TOPIC 2: Red Corporativa

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

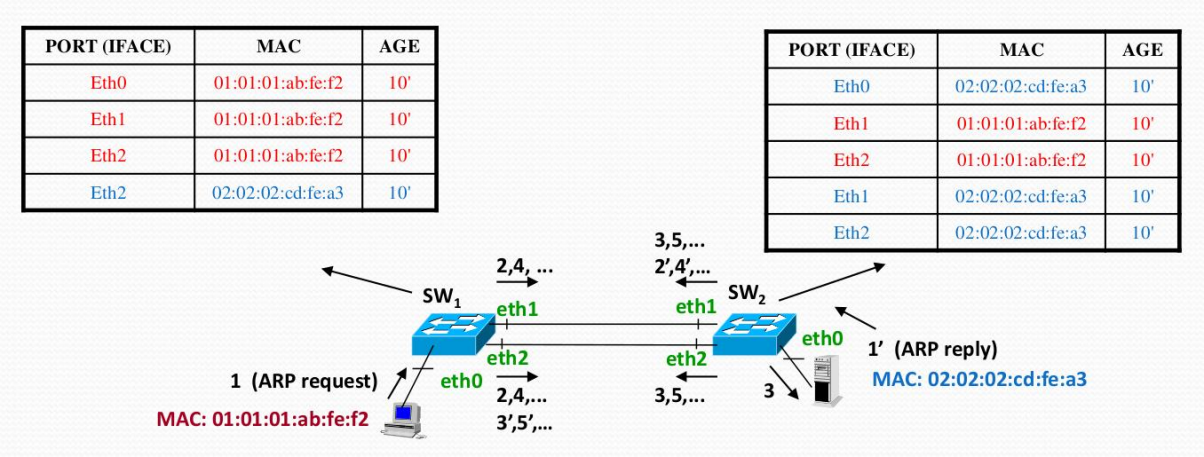
En una red, se quiere que se tenga el **mínimo tiempo de espera** posible cuando hay un fallo en una conexión.

Esto se soluciona poniendo **redundancia en la red**, el problema reside en que cuando se pone redundancia (bucles), aparecen **tormentas broadcast** (se crean paquetes de manera exponencial debido al ARP).

Para solucionar las tormentas broadcast (tolerancia a fallos de nivel 2), se usa el STP. Este protocolo **convierte una red con bucles, a una red con jerarquía en forma de árbol**, desactivando los cables que crean redundancia. En caso que uno de estos falle, el mismo protocolo ya se encarga de activar los cables necesarios para que la red vuelva a funcionar.

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

Una tormenta broadcast sucede cuando **hay un bucle** en una red y dos hosts se quieren comunicar, y debido al bucle de la red, **hay una generación exponencial de paquetes ARP request** haciendo que la red se sature y no se pueda resolver la dirección.



Se puede solucionar usando el protocolo STP, que **elimina virtualmente los bucles de la red**, convirtiendo su topología en un árbol.

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**, los puertos de los conmutadores y hubs, se les **asigna una VLAN al puerto** (poniendo el switch port en **modo access**), independientemente del dispositivo que se conecte en ese puerto.

En las **VLAN dinámicas**, son las **direcciones MAC** de los dispositivos que se les **asigna un VLAN**, independientemente del puerto de conmutador y hub al que se conecten. Esto se hace gracias al servidor **VMPS**, que comparte las asignaciones con otros switches de la misma red, y así tener asignada la VLAN **independientemente del switch conectado**.

Cuando una MAC se conecta en una red donde no tiene definida la VLAN (dinámica), se puede decidir qué hacer con dos modos:

- **Modo open**: si esta MAC no está definida, se le asigna una **VLAN por defecto (declarada con la comanda vmps fallback <vlan>, puede recibir el parámetro -NONE- que deniega la conexión). Si conectas una mac asignada en el servidor vmps, se le asigna la vlan que tiene asignada.**
- **Modo secure**: si esta MAC no está definida, se **desactiva el puerto (modo shutdown). Si conectas una mac correcta después, el puerto continuará en modo shutdown.**

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

Los puertos seguros nos ayudan a **limitar las direcciones MAC** de los puertos y gestionarlas. Los puertos se pueden configurar de 3 formas:

- **Estáticas**: Indicas las @MAC permitidas en el puerto.
- **Dinámicas**: Indicas el número máximo de @MAC que puede haber
- **Sticky**: La primera dirección que se conecta se queda como estática.

Cuando hay alguna violación (eg. se conecta en un puerto una MAC no identificada), se puede gestionar de 3 formas:

- **Protect**: no permite el tráfico de las MAC desconocidas
- **Restrict**: igual que protect pero avisa al administrador
- **Shutdown**: no permite el tráfico y corta todo el tráfico del puerto. Para permitirlo otra vez, se tiene que activar manualmente

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).

Al hacer agregación, aumentará la velocidad del canal y STP lo entenderá como una sola conexión, no como múltiples que en un principio formarían un bucle.

- **STP:** 1 instancia STP para todas las VLAN.
- **PVST:** 1 instancia STP para cada VLAN (propietario CISCO, no compatible con IEEE)
- **PVST+:** igual que PVST pero en este caso sí que es compatible con IEEE
- **MSTP:** 1 instancia STP para cada VLAN (propietario IEEE)
- **RSTP:** MSTP pero con las etapas de learning y listening aceleradas.

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

La red conmutada está unos 30 segundos en modo **listening y learning**, en esta etapa, los conmutadores se están enviando sus **BIDS en BPDUs** para ver cual es más pequeño y ser el **Root Bridge**. Una vez seleccionado el **Root Bridge**, todos sus puertos pasan a ser **designated ports**.

Todos los switches que no son RB, tienen que **seleccionar un puerto para que sea el Root Port** (que este llevará al RB). El criterio usado para seleccionar el root port es el siguiente, si hay un empate, se decide por la siguiente opción:

1) **Root bridge:** Si está conectado directamente al Root Bridge
2) **Cost Bridge:** El mínimo coste del switch al RB
3) **Sender Bridge:** De donde viene el BID adyacente más pequeño
4) **Port-ID:** El Port-ID más pequeño del switch de donde viene el BDPU

Si había varias opciones para el Root Port de un switch, el puerto seleccionado pasa a ser Root port, y las otras opciones en modo blocked, y la resta de puertos pasan a ser designated ports.

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

Dada una red conmutada en la que se le ha aplicado el STP, la red se convierte en una jerarquía en forma de árbol cuyo nodo inicial es el root bridge (conmutador cuyo BID es el menor de todos) y en el que los puertos de los conmutadores se han configurado de tal forma que han eliminado cualquier bucle que se pudiese encontrar en esta red.
Así, estos puertos pueden ser root ports (puertos por los que pasar para dirigirse al root bridge) o designated ports (puertos en modo forwarding, que no han sido bloqueados). El resto de puertos están bloqueados evitando así los bucles.

La configuración tanto del root bridge como la de los tipos de puertos se ha hecho a través de la comparación, en base a un algoritmo, del contenido de las BPDUs que se han enviado entre los conmutadores.

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).

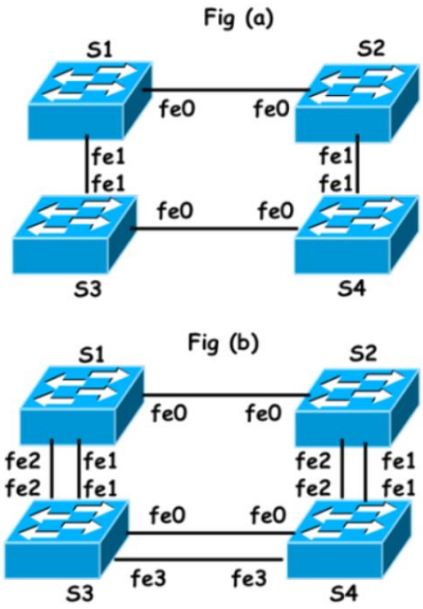
BID4 < BID3 < BID2 < BID1, ya que así el RB será el S4, y el S1 se conectará con el S3 ya que el BID3 < BID2

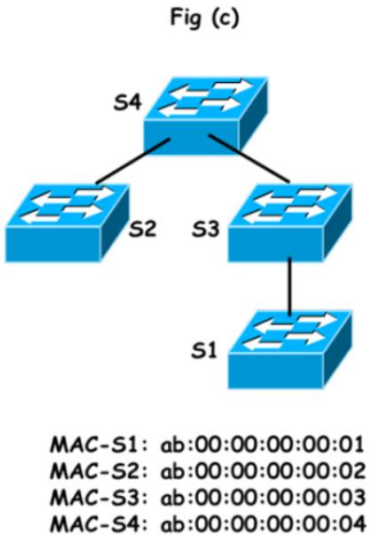
(b) Indica cómo conseguir tener una topología STP como la de la Fig (c) partiendo de la red de la Fig (b), pero ahora los enlaces activos de la Fig (c) son: de S4 a S2, fe1-fe1; de S4 a S3 fe3-fe3 y de S3 a S1, fe2-fe2. Los enlaces bloqueados no aparecen en la Fig (c).

BID4 < BID3 < BID2 < BID1
S4-fe1<S4-fe2
S4-f3 < S4-f0
S3-f2 < S3-f1

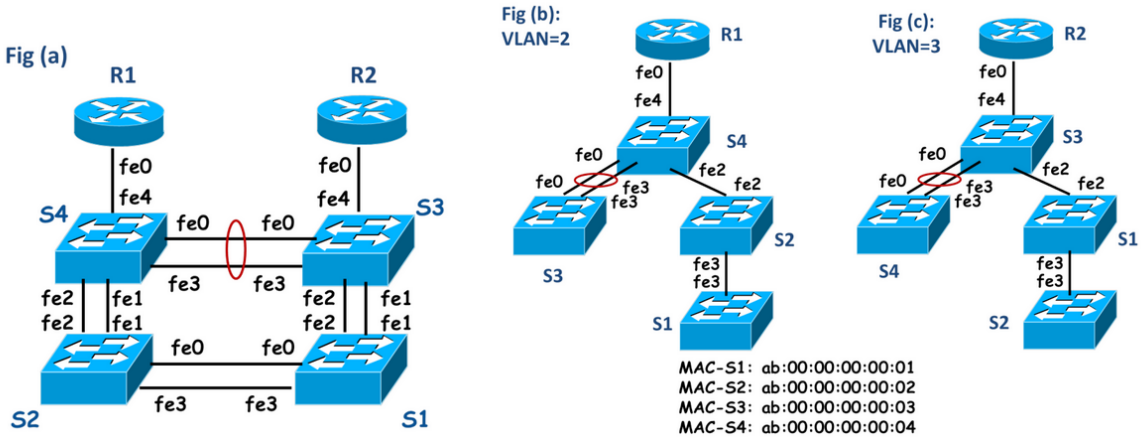
(c) Si tenemos 2 VLANs (VLAN=2 y VLAN=3), indica cómo podríamos modificar la respuesta del apartado (b) para que entre el switch S1 y S3 el tráfico de la VLAN=2 vaya por el enlace fe2- fe2 y el de la VLAN=3 por el enlace fe1-fe1.

VLAN2: S3-f2 < S3-f1
VLAN3: S3-f1 < S3-f2





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 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).

BIDsw4<BIDsw2<BIDsw3<BIDsw1

(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).

BIDsw3<BIDsw1<BIDsw4<BIDsw2

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.

Iría por 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.

El port fe3 pasa a estar modo listening y learning y después a blocked porque fe0 es el root port.

Si fe0 y 3 caen entonces tendremos que el root port de S1 es fe1 y fe2 seguirá bloqueado.

El camino a seguir sería sw1->sw3->sw4->R1.

(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.

Ahora el router backup (R2) hace de master y todos los mensajes pasan por allí. El tráfico del server 1 sería: sw1->sw3->R2

(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 dónde va el tráfico del Server.

n

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

Cada STP requereix almenys d'un port virtual com a mínim per a funcionar i els ports virtuals es troben limitats per el fabricant de la line card (hardware que gestiona els ports virtuals). Aquest fabricant especifica el màxim factible de ports virtuals que pots crear en aquella line card sense perdre rendiment, i com el commutador té tantes line cards com ports lògics, el commutador soportarà tantes instàncies stp com ports virtuals es puguin crear en conjunt de la suma dels límits màxims de ports virtuals de les line cards de tots el ports lògics.

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.

Dado un host que quiera comunicarse con otro host de una VLAN distinta a la suya, los paquetes tendrán que atravesar el router para llegar a este otro host. En el router se mirará la tabla de encaminamientos y se redirigirán los paquetes a la dirección física correspondiente.

La consulta de la tabla de enrutamientos es un proceso que puede perjudicar a la latencia del sistema. Es por esto que surge la idea de crear un conmutador de nivel 3 en redes conmutadas con varias VLANs. El sistema es el siguiente:

El primer paquete IP de una comunicación entre 2 VLANs llegará hasta el router. En nivel 3, se consultará la tabla de encaminamientos y se realizará el proceso de siempre solo que, además, se calculará en base a unos campos a determinar del paquete (MAC, IP origen/destino…) una función hash y se guardará en una caché. A esta entrada de la caché se le asignará la VLAN a la que se tiene que redirigir. A partir de este momento, a cada paquete que llegue se le calculará su hash correspondiente dependiendo de los campos escogidos. Si el hash coincide con alguna de la caché, el paquete se redirigirá directamente sin consultar la tabla de encaminamientos.

De esta forma conseguimos crear una tabla IPs parecida a la de MACs en la cual el primer paquete de una comunicación entre 2 hosts de distintas VLANs sí sube al nivel 3 pero el resto de paquetes no.

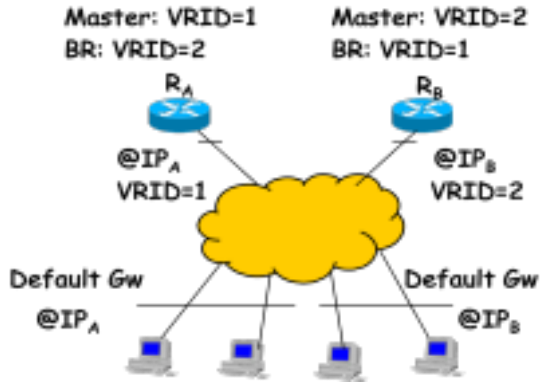
Pregunta 12. Explica qué es la tolerancia a fallos en el L3 respecto a los Hosts (clientes y servidores) y explica el funcionamiento básico del protocolo/mecanismo que puede usarse para evitar dichos fallos.

La tolerancia a fallos en L3 respecto a los Hosts es la pérdida de su gateway (de la conexión con el router que les hacía de gateway). Para contrarrestar este tipo de problemas, existe el protocolo VRRP, que nos permite tener un router master por donde pasan las conexiones y un router backup del máster que está preparado para ser utilizado si el router master fallase.

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

Un ARP gratuito es un tipo de mensaje ARP que puede ser tanto de tipo requets o reply. Si es un ARP request, la dirección IP origen y destino se establecen como la dirección del host que ha enviado el paquete. Además, la dirección MAC destino es la dirección MAC broadcast (ff:ff:ff:ff:ff:ff).
Una de las funcionalidades que tiene, y es la que aprovecha el protocolo VRRP, es la limpieza de cachés de los hosts de la red conmutada para, en caso de la pérdida de un router master, poder reconfigurar los conmutadores de la red para que estos redirijan al router de backup.

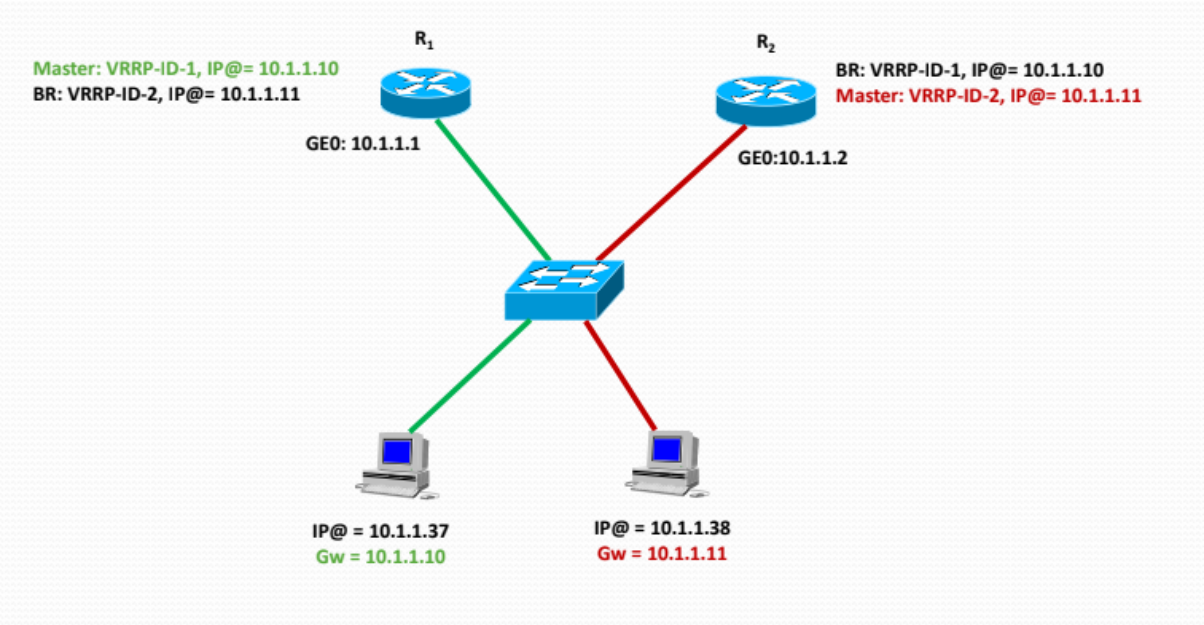
Pregunta 14. Explica el funcionamiento general de VRRP y explica para qué es necesario usar VRRP en un bloque de conmutación. Ayúdate de la figura.



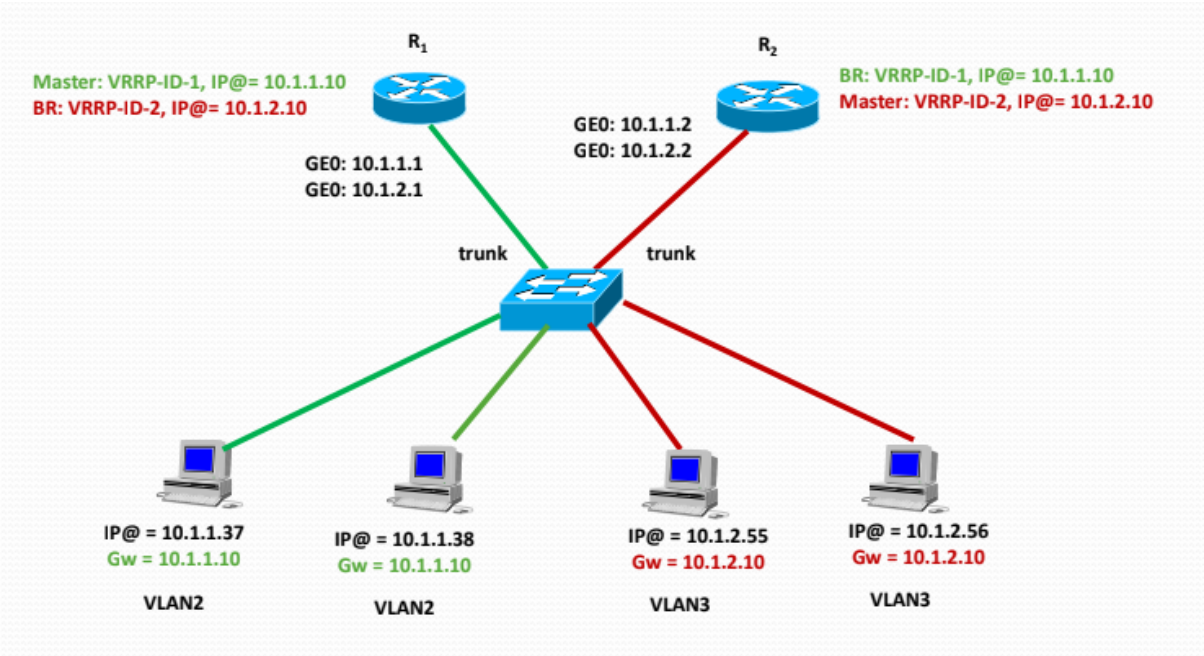
El uso de más de un router de salida en una red conmutada nos permite tener redundancia y, por lo tanto, tolerancia de fallos a nivel 3 siempre y cuando haya una forma de gestionar el uso de uno si el otro falla. VRRP es un protocolo que nos ayuda a conseguir esta gestión para poder utilizar un router u otro dependiendo cual falle. Su funcionamiento es el siguiente:

Se crea una instancia VRRP con un identificador. A cada router, le asignaremos su dirección física y, además, por cada instancia VRRP le asignaremos una @IP que será usada como gateway y una prioridad. En una misma instancia, la @IP de gateway ha de ser la misma para todos los routers, en cambio la prioridad será distinta.
Habiendo hecho esto con todos los routers, por cada instancia VRRP el router que tenga prioridad más alta será el router master y el resto trabajarán como backups (de esta instancia en concreto!). Esto quiere decir que un router, dependiendo de qué instancia, puede ser master o backup.
Finalmente, cada host recurrirá al protocolo ARP para descubrir la dirección física de su gateway y recibirán la dirección del router master correspondiente a su gateway

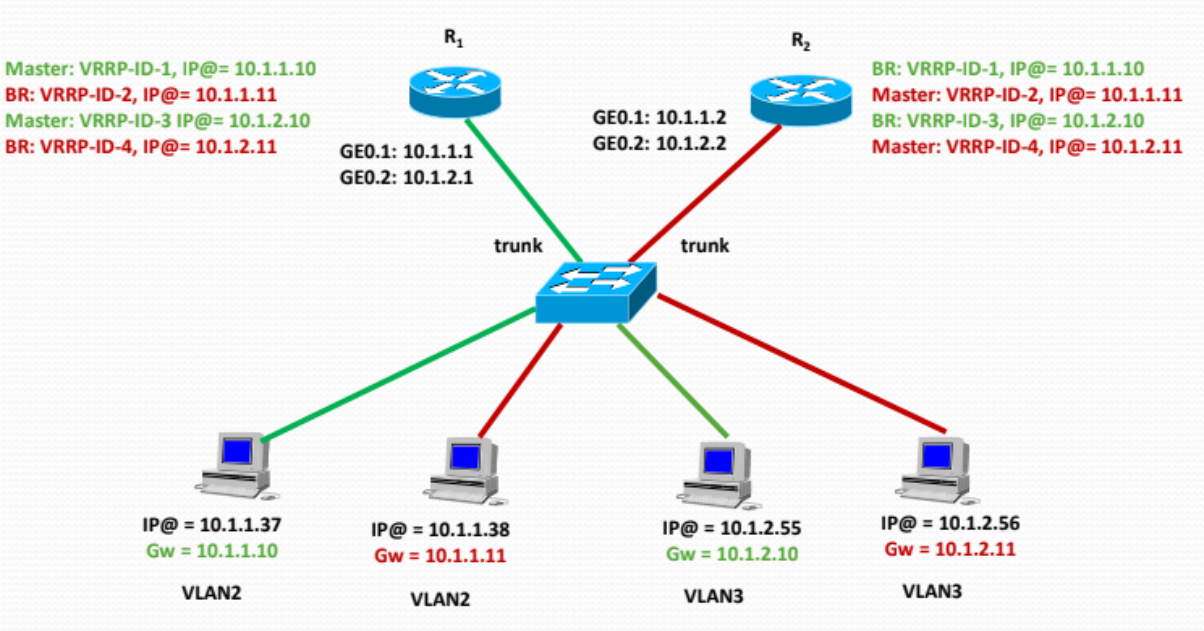
Pregunta 15. Pon un ejemplo de funcionamiento de VRRP con dos routers y dos Hosts con balanceo de cargas. Los dos Host en la misma VLAN.



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).

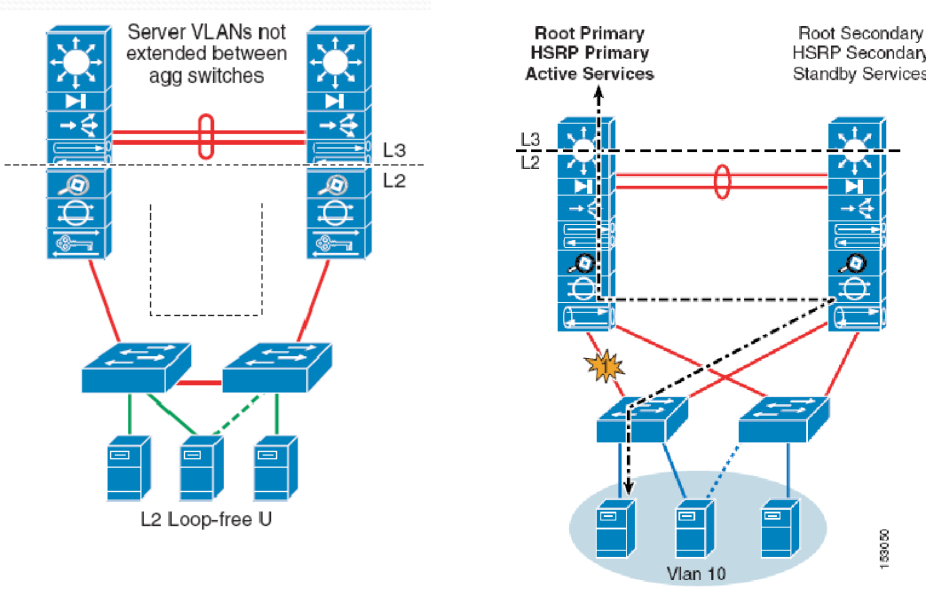


Pregunta 17. Pon un ejemplo de funcionamiento con dos routers y cuatro Hosts (dos en VLAN=2 y 2 en VLAN=3) con balanceo de cargas de tal manera que H1 de VLAN=2 y H3 de VLAN=3 salga por el router R1 (backup el R2) y H2 de VLAN=2 y H4 de VLAN=3 salga por el router R2 (backup el R1).



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. b) Explica por qué una de ellas escala las VLANs entre conmutadores y la otra no.

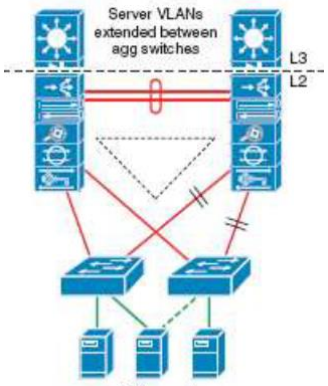
a) Una topología de STP organizada en U es looped-free, esto provoca que no hayan conexiones bloqueadas y por tanto no haya redundancia de nivel 2, com a molt poden haver 2 switches d'accés i no hi han extensions VLAN.
La topología de STP organizada en triángulo es looped, así que posee las características opuestas a las anteriores.
Mientras que la topología en triángulo proporciona más redundancia y más variabilidad de configuraciones también es cierto que requiere de más cableado y puertos llegando a ser totalmente inviable para CPD's medianos-grandes.
Las dos topologías requieren del uso de STP.



b) La topología en triángulo permite el escalado de VLANs, ya que, los conmutadores están conectados a los mismos módulos agregación y por tanto los broadcasts de las VLANs se pueden extender a diversos switches.

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 donde se vea la topología.

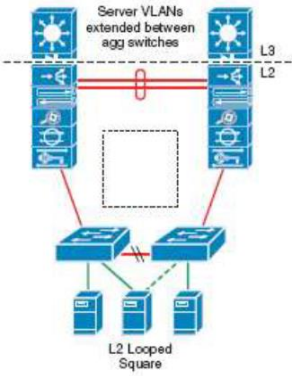
Topología en triángulo Looped:



L2 Looped Triangle

Es necesario usar STP en ella.
Ventajas:
Dispone de extensión de VLAN, y redundancia L2.
Desventajas:
Costes y limitación de puertos para CPDs medianos-grandes.

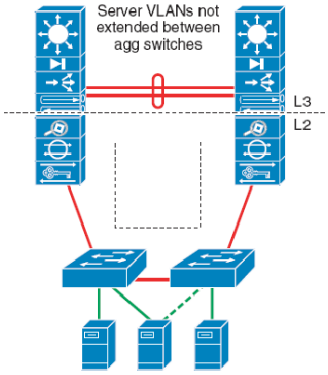
Topología en square Looped:



L2 Looped Square

Es necesario usar STP en ella.
Ventajas:
Dispone de extensión de VLAN y cierta redundancia L2.
Desventajas:
Costes elevados para CPDs medianos-grandes.

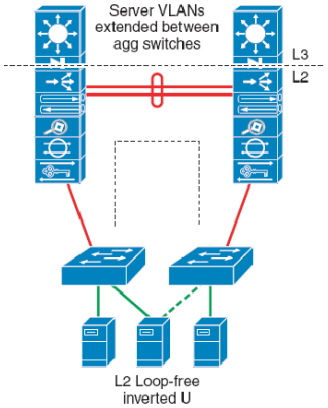
Topología en U Looped-free:



L2 Loop-free U

No es necesario usar STP en ella pero es recomendable.
Ventajas:
Barato. Redundancia L2. (Tolerancia a fallo)
Desventajas:
No se puede escalar y sin Extensión VLAN.

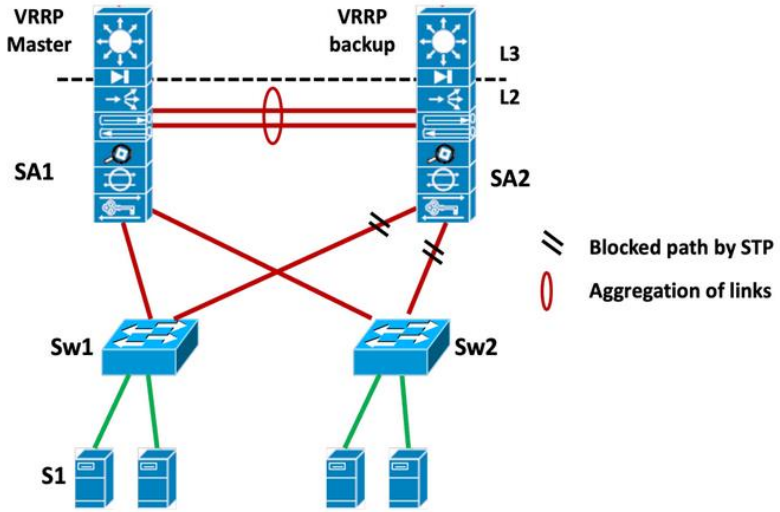
Topología en ∩ Looped-free:

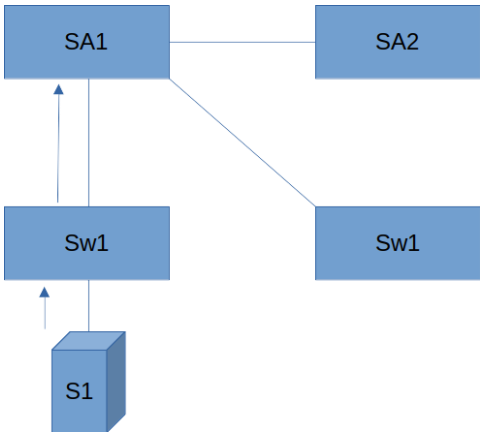


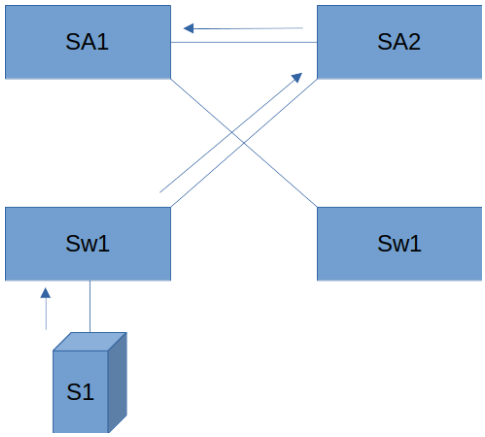
L2 Loop-free inverted U

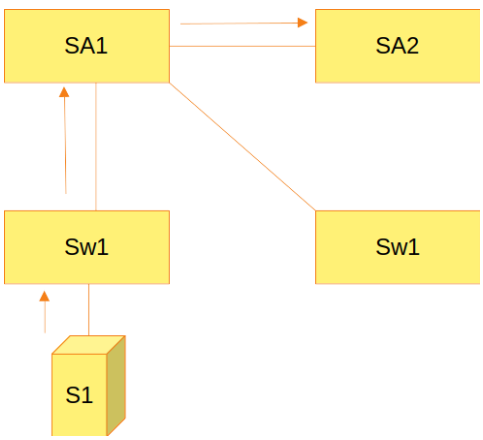
No es necesario STP en ella pero es recomendable.
Ventajas:
Barato, escalable.
Desventajas:
Sin extensión VLAN, sin redundancia.

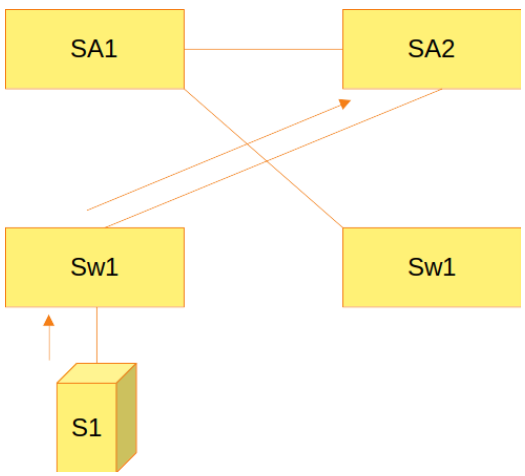
Pregunta 20. Suponemos que en ambas configuraciones VRRP está configurado para que el switch de agregación SA1 sea master de todos los servidores y el segundo switch SA2 sea backup. Indica el tipo de topología de nivel 2 que se ha configurado con STP, por dónde iría el tráfico generado por el servidor S1 y por dónde iría dicho tráfico si el enlace SA1-Sw1 cae. Repite el ejercicio si el Master VRRP está situado en SA2 y el backup en SA1.









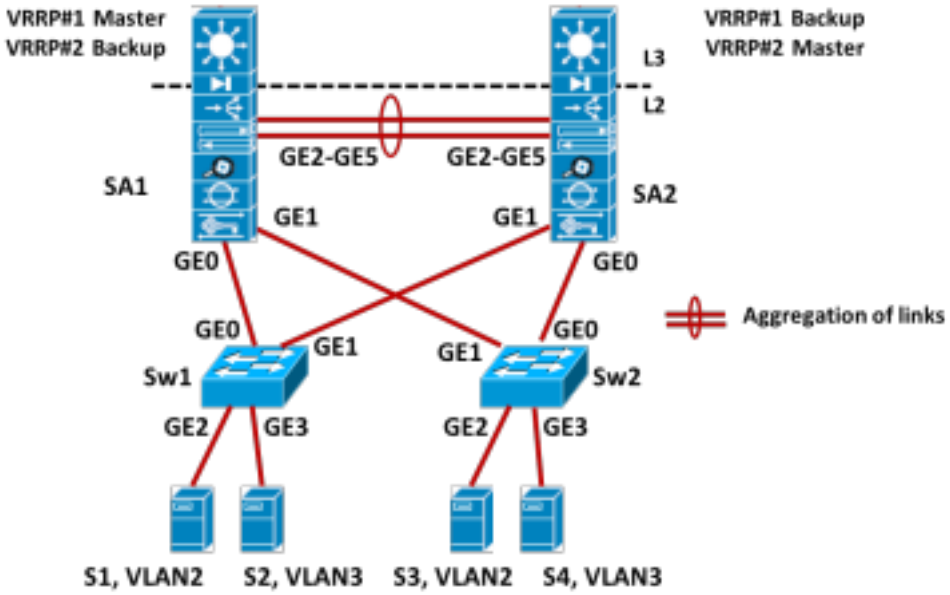


Pregunta 21. Contesta a las siguientes preguntas respecto a la red de la figura, teniendo en cuenta qué queremos que los servidores de la VLAN 2 tengan como Gateway a SA1 y los de la VLAN 3 a SA2. (Nota: GEx = interface GigabitEthernet número x, GEx-GEy indica grupo de interfaces desde la x a la y).

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

b) Indica qué enlaces se bloquerian (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).



Pregunta 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.

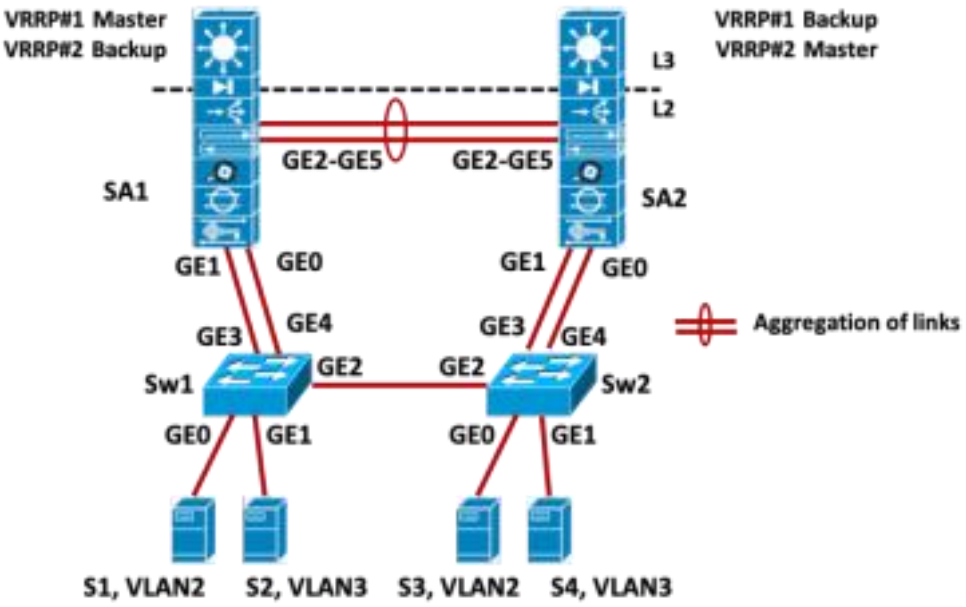
(a) Supongamos qué MAC-Sw2 < MAC-Sw1 < MAC-SA1 < MAC-SA2, indica cuál es la topología resultante (dibuja un esquema en el qué solo aparezcan los enlaces no bloqueados e indica quien es el root bridge y quienes son los root ports para cada switch).

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

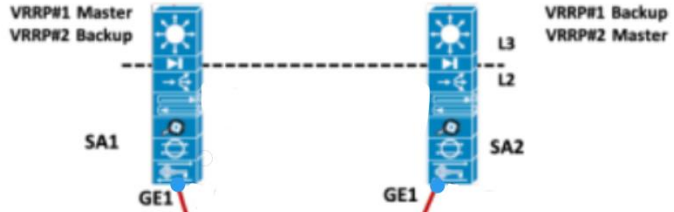
(c) Indica el camino qué sigue el tráfico en cada servidor en los casos a) y b).

(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.

(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 trafico 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.

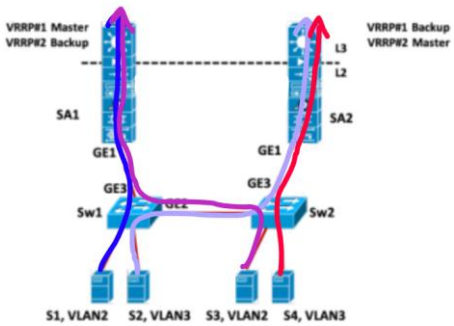


a)



b)

c)


VRRP#1 Master
VRRP#2 Backup
VRRP#1 Backup
VRRP#2 Master
L3
L2
SA1
SA2
GE1
GE1
GE3
GE3
Sw1
Sw2
S1, VLAN2
S2, VLAN3
S3, VLAN2
S4, VLAN3

Pregunta 22. 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?

4 * 10 / 96 *1 = 0,416 -> 41,6% -> 0,416 Gbps

1/0.416 = 2.4 -> cada 2.4 servidors estem fent servir 1Gb/s

0,2 = 4*10 / 1*x -> 200

Pregunta 23. 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 / 192*1 = 0.416 -> 41,6%
0,55 = x * 10 / 192 * 1 -> 10.56 -> 11