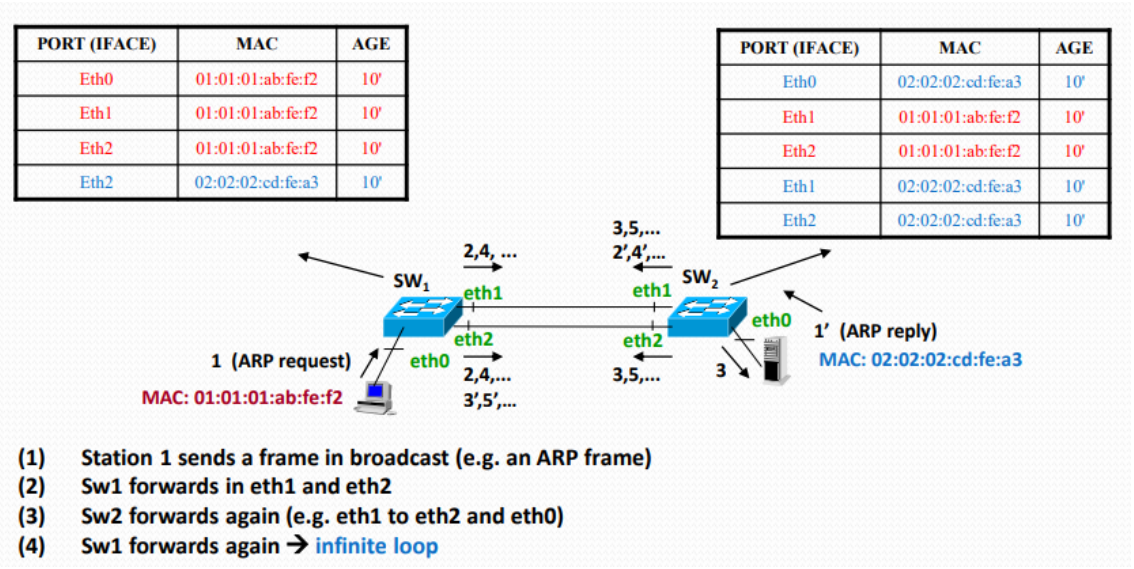
TOPIC 2: Red Corporativa

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

El Spanning Tree Protocol tiene tolerancia a fallos de nivel 2, y es necesario debido a que se pueden producir bucles (tormentas broadcast por ejemplo) entre las diferentes conexiones (pueden ser enlaces redundantes) que hay entre los diferentes conmutadores, las cuales podrían hacer que un paquete IP estuviera durante un tiempo relativamente grande viajando a través de los mismos switches, sin llegar a su destino, y esto provocaría que la red podría llegar a colapsar debido a la gran cantidad de información.

Pregunta 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 de broadcast se produce cuando en un switch llega un mensaje en broadcast, y como consecuencia, este envía el mensaje al resto de puertos (interfaces) que tiene ya que no tiene un destino definido al que ir. El segundo switch que le llega el mensaje hace lo mismo y lo envía a sus respectivos interfaces, uno de ellos, de vuelta al primer switch, y así todo el rato formando un bucle infinito. Provoca que haya una gran cantidad de información viajando a lugares a los cuales no es necesario, pero para asegurar que llegan al destino, y también puede provocar entradas en la tabla MAC erróneas.
Esto se puede evitar aplicando un STP (Spanning Tree Protocol) y así eliminar los enlaces redundantes y los bucles que podrían formar.



Pregunta 3.Explica cómo funcionan las VLAN estáticas y las VLAN dinámicas. En estas últimas (VLANs dinámicas) indica cómo se deniegan las MAC de una VLAN determinada en un puerto/s de conmutador.

En las VLAN estáticas, un grupo de puertos pertenecientes a un conmutador/conmutadores están asignados al mismo dominio broadcast y esa red IP pertenece a ese VLAN en concreto.
En las VLAN dinámicas, un conmutador asigna automáticamente el puerto a una VLAN utilizando la dirección MAC o la dirección IP. Cuando un dispositivo está conectado a un puerto de conmutador, el conmutador consulta una base de datos para establecer la membresía de VLAN (VMPS - servidor que asocia @MAC - VLAN y así saber a qué VLAN pertenece). Puede usarse --NONE-- para denegar explícitamente el acceso de las MAC a cualquier VLAN (!MAC Addresses).

Pregunta 4.Indica cómo funcionan los puertos seguros e indica la diferencia entre las direcciones MAC estáticas, dinámicas y "sticky".

La funcionalidad de los puertos seguros brinda la capacidad de limitar qué direcciones podrán enviar tráfico en puertos de conmutación individuales a través del conmutador. Pueden estar en modo protección, restricción o shutdown.

Una dirección MAC estática es una que se ha ingresado manualmente en la tabla MAC.
Una dirección MAC dinámica es aquella que se ha aprendido a través de una solicitud ARP.
Una dirección MAC sticky es una que se ha aprendido dinámicamente, pero se convierte en estática hasta que se reinicie, es una combinación de estática y dinámica.

Pregunta 5. Explica cómo se integra STP con el protocolo IEEE802.3ad (agregación) y cómo se integra STP con las VLANs en sus varias vertientes (PVST, IEEE802.1Q, IEEE802.1s también llamado MSTP).

El protocolo IEEE802.3ad consiste en un conjunto de cables que actúan como si fueran uno solo, por tal de conseguir una mayor velocidad en la red, debido a que el ancho de banda sería la suma de todos los cables que lo conforman.
Con el IEEE802.1Q se permite el protocolo de etiquetado para VLAN sobre puertos trunk, que permitiría una mayor conexión entre las mismas. En la versión PVST se incorpora que cada VLAN una instancia de STP, y en el MSTP, múltiplos, entonces este protocolo ayuda a que en el caso de que una rama de los árboles, los cuales conforman la estructura de la red cae, pueda haber una ruta alternativa por el otro spanning tree, la cual permita que la información pueda ser transmitida de forma correcta. Estas regiones están interconectadas mediante un único spanning tree común.

Pregunta 6.Dá una corta descripción de cómo funciona el STP.

El Spanning Tree Protocol (STP) consiste en evitar que haya bucles y eliminar enlaces redundantes en los cuales la información viaje de forma innecesaria durante un tiempo determinado.

Pregunta 7.Explica qué es un "root bridge", un "root port" y un "designated port" en STP.

Root bridge:
Es el punto desde el cual partimos en el STP, y el cual debemos hacer que sea el punto más simétrico, para así hacer que los caminos desde un terminal a otro, sean lo más cortos posibles y así tarden menos en interaccionar.
Root port:
Es el puerto que permite comunicar nuestro switch (todos los switches tiene uno menos el RB) en una estructura STP, mediante este puerto se pasará la información al Root Bridge. Los puertos los cuales puedan generar bucles, no serán root ports y por tanto se desactivarán (Blocked Port).
Designated Port:
Son los puertos los cuales están en cada segmento, y aseguran que se pueda llegar. Un Root Port no puede ser un Designated Port. El Root Bridge, solo tiene Designated Ports, debido a que es el nivel más alto.

Pregunta 8. Sabiendo que la prioridad de un switch es el valor 8000(hex):MAC-Sw, que 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 tendria 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).

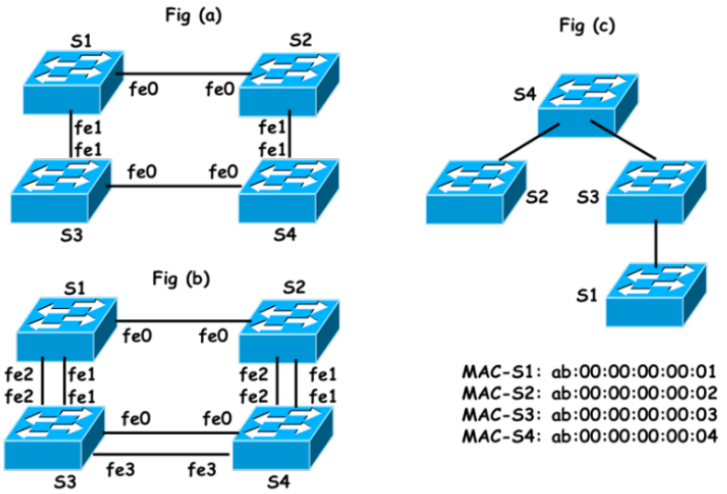
BID4 < BID3 < BID2 < BID1 (Sender Bit 3 < 2 por eso 1 cuelga de 3)
Pondremos de Root Bridge el S4, y partir de este tenemos dos Designated Ports hacia S2 y S3, que serán Root Ports (fe1, fe0) debido a que es la única salida que tendrían al exterior. Y con S3, habrá un Forwarding hacia S1, que será Root Port, para que este tenga conexión, a través de fe1.

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).

Es igual que en el caso anterior pero ahora lo que deberíamos hacer antes de todo es hacer que las conexiones en las cuales hay más de un cable entre un switch y otro, se junten en uno mediante la agregación y así tenemos el mismo esquema que en la figura a, pero con una mayor velocidad entre S1 y S3, entre S3 y S4, y entre S4 y S2.

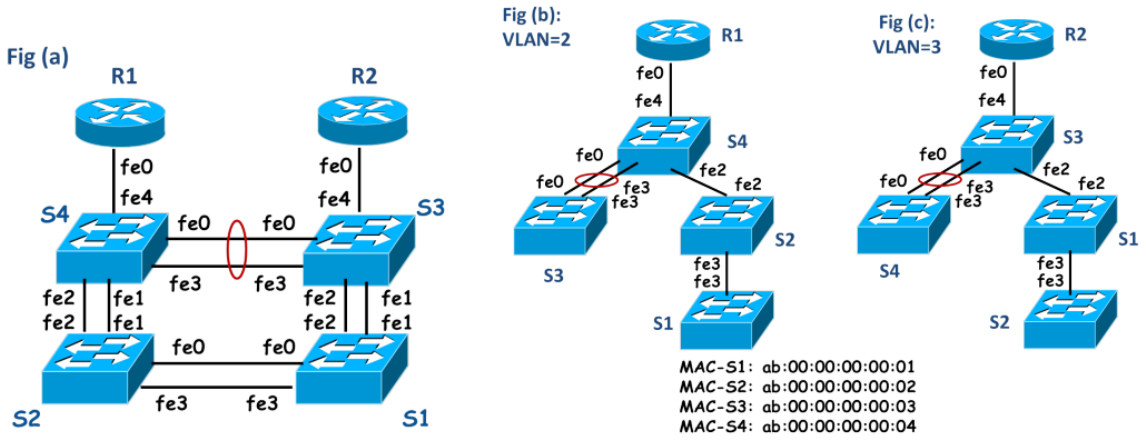
c) Si tenemos 2 VLANs (VLAN=2 y VLAN=3), indica cómo podríamos modificar la respuesta del apartado (b) para que entre el switch S1 y S3 el tráfico de la VLAN=2 vaya por el enlace fe2-fe2 y el de la VLAN=3 por el enlace fe1-fe1.

Haríamos que por cada fe fuera una VLAN (la que toca según el enunciado) distinta hasta llegar al switch S4, en el cual se podría hacer el intercambio de información entre las VLANs y por consiguiente al haber dos cables durante toda la ruta, la velocidad de las dos VLANs, sería exactamente la misma.



ASUMIENDO QUE MAC4 < MAC3 < MAC2 < MAC1

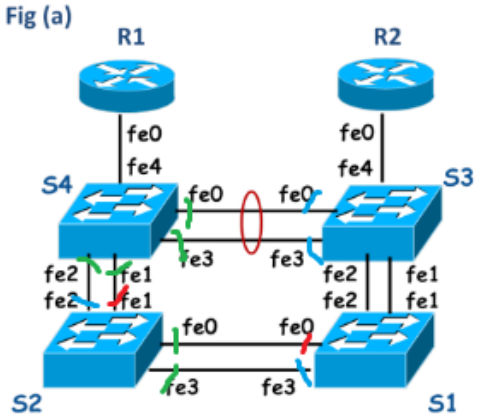
Pregunta 9. Sabemos que la prioridad de un switch es el valor 8000(hex):MAC-Sw, que la menor prioridad de un switch tiene preferencia, que todos los enlaces de los Sw de la figura son de igual coste y que la prioridad de los puertos es de 128:ID (a menor valor mayor prioridad) y el ID es el 2 número de interface (e.g. interface fe1 tendría prioridad 128:1). Se crean 2 VLANs (VLAN=2 y VLAN=3). Todos los puertos son trunk.



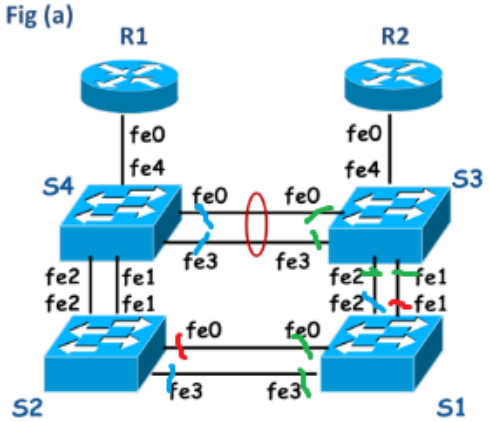
ASUMIENDO QUE MAC4 < MAC3 < MAC2 < MAC1

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).

BID4 < BID2 < BID3 < BID1 (Sender Bit 2 < 3 por eso 1 cuelga de 2)



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 (c).



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=3 y backup para VLAN=2. Asumimos que tenemos un servidor "Server 1" conectado al conmutador S1 y pertenece a la VLAN=2. Asumimos las topologías de los apartados a) y b) (Fig(b) y Fig(c)).

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

Si cae fe3 se activaría fe0 (fe0, fe2, fe4, fe0).

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 estos enlaces, no se podrá llegar a S2 sin cambiar la topología, lo que provocará que el STP, conecte S3-S1 en la topología 1 (fe1, fe0-3, fe4, fe0) teniendo de Designed Port fe1.

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

Ocurriría que todo el tráfico hacia la red pasaría por el router R2 (topología 2), y por tanto podría llegar a haber un cuello de botella (fe2, fe4, fe0).

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

Pasaría como el apartado anterior, pasando de fe2 a fe4 a fe0

Pregunta 10. ¿Cuál es la limitación en el número de instancias STP que puede haber en un conmutador?

IEEE 802.1Q (VLAN) asume un esquema de etiquetado de n bits para una etiqueta VLAN, si n = 12, 2^12 = 4096 VLAN. Pero lo limita:
-El número de puertos virtuales por Line Card.
-El número de puertos lógicos STP activos.

Pregunta 11.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 conmutador L3 permite el tráfico entre diferentes VLAN (hosts - servidores), sin tener que pasar por un router (siempre y cuando este tenga conexiones de las VLANs respectivas). Esto nos permite eliminar tráfico innecesario hacia un mismo punto de la red y genere un cuello de botella.
Un switch convencional no puede interaccionar las diferentes VLANs que tiene dentro del mismo, pero en el caso de un router, hace lo mismo pero con un tiempo menor, ya que no tiene que mirar la tabla de encaminamiento, por tanto reduce la latencia.

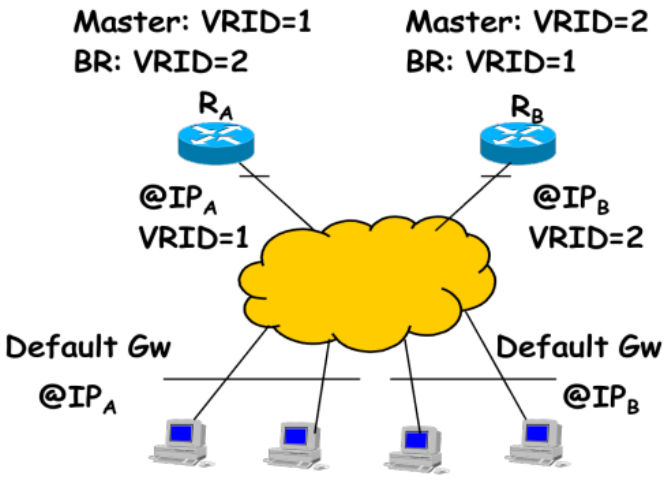
Pregunta 12.Explica qué es la tolerancia a fallos en el L3 respecto a los Hosts (clientes y servidores) y explica el funcionamiento básico del protocolo/mecanismo qué puede usarse para evitar dichos fallos.

La tolerancia a fallos en la L3, es la pérdida del gateway, y su objetivo principal es obtener una ruta predeterminada para salir de la red. Respecto a hosts, la mayoría de estos y servidores utilizan una ruta predeterminada configurada estáticamente u obtenida a través de DHCP. Si aparece un punto de falla supone la pérdida de conectividad de hosts/servidores. Para evitar dichos fallos, se podría emplear VRRP (Virtual Router Redundancy Protocol), diseñados para eliminar estos puntos de falla relacionados con rutas por defecto, que tiene un router backup por si el master (principal) falla.

Pregunta 13.Explica cómo funciona un ARP gratuito y para qué lo usa el protocolo VRRP.

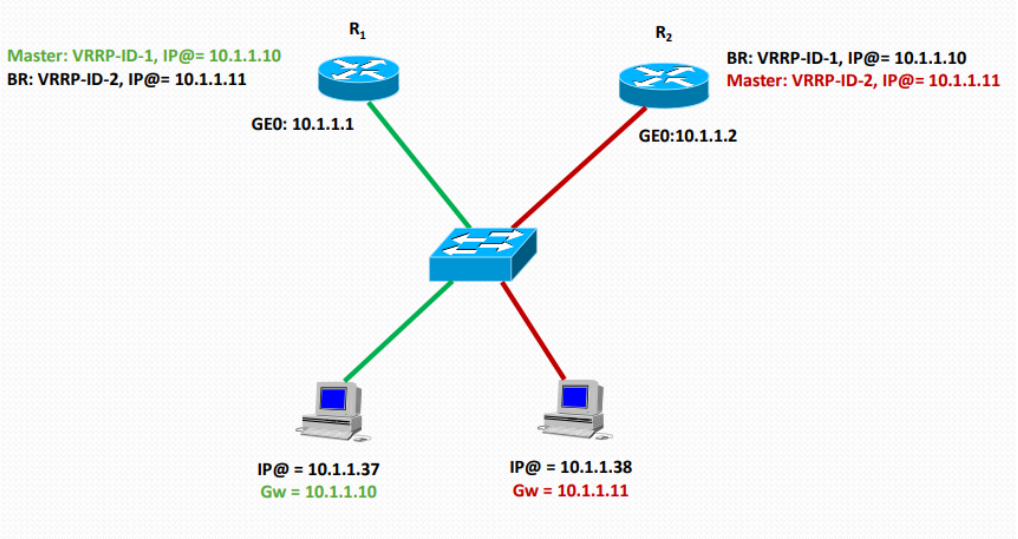
En el ARP gratuito request se configura como dirección de IP origen y de IP objetivo la IP del host que envía el paquete y pone la dirección de destino MAC = ff:ff:ff:ff:ff:ff (dirección de broadcast). Su objetivo es detectar IPs duplicados, limpiar tablas ARP, rellenar las tablas MAC…
Se utiliza en el protocolo VRRP cuando el master (router principal) falla y el máster cambia a ser el de backup y hay que limpiar las tablas ARP.

Pregunta 14.Explica el funcionamiento general de VRRP y explica para qué es necesario usar VRRP en un bloque de conmutación. Ayúdate de la figura.

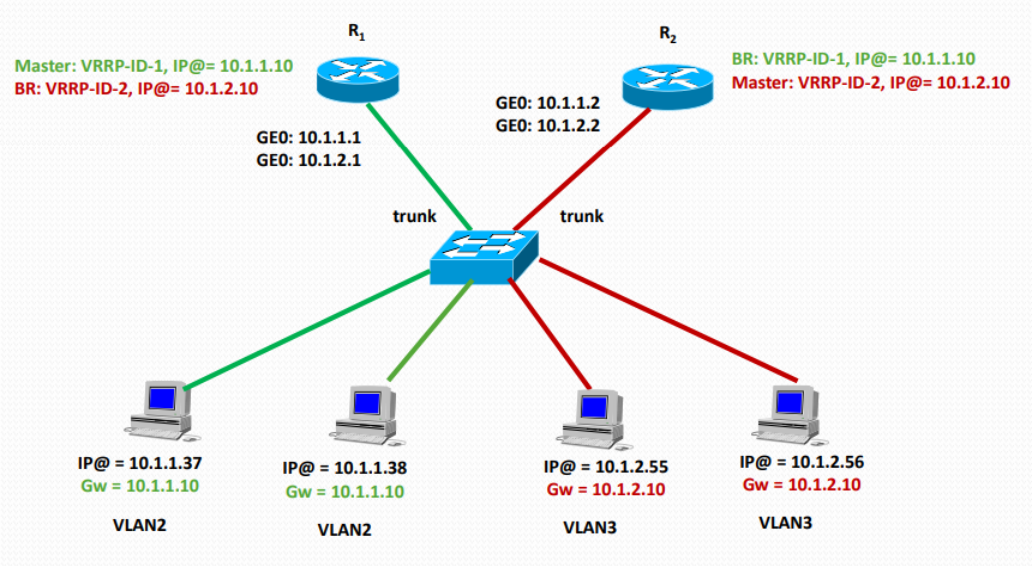


VRRP (Virtual Router Redundancy Protocol) consiste en eliminar los puntos de falla relacionados con rutas por defecto. El VRRP en un conmutador, nos permite diferenciar dentro de este, las IP primarias de cada una de las VLANs, y nos permite en el caso de que haya más de un router, tener un backup del master, en caso de que este fallase y así se puedan seguir manteniendo una comunicación.
Si el router A fallase, pasará a ser master VRID = 2, como en el router B.

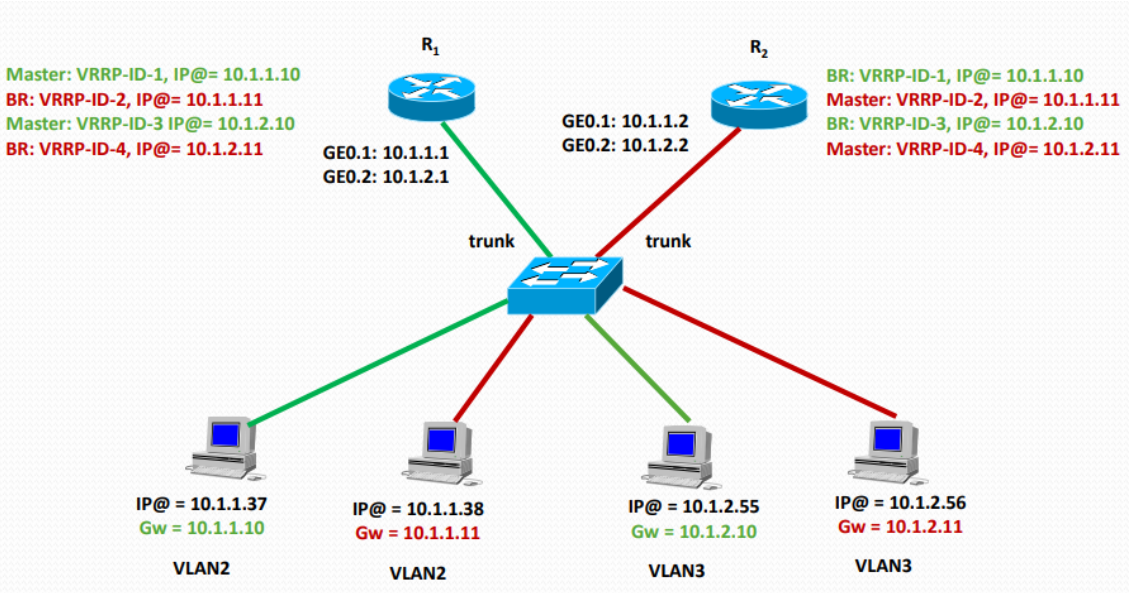
Pregunta 15.Pon un ejemplo de funcionamiento de VRRP con dos routers y dos Hosts con balanceo de cargas. Los dos Host en la misma VLAN.



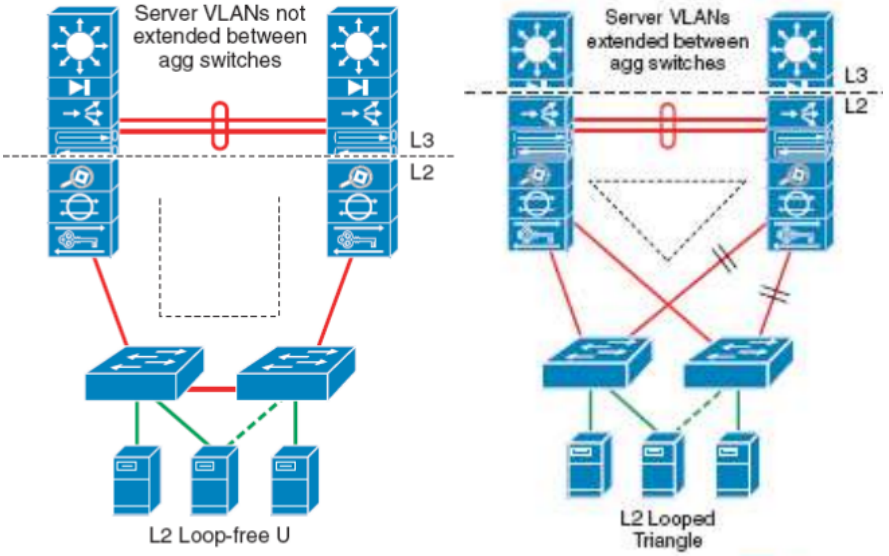
Pregunta 16.Pon un ejemplo de funcionamiento con dos routers y cuatro Hosts (dos en VLAN=2 y 2 en VLAN=3) con balanceo de cargas de tal manera que tráfico de VLAN=2 salga por el router R1 (backup el R2) y tráfico de VLAN=3 salga por el router R2 (backup el R1).



Pregunta 17.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).



Pregunta 18.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 porqué y una de ellas escala las VLANs entre conmutadores y la otra no.



<u>Triángulo > U:</u>

-Se forman bucles que después decides qué puertos no usar y van mejor, si un enlace falla puedes usar el otro, es más fiable.

-Es escalable (extensión VLAN), en caso de U tendrá que poner otra VLAN.

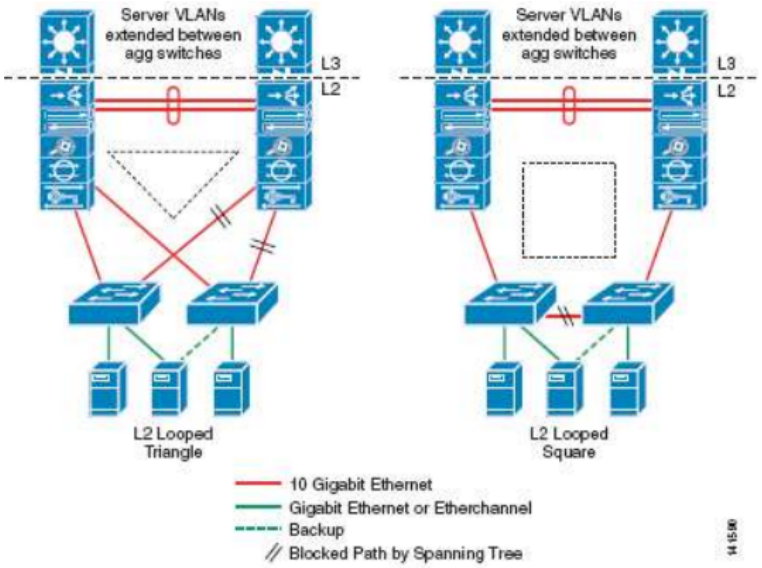
-Robusta (tolerancia a fallos L2 y L3 gw).

-Todas las operaciones se hacen en L2, no como U que tiene que subir L2-L3 y luego bajar.

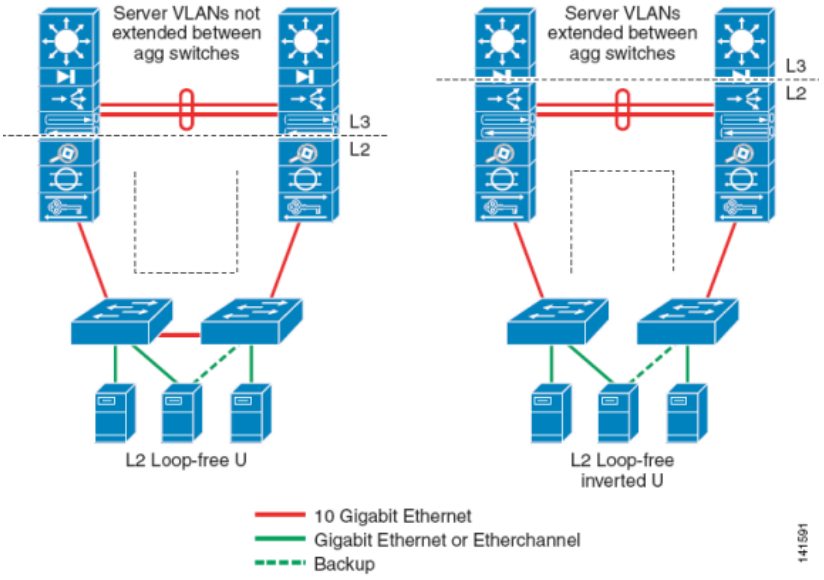
U > Triángulo:
-Más fácil de montar, más barato.

Pregunta 19. 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.

Se pueden implementar los en bucle (triángulo, cuadrado) o sin bucle (U, U invertida).

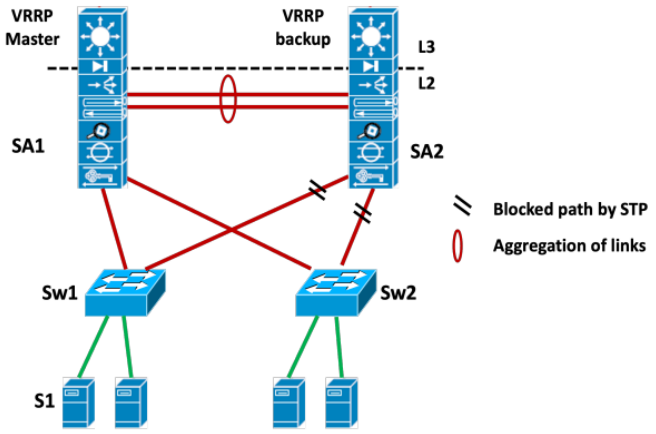


-Se forman bucles que después decides qué puertos no usar y van mejor, si un enlace falla puedes usar el otro, es más fiable.
-Es escalable (extensión VLAN).
-Robusta (tolerancia a fallos L2 y L3 gw).
-Todas las operaciones se hacen en L2, menos costoso.
-Aunque se bloquean los enlaces que no se usan, se activa el STP por si acaso.



-No tienen bucles por tanto si un enlace falla es menos fiable, y están todos activos.
-U no es escalable (tendrá que poner diferentes VLAN), U invertida es escalable (extensión VLAN).
-No robusta (no tiene tolerancia a fallos L2 y L3 gw).
-U tiene que subir L2-L3 y luego bajar, así que es muy costoso.
-Aunque no tengan bucles ya de por sí, se activa el SP por si acaso.

Pregunta 20. Suponemos qué en ambas configuraciones VRRP está configurado para que el switch de agregación SA1 sea máster 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. Repite el ejercicio si el Master VRRP está situado en SA2 y el backup en SA1.



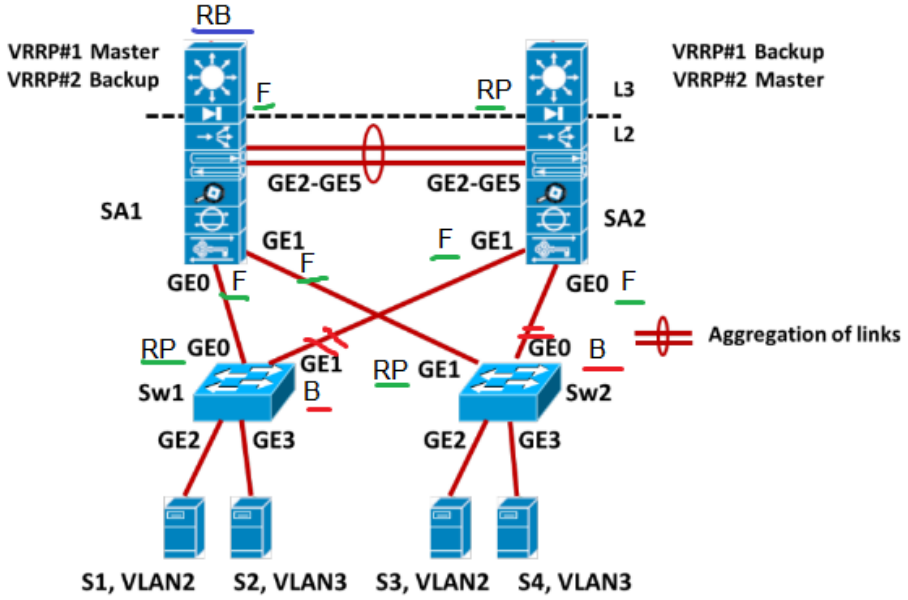
Podemos ver claramente que se está usando la topología del triángulo en este caso. El tráfico generado por el servidor S1 iría por Sw1-SA1, si cayera este enlace, se desbloquearía el enlace Sw1-SA2 (para evitar bucles como es topología triángulo se bloqueó por STP) y pasaría por allí el tráfico.
En el segundo caso, teniendo de master VRRP el SA2 y backup el SA1, y teniendo los enlaces de SA2 bloqueados, no pasaría nada ya que la información se sigue pudiendo pasar de los Sw1, Sw2 al SA1, y este luego al master en los enlaces agregados.

Pregunta 21.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).

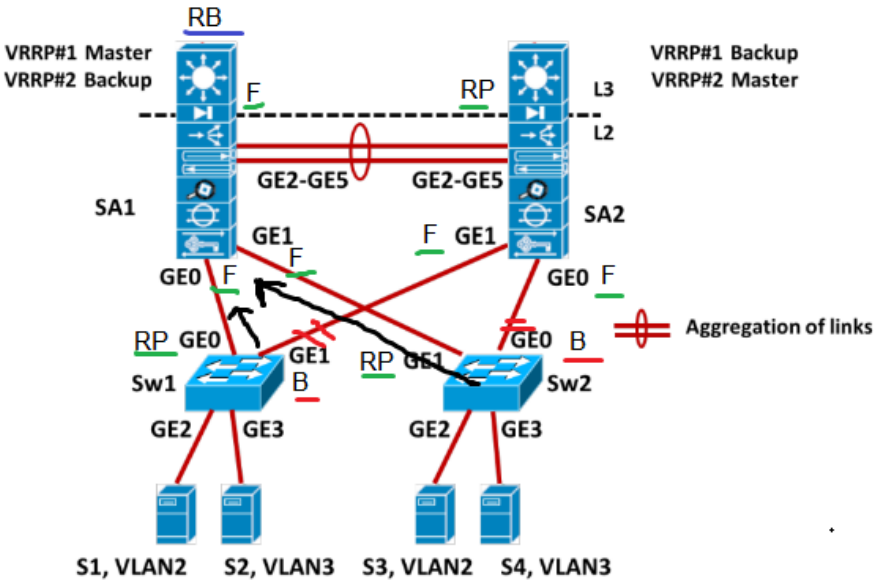
a) Indica qué enlaces son "trunk": Equipo (SA1, SA2, Sw1, Sw2, S1,S2,S3,S4) – interfaces (GEx, GEx-GEy, All, None).

Podría ser:
BID SA1 < BID SA2 < BID SW1 < BID SW2, digamos que elegimos esta.
BID SA2 < BID SA1 < BID SW2 < BID SW1
Son trunk todos los G2 y G3 de los Sw1 y Sw2, y en mi caso he decidido coger de Sw1, GE0 y de Sw2 GE1, para así evitar bucles.

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.



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).

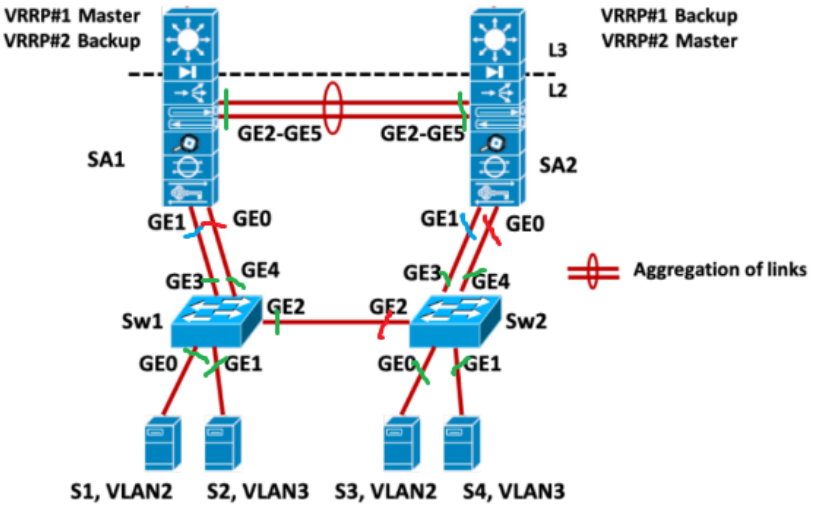


Al caer VRRP1 sus enlaces también caen, entonces se cambia la topología desbloqueando Sw1-GE1 y Sw2-GE0 y el camino de S1 sería S1-Sw1-GE1-SA2 y el camino de S3 sería S3-Sw2-Ge0-SA2.

Pregunta 22. Sabemos que 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 círculo 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 quién es el root bridge y quienes son los root ports para cada switch).**

   Como sabemos, cuanto más bajo el BID más prioridad, así que Sw2 tiene preferencia y será el Root Bridge: (cambio posiciones sw2 con sw1 que se he visto mal xd)



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.**

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

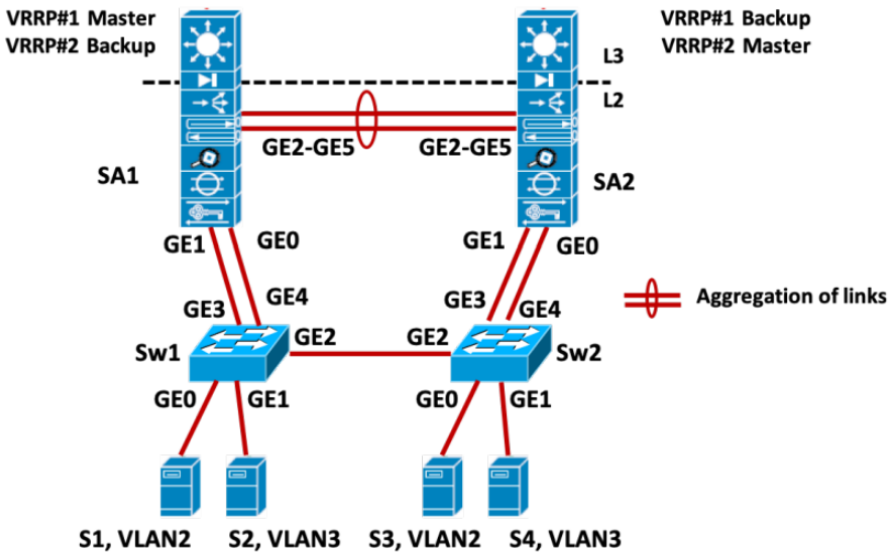
   S1, VLAN2: ge0 -> ge3 -> ge1 -> SA1 (VRRP1 Master)
   S2, VLAN3: ge1 -> ge3 -> ge1 -> ge2-ge5 -> SA2 (VRRP2 Master)
   S3, VLAN2: ge0 -> ge3 -> ge1 -> ge2-ge5 -> SA1 (VRRP1 Master)
   S4, VLAN3: ge1 -> ge3 -> ge1 -> SA2 (VRRP2 Master)

d) Indica cómo afecta al tráfico qué caigan los enlaces Ge3 y Ge4 del Sw1. Recuperamos los enlaces Ge3 y Ge4 del Sw1. Indica qué ocurre si cae el VRRP#1.

Si cayeran los enlaces ge3 y ge4 del Sw1 no podríamos llegar a SA1 de ningún modo, así que activaríamos el enlace ge2 entre los switches 1 y 2. Para el S1 tendría que pasar por Sw2-SA2 y volver a SA1. Para el S2 tendría que pasar por el Sw2 para llegar a SA2.
Si cayera VRRP#1, SA2 se convertirá en Master del VLAN2 también, por lo que todo el tráfico irá para allá.

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 y Sw2 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.

NO HE ENTENDIDO MUY BIEN EL ENUNCIADO POR LO QUE :D



Pregunta 23.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 se usa para cuando en un data center, hay más información que entra, que la que puede salir, por tanto se genera un cuello de botella, lo cual no permite gestionar bien todas las peticiones. Por tanto hay que adaptar el ancho de banda de todas estas conexiones al throughput del servidor y así que este no genere retrasos en las conexiones. Es la operación inversa del throughput.

Teniendo 4 enlaces de 10 Gbps y 96 puertos de 1 Gbps:
th = 4 * 10 Gbps / 96 * 1 Gbps = 0.416 Gbps
ov = 1 / th = 1 / 0.416 = 2,4:1
Si solo ocuparan un 20% los servidores -> th = 0,2 < 0.416
0,2 * 96 = 19,2 * 1Gbps (20%)
Entonces 0,2 = 4 * 10 Gbps / M * 1 Gbps = M = 40 / 0,2 = 200 enlaces se podrían poner en caso de que solo ocuparan un 20%.

Pregunta 24.Calcula el throughput medio y el “oversubscription ratio” de un conmutador con 8 enlaces 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.

th = 8 * 10 Gps/ 192 * 1Gps = 0.416 Gbps
ov = 1 / th = 1 / 0.416 = oversubscription ratio de 2.4:1
0.55 = 8 * 10 Gbps / M * 1 Gbps = M = 80 / 0.55 = 145,45 -> 145
No está bien diseñada, debido a que siguen consumiendo más de lo que pueden, ya que es demasiada información si están todos transmitiendo (solo 145 servidores lo podrían hacer). Debía poder sacar 105,6GB/s para poder hacer frente a esta demanda.