de fallo, ha de atravesar otro conmutador por lo que pierde eficiencia.

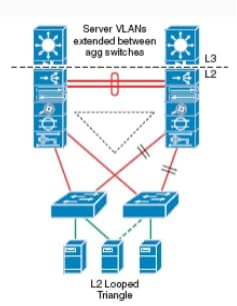


TOPIC 2: Red Corporativa

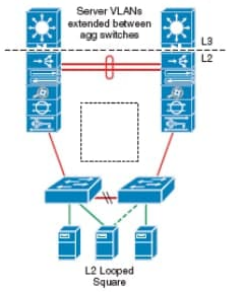
En la topología en triángulo: ha de utilizar STP para bloquear puertos y evitar bucles, por lo que hay que tener experiencia. Puede utilizar más switches por lo que es más escalable en VLANs, conmutadores y hosts. En caso de fallo simplemente usa otra ruta, por lo que no pierde eficiencia.



17- Explica qué topologías se pueden implementar en un CPD multi-tier indicando sus ventajas y desventajas y si es necesario usar STP en ellas. Haz un esquema dónde se vea la topología.



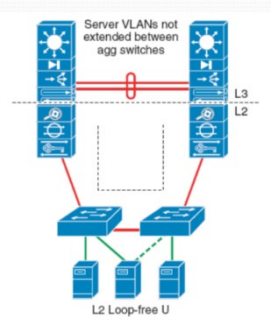
· Triángulo: ha de utilizar STP para bloquear puertos y evitar bucles, por lo que hay que tener experiencia. Puede utilizar más switches por lo que es más escalable en VLANs, conmutadores y hosts. En caso de fallo simplemente usa otra ruta, por lo que no pierde eficiencia.



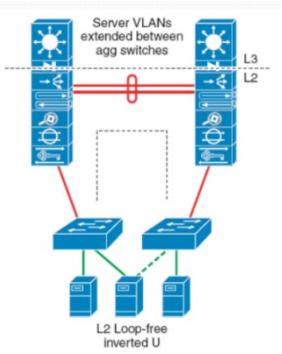
· Cuadrado: ha de utilizar STP para bloquear puertos y evitar bucles, por lo que hay que tener experiencia. Puede utilizar más switches por lo que es más escalable en VLANs, conmutadores y hosts. En caso de fallo, ha de atravesar otro conmutador por lo que pierde eficiencia.

TOPIC 2: Red Corporativa

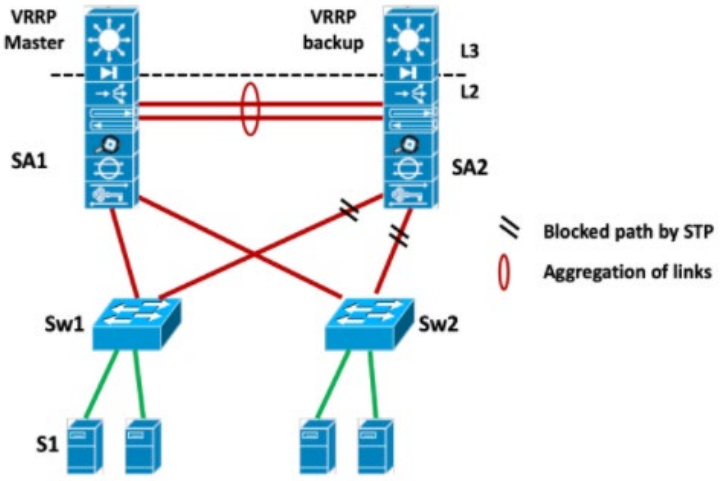
· U: todos los links están activados, es sencillo. Está limitado al uso de sólo dos switches, por lo que no es escalable. En caso de fallo, ha de atravesar otro conmutador por lo que pierde eficiencia. No es necesario STP porque no hay bucles, aunque puede utilizarse para evitarlos.



· n: al no tener bucles, perder un enlace implica perder la conexión, por lo que tiene poca fiabilidad. Está limitado al uso de sólo dos switches, por lo que no es escalable. No es necesario STP porque no hay bucles, aunque puede utilizarse para evitarlos.



18- Suponemos que en ambas configuraciones VRRP está configurado para que el switch de agregación SA1 sea master de todos los servidores y el segundo switch SA2 sea backup. Indica el tipo de topología de nivel 2 que se ha configurado con STP, por dónde iría el tráfico generado por el servidor S1 y por dónde iría dicho tráfico si el enlace SA1-Sw1 cae.

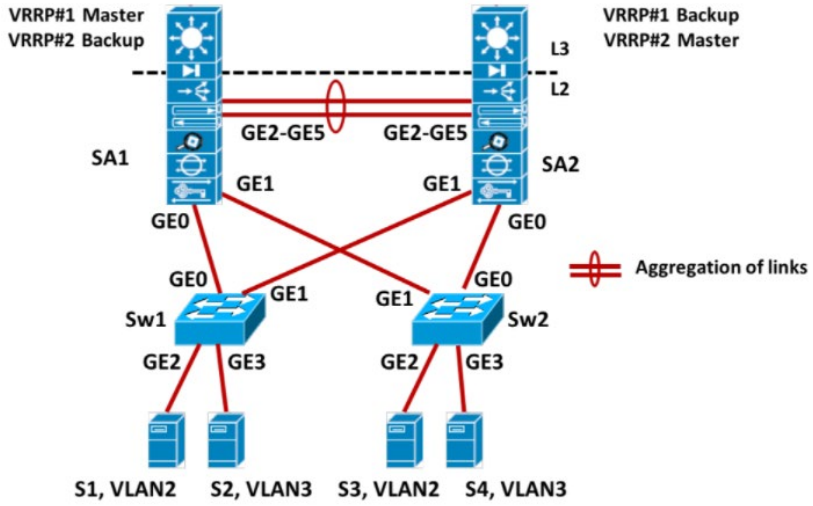


Se trata de una topología en triángulo.
El tráfico del S1 iría por el SW1 y subiría al SA1. Si este enlace cayese se desbloquearía el puerto hacia SA2 y lo usaría como backup.

Repite el ejercicio si el Master VRRP está situado en SA2 y el backup en SA1.
Si el master fuese SA2 los enlaces bloqueados estarían invertidos, por lo que el tráfico de S1 iría a SW2 y de ahí a SA2. Si cayese el enlace SW1-SA1 no importaría porque no se usaría, y el SA1 sólo sería el backup.

TOPIC 2: Red Corporativa

19- Contesta a las siguientes preguntas respecto a la red de la figura, teniendo en cuenta qué queremos que los servidores de la VLAN 2 tengan como Gateway a SA1 y los de la VLAN 3 a SA2. (Nota: GEx = interface GigabitEthernet número x, GEx-GEy indica grupo de interfaces desde la x a la y).



a) Indica qué enlaces son "trunk": Equipo (SA1, SA2, Sw1, Sw2, S1,S2,S3,S4) – interfaces (GEx,GEx-GEy, All, None).

Todos los que no van de los sw a los servidores.

b) Indica qué enlaces se bloquerían (Equipo (SA1, SA2, Sw1, Sw2, S1,S2,S3,S4) – interfaces (GEx,GEx-GEy)), teniendo en cuenta que usamos Multiple-STP y formamos topologías en triángulo. La configuración tiene que ser eficiente.

Puertos bloqueados en STP2: GE1 de SA1 y GE0 de SA2.
Puertos bloqueados en STP3: GE0 de SA1 y GE1 de SA2.

c) Indica el camino qué siguen los paquetes de los servidores S1 y S3. Si la instancia VRRP#1 Master cae, indica cómo cambia la topología STP (si cambia) e indica el camino de los paquetes de los servidores S1 y S3 (si cambian).

S1 – SW1 – SA1 S3 – SW2 – SA1

Si el master cae, los enlaces bloqueados en STP2 se invierten y el camino sería:

S1 – SW1 – SA2 S3 – SW2 – SA2

TOPIC 2: Red Corporativa

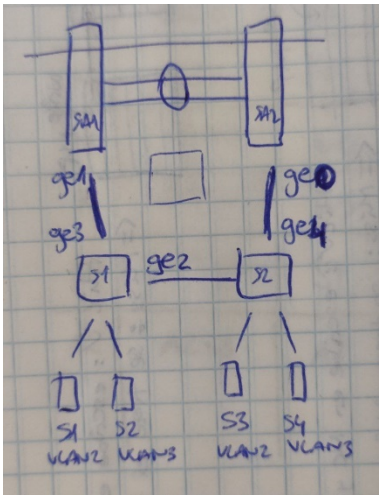
20- (22) Sabemos qué la prioridad de un switch es el valor 8000(hex):MAC-Sw, qué la menor prioridad de un switch tiene preferencia y que la prioridad de los puertos es de 128:ID (a menor valor mayor prioridad) y el ID es el número de interface (e.g. interface Ge1 tendría prioridad 128:1). Todos los enlaces que unen conmutadores son a 10 Gb/s y los de servidores son a 1 Gb/s. Se crean 2 VLANs (VLAN=2 y VLAN=3). Todos los puertos entre conmutadores son trunk y usamos MSTP. El circulo rojo indica enlaces agregados. Creamos 2 instancias VRRP, una para la VLAN=2 (la llamamos VRRP-1) y otra para la VLAN=3 (la llamamos VRRP-2).R1 es master para VLAN=2 y backup para VLAN=3 y R2 es master para VLAN=3 y backup para VLAN=2.

a) Supongamos qué MAC-Sw2 < MAC-Sw1 < MAC-SA1 < MAC-SA2, indica cuál es la topología resultante (dibuja un esquema en el qué solo aparezcan los enlaces no bloqueados e indica quien es el root bridge y quienes son los root ports para cada switch).

RB: SW2

Root Ports:: SW1: ge2 / SA1: ge0 / SA2: ge0

Es una topología en cuadrado.

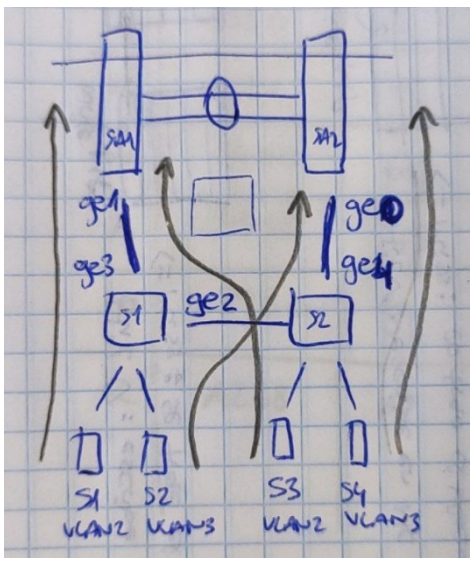


b) Propón una combinación de prioridades para qué los servidores S1, S2, S3 y S4 envíen su tráfico por el camino más eficiente de acorde a una topología en cuadrado.

STP2: SW1-> ge3: 127:4

STP3: SW2 -> ge4: 127:4

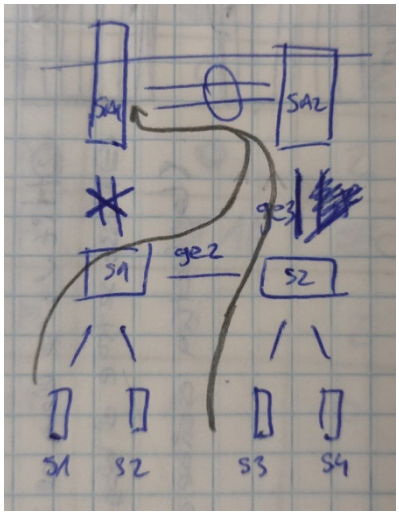
c) Indica el camino qué sigue el tráfico en cada servidor en los casos a) y b).



TOPIC 2: Red Corporativa

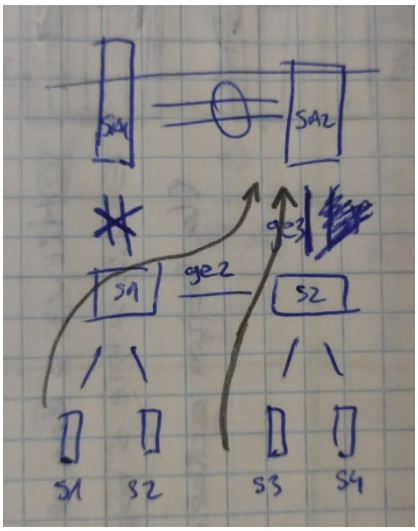
d) Indica cómo afecta al tráfico que caigan los enlaces Ge3 y Ge4 del Sw1.

Si caen ambos enlaces se desbloquean otros puertos para llegar a SA1 desde SA2. Queda así:



Recuperamos los enlaces Ge3 y Ge4 del Sw1. Indica qué ocurre si cae el VRRP#1.

Si caen ambos enlaces la VLAN2 se queda sin master y el SA2 tiene que entrar en juego como backup. Se desbloquean los enlaces y queda así la topología:



TOPIC 2: Red Corporativa

e) **Asume que existe un nuevo enlace Ge5 en Sw1 y en Sw2. Este nuevo enlace se conecta a un SA1 y SA2 respectivamente de un módulo distinto (M2) de conmutación y viceversa (los Sw1 ySw2 del otro módulo tienen un enlace a los SA1 y SA2 del módulo M1). Disponemos también de puertos en Sw1 para conectar 40 servidores de la VLAN 2 y otros 40 de la VLAN 3 en Sw1(ídem en Sw2). Sw1 y Sw2 balancean su tráfico uniformemente entre los dos módulos M1 y M2 independientemente de que a módulo estén conectados. Indica cuál es el oversubscription ratio para cada servidor de cada VLAN y el throughput medio por servidor.**

21- (20). Explica el concepto de "oversubscription ratio" para diseñar redes de conmutación y para qué se usa. Relaciona el concepto de "oversubscription ratio" con el throughput que puede obtener un servidor. Calcula el throughput medio y el "oversubscription ratio" de un conmutador con 4 enlaces de 10 Gb/s en el nivel de agregación y 96 puertos de 1Gb/s de capacidad en el nivel de acceso. Si dispones de servidores que solo "ocupan" un 20% del enlace de acceso (1 Gb/s) y se disponen de 2 enlaces de 10 Gb/s hacia agregación. ¿Cuántos enlaces de acceso podría soportar el conmutador?

El oversubscription ratio es la media de servidores que ocupan la capacidad total de un enlace y el throughput es el % de capacidad que ocupa un servidor de un enlace. Por tanto, uno es la inversa del otro y viceversa, pues se divide la capacidad total entre la capacidad de cada uno para saber cuántos servidores podremos tener conectados.
4x10GE enlaces de agreg. y 96 puertos a acceso -->
throughput: 40/96= 0.416
oversubs.: 1/0.416= 2.4:1

Tenemos un 20% ocupado del enlace de acceso, que sería un throughput de 0.2 (200MB/s) y dos enlaces de agreg. de 10GE. Queremos saber cuántos enlaces de acceso soporta el conmutador, pues sería: 20/x = 0.2 -> x= 10 enlaces y 20GB/200MB = 100 servers

22- (21) Calcula el throughput medio y el "oversubscription ratio" de un conmutador con 8enlaces de 10 Gb/s en el nivel de agregación y 192 puertos de 1Gb/s de capacidad en el nivel de acceso. Si los 192 servidores del nivel de acceso ocupan un 55% del enlace, ¿Está bien diseñada la red (justifica tu respuesta)? Si la respuesta es no, indica cómo debería ser el conmutador para soportar los 192 servidores del nivel de acceso.

thr: 0.55 * 1 = 550MB/s ov.r= 1/0.416= 2.4:1 thr=80/192=0.416GB/s
No está bien diseñada la red porque con un over-subscription ratio de 2,4 el throughput medio por servidor será de 416 Mbps. Para un correcto funcionamiento en el nivel de acceso el conmutador de agregación debe de garantizar 105,600 Gbps.