TEMA 2 – Redes corporativas.

Objetivos

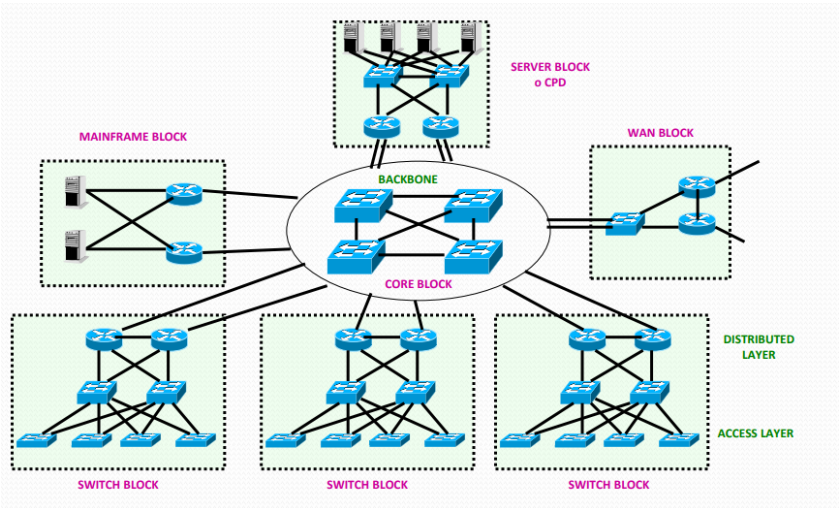
1. Introducir conceptos básicos de conmutadores
2. Entender el diseño de redes corporativas
3. Entender los conceptos y protocolos L2/L3 reliability
4. Aprender técnicas de diseño de CPDs (Centros de procesamiento de datos)

Redes corporativas

- Son compañías con **end users** y **end services**.
- Conectados a otros end users o a otras redes corporativas **via un ISP**.
- Las redes corporativas pueden estar…pequeña empresa con pocos usuarios a una gran compañía con miles de usuarios. (**RANGO**)
- Debe gestionar sus **servicios** en un **CPD** (ubicado en el sitio principal) y sus servicios **a través de otros** que proporciona el servicio.

Diseño red corporativa

- Uso de **bloques de conmutación interconectados** por una red troncal de conmutación rápida.
- Formado por:
  - **Switch Block** → Los end users se conectan para acceder a los conmutadores. Estos están conectados a los conmutadores de agregación que agregan el tráfico de usuarios a los routers que les sacan del switch Block.
  - **CPD** → Es un switch block específico en el que los switches dan servicio a servidores en lugar de end users.



- **Backbone block** → Grupo de switches centrales que interconectan los switch blocks.
- **WAN block** → Bloque que da acceso a Internet y a conectividad VPN.

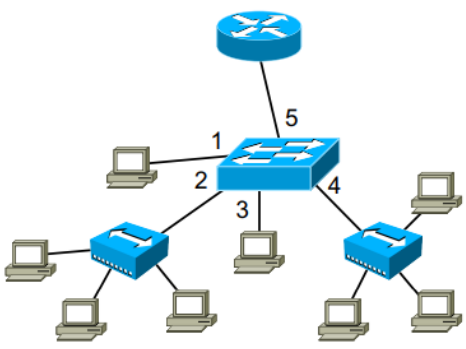
(Mainframe block no se hace)

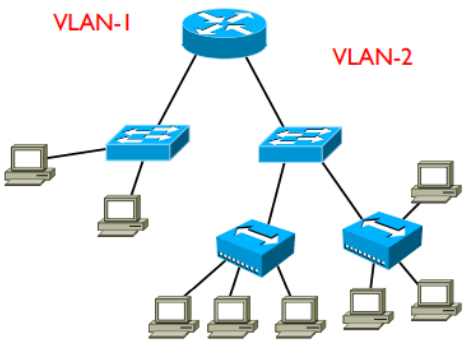
Tecnologías Ethernet (no se pregunta)

- Importantes:
  - Puertos **simétricos** → Misma tasa
  - Puertos **asimétricos** → Diferentes tasas
  - Puertos **Half Duplex** (típicamente 10BaseT) → Una estación puede o transmitir o recibir, nunca las dos cosas a la vez. Si es a la vez, hay colisión.
  - Puertos **Full Duplex** (típicamente Fast Ethernet and GigaBit Ethernet) → Una estación puede transmitir y recibir al mismo tiempo.
  - **Tablas MAC** (en los switches) → Con entradas estáticas o dinámicas. Es una tabla que contiene las @MAC de los clientes con la interface con la que están conectados al switch.

VLANs

- Una **VLAN**, acrónimo de *virtual LAN*, es un método para crear redes lógicas independientes dentro de una misma red física.
- Varias VLAN pueden coexistir en un **único switch físico o en una única red física**. Se necesita mínimo, un router y un switch.
- Tipos:
  - VLAN **estática** (o basadas en el puerto)→ Las asignaciones se crean mediante la asignación de los puertos de un switch a dicha VLAN. (XC)
  - VLAN **dinámica** → La asignación se realiza automáticamente mediante paquetes de software **(servidor VMPS)** que asignan hosts a la VLAN basándose en su dirección MAC.
- Trunking → Enlaces que admiten multiples VLANs utilizando técnicas de "etiquetado". En ejemplo de abajo, sería el 5. (virtualmente es como si tuviera tantos enlaces e interfaces como VLAN se crean)





Configuración VLANs dinámicas (estáticas, hecho en la segunda práctica)

Los puertos se configuran automáticamente **atendiendo al MAC** del dispositivo que accede al puerto (host).

Inicialmente los clientes configuran los puertos con una VLAN dinámica. ¡Con esto, no se está asignando ninguna VLAN al puerto!

Cuando el switch recibe la primera trama de un host conectado a uno de los puertos con VLAN dinámica, el switch se conecta al servidor VMPS para descubrir la VLAN a la que pertenece este host y se la devuelve. Si el host se desconecta del puerto y se conecta a otro distinto, VMPS reconfigurará dinámicamente las VLAN de los puertos.

SOLO los switches de gama alta implementan un servidor VMPS, hay que descargar la libre distribución OpenVMPS (hecho en LAB).

Hay un fichero (en el lab) que se usa para configurar el servidor VMPS según como nos interese. Con lo siguiente:

```
1.  !vmps domain <domain-name> - The VMPS domain must be defined.
2.  !vmps mode { open | secure } - The default mode is open.
3.  !vmps fallback <vlan-name>
4.  !vmps no-domain-req { allow | deny } - The default value is allow.
5.  !
6.  vmps domain mydomain
7.  vmps mode open
8.  vmps fallback --NONE--
9.  vmps no-domain-req deny
10. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
11. !MAC Addresses
12. ! address <addr> vlan-name <vlan_name>
13. !
14. vmps-mac-addrs
15. !
16. address 0010.a49f.30e1 vlan-name --DEFAULT--
17. ! disabled - no access
18. address 0010.a49f.30e2 vlan-name --NONE--
19. ! vlan TEST restricted
20. address 0010.a49f.30e3 vlan-name TEST
21. ! vlan TEST1 unrestricted
22. address 0010.a49f.30e4 vlan-name TEST1
```

```
23. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
24. !Port Groups
25. !vmps-port-group <group-name>
26. ! default-vlan <vlan-name>
27. ! fallback-vlan <vlan-name>
28. ! device <device-id> { port <port-name> | all-ports }
29. !
30. vmps-port-group myswitch
31. device 10.0.0.1 port 2/4
32. device 10.0.0.2 all-ports
33. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
34. !VLAN groups
35. !vmps-vlan-group <group-name>
36. ! vlan-name <vlan-name>
37. !
38. vmps-vlan-group myvlans
39. vlan-name TEST
40. !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
41. !VLAN port Policies
42. !vmps-port-policies {vlan-name <vlan_name> | vlan-group <group-name> }
43. ! { port-group <group-name> | device <device-id> port <port-name> }
44. !
45. vmps-port-policies vlan-group myvlans
46. port-group myswitch
```

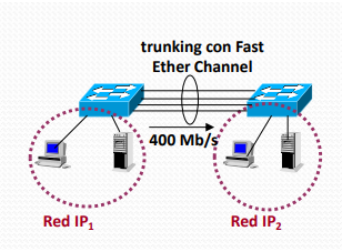
Las líneas que empiezan con el carácter '!' son comentarios. A continuación hay una breve descripción:

- Hay que definir un *VMPS domain* (línea 6), este dominio debe coincidir con el dominio VTP del switch. VTP (Virtual Trunking Protocol) es un protocolo propietario de CISCO que permite propagar la configuración de las VLANs a todos los switches de un mismo dominio. Por ejemplo, al crear una VLAN en un servidor VTP, la VLAN se propaga a todo el dominio.
- VMPS puede operar en modo *open* o *secure* (línea 7). En modo *open*: Si una MAC no está definida, se le asigna una VLAN por defecto (línea 8). En modo *secure*: Si una MAC no está definida se bloquea el puerto. Para desbloquear un puerto hay que ejecutar los comandos *shutdown / no shutdown*.
- En la sección *MAC Addresses* (línea 11) se asignan las VLANs a las que pertenecen las direcciones MAC. Puede usarse --NONE-- para denegar explícitamente el acceso a cualquier VLAN. Notar que para identificar las VLANs se usa el VLAN-name, no el VLAN-id. En el switch deben haberse creado las VLANs con el mismo nombre que el indicado en esta sección del fichero de configuración.
- Una VLAN se puede restringir a un switch específico, o a un grupo de puertos de un switch. Para ello hay que especificar:
  1. Los puertos permitidos (sección *Port Groups*, línea 24). Por ejemplo, la línea 31 especifica el puerto 2/4 del switch 10.0.0.1, y la línea 32 especifica todos los puertos del switch 10.0.0.2.
  2. Las VLANs a las que se les aplicará alguna restricción (sección *VLAN groups*, la línea 34).
  3. La asociación entre las definiciones anteriores (sección *VLAN port Policies*, línea 43).

(pasar a texto)

Agregación de enlaces en L2

- Técnica que consiste en utilizar varios enlaces Ethernet (alrededor de n = 2 a 4)
- Con el objetivo de **aumentar el rendimiento** (más Mb/s) más allá de lo que podría mantener una sola conexión **i proporcionar redundancia** en caso de que alguno de los enlaces fracase, siga funcionando.
- Agregación implica una reducción del número de puertos físicos en un switch ya que normalmente se usan para otros propósitos → Conectar hosts
- Formas de llamarlo:
    - IEEE 802.3ad (normalizado)
    - CISCO → **Port trunking** (no tiene nada que ver con trunking de VLANs)
    - Otros…Nic-team (ing)



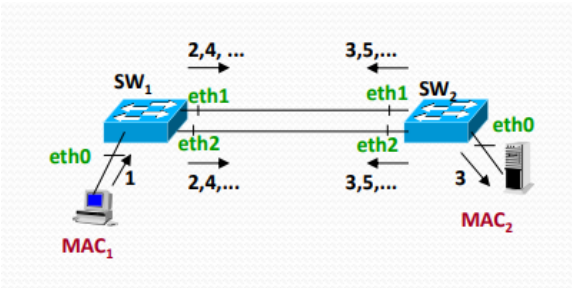
- Configuración:

```
!!!! Create the port-channel and assign ports
!!!! The ports have to be in the same VLAN or to be trunk
Sw(conf)# interface port-channel 1

Sw(conf)# interface Ge1
Sw(config-if)# channel-group 1 mode on

Sw(conf)# interface Ge2
Sw(config-if)# channel-group 1 mode on
```

Broadcast Storm (bucles)



(1) Station 1 sends a frame in broadcast (e.g. an ARP frame)
(2) Sw1 forwards in eth1 and eth2
(3) Sw2 forwards again (e.g. eth1 to eth2 and eth0)
(4) Sw1 forwards again → infinite loop

- Se produce cuando un sistema de red se ve colapsado por el tráfico continuo de tramas broadcast por los diferentes switchs a causa de bucles.

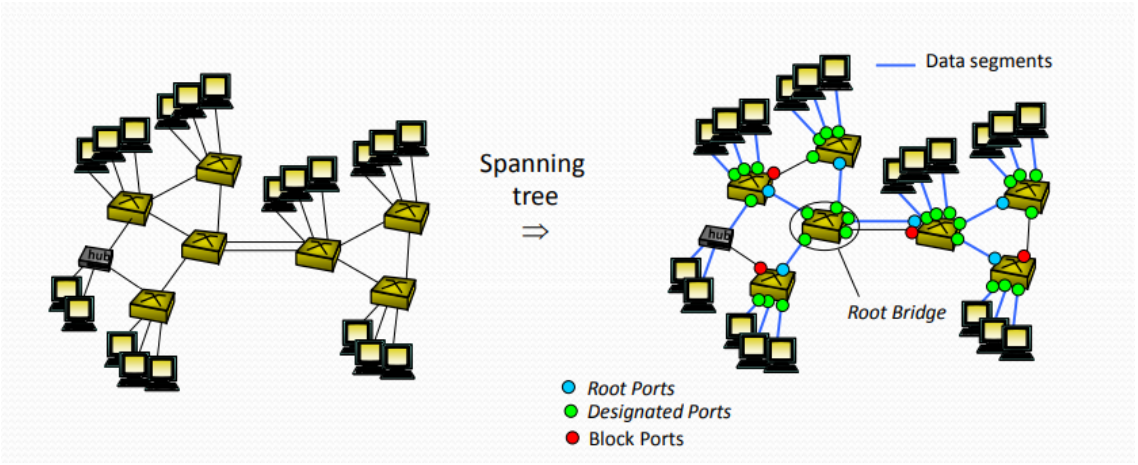
  → Provocando obviamente que la comunicación falle (no lleva a cabo su propósito).
- La manera de romper el bucle es desconectando físicamente los cables de los enlaces redundantes que provocan el bucle.
- ¡Para entenderlo, hay que tener en cuenta que un switch cuando recibe una trama broadcast, **el switch replica la trama por todos sus puertos excepto** el puerto por **el que le ha llegado la trama**!

Spanning Tree Protocol (STP) → Opera en la capa 2 del OSI

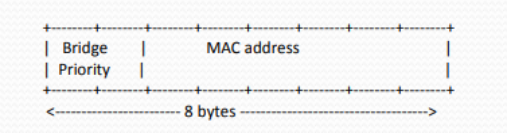
- El **objetivo principal** es evitar y eliminar los bucles / links redundantes. → Evitar broadcast storms
- ¿Cómo? Organizando la red en una **topología de árbol**, bloqueando aquellos puertos del switch que producen un bucle.
- Los costes de uso se basan en las tarifas de enlace como métricas.

Link capacity	Cost
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

- Para construir el Spanning Tree, el protocolo debe escoger lo siguiente:
    - **Root Bridge** (**RB**) → Para todo el dominio broadcast.
    - **Root Port** → Para **cada switch que no sea el RB**. Esto permite enviar tráfico hacia el RB y por tanto la topología de árbol.
    - **Designated Port** → Garantiza que todos los dominios de colisión sean accesibles. El resto de puertos NO elegidos como Root o Designated Port serán bloqueados.



- Los **switches se identifican** por el **Bridge ID (BID),** formado por → campo de **prioridad** y **una de las direcciones MAC del switch**.
- Se envían mensajes de señal, llamados **BPDU** (Bridge Protocol Data Unit) que envían los **switches entre ellos**.



- Los campos BPDUs usados en el cálculo del árbol son: (IMPORTANTE EL ORDEN)
    - Root BID (Bridge ID del root)
    - Root Path Cost → Se incrementa con el costo del puerto donde se recibe.
    - Sender BID → BID del switch que envía el BPDU.
    - Port ID → ID del puerto que transmite el BPDU (todos los puertos del mismo switch tienen diferentes ID y tienen una prioridad de puerto).

- STP lo **hace automáticamente todo**, pero **puede ser que nos interese** a nosotros escoger tanto el RB, el root port y el designated port, ya que la que nos ha hecho por defecto no nos interesa o nos va mal. (ej. switches más caros…no son el RB)

- <u>Elección RB</u>:

  Inicialmente todo los switches generan BPDUs con Root BID = Sender BID (se creen que todos son el RB). Si los switches reciben un BPDU con un Root BID más bajo, se para de enviar BPDUs y se asume ese BID como Root BID.

  La priority del Switch puede **ser configurable manualmente**. Inicialmente, es 0x8000 → 32768+num VLAN. Cuanto más bajo, más "prioridad" para ser root bridge. En caso de ser misma priority, se haría con la MAC más baja para acabar de descartar.

  La elección del RB puede afectar el rendimiento: debe ser el switch más centrado.

  + ¡Para cambiar la priority, tienen que ser siempre multiplos de 4096!

  ¡Acordarse de que la priority está dentro del BID! Buscamos el BID más pequeño siempre.

- <u>Elección del root port</u>

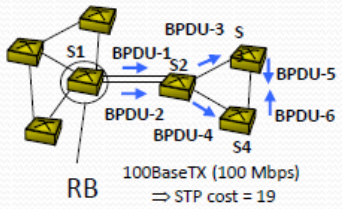
  Cada switch que no es el RB selecciona **un** puerto como Root Port.

  El puerto seleccionado es el que ha recibido una BPDU que cumple la siguiente secuencia de condiciones:

- Lowest *Root BID* (towards the *Root Bridge*).
- Lowest *Root Path Cost* (optimal path towards the *Root Bridge*).
- Lowest *Sender BID*
- Lowest *Port ID*

} In order the selection is unique.

Root BID = BID-S1 = 00:00:00:00:00:11:11:11
BID-S2 = 80:00:00:00:00:22:22:22
BID-S3 = 80:00:00:00:00:33:33:33
BID-S4 = 80:00:00:00:00:44:44:44



BPDU-1: Root BID = Sender BID = BID-S1
Root Path Cost = 0, Port ID = 1

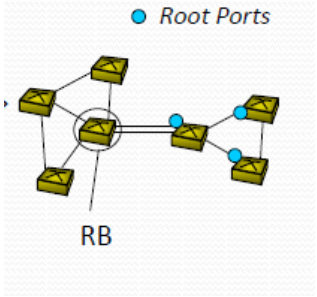
BPDU-2: Root BID = BID-S1, Sender BID = BID-S1
Root Path Cost = 0, Port ID = 2

BPDU-3: Root BID = BID-S1, Sender BID = BID-S2
Root Path Cost = 19, Port ID = 1

BPDU-4: Root BID = BID-S1, Sender BID = BID-S2
Root Path Cost = 19, Port ID = 2

BPDU-5: Root BID = BID-S1, Sender BID = BID-S3
Root Path Cost = 38, Port ID = 1

BPDU-6: Root BID = BID-S1, Sender BID = BID-S4
Root Path Cost = 38, Port ID = 1

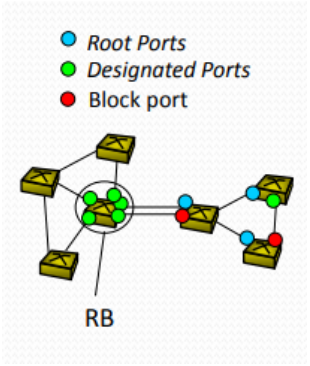


- <u>Elección Designated Port</u> → Garantiza dominio de colisión accesible

  TODOS los puertos del switch RB son Designated Ports, excepto aquellos que pueden formar un bucle de nivel 1. (dos puertos conectados a un hub)

  Para el resto de los switches, los puertos que no reciben BPDU son Designated Port.

  Los puertos que reciben BPDU y no son Root Port: Comparan la información contenida por las BPDU recibidas y enviadas en ese puerto. El puerto será Designated Port si cumple las condiciones siguientes: (las mismas que para el Root Port)



- Lowest *Root BID* (towards the *Root Bridge*).
- Lowest *Root Path Cost* (optimal path towards the *Root Bridge*).
- Lowest *Sender BID*
- Lowest *Port ID*

} In order the selection is unique.

+

EN ENLACES:

Root Port – Designated Port

Designated Port – Bloqueado

NUNCA:

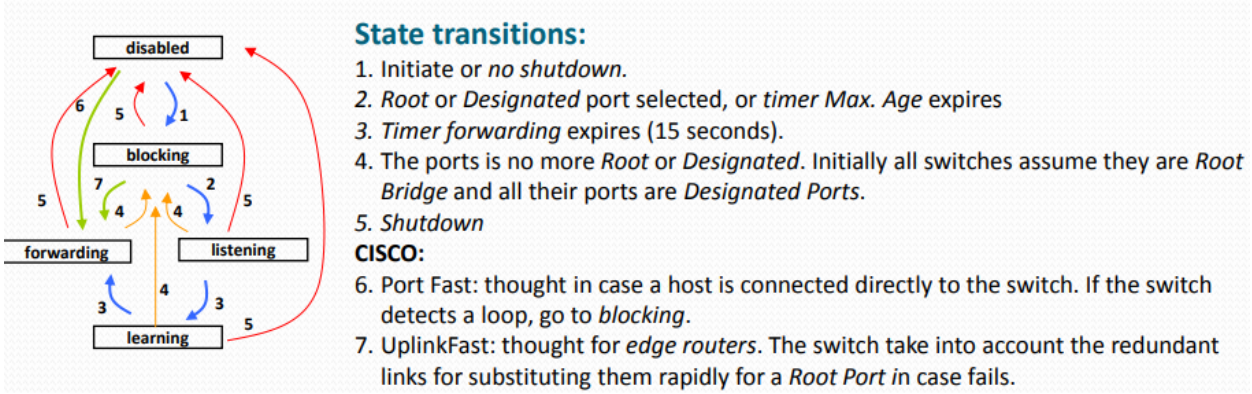
Root Port – Root Port

Root Port – Bloqueado

(por definición de root port)

- <u>Estados de los puertos</u> (Para acordarse→BEARD)
  - **Bloqueado** → BPDUs se bloquean y escuchan.
  - **Escuchando** → BPDUs escuchan y **transmiten** (construyen el árbol)
  - **Aprendizaje** → Aprenden direcciones, BPDUs escuchan y transmiten.
  - **Forwarding** (Reenvío) → Reenvío de frames y direcciones de aprendizaje.
  - **Disabled** → No se escucha / transmite ningún reenvío de trama y BPDU.
- <u>Timers STP</u>
  - **Hello**: tiempo entre BPDU enviados por un Root Bridge (2 seg)
  - **Forward**: tiempo pasado en los estados de escuchando y aprendizaje (15 seg)

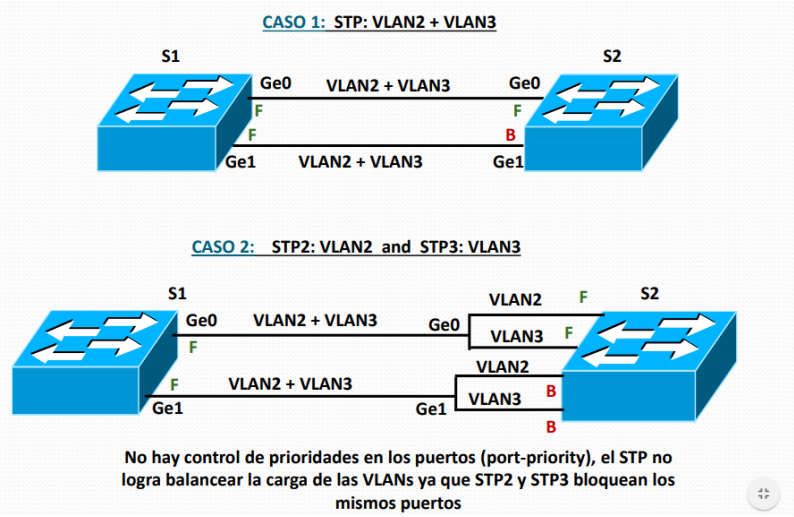
- **Max Age**: Tiempo máximo que tarda en almacenarse una BPDU (20 seg)



https://www.youtube.com/watch?v=japdEY1UKe4

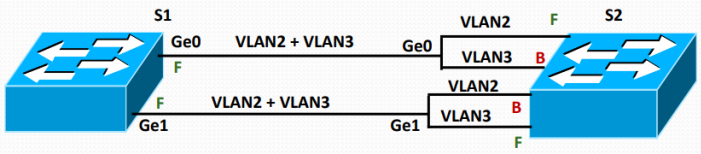
Spanning Tree + VLANs

- Inicialmente, el diseño de STP estaba pensando para una **SOLA VLAN**. (802.1D)
- CISCO **definió PVST** (Per Vlan Spanning Tree) → Una instancia STP por VLAN (no compatible con 802.1Q). Más tarde, PVST+ que si era compatible.
- Entonces, **IEEE** adoptó el concepto de CISCO de **una instancia STP por VLAN**. Lo llamaron **MSTP** (Multiple Spanning Tree Protocol) que fue incluido en el 802.1Q más tarde.
- Ejemplos:



(CUIDADO: En realidad solo hay dos enlaces, pero al haber dos VLANs se representa así)

CASO 3: STP2: VLAN2 and STP3: VLAN3



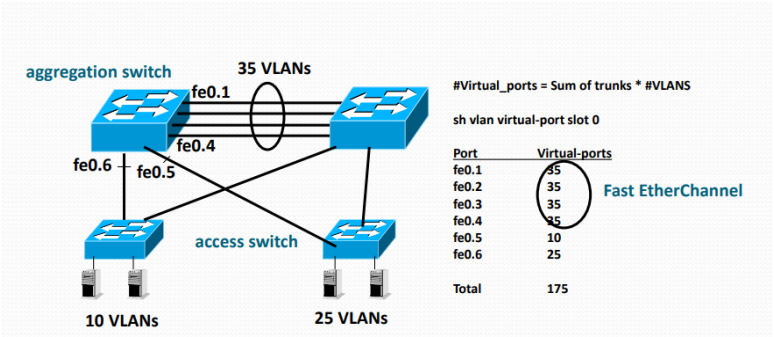
Hay control de prioridades en los puertos (port-priority, value from 0-255, default 128), el STP logra balancear la carga de las VLANs. Cuidado, el port-priority que hay que manipular es el de S1 (el transmisor para que S2 decida)

Para ello hay que poner en la fe0 una prioridad menor en el STP2 (VLAN2) que en la fe1 del mismo STP2. De manera simétrica, hay que poner en la fe0 una prioridad mayor en el STP3 (VLAN3) que en la fe1 del mismo STP3.

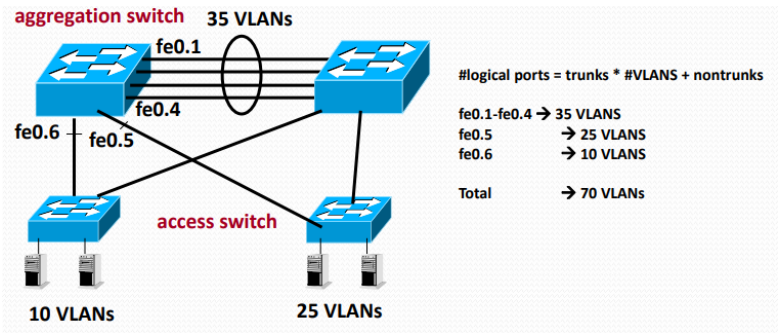
Ahora, los STP2 y STP3 bloquean puertos distintos.

STP + Agregación de enlace (¿Cómo lo trata STP?)

- FastEthernet con 4 puertos paralelos suele funcionar con balanceo de carga de flujo.
- ¡Los enlaces paralelos **son tratados por STP como un enlace único**!
- Dos casos:
  - **Virtual Ports** → Refleja el número total de VLANs soportadas por trunks en una Line Card y un límite en el número de instancias del spanning tree en una Line Card. (cada línea puede tener varias interfaces, ej. Line Card Fe0 fe0.0, fe0.1, fe0.2)



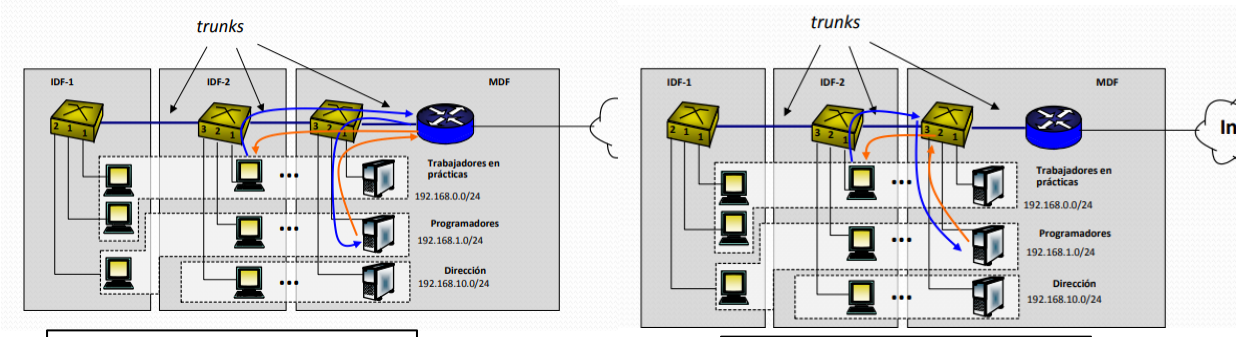
  - **Logical Ports** → Número de instancias STP en todo el sistema de conmutación.



Switches MultiLayer (MLS) o switches L3

- Es un dispositivo de red que tiene la capacidad de operar en capas altas del modelo OSI (examinan de la 2 a la 7).
- Tradicionalmente, los switches envían datos basados en la capa 2 y los routers capa 3. **Característica clave MultiLayer**: Puede realizar las funciones de un switch como las de un router a velocidades increíblemente rápidas.
- Funcionamiento:

  La primera vez que un datagrama IP para un router cruza un MLS-switch; este registra el flujo de alguna de estas maneras: 1. La IP de destino 2. IP origen y destino 3. Direcciones IP y puertos. Activa MLS usando una cache (primera vez, necesario mirar la routing table, para llenarla). Cualquier paquete IP de ese flujo que llegue al switch será **rápidamente** enrutado hacia su destino**. → HACE DE ROUTER.**



Caso router cuello de botella

Caso MLS-Switch

Tolerancia a fallos en L3 (Capacidad de seguir funcionando en caso de fallo)

- **Objetivo del Host:** Obtener un default route para dejar la red. Solución:

  Dynamic routing → Configuración dinámica de enrutamiento por defecto → Es tolerante a fallos por definición, ya que en caso de error reconfigura cualquier tabla de enrutamiento.
- Pero, la mayoría de hosts y servers usan **una ruta predeterminada estáticamente** configurada o obtenida a través de DHCP. → Si un punto falla, el host pierde conectividad.

ARP gratuito

- **(REPASO) ARP** → A partir de una @IP descubre la @MAC de otros dispositivos (hosts/routers) que pertenecen a la misma red. Almacenan estas resoluciones en una tabla ARP. @IP → @MAC.
- **ARP gratuito** → Paquete de solicitud ARP donde tanto la @IP origen y la de destinación son iguales (del host origen) y la @MAC de destino es ff:ff:ff:ff:ff:ff (broadcast address).
- Sus utilidades son:
  - Detectar conflictos IP → Debido a @IPs duplicadas (IMPORTANTE)

- Forzar a actualizar la entrada de la tabla correspondiente sin peticiones directas
- Limpiar tablas ARP

Virtual Router Redundancy Protocol (VRRP) → Estándar de HSRP CISCO

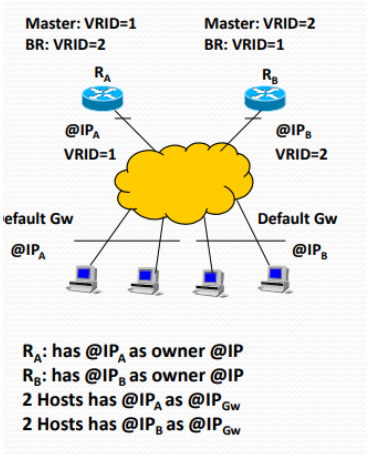
- Diseñado para eliminar puntos de fallo relacionados con las rutas predeterminadas estáticas. ¡Proveyendo redundancia!
- VRRP permite configurar dos o más routers de manera que una de sus interfaces comparta una dirección IP y una dirección MAC "virtual".
- Terminología importante:
  - **VRRP router** → Router que ejecuta el protocolo VRRP
  - **Virtual router** → Objeto abstracto utilizado por VRRP que actúa como default router para los hosts de una VLAN. → 1 owner + 1 o más backups
  - **@IP owner** → El VRRP router que tiene la @IP física del virtual router.
  - **@IP primaria** → @IP seleccionada del conjunto de @IPs físicas
  - **Virtual router master** → Es el VRRP router responsable del envío de paquetes IP.
  - **Virtual router backup** → Es el router que hace de backup que coge la responsabilidad de master en caso de fallo del router master.
- Funcionamiento:

  VRID=1 identifica un Virtual Router y está asociado a la @IPa, mientras que VRID=2 identifica un Virtual Router y está asociado a la @IPb

  Se activa VRRP tanto en Ra como Rb, y VRID=1 se convierte en master con 255 y VRID=2 como backup. Con Rb pasa lo mismo.

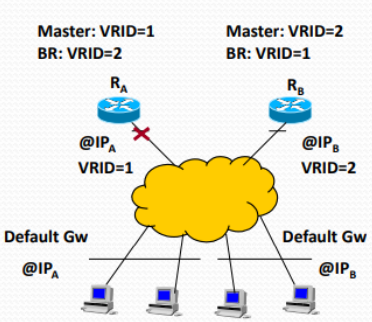
  Mientras ambos routers trabajen bien → **load balancing**

  Si uno de los dos falla, el otro cogerá la responsabilidad de ser el master como el default Gw.



- Mientras el **router trabaja como master**, tiene una @IP asociada al virtual router. En estado master, el router:
  - Debe responder a solicitudes ARP dirigidas a la @IP asociada al virtual router. Utiliza una virtual @MAC (no es fisica). Siempre será 00-00-5E-00-01-VRID.
  - Debe enviar paquetes con @MAC destino = @MAC del virtual router.
  - No debe aceptar paquetes dirigidos a la @IP asociada al router virtual el cual no es propietario @IP.
  - Debe aceptar paquetes dirigidos a la @IP asociada al virtual router.

- Mientras el **router trabaja como backup**, el router:
    - No debe contestar a los ARP requests dirigidas a @IP asociadas al virtual router
    - Debe descartar paquetes con @MAC destino = @MAC del virtual router
    - No debe aceptar paquetes dirigidos a la @IP asociada al virtual router.
- **En caso de fallo:** (ARP gratuito)



R_A: has $@IP_A$ as owner @IP
R_B: has $@IP_B$ as owner @IP
2 Hosts has $@IP_A$ as $@IP_{Gw}$
2 Hosts has $@IP_B$ as $@IP_{Gw}$

R_A fails: R_B detects the master failure (VRRP messages are not listened) and detects that there is n other backup with higher priority than himself

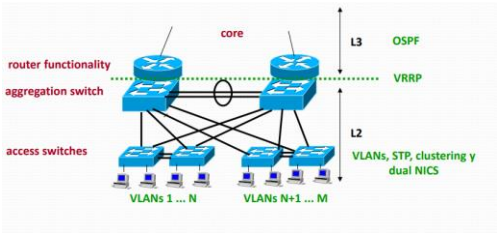
R_B sends ARP gratuitous in order that all Hosts "clean" their ARP cache and will update switching tables creating new L2 routing towards R_B

ARP gratuitous → If A fails and B sends a ARP request with $@IP_{dst}$= $@IP_{src}$=$@IP_A$ and $@MAC_{dst}$= broadcast and $@MAC_{src}$= $@MAC_{virtual\text{-}ID=1}$ → all hosts will refresh their ARP table with the MAC that B wants to associate to the $@IP_A$

VRRP does that with the virtual MAC

Mirar ejemplo en el power, pag 43 (con su configuración respectiva) → VRRP+STP+VLANs

Data Processing Centers (CPD)



- Un CPD/ centro de datos es una instalación que se utiliza para alojar sistemas informáticos y componentes asociados, como sistemas de telecomunicaciones y almacenamiento.
- Generalmente incluyen:
    - Fuentes de alimentación redundantes o de respaldo
    - Datos redundantes
    - Conexiones de comunicaciones de datos redundantes
    - Controles ambientales (aire acondicionado, extinción de incendios…)
    - Dispositivos de seguridad

+ Tier → Indica el nivel de fiabilidad de un centro de datos.

- Los CPD se clasifican por **Tier Levels:** (hay cuatro niveles; de menor a mayor fiabilidad)

Tier I: Centro de datos Básico: Disponibilidad del 99.671%.

- El servicio puede interrumpirse por actividades planeadas o no planeadas.
- No hay componentes redundantes en la distribución eléctrica y de refrigeración.
- Puede o no puede tener suelos elevados, generadores auxiliares o UPS.
- Tiempo medio de implementación, 3 meses.
- La infraestructura del datacenter deberá estar fuera de servicio al menos una vez al año por razones de mantenimiento y/o reparaciones.

Tier II: Centro de datos Redundante: Disponibilidad del 99.741%.

- Menos susceptible a interrupciones por actividades planeadas o no planeadas.
- Componentes redundantes (N+1)
- Tiene suelos elevados, generadores auxiliares o UPS.
- Conectados a una única línea de distribución eléctrica y de refrigeración.
- De 3 a 6 meses para implementar.
- El mantenimiento de esta línea de distribución o de otras partes de la infraestructura requiere una interrupción de las servicio.

Tier III: Centro de datos Concurrentemente Mantenibles: Disponibilidad del 99.982%.

- Permite planificar actividades de mantenimiento sin afectar al servicio de computación, pero eventos no planeados pueden causar paradas no planificadas.
- Componentes redundantes (N+1)
- Conectados múltiples líneas de distribución eléctrica y de refrigeración, pero únicamente con una activa.
- De 15 a 20 meses para implementar.
- Hay suficiente capacidad y distribución para poder llevar a cabo tareas de mantenimiento en una línea mientras se da servicio por otras.

Tier IV: Centro de datos Tolerante a fallos: Disponibilidad del 99.995%.

- Permite planificar actividades de mantenimiento sin afectar al servicio de computación críticos, y es capaz de soportar por lo menos un evento no planificado del tipo 'peor escenario' sin impacto crítico en la carga.
- Conectados múltiples líneas de distribución eléctrica y de refrigeración con múltiples componentes redundantes (2 (N+1) significa 2 UPS con redundancia N+1).

- **Alta disponibilidad** (HA): → Busca dar continuidad ininterrumpida a un servicio.

Las aplicaciones, los equipos de red (servers, routers, switches) y las interfaces de red pueden fallar y por tanto interrumpir el servicio. Es por eso que es necesario mejorar la tolerancia a fallos y garantizar una mayor disponibilidad. ¿Cómo?

- **Aplicaciones** → Scripts automáticos para reiniciar procesos
- **L2** → STP maneja tolerancia a fallos en L2
- **L3** → VRRP y OSPF (tema 3) maneja tolerancia a fallos en L3.
- **Equipamiento** → Mejorar el rendimiento del servidor (mediante la agrupación y dual connections como ejemplo)

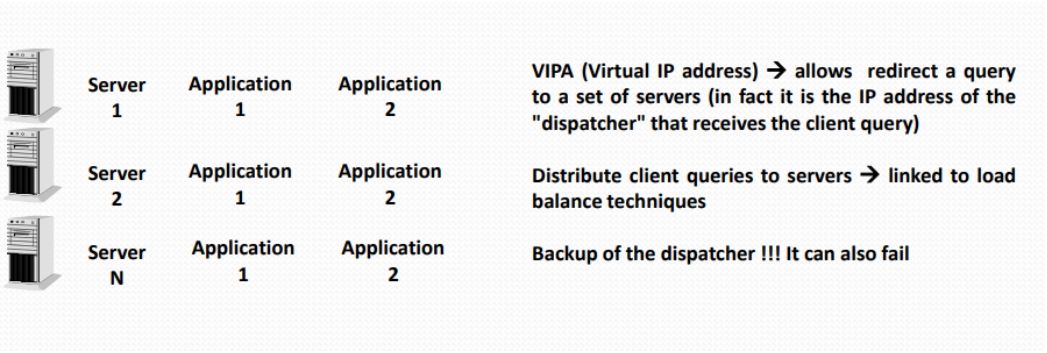
- **Escalabilidad / Scalability** → Reaccionar ante el crecimiento de la empresa sin perder la calidad del servicio.

  Que implica un crecimiento en el número de conexiones de red, en la capacidad de la red y de las capacidades del cómputo (es decir, de hacer operaciones)

  Se usan **clusters** como solución para aumentar la capacidad del servidor, la capacidad computacional y la confiabilidad.

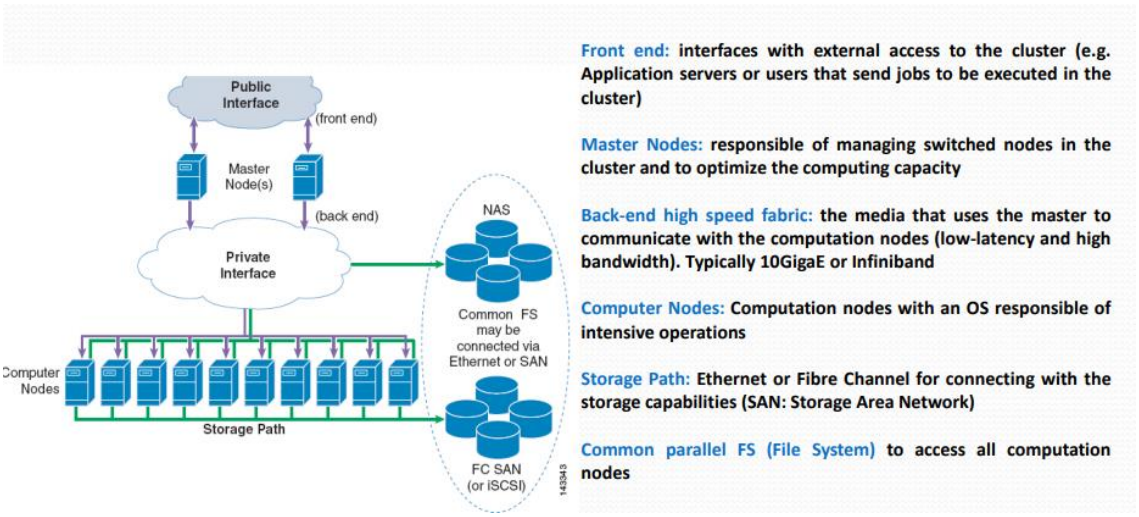
- **Clusters servers** → Se basan en la unión de varios servidores que trabajan como si de uno solo se tratase, unidos mediante una red de alta velocidad.

  Su **objetivo principal:** Ejecutar múltiples aplicaciones en múltiples maquinas.



Los servidores pueden estar interconectados para intercambiar información, en caso de haber más de dos servidores, se interconectan vía LAN.

En general, un cluster necesita de varios componentes de software y hardware para poder funcionar:

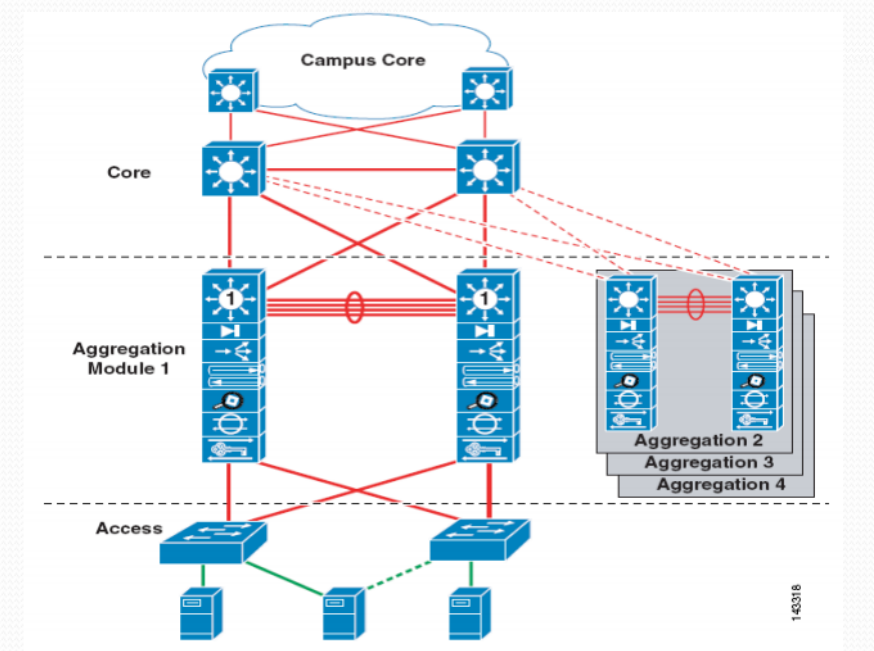


+ Nodos → Simples ordenadores, sistemas multiprocesador o estaciones de trabajo.

+ SAN → Storage Area Network; Es una red dedicada al almacenamiento que está conectada a las redes de comunicación de una compañía.

Load Balancing /Balanceo de carga → Si hay varias líneas que interconectan los servidores, podemos distribuir la carga de tal manera que tiende a ser más **simétrico** (es decir, cargas equivalentes para cada uno de los servidores)

- La típica técnica de diseño de CPDs en muchas compañías tiene esta pinta: (3 capas diferentes)



- Capa **Core/central** → Conecta la capa Campus Core (capa de distribución) con la capa de agregación del CPD.

  Da una alta velocidad de conexión hacia los módulos de agregación. Pero, no siempre es requerido. 10 GEth ports. Normalmente, con switches L3 (switches con funciones de router, NO routers)

- Capa de **Agregación** → Agrega miles de conexiones que quieren acceder al CPD.

  Switch de agregación → Suelen ser Multilayer Switch (Switches multinivel), son switches que funcionan como un switch ordinario y proporcionan además funcionalidades extra de los otros niveles más altos del OSI.

  Los switches de agregación deben ser capaces de admitir muchas interconexiones de 10 GigE a la vez que proporcionan una alta tasa de reenvío.

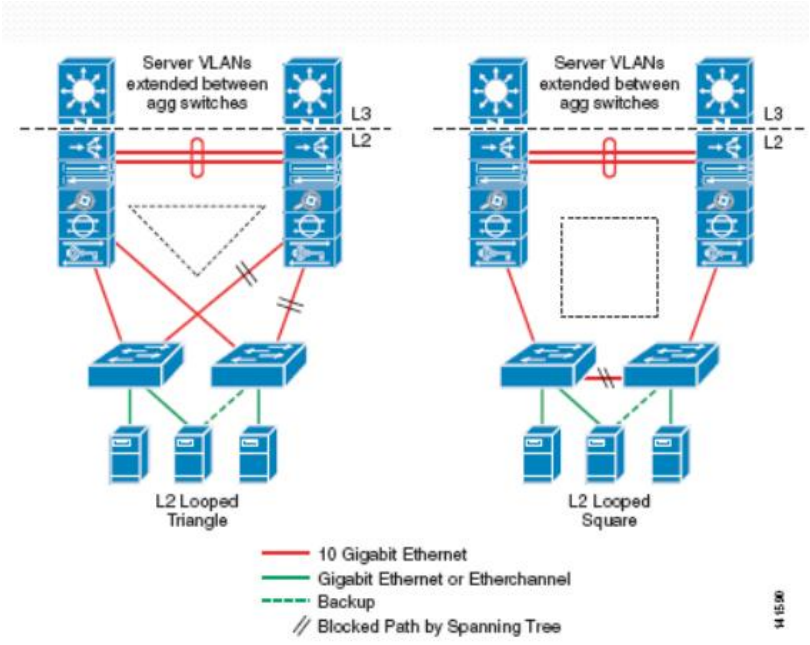
  Llevan la carga de trabajo del procesamiento de STP y del default gateway redundancy protocol.

- Capa de **Acceso** → Da un punto de conexión a los servidores y opera tanto en L2 como en L3.

  Desempeña un papel fundamental en el cumplimiento de los requisitos del servidor. Es, además, el primer **punto de sobresuscripción** en el CPD.

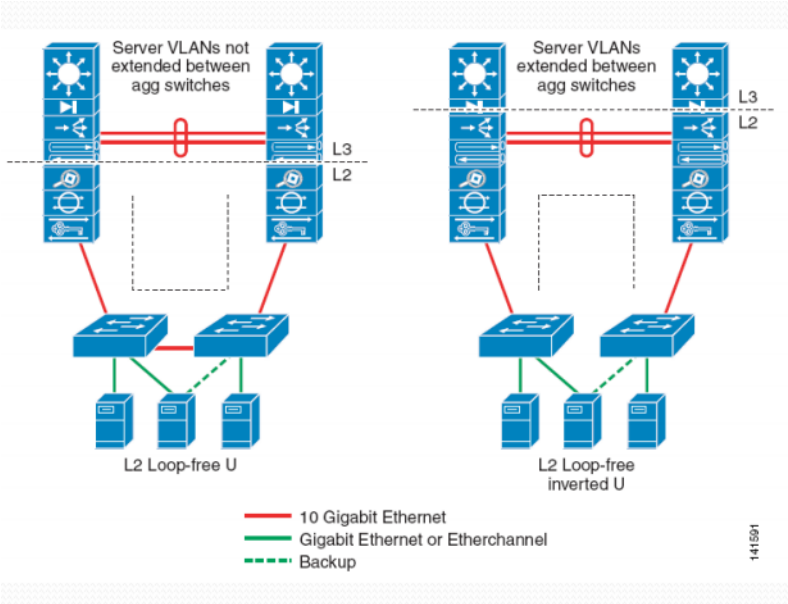
- **SIEMPRE se busca redundancia** → Al menos un par de switches interconectados con STP. Con configuraciones **en bucle** como triangulo y cuadrado o **sin bucle (looped-free)** como U o U-down.

- En bucle (triangulo/cuadrado)**:**



(mirar en caso de fallo que pasa en las dos topologías →pag 68-70)

- Sin bucle (U/U para abajo)



- Diferencias principales en la configuración entre con bucle y sin bucle:
    - Sin bloqueo en los enlaces ascendentes, todos los enlaces están activos en una topología sin bucles.
    - La adyacencia de layer 2 para servidores se limita a un solo par de switches de acceso en una topología sin bucles.
    - La extensión VLAN no se admite en topología U, pero si se admite en topología U-down.
- En cualquier caso, **incluso en topologías sin bucles**, ¡se activa STP para evitar los bucles!
- <u>Cálculos</u> (que se pueden preguntar en el examen)
    - **Throughput** (rendimiento) o **ancho de banda promedio** (por **server**)→ El SO y la NIC (tarjeta de interfaz de red) pueden generar tráfico que ocupa un % de la capacidad del enlace.

      Ej. Un servidor ocupa un 60% de un enlace de 1Gb/s; está ocupando 600 Mb/s.

      Thrput = N*(K Gb/s) / M; donde N = num de puertos hacia la agregación y M = num de puertos de servidor.
    - **Oversupscription ratio** (por **server**) → Número medio de servidores en un enlace para ocupar su capacidad.

      Ej. Un servidor ocupa el 60% de un enlace, entonces es 1/0.6 = 1.6666:1 (porque solo hay un servidor)

      Oversubscr ratio = (R Gb/s)/Thrput (Gb/s):1; donde R es la velocidad del acceso.
    - **Oversupscription ratio** (por **switch**) → Igual que el anterior, pero para ocupar un enlace ascendente(uplink) de un switch.

  Tenemos que tener en cuenta todos los enlaces conectados a los servidores y todos los enlaces agregados de enlace ascendente hacia el switch de agregación.

  (Ejemplo pag 79)

Calculate the real bandwidth per server: apply formula a:b = c:d
if the access has 416 Mbps and the aggregation has 1.5:1 oversubscription, then

2.4:1 = x:1.5 → x=3.6 → 3.6:1
0.416:1 = x:0.666 → x=277 Mbps