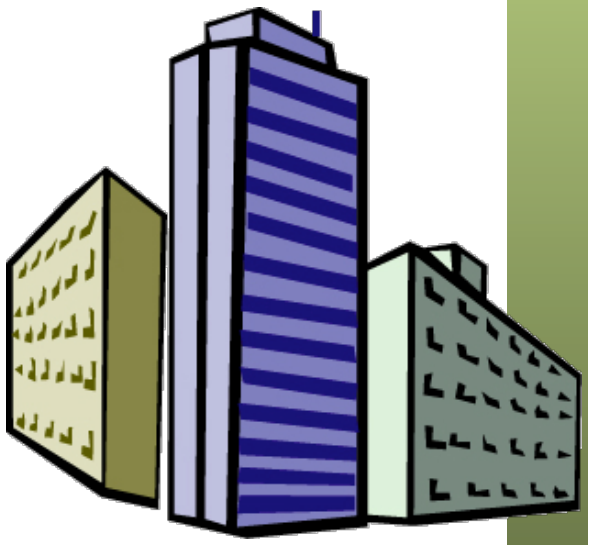
Diseño de Campus LAN (parte 1)

Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 3º

Campus LAN

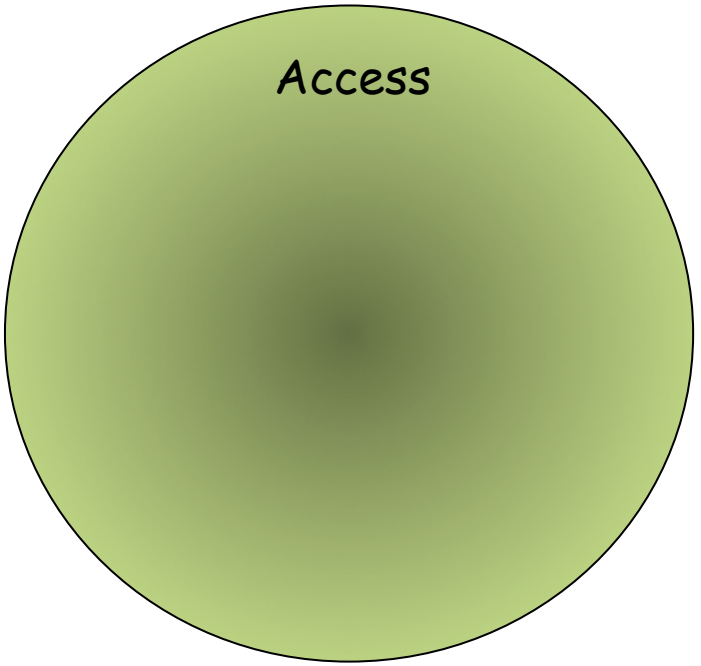
- Un conjunto de edificios próximos entre sí (distancias de LAN)
- Por ejemplo una empresa con varios edificios en un parque empresarial
- O el campus de una universidad centralizada
- Puede tener conexión a sedes remotas a través de una WAN (no es parte del campus)
- Alta disponibilidad es crucial
- Los edificios suelen compartir los servicios de un CPD (Centro de Procesado de Datos)
- No entramos en diseño de redes para grandes CPDs



Terminología de 3 capas

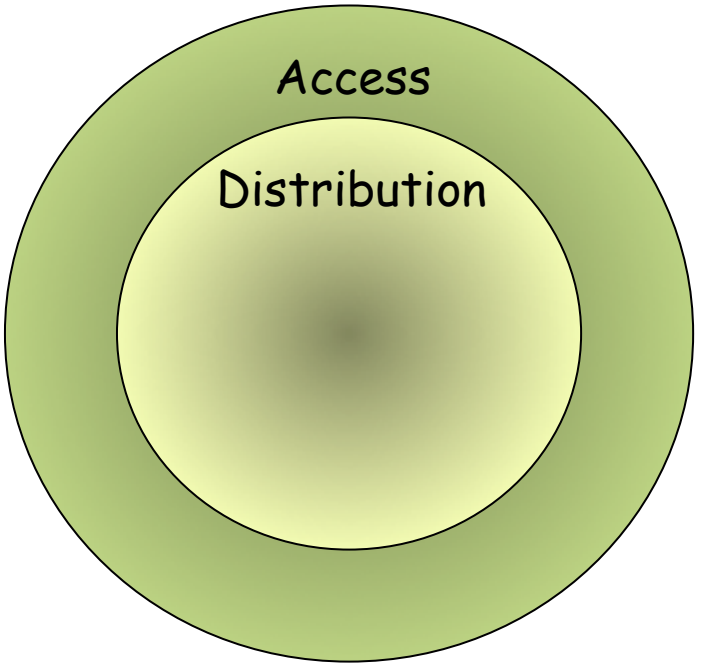
Terminología para 3 capas

- **Access**
  - Acceso de los usuarios a la red
  - Usuarios locales o remotos
  - Debe dar acceso solo a usuarios autorizados
  - IDF (Intermediate Distribution Frame)
  - Hay que tener en cuenta:
    - Número de usuarios
    - Aplicaciones
    - Uso de VLANs
    - Redundancia



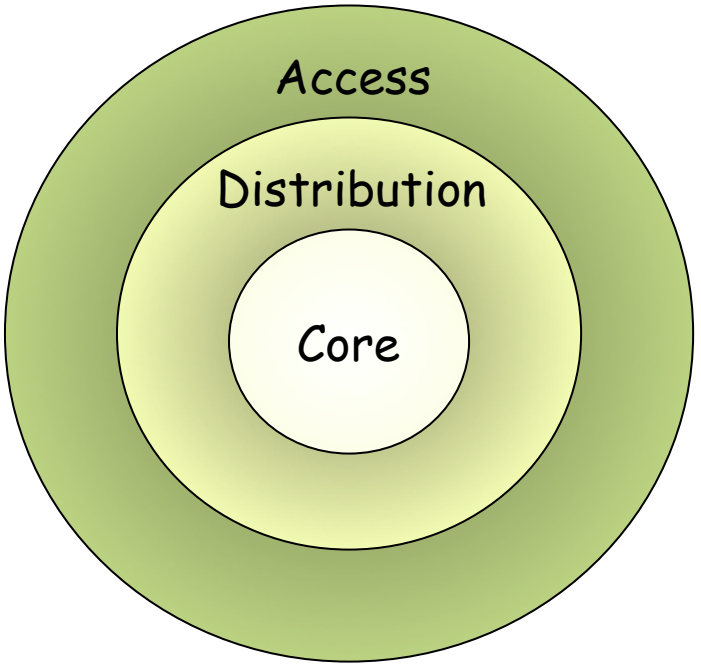
Terminología para 3 capas

- **Distribution/Agregación**
  - Conexión entre grupos de trabajo y de ellos al núcleo
  - Agrega accesos de baja velocidad en enlaces de alta velocidad
  - Aplica políticas de filtrado y prioridad de tráfico
  - Resumir rutas
  - Ofrecer conexiones redundantes
  - MDF (Main Distribution Frame)
  - Hay que tener en cuenta:
    - Número de conmutadores a agregar
    - Redundancia
    - Routing
    - Tipo de interfaces del “core”



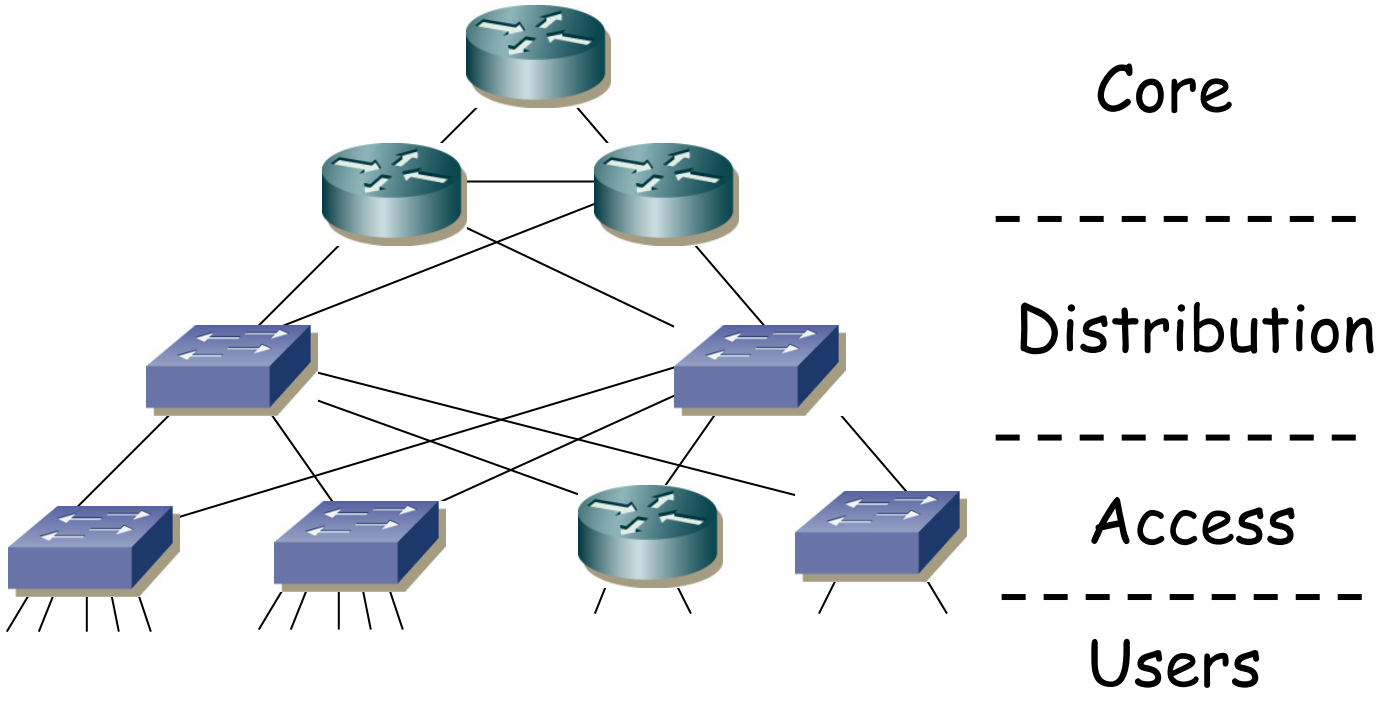
Terminología para 3 capas

- **Core**
  - Backbone de alta velocidad y baja latencia
  - Alta disponibilidad (redundancia)
  - Transporte entre los dispositivos de distribución
  - Rápida adaptación a cambios en el enrutamiento



Terminología para 3 capas

- **Access**: Acceso de los usuarios a la red
- **Distribution**: Conexión entre grupos de trabajo y de ellos al núcleo
- **Core**: Transporte de alta velocidad entre los dispositivos de distribución



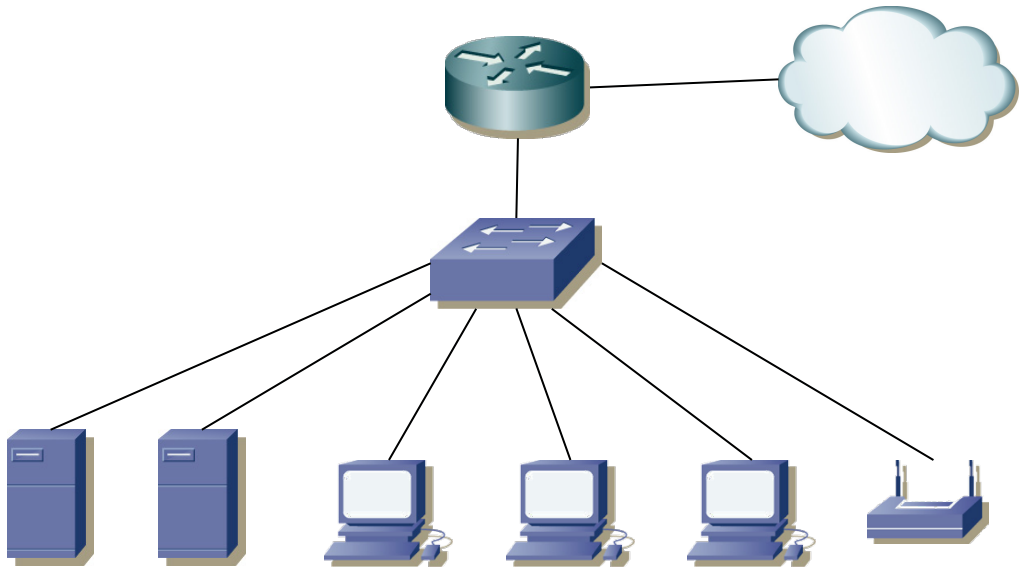
Diseño para pequeño número de usuarios

Pocos usuarios

- Unas pocas decenas de usuarios
- Cuidado con las diferentes “calidades” en los equipos (particulares, empresa, operadora...)
- Hoy en día al escritorio al menos 100Mbps
- Probablemente ya no tenga sentido ni eso, Gigabit es asequible
- Puede ser switch Gigabit pero forzar los puertos a FastEthernet para controlar el flujo de los usuarios
- Conmutación capa 3 (...)

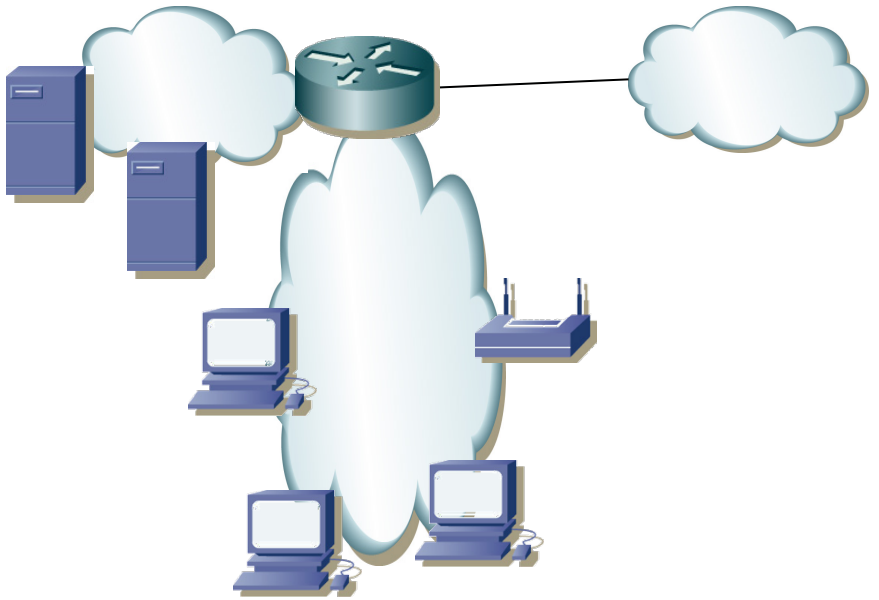
Access

Users



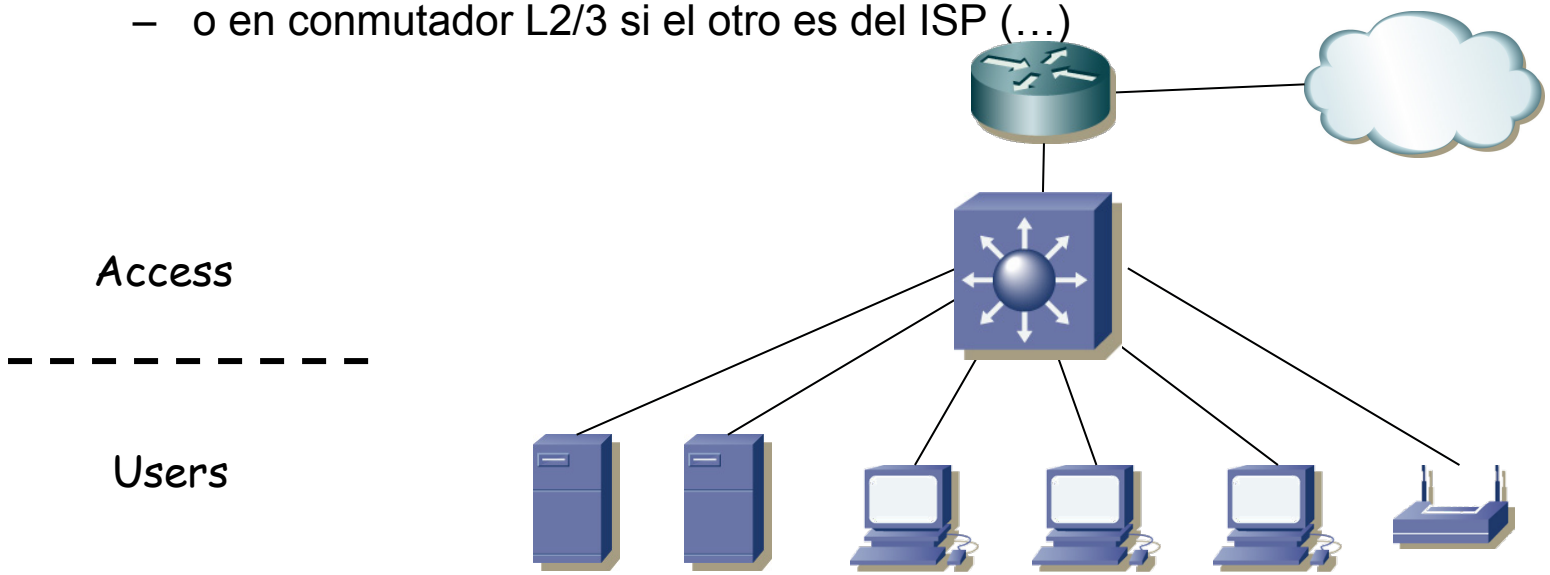
Pocos usuarios

- Unas pocas decenas de usuarios
- Cuidado con las diferentes “calidades” en los equipos (particulares, empresa, operadora...)
- Hoy en día al escritorio al menos 100Mbps
- Probablemente ya no tenga sentido ni eso, Gigabit es asequible
- Puede ser switch Gigabit pero forzar los puertos a FastEthernet para controlar el flujo de los usuarios
- Conmutación capa 3
  - En router de acceso
  - o (...)



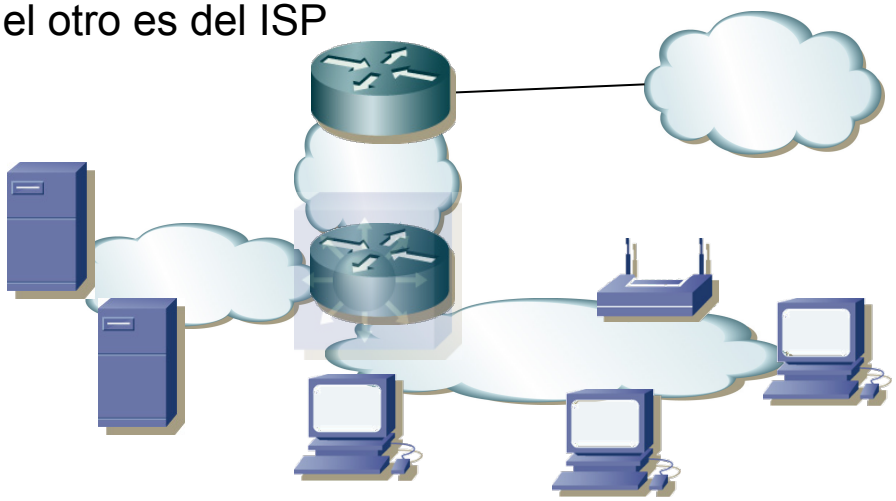
Pocos usuarios

- Unas pocas decenas de usuarios
- Cuidado con las diferentes “calidades” en los equipos (particulares, empresa, operadora...)
- Hoy en día al escritorio al menos 100Mbps
- Probablemente ya no tenga sentido ni eso, Gigabit es asequible
- Puede ser switch Gigabit pero forzar los puertos a FastEthernet para controlar el flujo de los usuarios
- Conmutación capa 3
  - En router de acceso
  - o en conmutador L2/3 si el otro es del ISP (…)



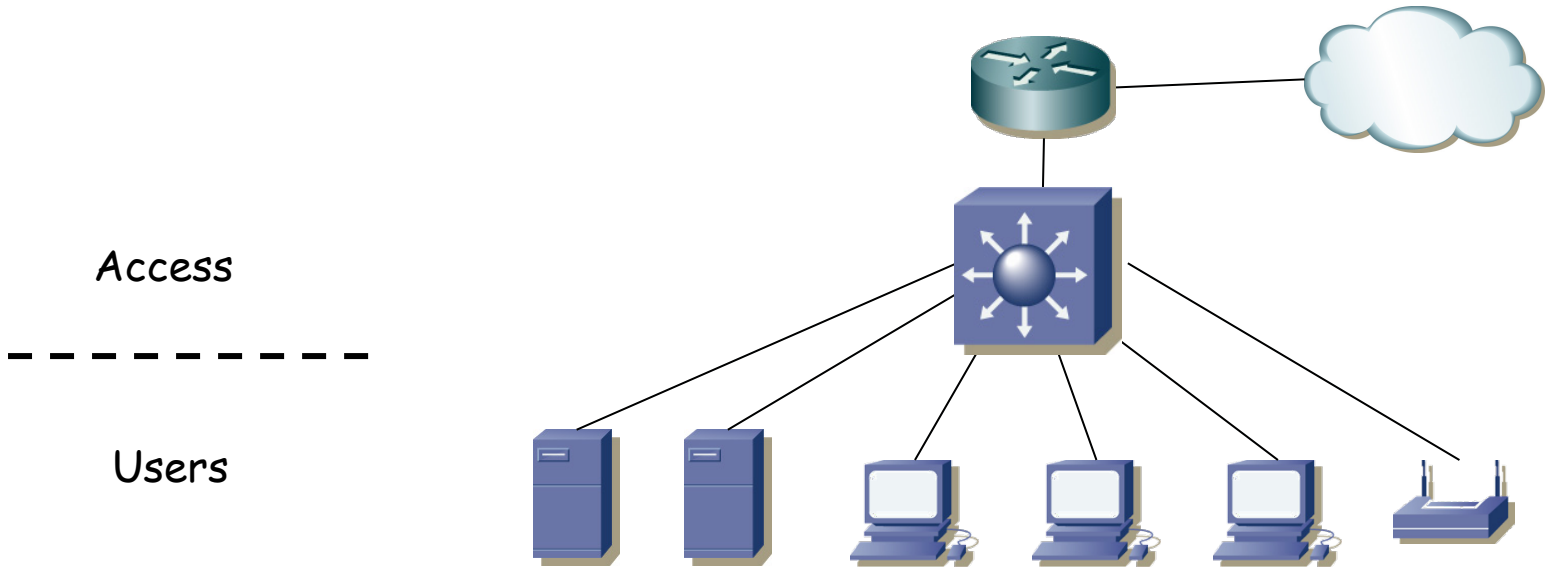
Pocos usuarios

- Unas pocas decenas de usuarios
- Cuidado con las diferentes “calidades” en los equipos (particulares, empresa, operadora...)
- Hoy en día al escritorio al menos 100Mbps
- Probablemente ya no tenga sentido ni eso, Gigabit es asequible
- Puede ser switch Gigabit pero forzar los puertos a FastEthernet para controlar el flujo de los usuarios
- Conmutación capa 3
  - En router de acceso
  - o en conmutador L2/3 si el otro es del ISP



Pocos usuarios

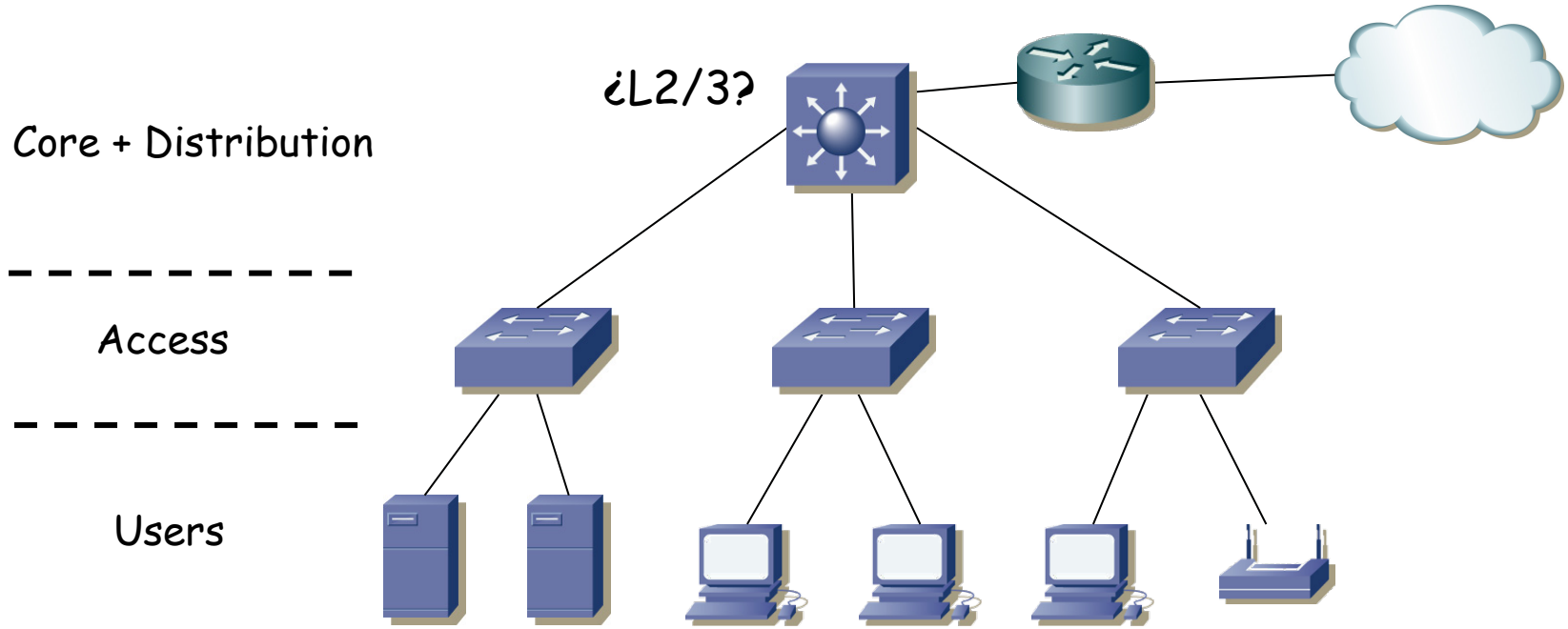
- No hay redundancia en la conmutación interna
- Aunque serviría de poco si los usuarios solo tienen un interfaz
- Tampoco hay redundancia en el acceso
- Pero para una red tan pequeña no suele ser crítico



Collapsed core

Collapsed core (2-tiers)

- Tal vez un centenar de usuarios o más
- Crecimiento añadiendo conmutadores de acceso
- No hay protección pero se activa STP para evitar bucles si alguien conecta algo mal
- Switch de distribución puede hacer tareas de capa 3 (...)



Collapsed core (2-tiers)

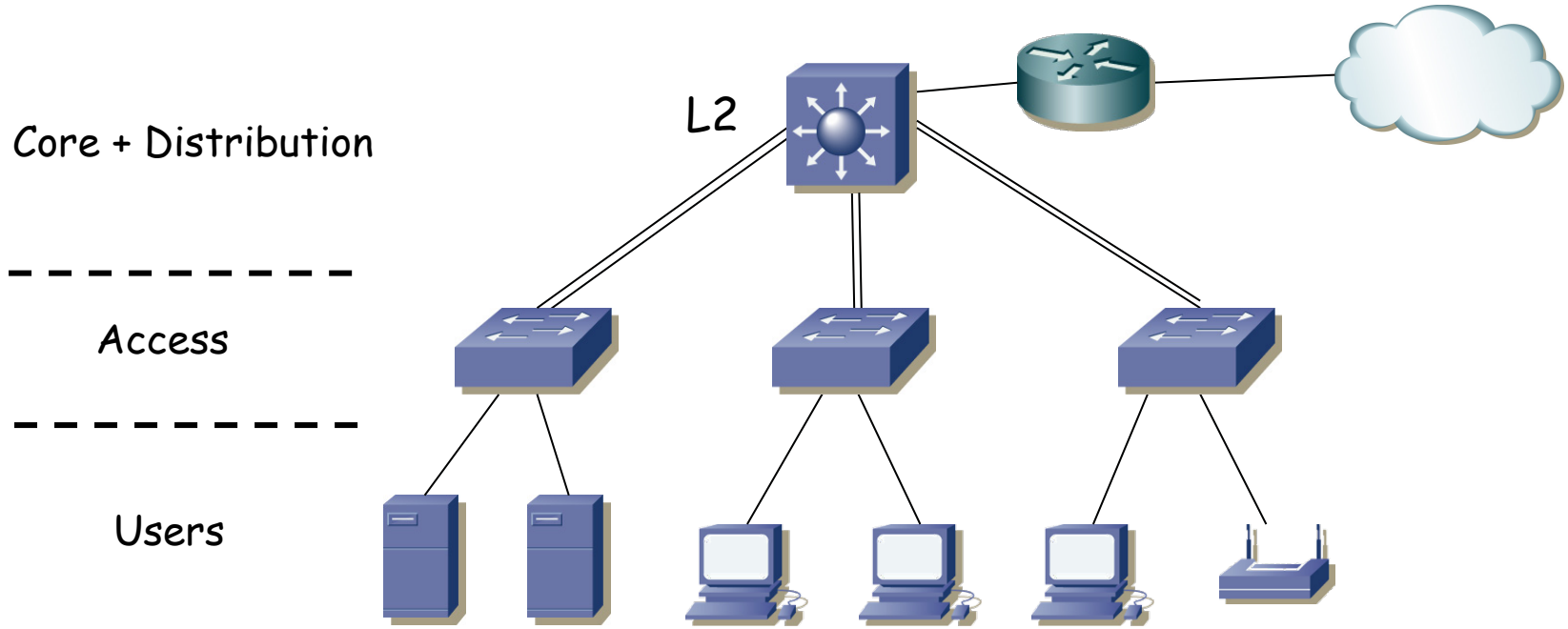
- Tal vez un centenar de usuarios o más
- Crecimiento añadiendo conmutadores de acceso
- No hay protección pero se activa STP para evitar bucles si alguien conecta algo mal
- Switch de distribución puede hacer tareas de capa 3 (...)

Collapsed core (2-tiers)

- Tal vez un centenar de usuarios o más
- Crecimiento añadiendo conmutadores de acceso
- No hay protección pero se activa STP para evitar bucles si alguien conecta algo mal
- Switch de distribución puede hacer tareas de capa 3 o no (entonces varios enlaces al router de acceso o un trunk)
- (...)

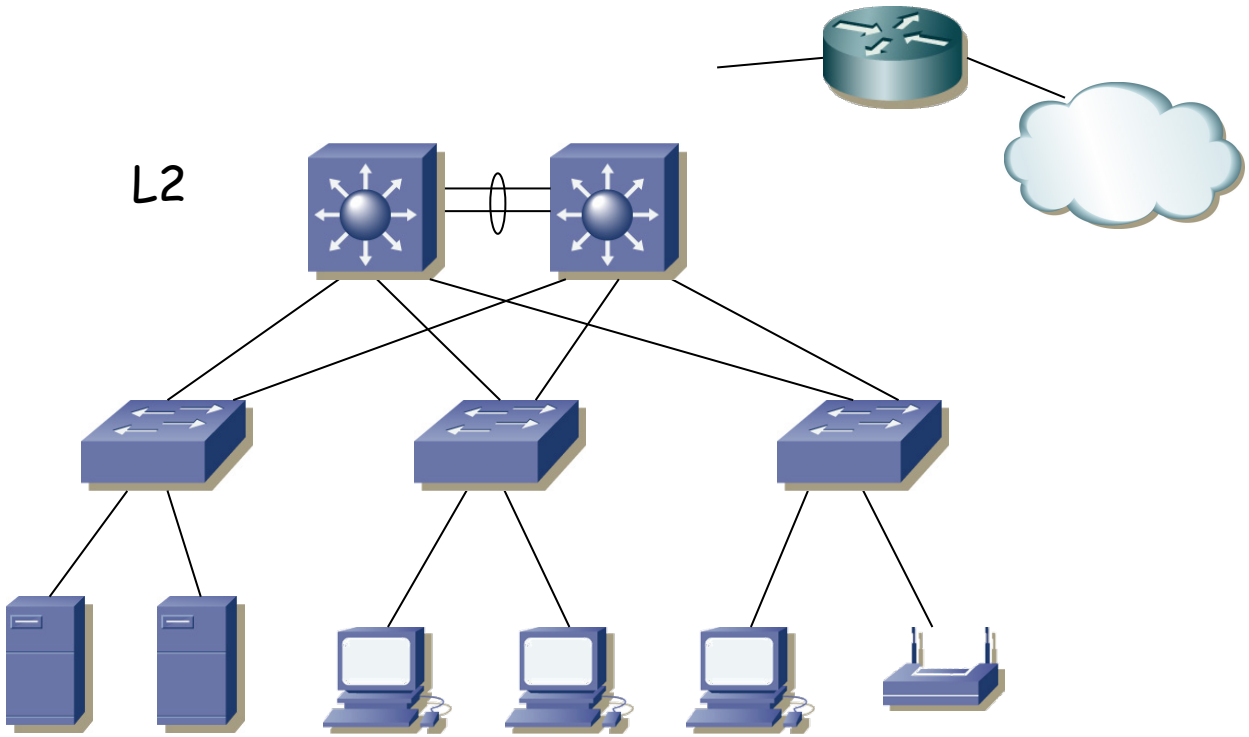
Collapsed core (2-tiers)

- Si la red es crítica, necesitará cierta protección
  - Desactivados con STP (árbol único) o agregados con 802.3ad
  - Cierta redundancia pero topología *loop-free* (si son agregados)
  - Switch de distribución es un punto de fallo



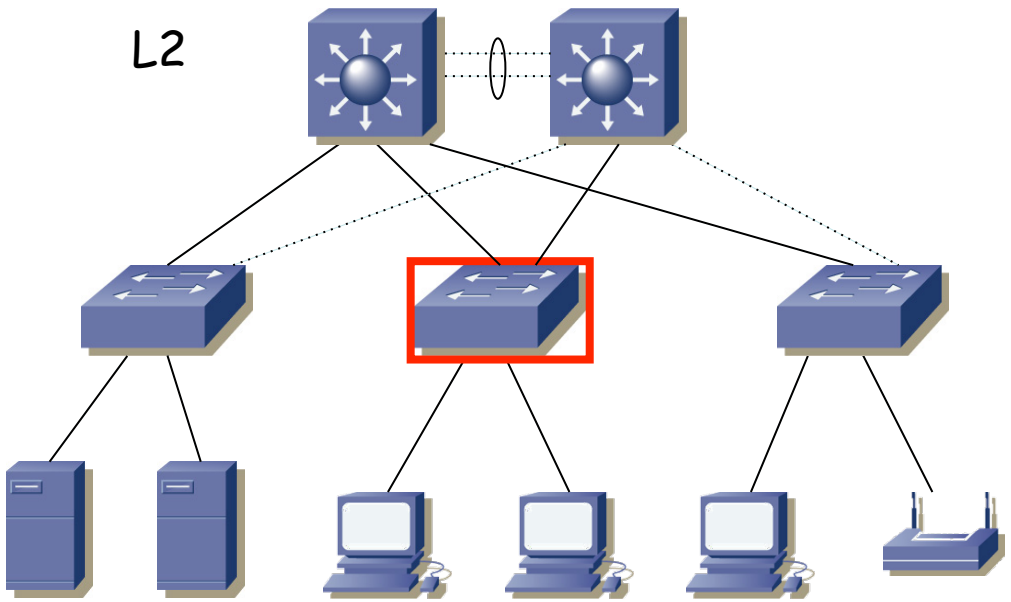
Redundant collapsed core

- Añade redundancia en el sistema de distribución
- Protección ante fallos de enlace acceso-distribución
- Y protección ante fallo de equipo del sistema de distribución
- Interconexión en el sistema de distribución agregada protege ese enlace y aumenta la capacidad
- ¿ Resultado de STP ? (...)



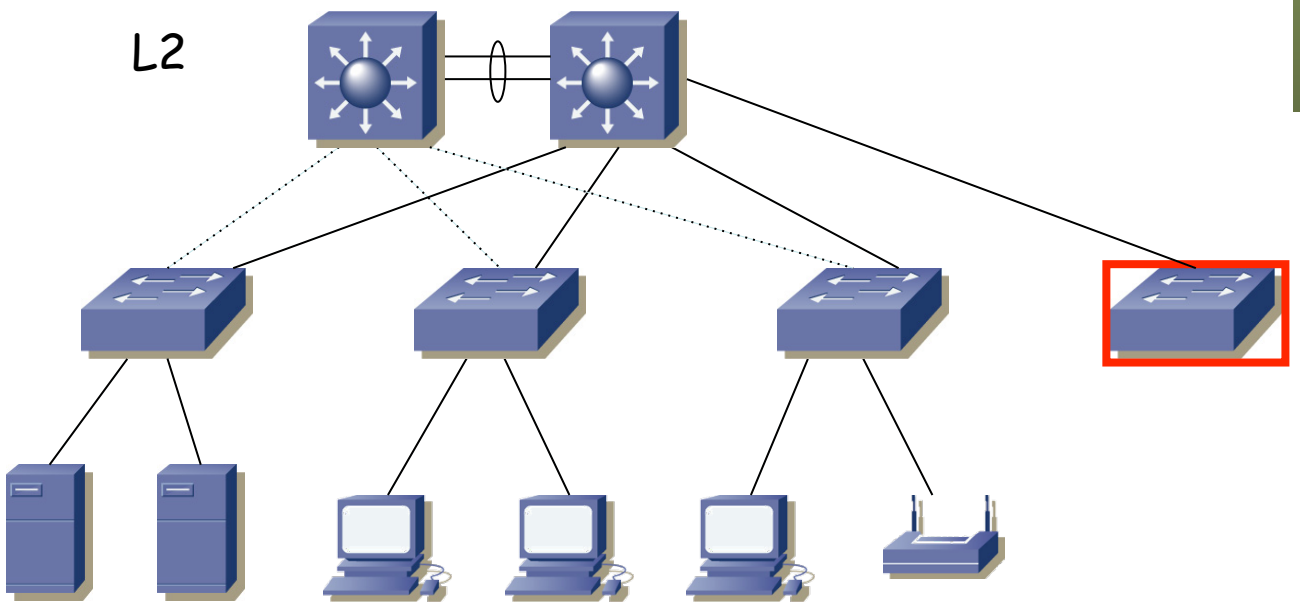
Redundant collapsed core

- Resultado de STP
  - Si el *root bridge* resulta ser uno del acceso y todos los enlaces igual coste
  - Los conmutadores del acceso son más “frágiles” (rotura o apagado), lo cual llevaría a cambios en la topología capa 2
  - Si alguien conecta un switch con menor BID (...)



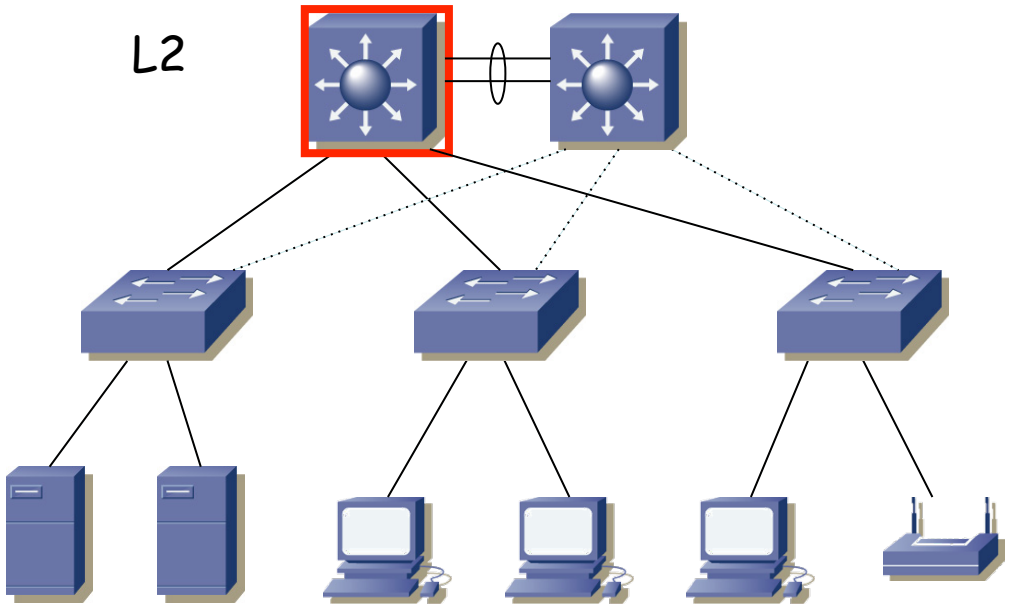
Redundant collapsed core

- Resultado de STP
  - Si el *root bridge* resulta ser uno del acceso y todos los enlaces igual coste
  - Los conmutadores del acceso son más “frágiles” (rotura o apagado), lo cual llevaría a cambios en la topología capa 2
  - Si alguien conecta un switch con menor BID cambia todo el árbol, con la interrupción correspondiente



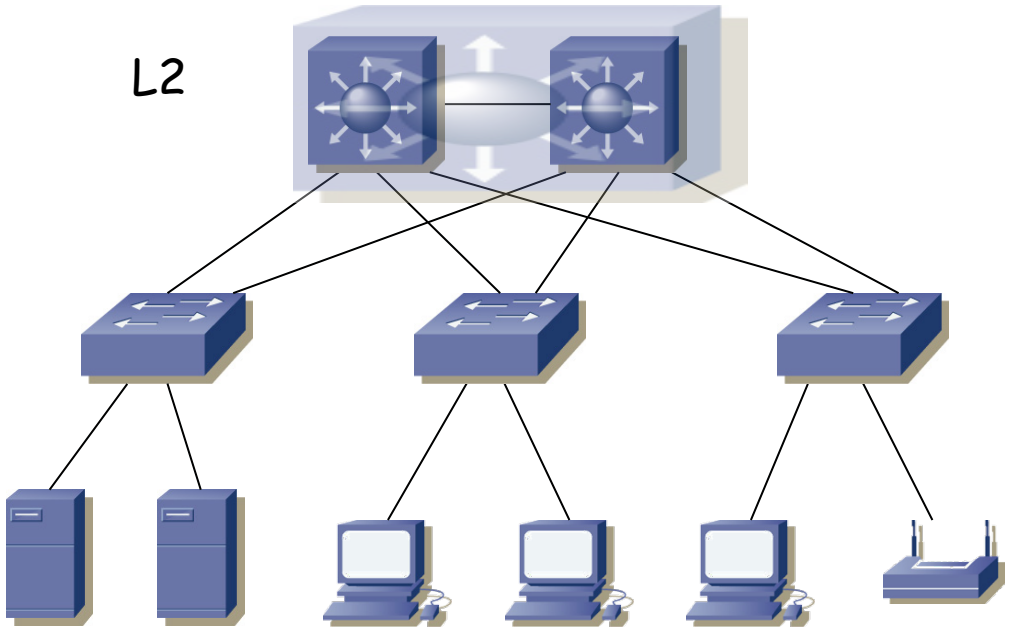
Redundant collapsed core

- Resultado de STP
  - Si el *root bridge* resulta o se configura para ser uno de distribución (con enlaces de igual coste)
  - No hay una gran diferencia en los enlaces activos pero ahora no cambia la topología ante la caída de un switch del acceso
  - Mejor seleccionar el *root bridge* y un secundario
  - En este caso el LAG en la distribución no es muy útil si no hay nada más en el conmutador derecho



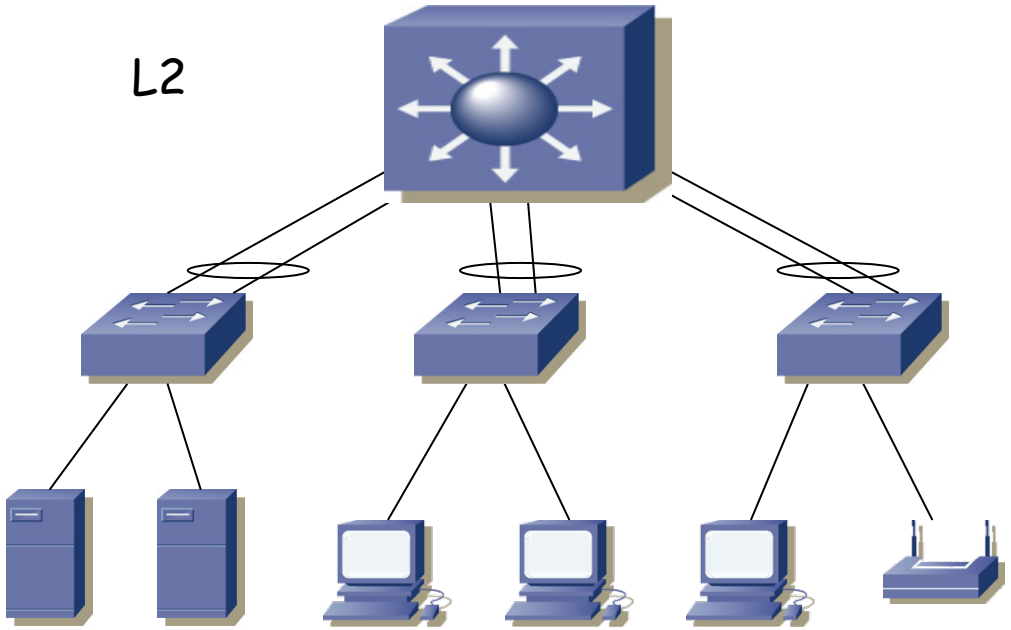
Redundant collapsed core

- Hemos acabado con varios enlaces bloqueados por STP
- Algunos fabricantes ofrecen otras posibilidades para sacar provecho a esos enlaces
- Por ejemplo convertir los dos conmutadores de la capa de agregación en un “conmutador virtual” (...)



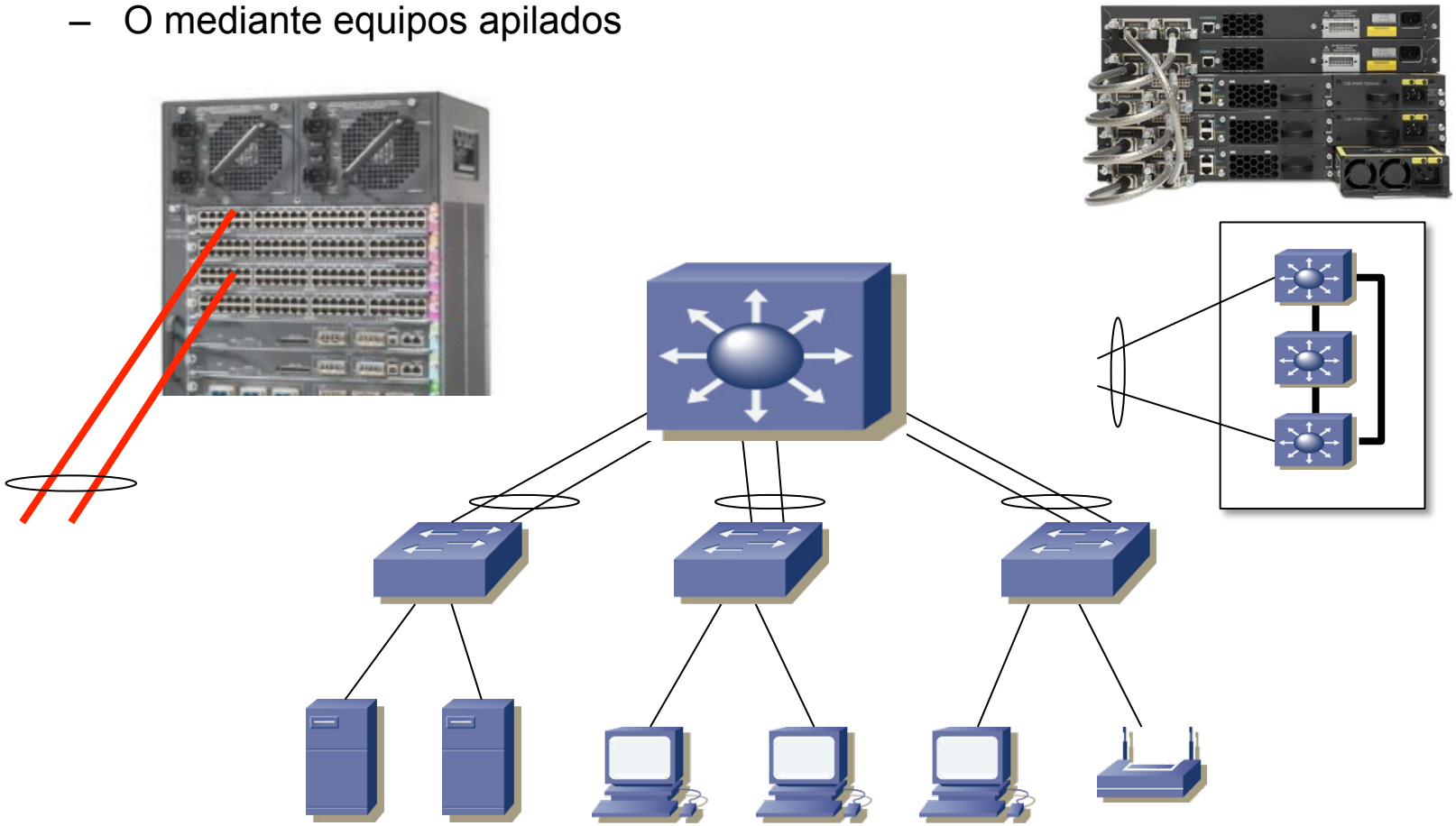
Redundant collapsed core

- Hemos acabado con varios enlaces bloqueados por STP
- Algunos fabricantes ofrecen otras posibilidades para sacar provecho a esos enlaces
- Por ejemplo convertir los dos conmutadores de la capa de agregación en un “conmutador virtual”
- Se comportan como un solo conmutador de cara a STP
- Los enlaces al acceso se convierten en agregados
- Conmutadores de gama alta



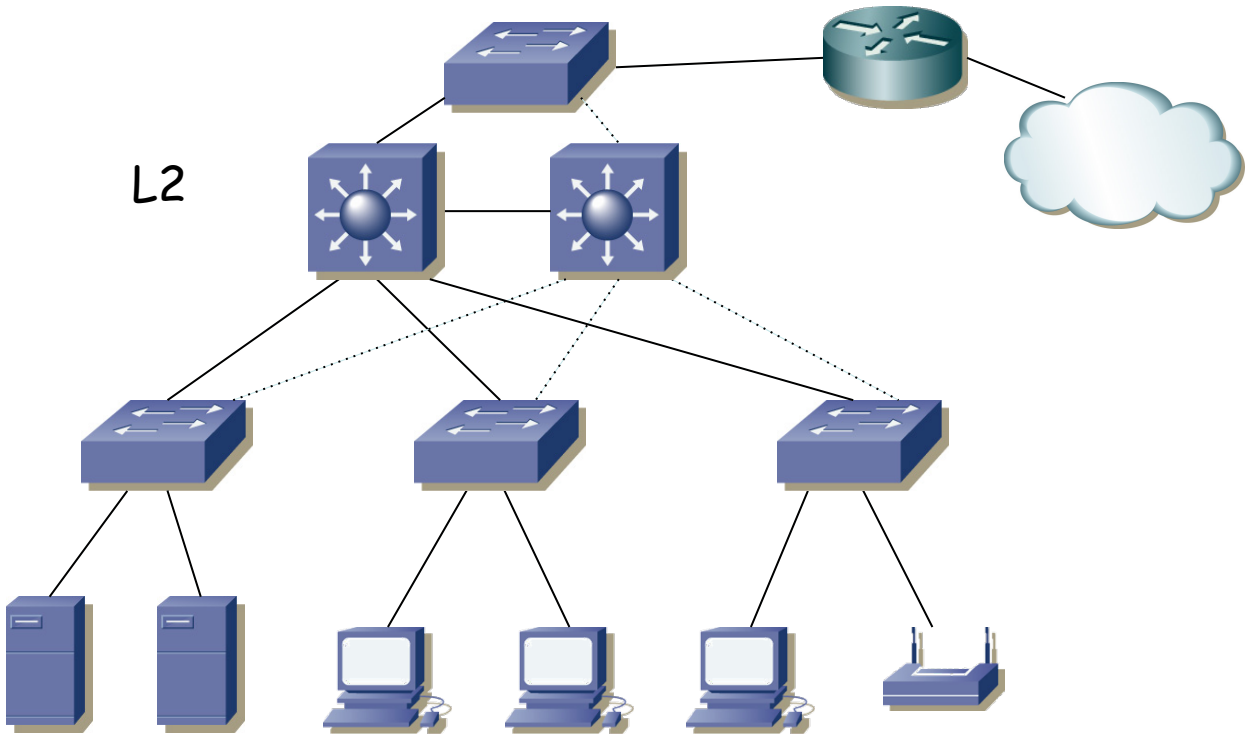
Redundant collapsed core

- Otra alternativa es que ese conmutador L2 tenga alta redundancia:
  - "Engine" redundante (controladora que haga el reenvío, si hay tal cosa)
  - Fuentes de alimentación redundantes
  - Enlaces agregados con los dos puertos en diferentes módulos
  - O mediante equipos apilados



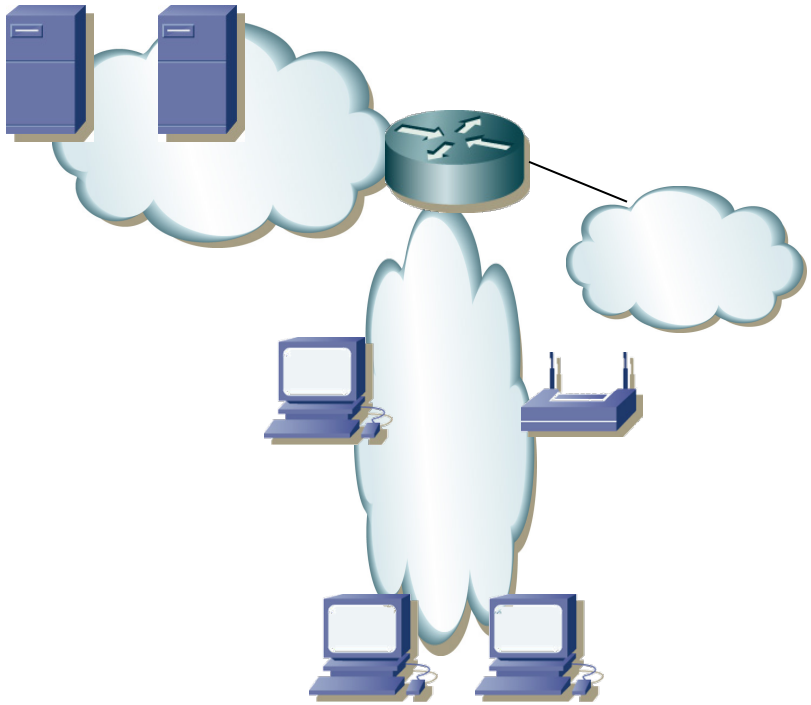
Enrutamiento

- Volviendo al caso con conmutadores de gama media (no se “agregan”)
- ¿Cómo hacemos en encaminamiento capa 3?
- Por ejemplo con un camino redundante hasta el router
- (…)



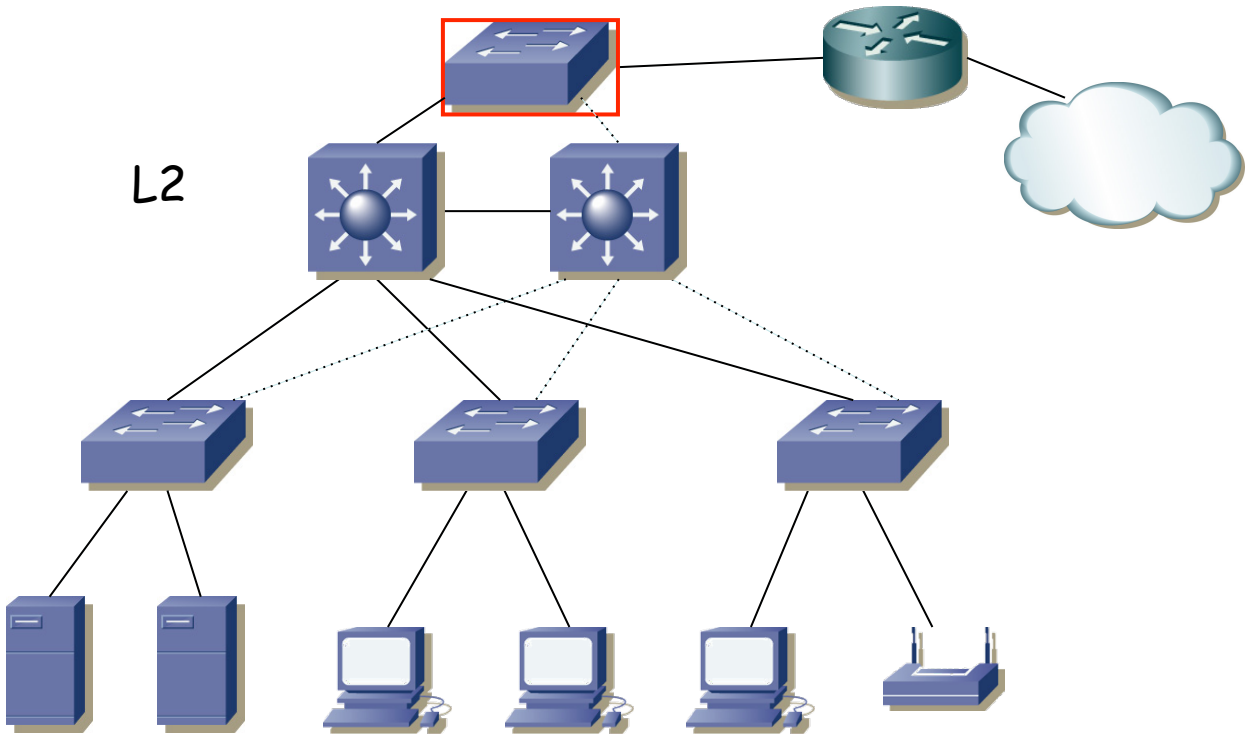
Enrutamiento

- Volviendo al caso con conmutadores de gama media (no se “agregan”)
- ¿Cómo hacemos en encaminamiento capa 3?
- Por ejemplo con un camino redundante hasta el router
- Enrutamos en él, pero tal vez no es lo deseado (que sea del ISP)
- (...)



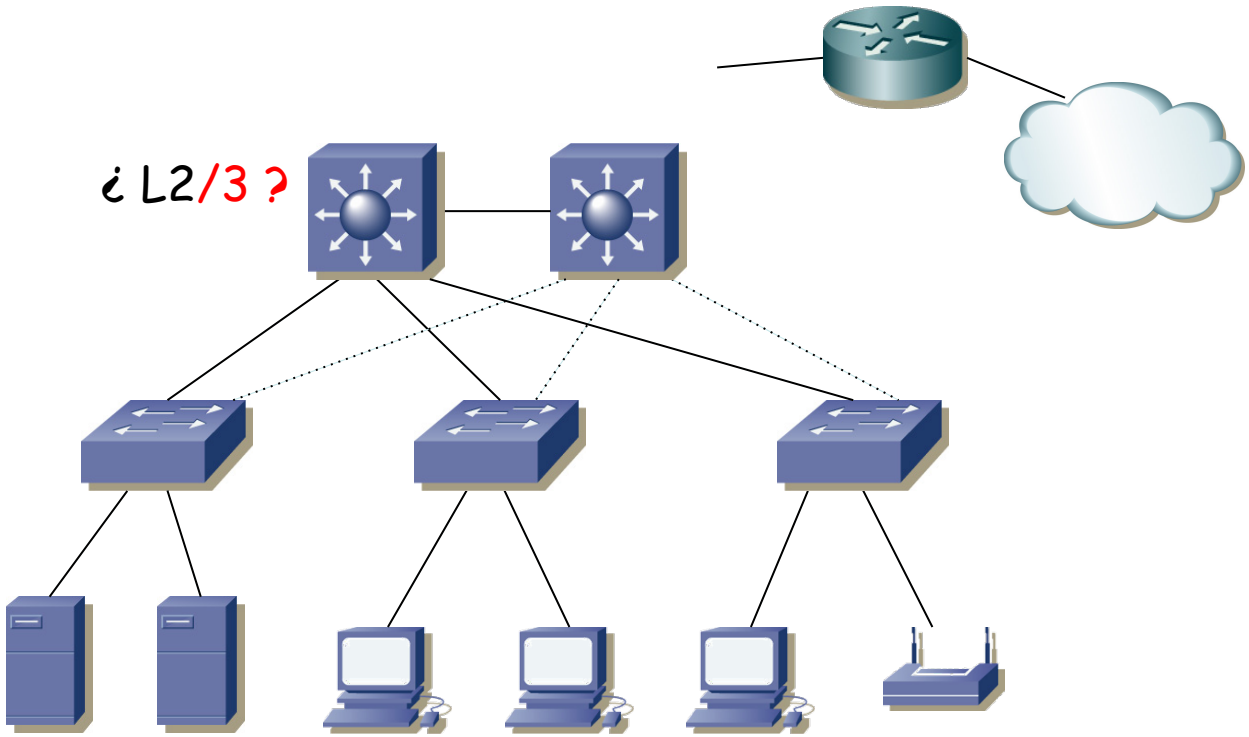
Enrutamiento

- Volviendo al caso con conmutadores de gama media (no se “agregan”)
- ¿Cómo hacemos en encaminamiento capa 3?
- Por ejemplo con un camino redundante hasta el router
- Enrutamos en él, pero tal vez no es lo deseado (que sea del ISP)
- Además volvemos a tener un punto de fallo



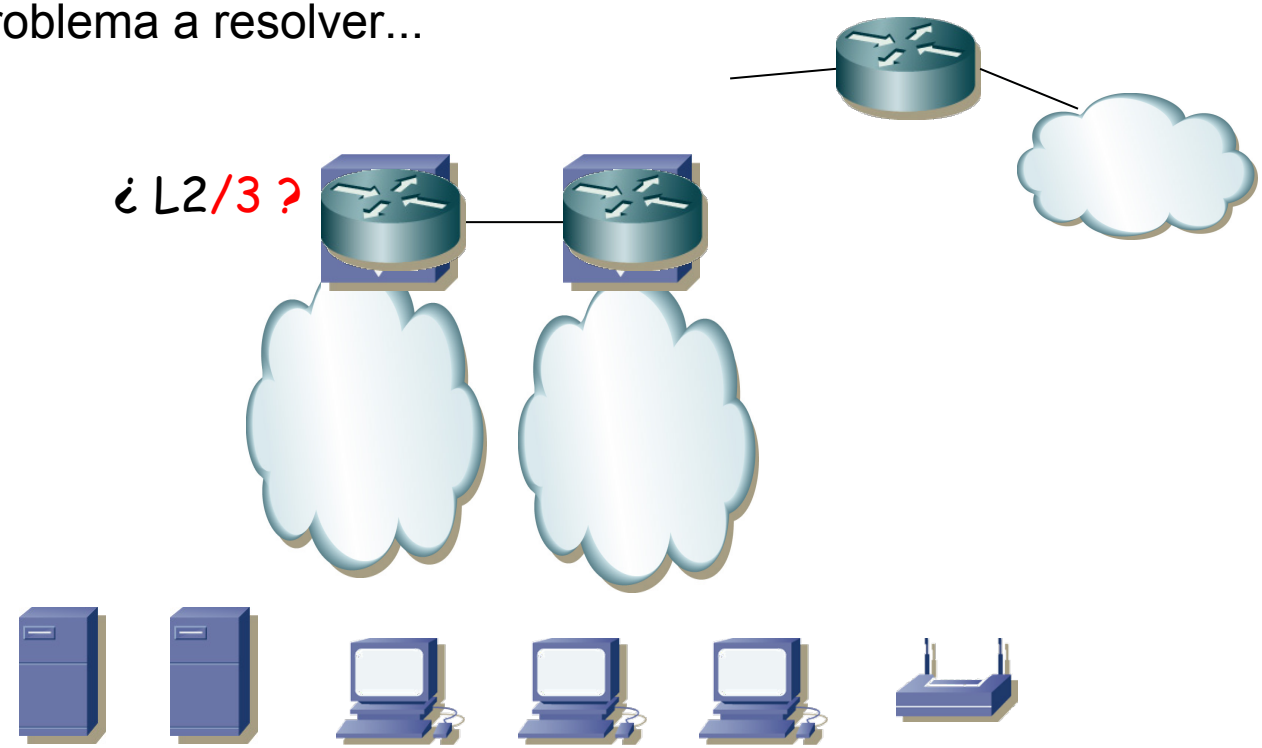
Enrutamiento

- Volviendo al caso con conmutadores de gama media (no se “agregan”)
- ¿Cómo hacemos en encaminamiento capa 3?
- ¿Podríamos enrutar en los conmutadores de distribución?
- (…)



Enrutamiento

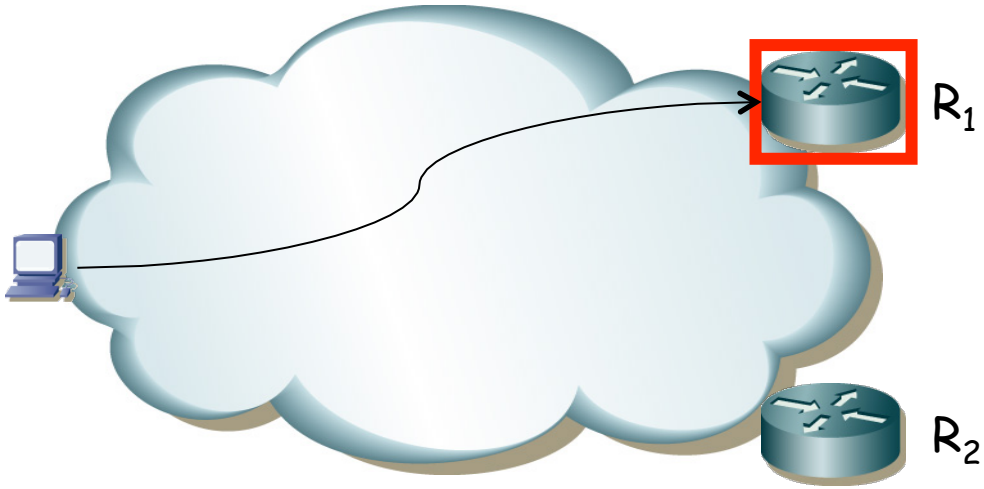
- Volviendo al caso con conmutadores de gama media (no se “agregan”)
- ¿Cómo hacemos en encaminamiento capa 3?
- ¿Podríamos enrutar en los conmutadores de distribución?
- ¿Y cómo sería eso en capa 3?
- ¿Repartimos los routers como router por defecto para las VLANs?
- El router por defecto sigue siendo un punto de fallo pues es único
- Eso es un problema a resolver...



FHRP

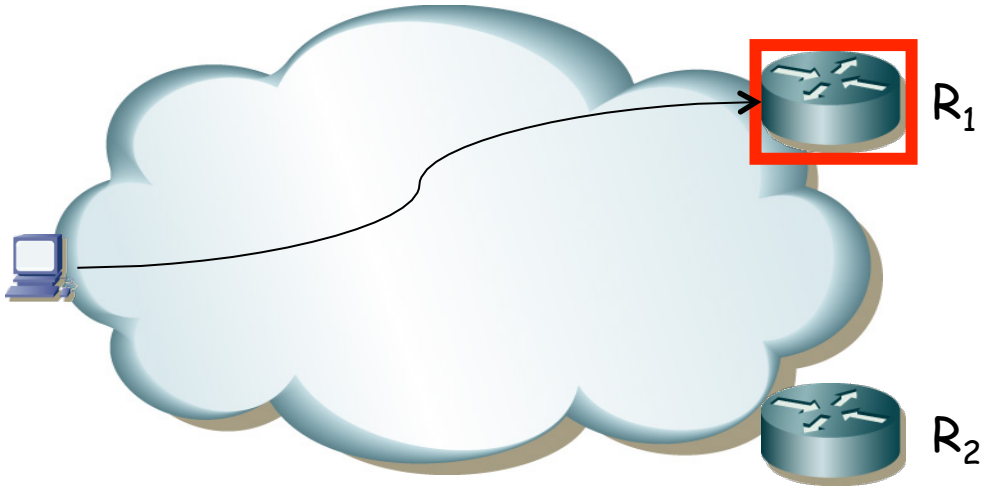
FHRP

- *First Hop Redundancy Protocols*
- Protocolos para ofrecer redundancia en el primer salto
- Hay varios routers que pueden servir de *default gateway*
- El protocolo permite la elección de uno de ellos (*Master*)
- El resto sirven de *backup*
- Si el maestro falla se elige uno de los de backup para la tarea de reenviar los paquetes
- No requiere cambio en los hosts
- Hay una dirección IP virtual que es la del router por defecto, que es empleada por el maestro



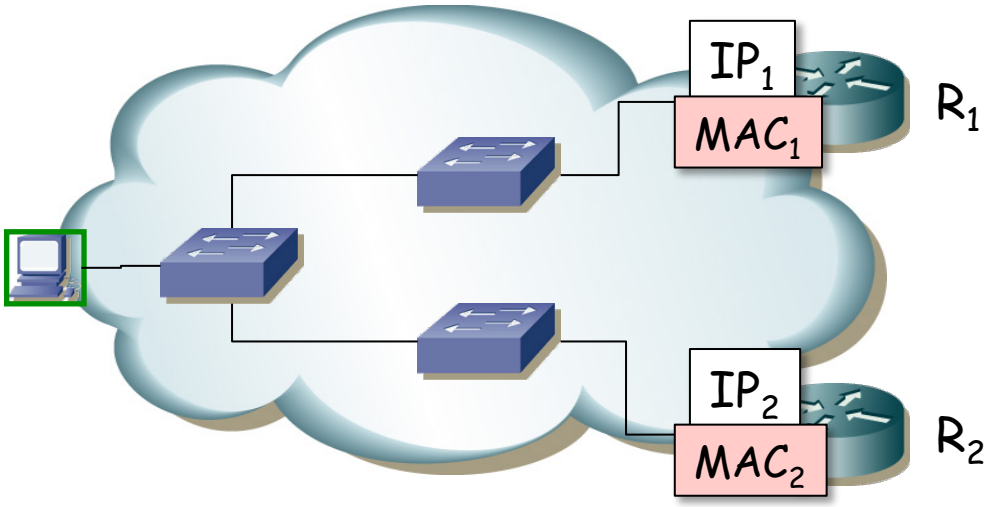
FHRP

- Hot Standby Router Protocol (HSRP): Propietario de Cisco
- Virtual Router Redundancy Protocol (VRRP): Similar pero abierto
- Common Addressable Redundancy Protocol (CARP): Similar y abierto
- Gateway Load Balancing Protocol (GLBP): Cisco
- NetScreen Redundancy Protocol (NSRP): Juniper
- Routed Split Multi-Link Trunking (R-SMLT): Avaya
- etc.



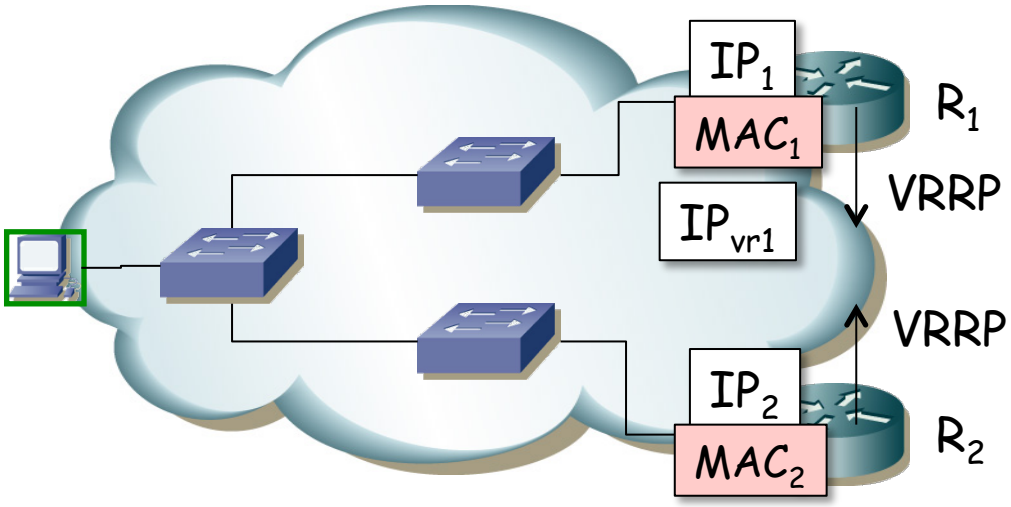
VRRP: Cómo funciona

- RFC 5798 “Virtual Rouer Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6”



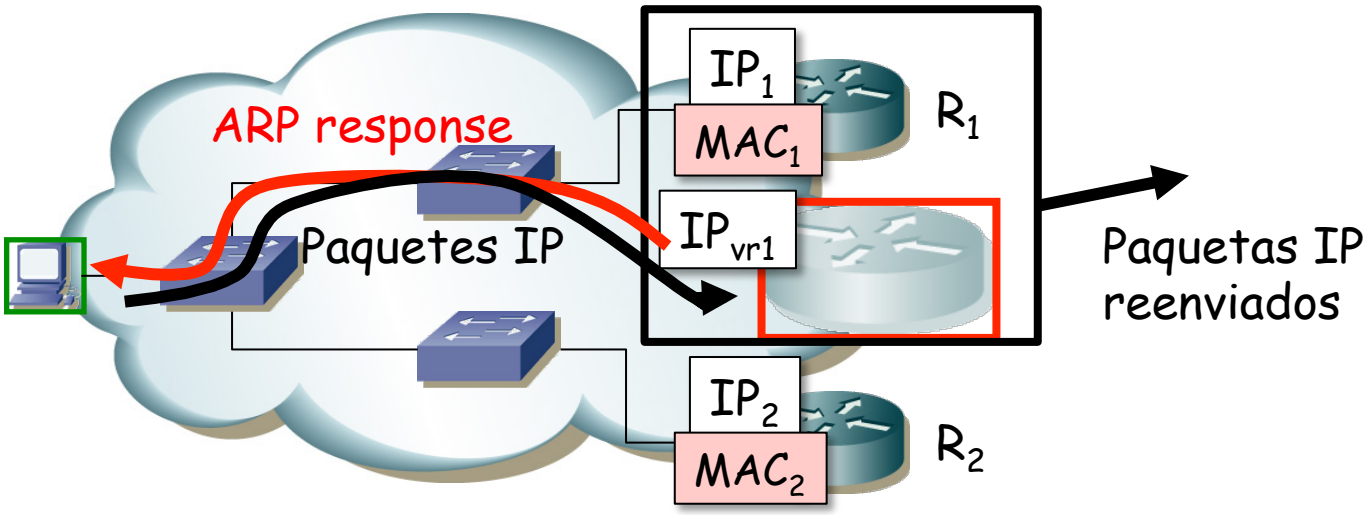
VRRP: Selección de maestro

- VRID = Virtual Router IDentifier (1 a 255)
- La dirección IP del router virtual puede ser la de uno de los routers (IP_{vr1}=IP_1) o ser diferente a las dos
- Los routers intercambian mensajes de VRRP para la elección del maestro
- Hay un campo de prioridad con el que controlar quién saldrá elegido
- Estos mensajes son paquetes IP dirigidos a 224.0.0.18 (mcast)
- El protocolo es 112 (no es UDP ni TCP ni ICMP, es VRRP)



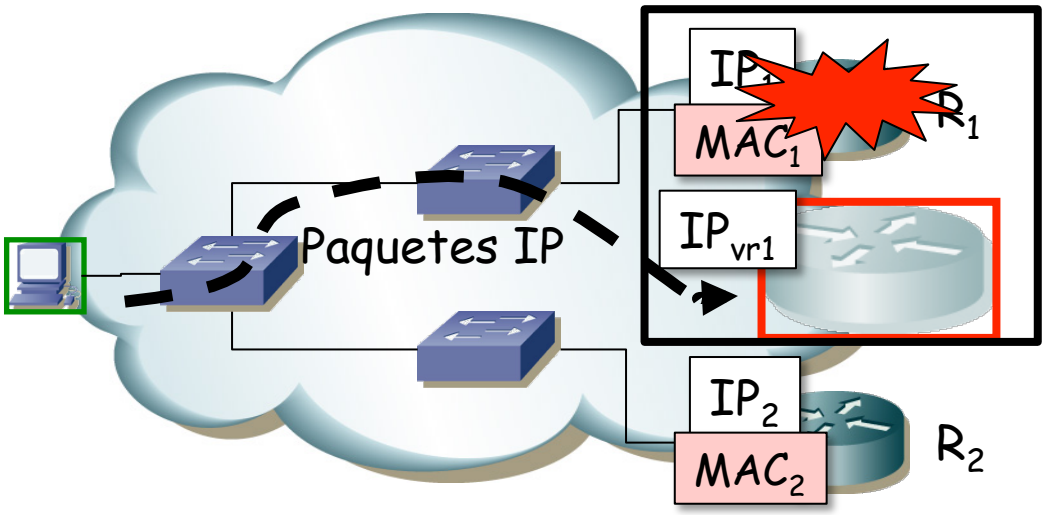
VRRP: Selección de maestro

- Se selecciona uno de los routers mediante el protocolo
- Ese router responderá a los ARP request para la IP_{vr1}
- La dirección MAC en la respuesta será 00:00:5E:00:01:{VRID}
- Está dentro del rango de direcciones MAC reservadas para IANA



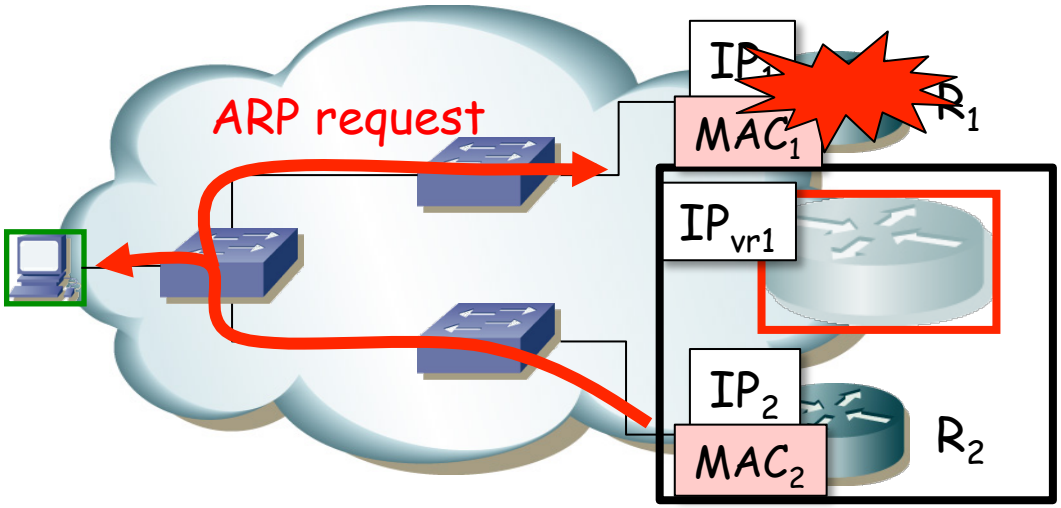
VRRP: Cómo funciona

- Si falla el maestro, el de backup deja de recibir los mensajes de VRRP y pasará a ser el maestro (...)



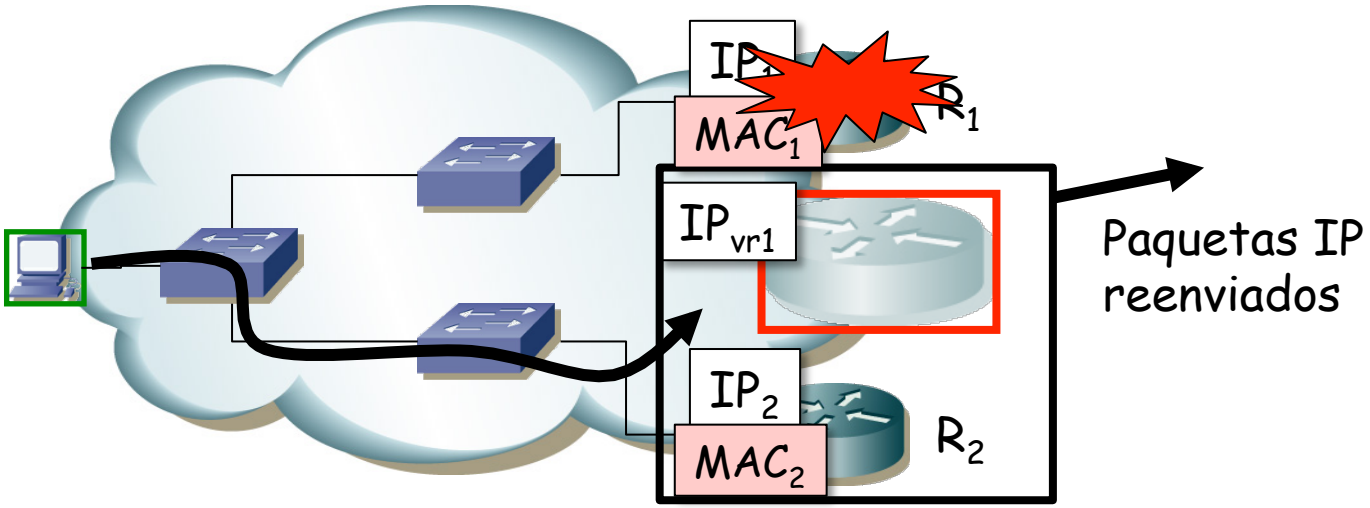
VRRP: Cómo funciona

- Si falla el maestro, el de backup deja de recibir los mensajes de VRRP y pasará a ser el maestro
- Envía un ARP gratuito (broadcast) con la dirección MAC virtual para que los conmutadores aprendan el camino hasta él (...)



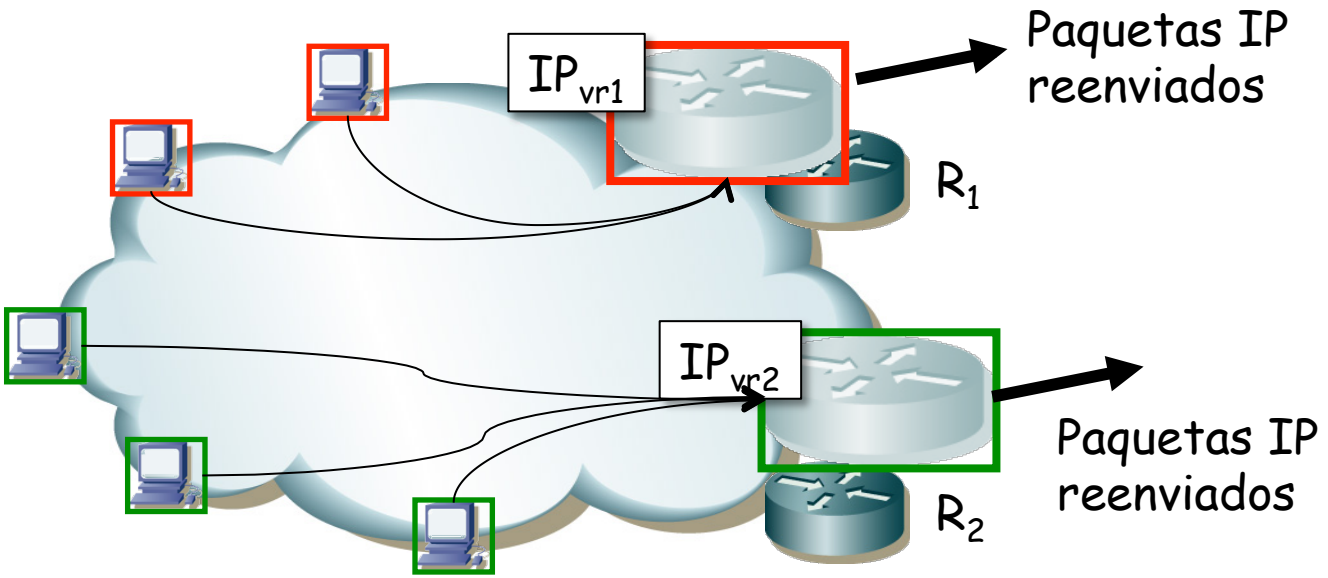
VRRP: Cómo funciona

- Si falla el maestro, el de backup deja de recibir los mensajes de VRRP y pasará a ser el maestro
- Envía un ARP gratuito (broadcast) con la dirección MAC virtual para que los conmutadores aprendan el camino hasta él (...)
- Nada ha cambiado para el host
- Convergencia en menos de 1s



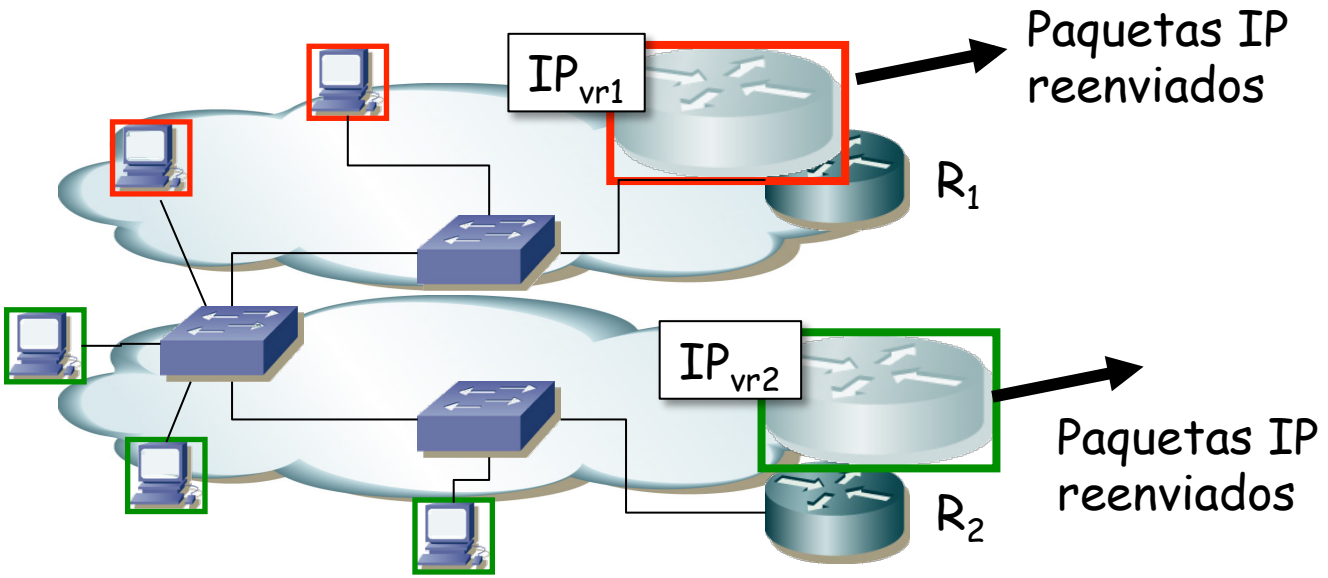
VRRP y reparto de carga

- Puede haber varios grupos por subred
- Dos subconjuntos de hosts, unos (rojos) tienen como router por defecto IP_{vr1} (VRID=1)
- Otros (verdes) tienen como router por defecto IP_{vr2} (VRID=2)
- R_1 maestro para el VRID=1
- R_2 maestro para el VRID=2
- Se ha repartido la carga de los hosts por los dos routers
- Cada uno es backup del grupo en el que el otro es el maestro



VRRP y reparto de carga

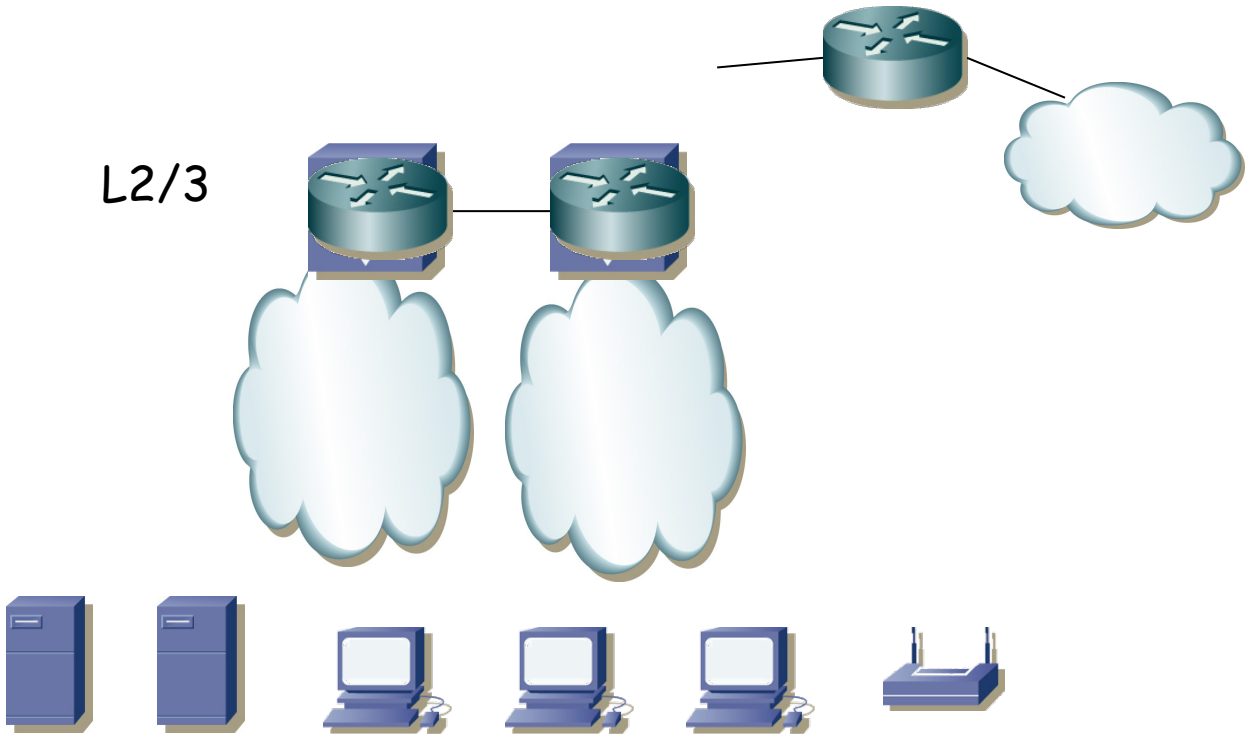
- O podríamos tener 2 VLANs
- Ambos routers tienen un interfaz en cada una
- Uno es maestro en la subred de una y secundario en la otra
- Y el otro al revés



Collapsed core y FHR

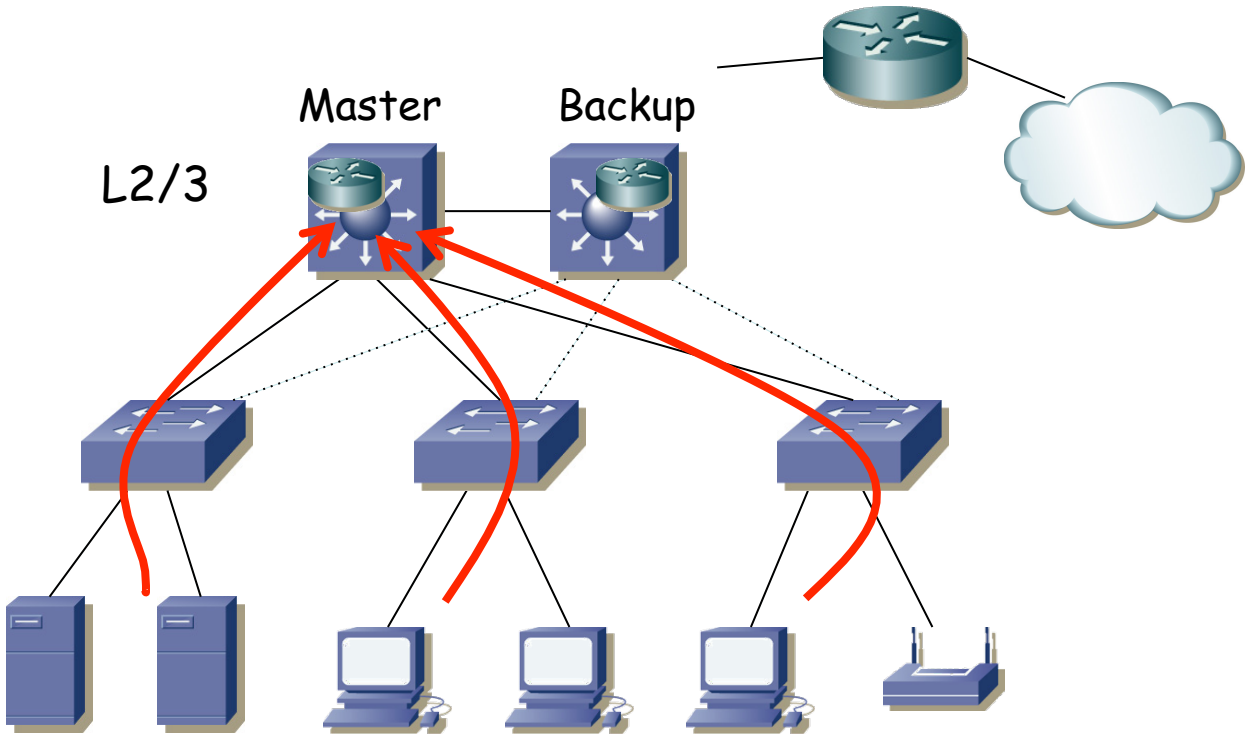
Colapsed core y FHR

- Tenemos dos routers (conmutadores capa 2/3)
- Uno de ellos podría actuar como gateway en todas las subredes
- O podemos repartir esa tarea
- Por ejemplo, con uno de ellos para todas las subredes, 2 VLANs, 1 ST
- (...)



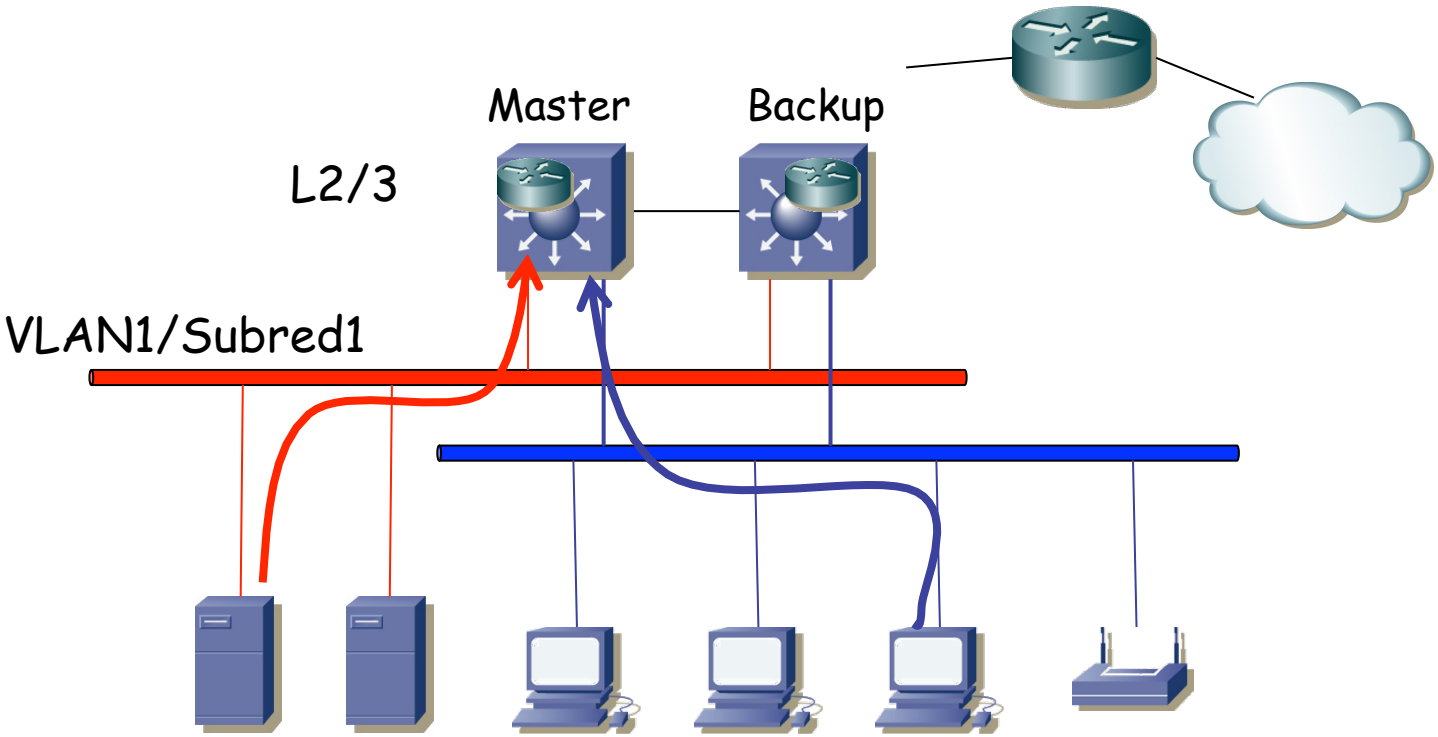
Colapsed core y FHR

- Tenemos dos routers (conmutadores capa 2/3)
- Uno de ellos podría actuar como gateway en todas las subredes
- O podemos repartir esa tarea
- Por ejemplo, con uno de ellos para todas las subredes, 2 VLANs, 1 ST
- Con 1 ST, mismo camino al gateway, que resulta ser el *root bridge*
- (...)



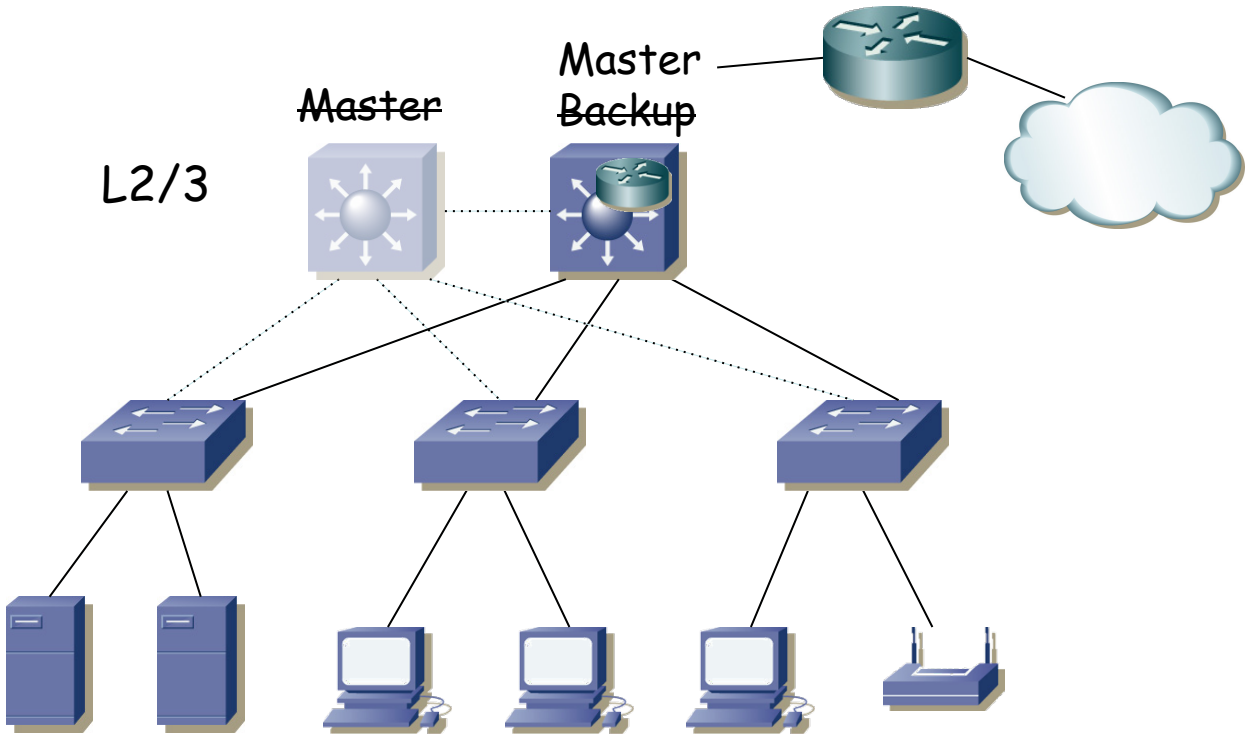
Colapsed core y FHR

- Tenemos dos routers (conmutadores capa 2/3)
- Uno de ellos podría actuar como gateway en todas las subredes
- O podemos repartir esa tarea
- Por ejemplo, con uno de ellos para todas las subredes, 2 VLANs, 1 ST
- Con 1 ST, mismo camino al gateway, que resulta ser el *root bridge*
- Representando las dos LANs



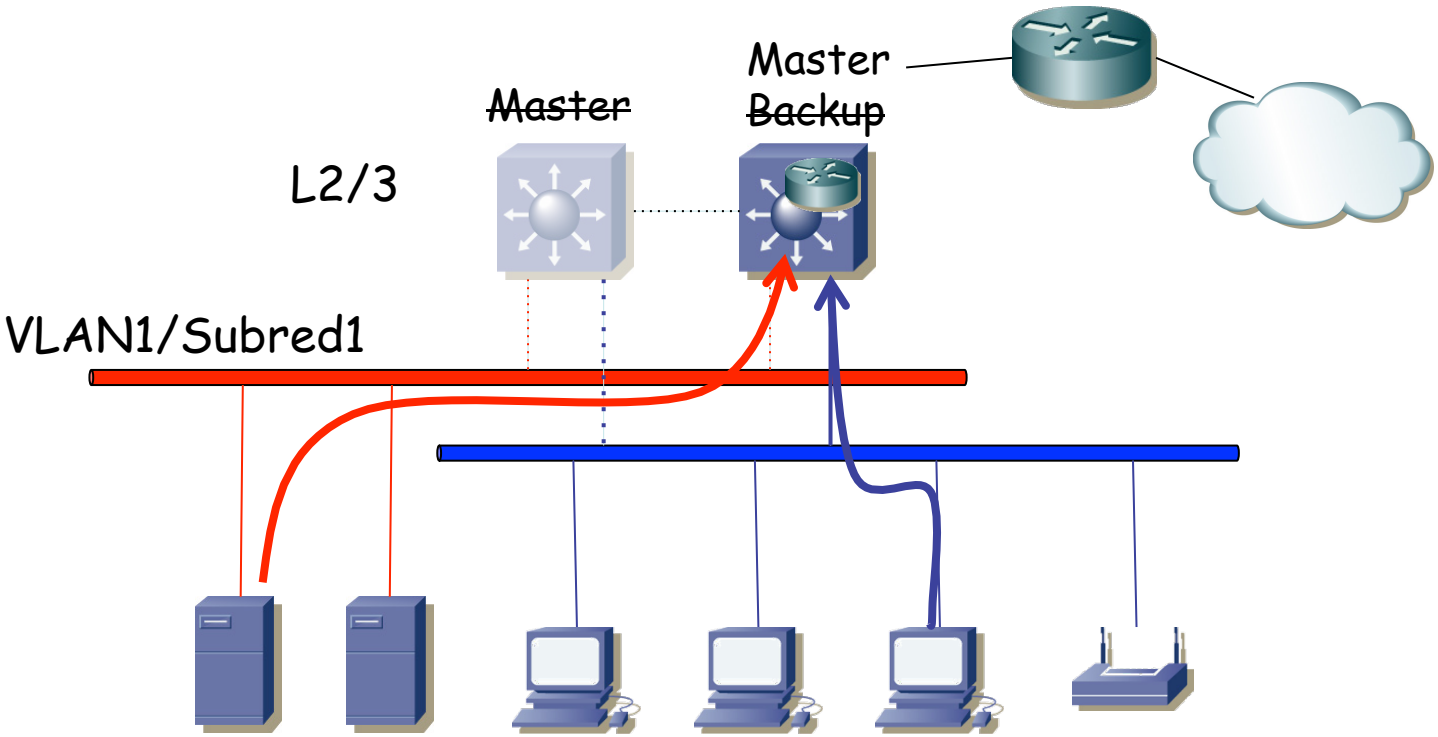
Colapsed core y FHR

- ¿Y si falla el master?
- No es que simplemente el backup pase a master empleando el FHRP sino que nos cambia el árbol porque era la raíz
- Probablemente tarde más en converger RSTP (2-3s) que el FHRP
- Y eso contando con que no tiene STP original (30-60s)
- (...)



Colapsed core y FHR

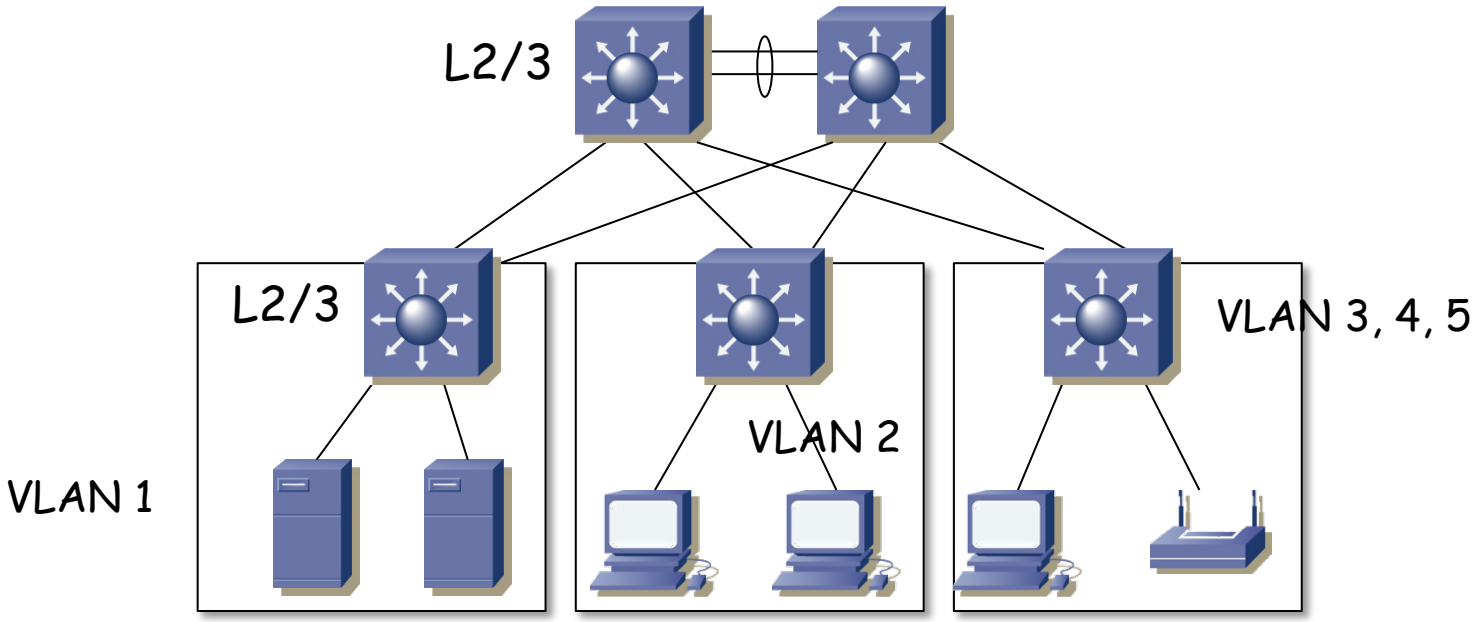
- ¿Y si falla el master?
- No es que simplemente el backup pase a master empleando el FHRP sino que nos cambia el árbol porque era la raíz
- Probablemente tarde más en converger RSTP (2-3s) que el FHRP
- Y eso contando con que no tiene STP original (30-60s)
- ¿2s es poco? Se pueden caer llamadas VoIP, detener streaming...



Layer 3 Collapsed core

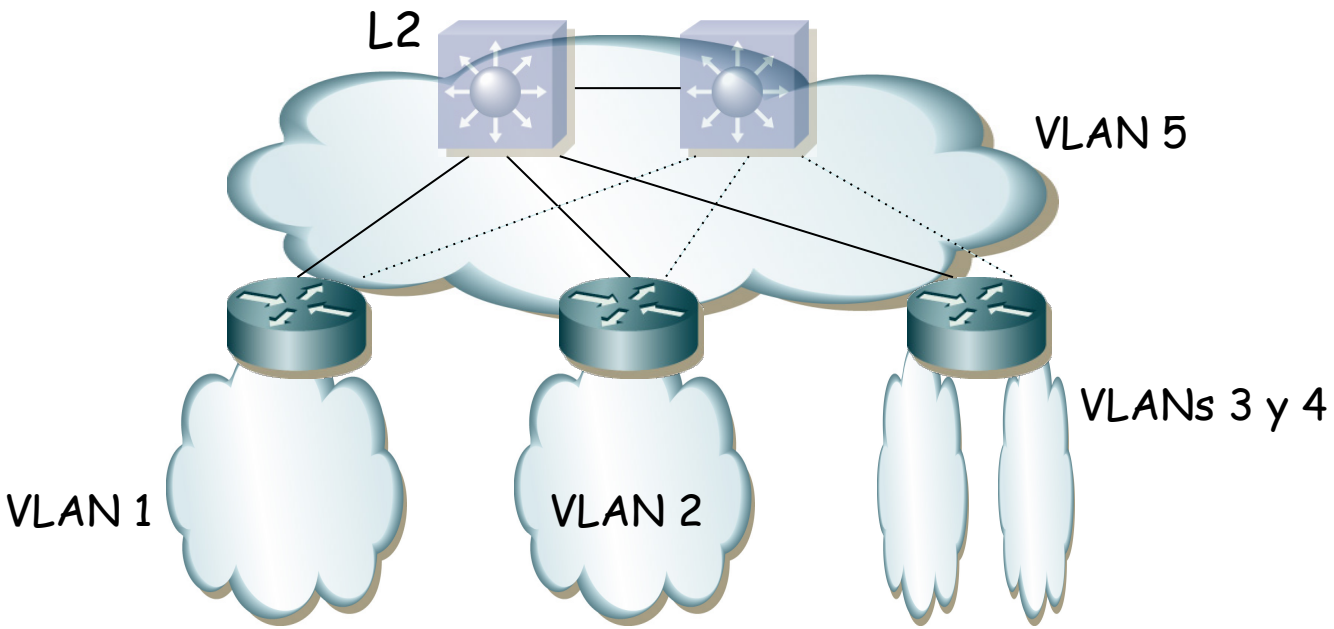
Layer 3 Collapsed Core

- ¿Qué ha cambiado? Ahora los conmutadores del acceso son también L2/3
- Esto permite limitar una VLAN a un IDF
- Reduce a ese armario el dominio de broadcast y los problemas que pueda dar
- ¿Y el sistema de distribución? (...)



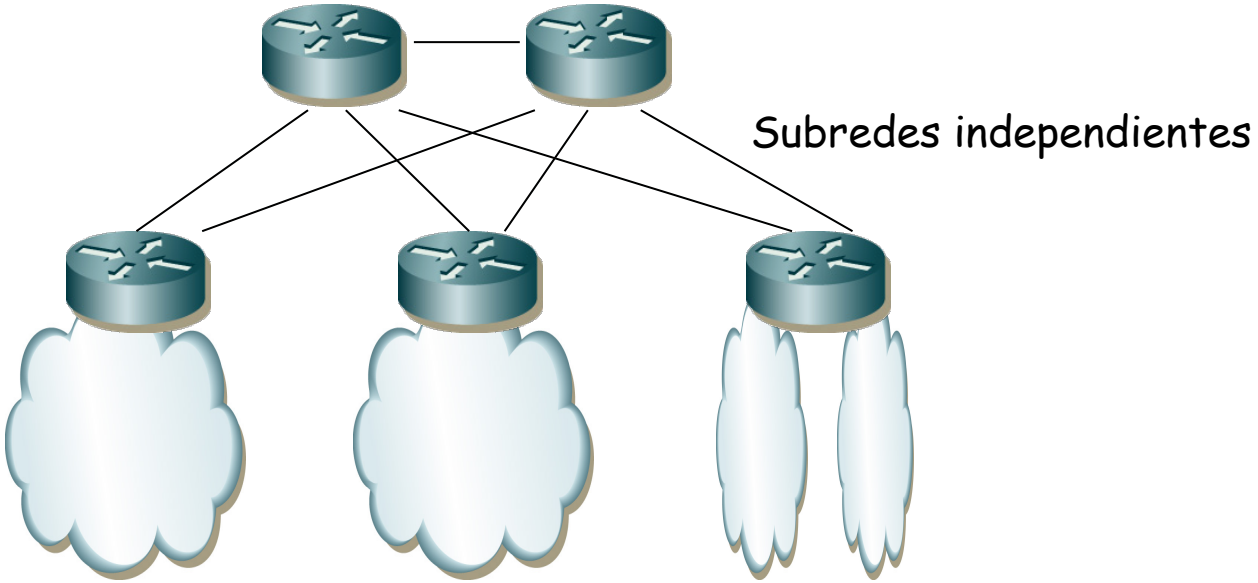
Layer 3 Collapsed Core

- ¿Y el sistema de distribución?
  - Puede trabajar en capa 2 (una VLAN/Subred de interconexión)
  - (...)



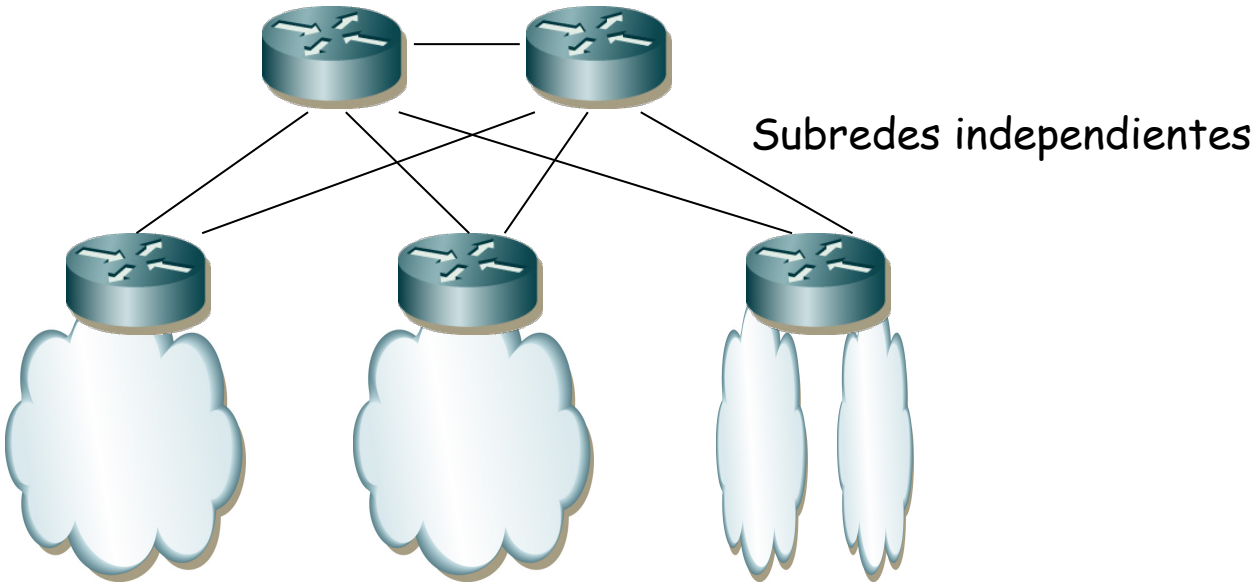
Layer 3 Collapsed Core

- ¿Y el sistema de distribución?
  - Puede trabajar en capa 2 (una VLAN/Subred de interconexión)
  - O en capa 3
  - En este caso son todo conmutadores capa 2/3 (o al menos uno por IDF) y cada enlace puede ser una subred
  - Ya no hay STP, sino que entre los comutadores/routers empleamos un protocolo de encaminamiento
  - Mejores tiempos de convergencia y más estable
  - El encaminamiento IP puede permitir usar varias rutas a la vez
  - Pero (...)



Layer 3 Collapsed Core

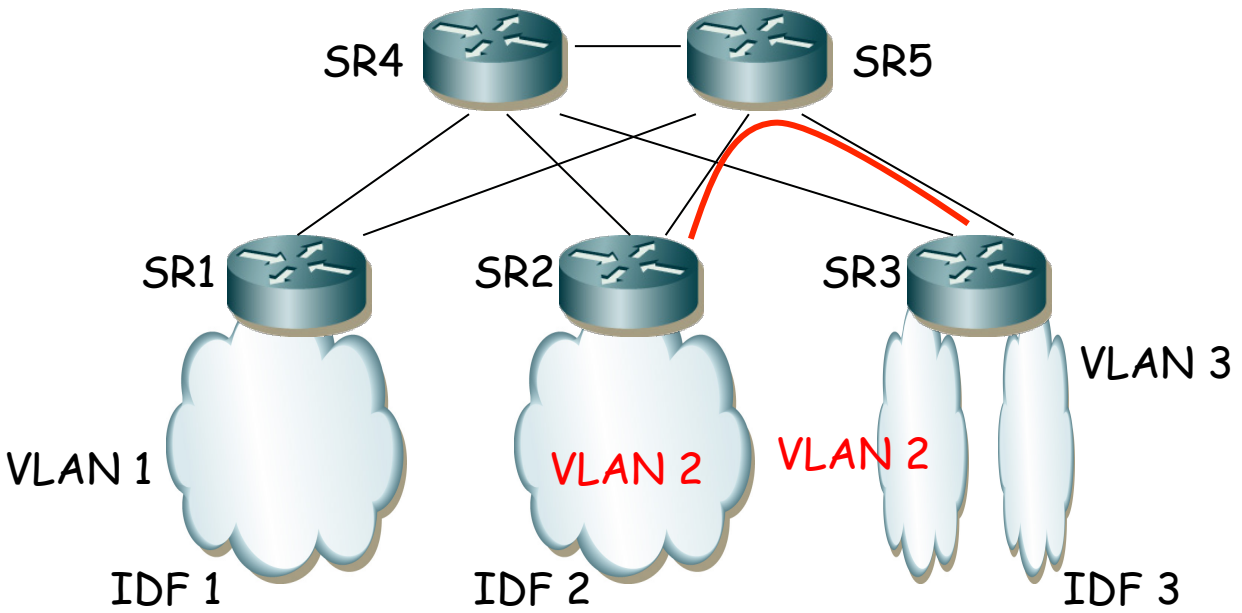
- Más configuración (direccionamiento, enrutamiento)
- VLANs limitadas a un IDF
- Dado que son conmutadores capa 2/3 podría haber alguna VLAN que se extendiera por todo el campus
- Esa VLAN tendría un STP más frágil
- Pero hay aplicaciones que requieren estar en la misma LAN y si los hosts están en diferentes IDF puede no haber otra opción
- Así que podemos terminar con soluciones híbridas (...)



Layer 3 Collapsed Core

Ejemplo:

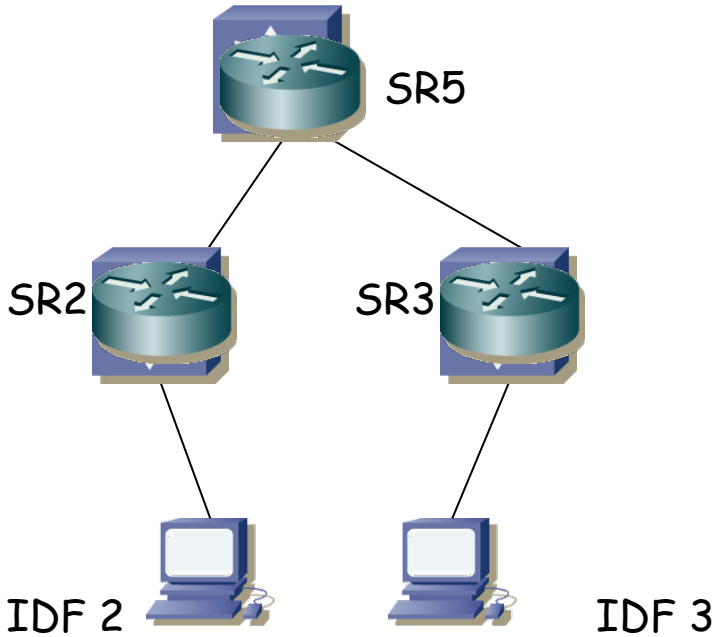
- Hosts de la VLAN 2 tanto en el IDF 2 como en el IDF 3
- Diferentes posibilidades en la distribución pero la VLAN 2 debe conmutarse en capa 2 al menos entre IDF 2 e IDF 3
- Comunicación entre dos hosts de VLAN 2 en diferente IDF (...)



Layer 3 Collapsed Core

Ejemplo:

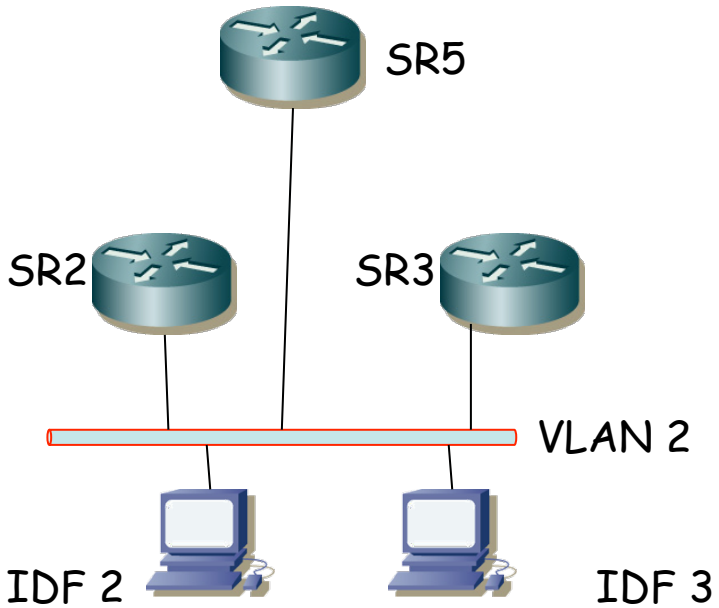
- Router por defecto de la subred de la VLAN 2 podrían ser SR2, SR3 o SR5 (si la VLAN no llega al resto de conmutadores)
- Otra representación (...)



Layer 3 Collapsed Core

Ejemplo:

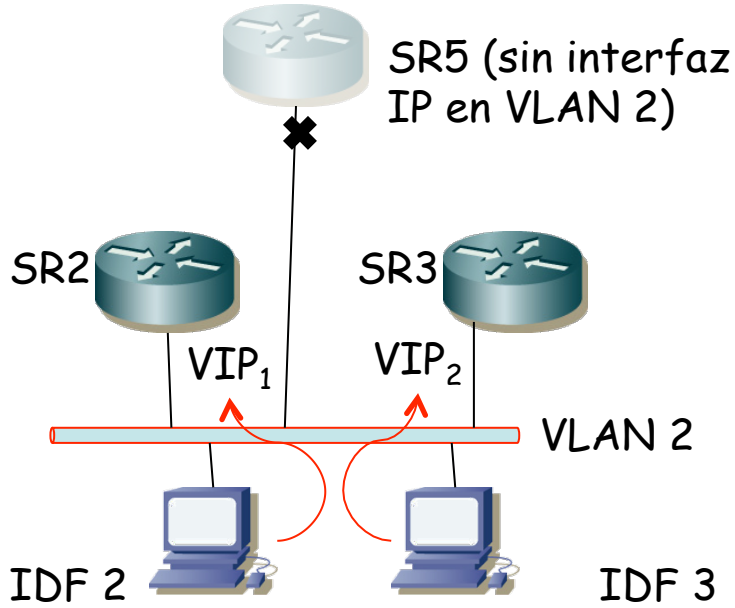
- Router por defecto de la subred de la VLAN 2 podrían ser SR2, SR3 o SR5 (si la VLAN no llega al resto de conmutadores)
- Otra representación, simbolizando la VLAN, independientemente de los conmutadores que se atraviesen
- Podríamos emplear un FHRP como VRRP (...)



Layer 3 Collapsed Core

Ejemplo:

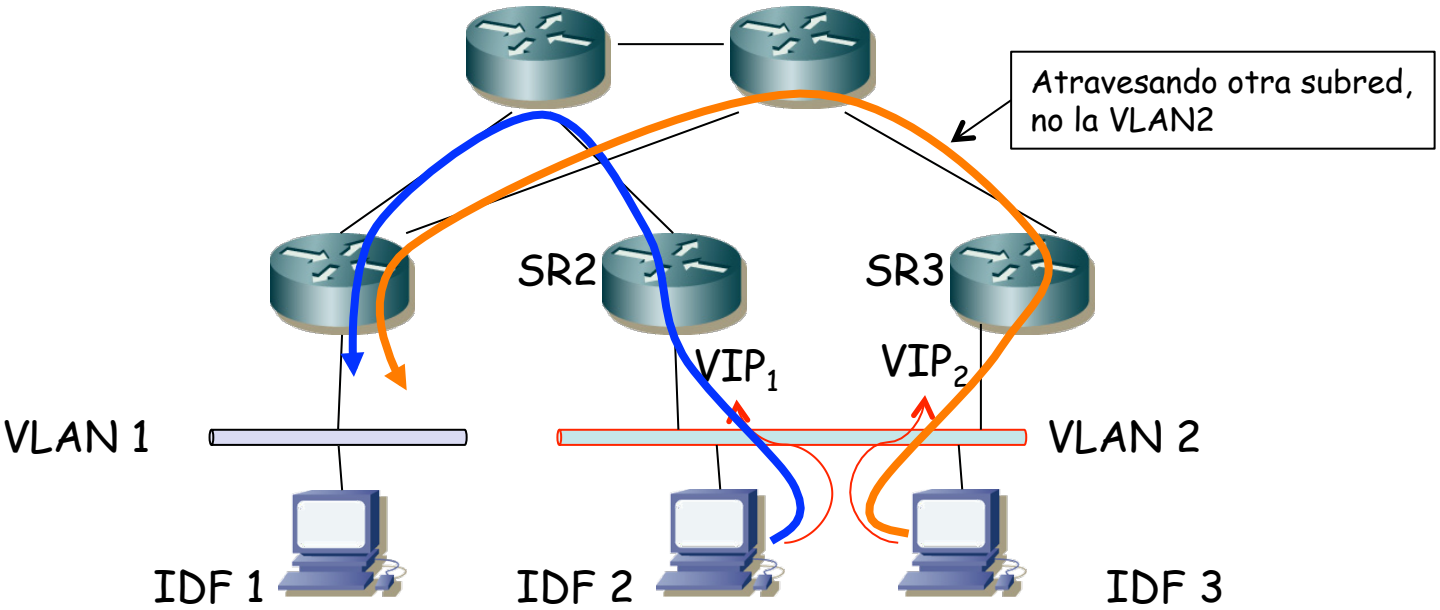
- Podríamos emplear VRRP con redundancia entre dos de ellos, por ejemplo SR2 y SR3 repartiendo a los hosts entre ellos
- La dirección virtual VIP_1 podría tener de master SR2 y backup SR3
- La dirección virtual VIP_2 podría tener de master SR3 y backup SR2
- Además los hosts de VLAN 2 en IDF 2 podrían tener VIP_1 como router por defecto y los de IDF 3 a VIP_2
- (...)



Layer 3 Collapsed Core

Ejemplo:

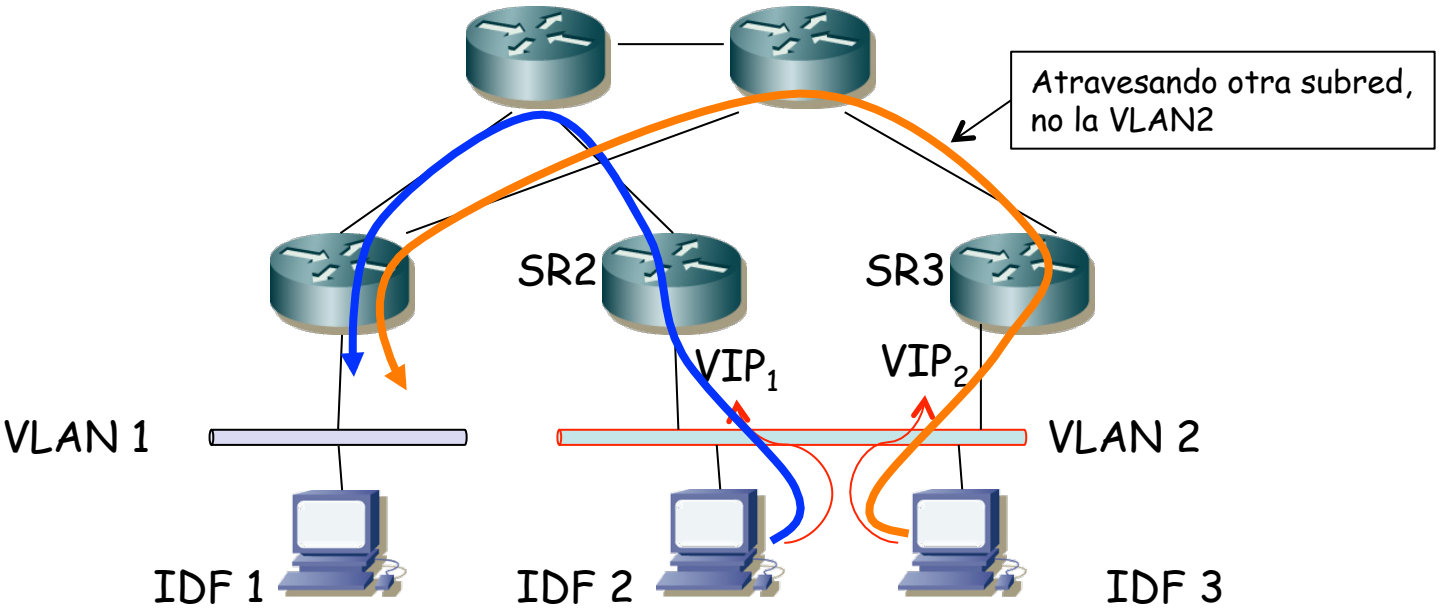
- Podríamos emplear VRRP con redundancia entre dos de ellos, por ejemplo SR2 y SR3 repartiendo a los hosts entre ellos
- La dirección virtual VIP_1 podría tener de master SR2 y backup SR3
- La dirección virtual VIP_2 podría tener de master SR3 y backup SR2
- Además los hosts de VLAN 2 en IDF 2 podrían tener VIP_1 como router por defecto y los de IDF 3 a VIP_2
- Encaminamiento hasta la subred de la VLAN 1 pasaría enrutado por el sistema de distribución



Layer 3 Collapsed Core

Ejemplo:

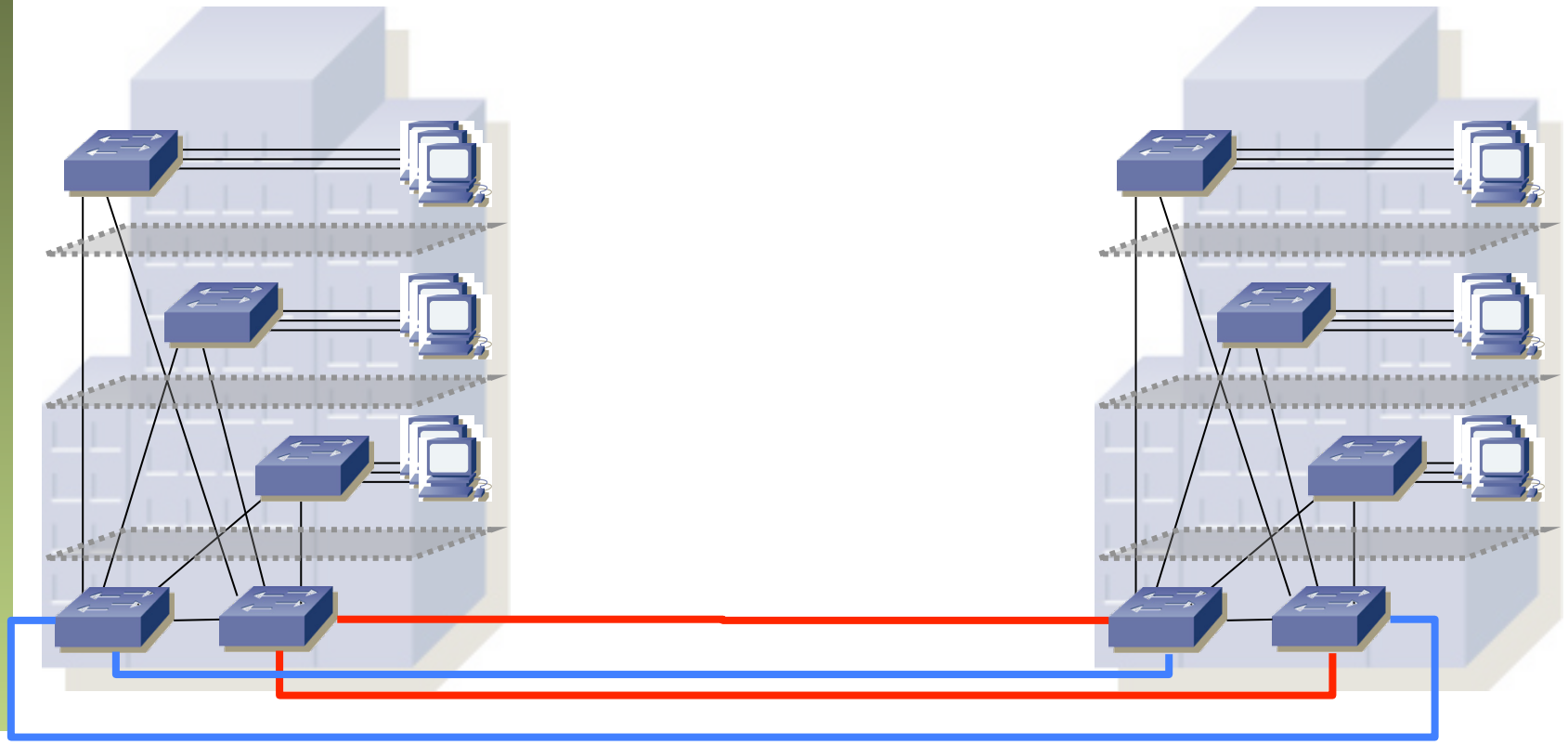
- Pero para implementar esta solución, con protección de caminos en el sistema de distribución, necesitamos un protocolo de encaminamiento en capa 3
- O sea, algo como OSPF, IS-IS, EIGRP, etc
- Lo cual es materia de otra asignatura



3-tier design

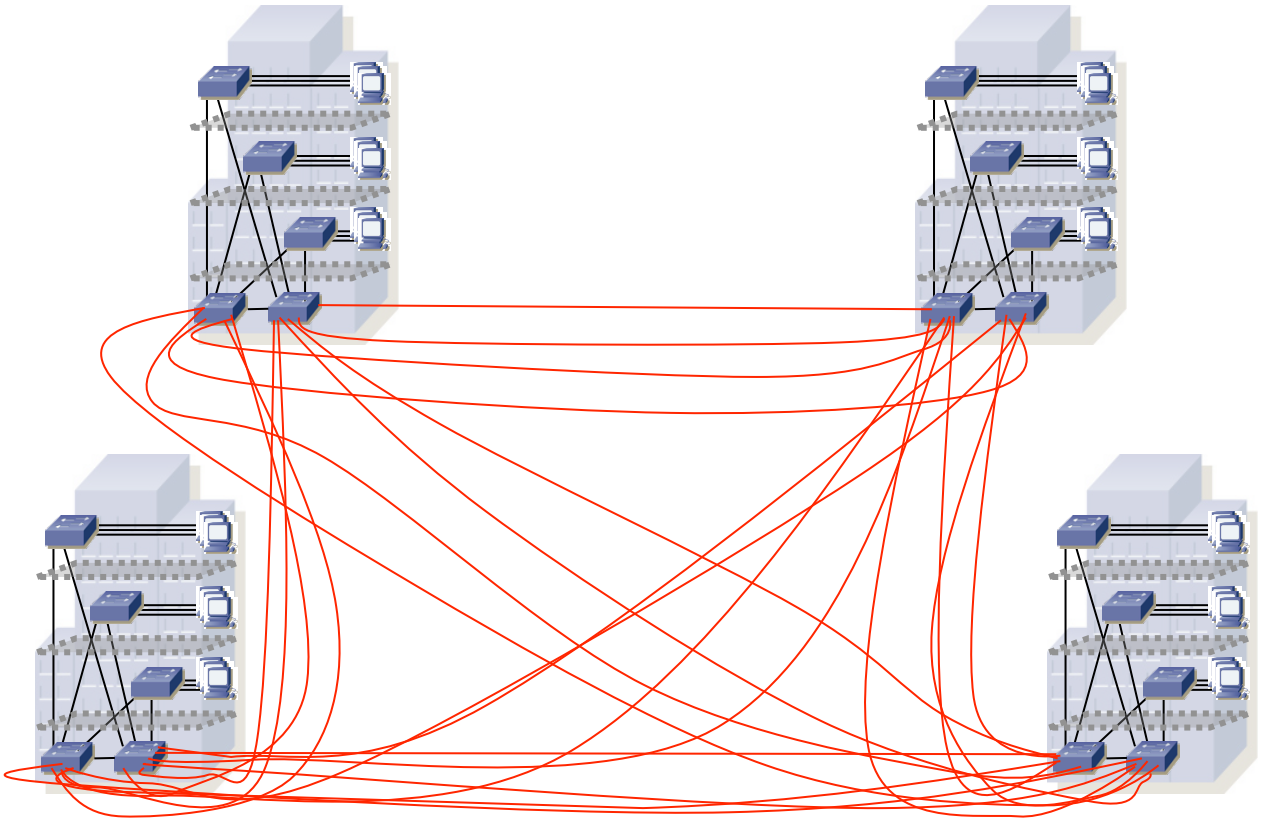
Redes más grandes

- El esquema IDF+MDF (acceso+distribución) sirve hasta una escala
- Por ejemplo cuando está todo contenido en un solo edificio
- ¿Y con varios edificios? Repetimos el diseño
- Y necesitamos interconectarlos
- Podemos hacerlo directamente, pero (...)



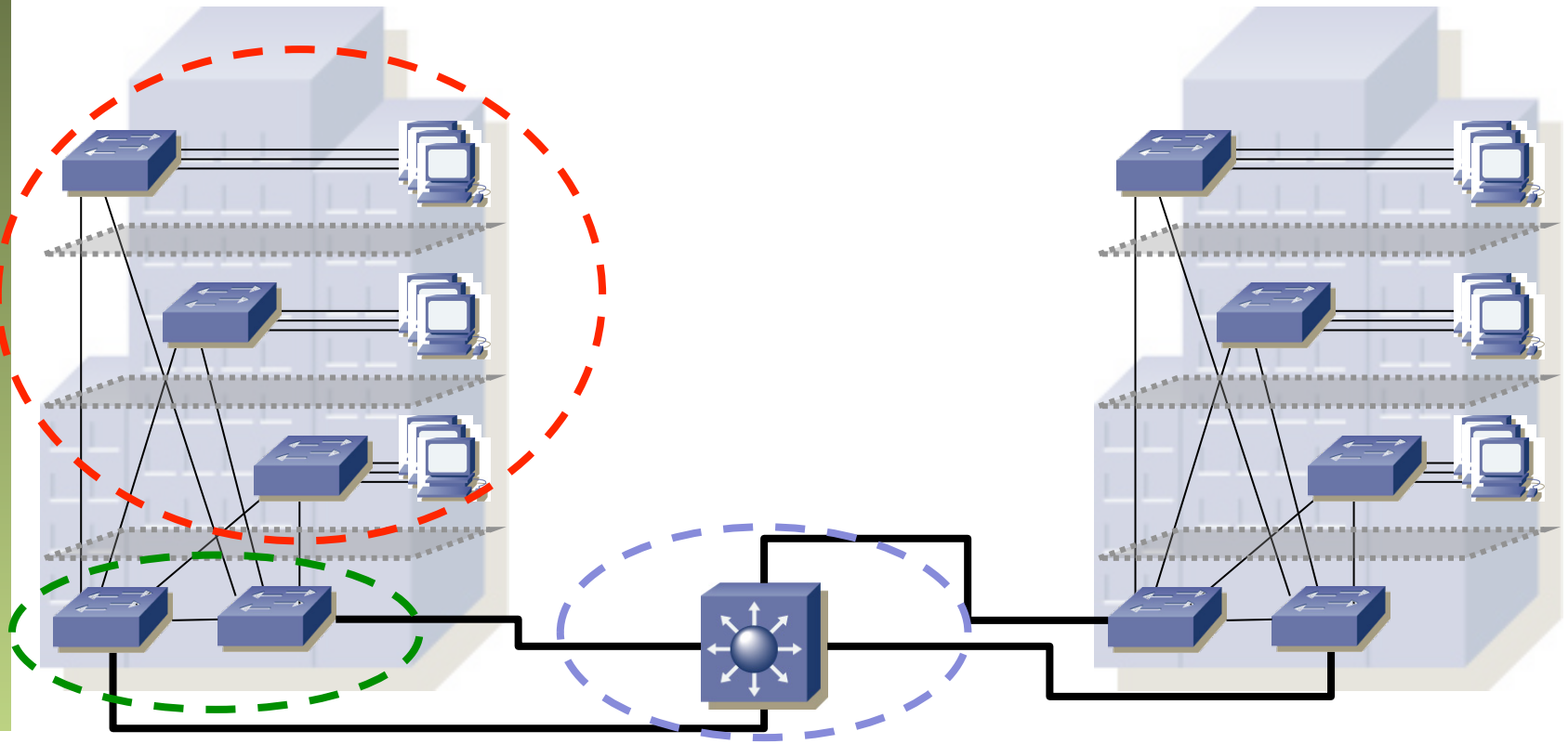
Redes más grandes

- El esquema IDF+MDF (acceso+distribución) sirve hasta una escala
- Por ejemplo cuando está todo contenido en un solo edificio
- ¿Y con varios edificios? Repetimos el diseño
- Y necesitamos interconectarlos
- Podemos hacerlo directamente, pero escala mal



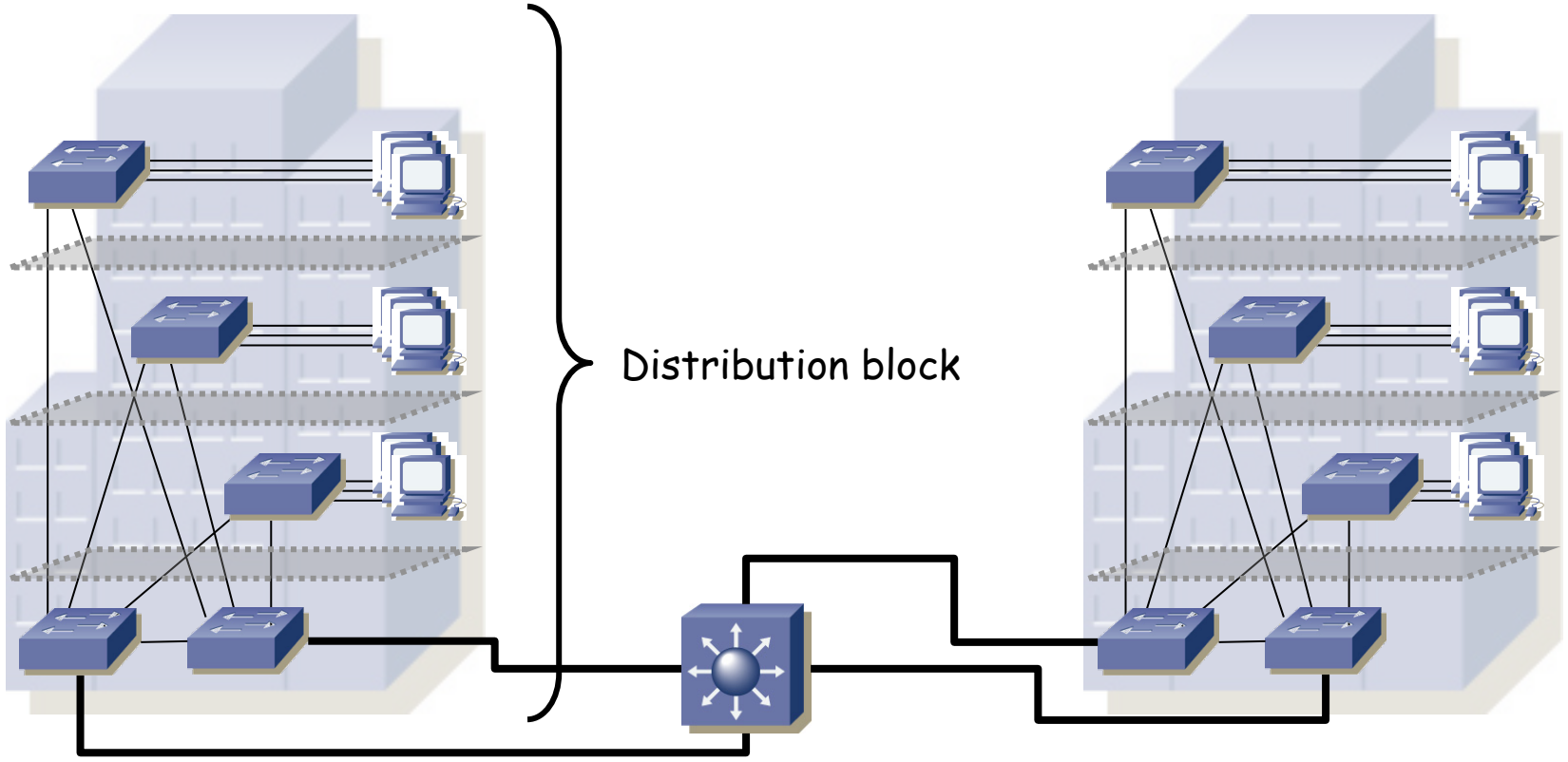
Redes más grandes

- El esquema IDF+MDF (acceso+distribución) sirve hasta una escala
- Por ejemplo cuando está todo contenido en un solo edificio
- ¿Y con varios edificios? Repetimos el diseño
- Y necesitamos interconectarlos: Core
- Acceso (access), distribución (distribution) y núcleo (core)



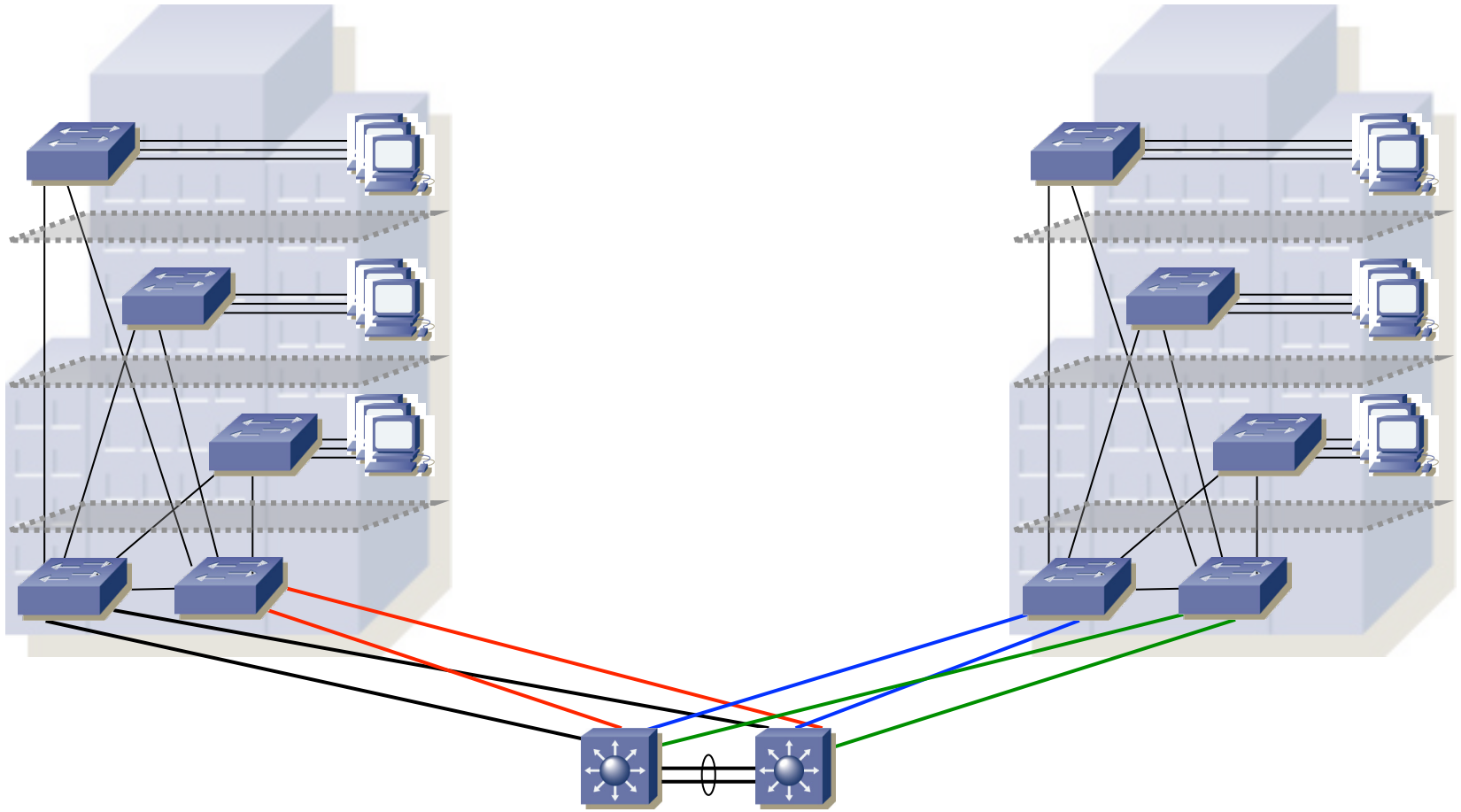
Redes más grandes

- El esquema IDF+MDF (acceso+distribución) sirve hasta una escala
- Por ejemplo cuando está todo contenido en un solo edificio
- ¿Y con varios edificios? Repetimos el diseño
- Y necesitamos interconectarlos: Core
- Acceso (access), distribución (distribution) y núcleo (core)



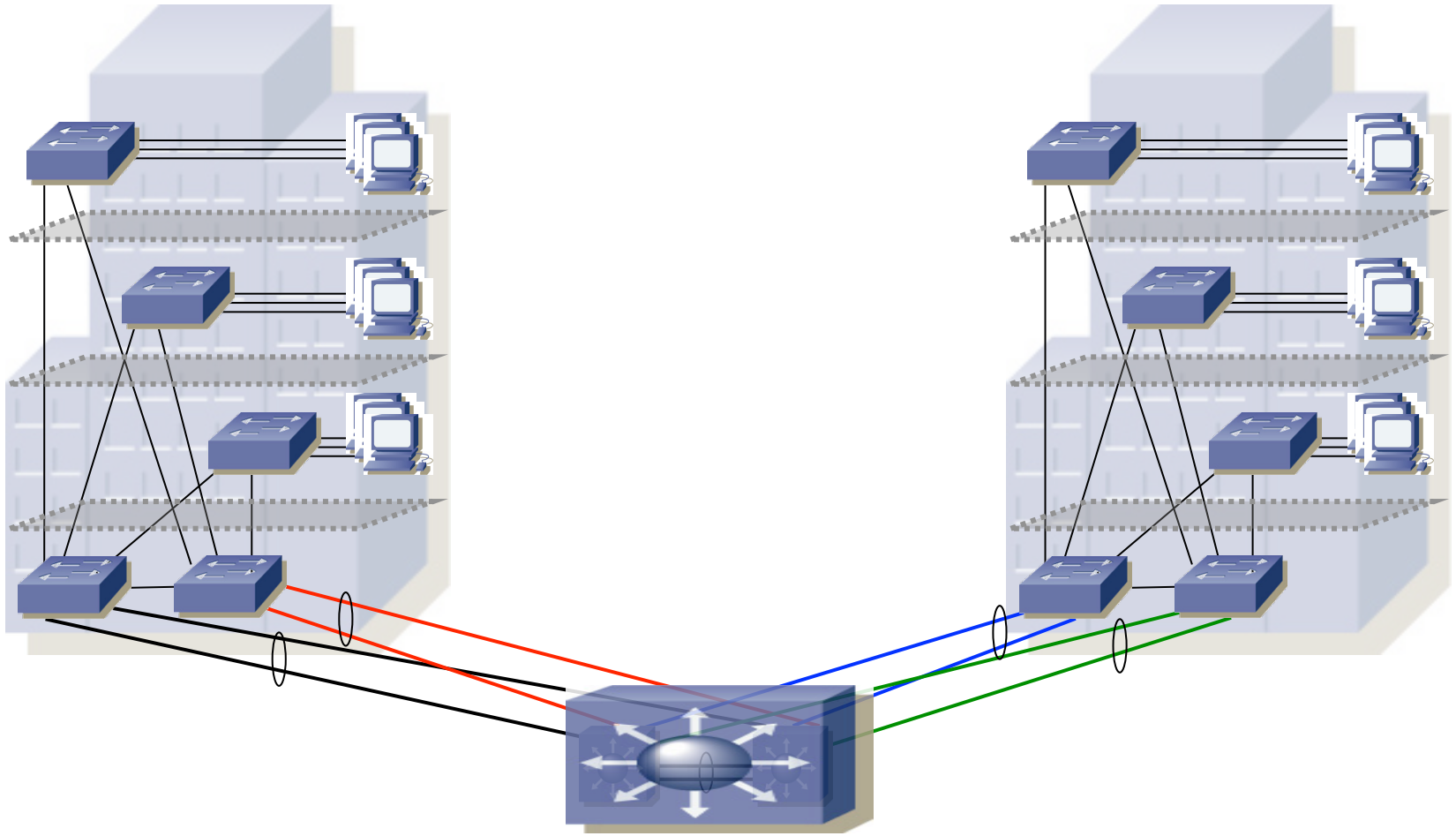
Core

- Evidentemente necesitamos redundancia en él
- Si los switches del core lo soportan podrían agregarse en un switch virtual y los enlaces del mismo color podrían ser un LAG (...)



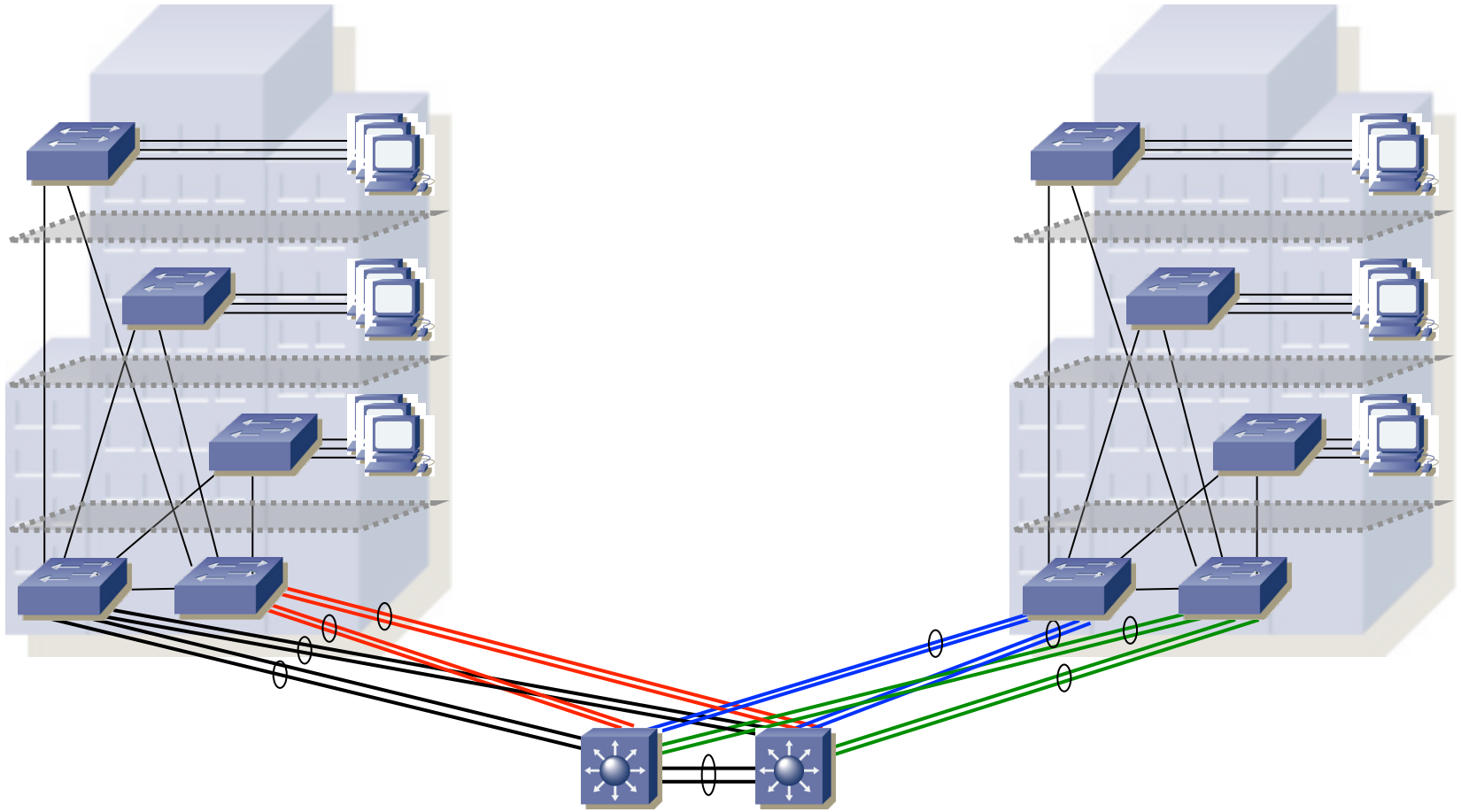
Core

- Evidentemente necesitamos redundancia en él
- Si los switches del core lo soportan podrían agregarse en un switch virtual y los enlaces del mismo color podrían ser un LAG
- O cada uno de esos enlaces podría ser un LAG (...)



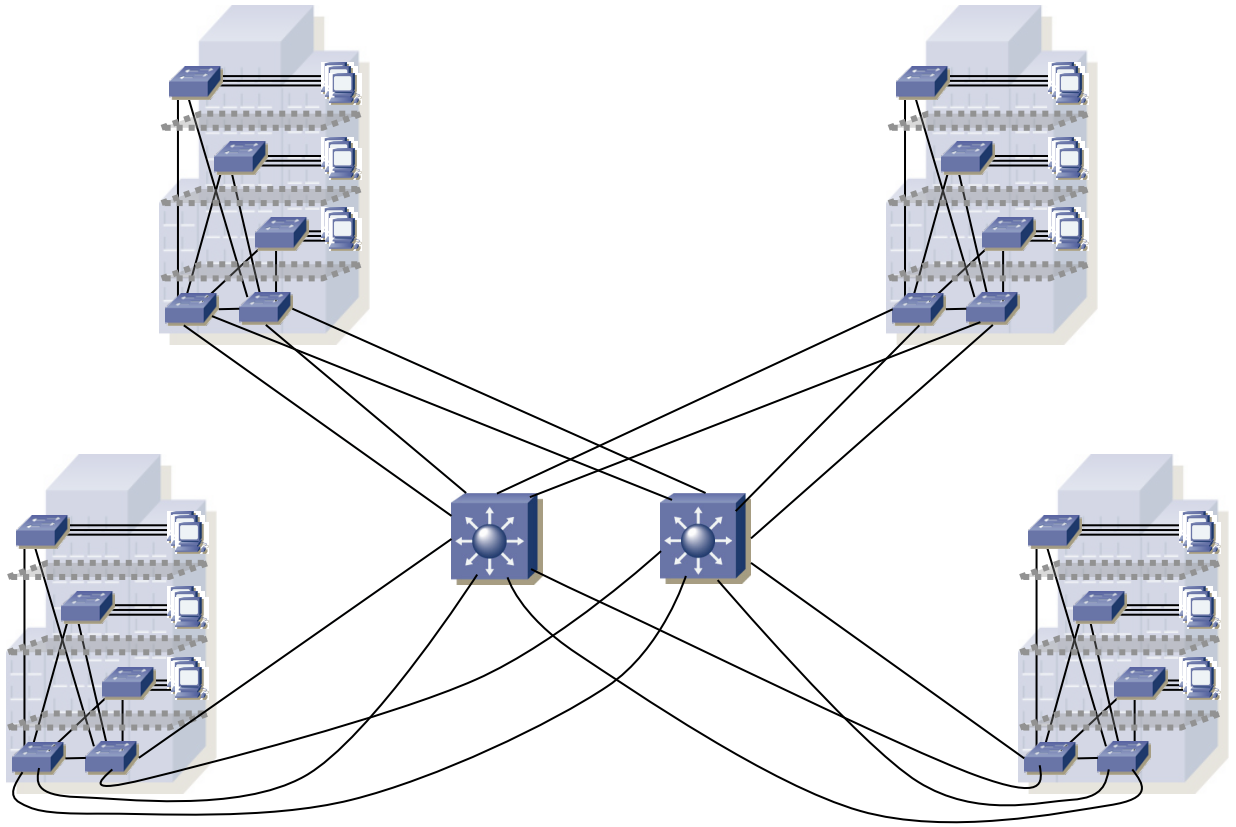
Core

- Evidentemente necesitamos redundancia en él
- Si los switches del core lo soportan podrían agregarse en un switch virtual y los enlaces del mismo color podrían ser un LAG
- O cada uno de esos enlaces podría ser un LAG



Redes más grandes

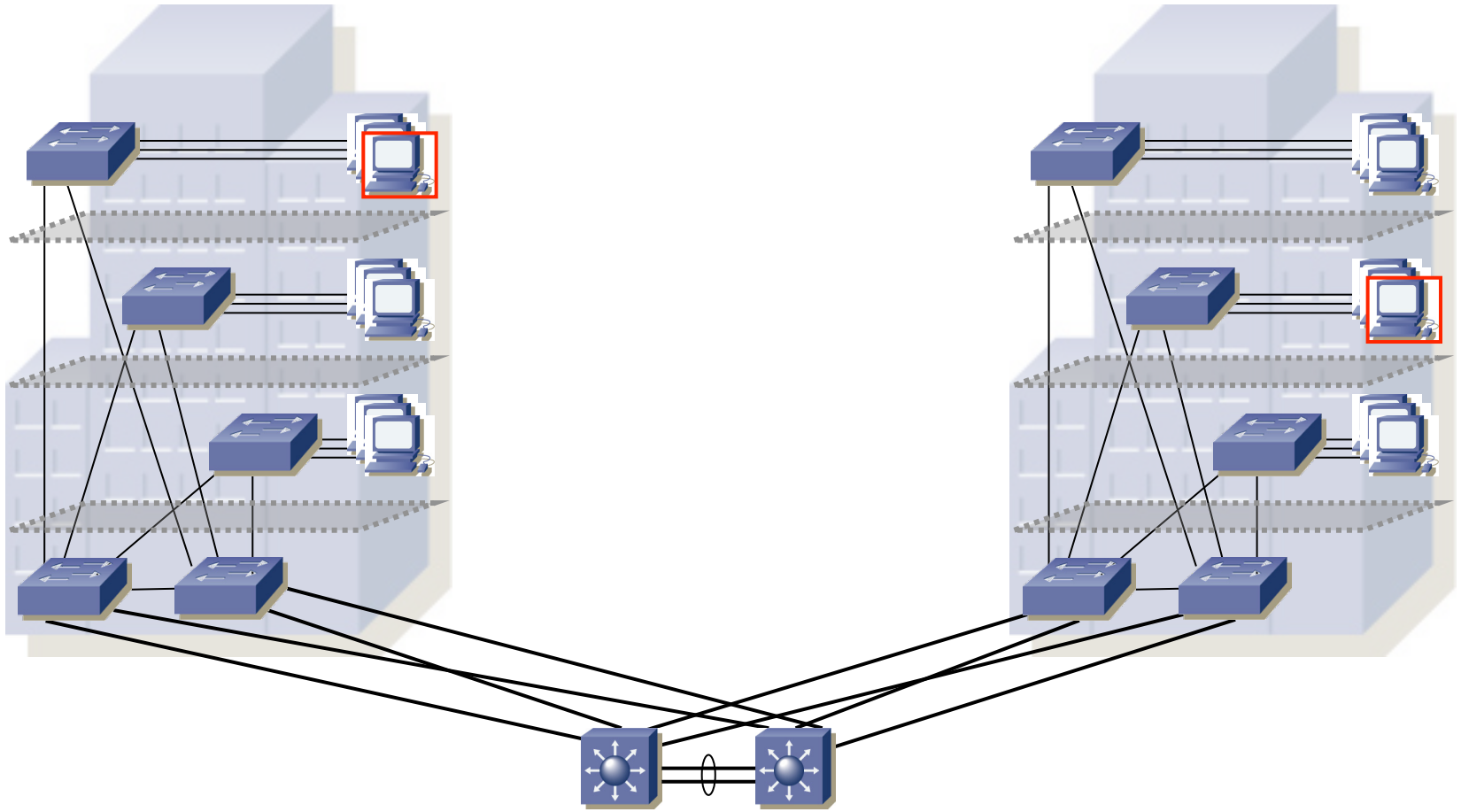
- La arquitectura con core permite escalar de forma sencilla para campus aún más grandes
- El core podría ser también más grande: 3 conmutadores, 4 en anillo, 4 en malla, etc.



Campus-wide VLANs

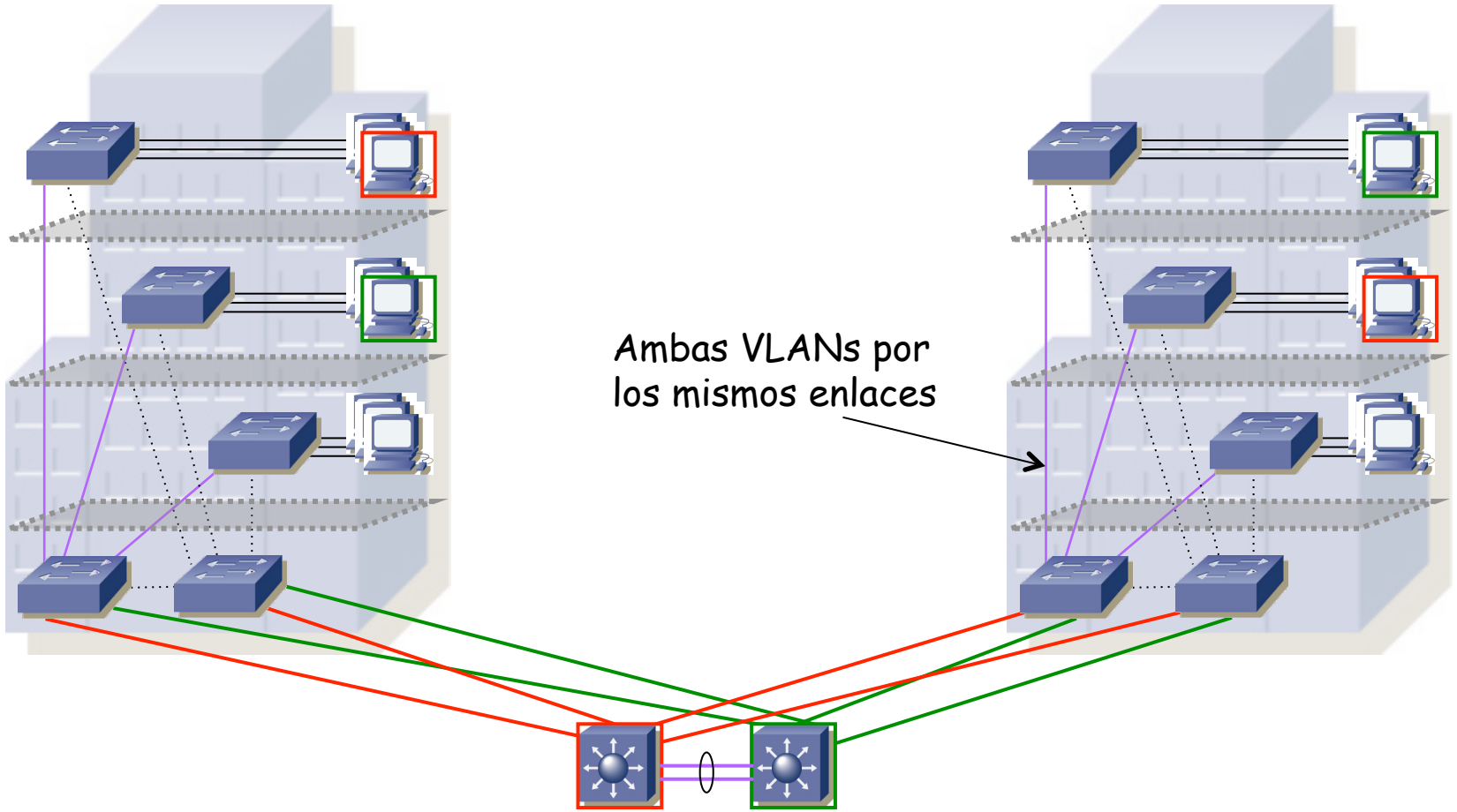
Campus-wide VLANs

- Podríamos necesitar extender VLANs por todo el campus
- Cuanto más grande sea el dominio de broadcast peor, no solo por los broadcast sino por la fragilidad de STP



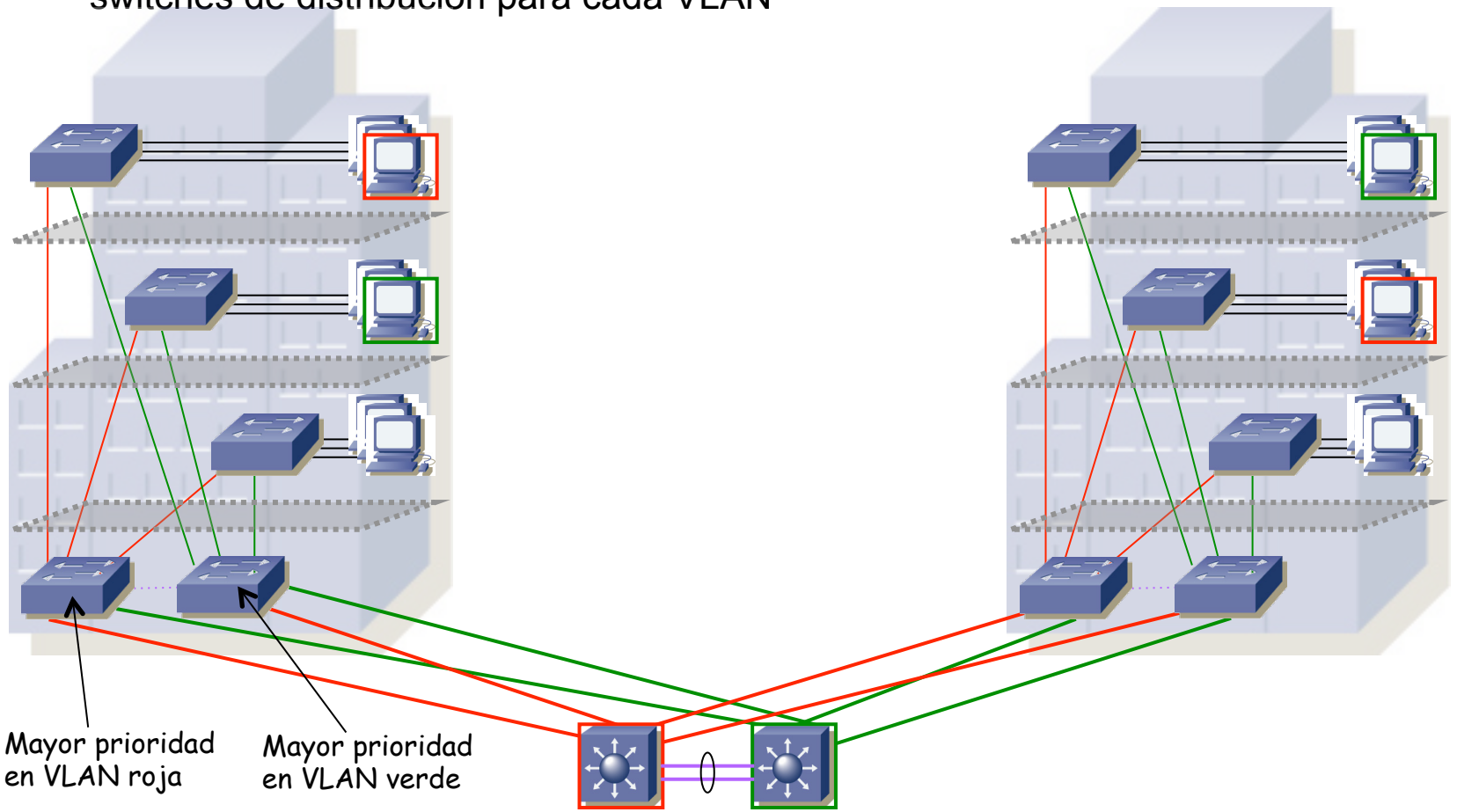
Mutiple Spanning Tree

- Podríamos emplear diferente raíz para dos grupos de VLANs
- Conseguimos utilizar todos los enlaces al core
- Pero no los de distribución



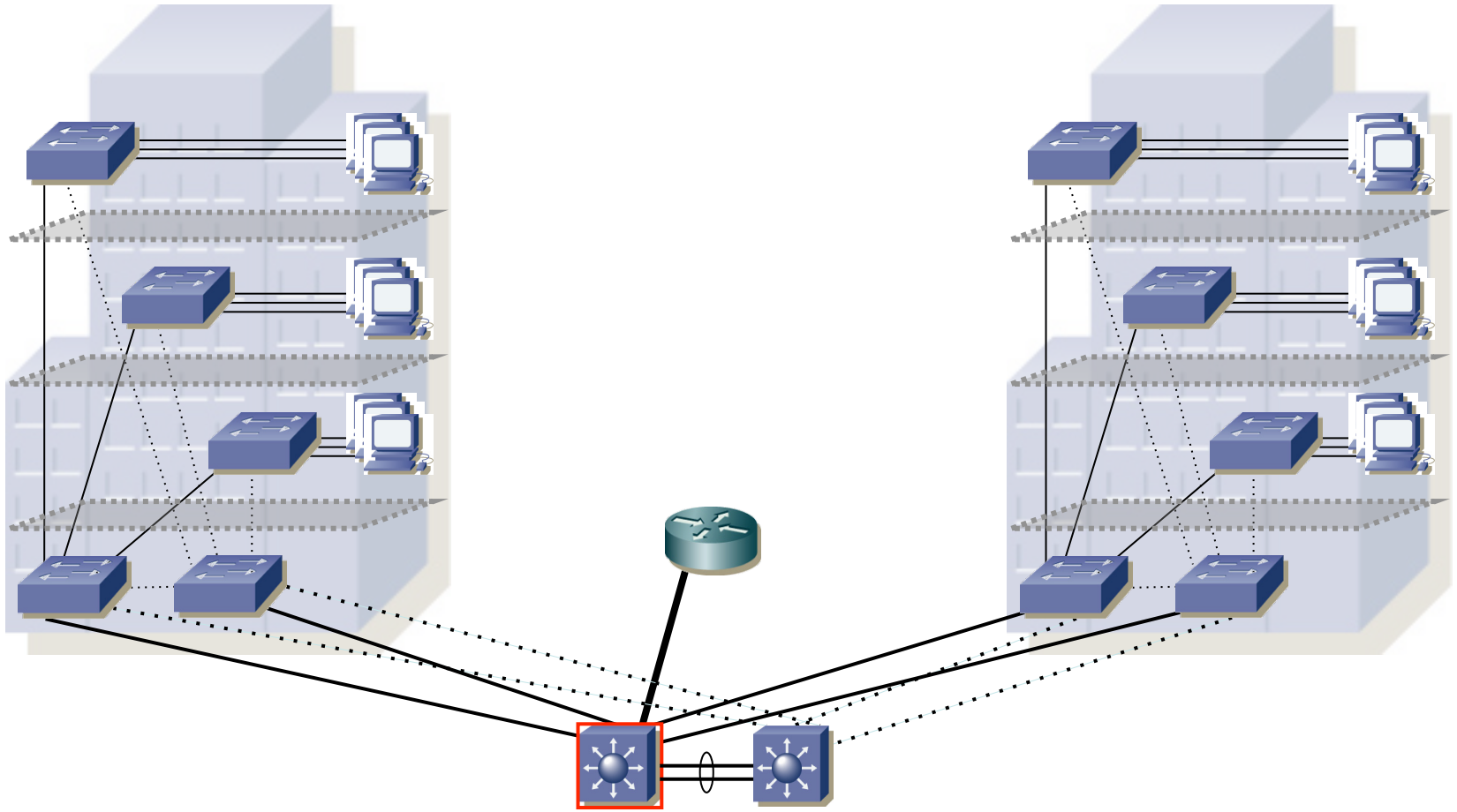
Mutiple Spanning Tree

- Podríamos emplear diferente raíz para dos grupos de VLANs
- Conseguimos utilizar todos los enlaces al core
- Pero no los de distribución
- Para aprovechar los enlaces de distribución podríamos alterar prioridades en los switches de distribución para cada VLAN



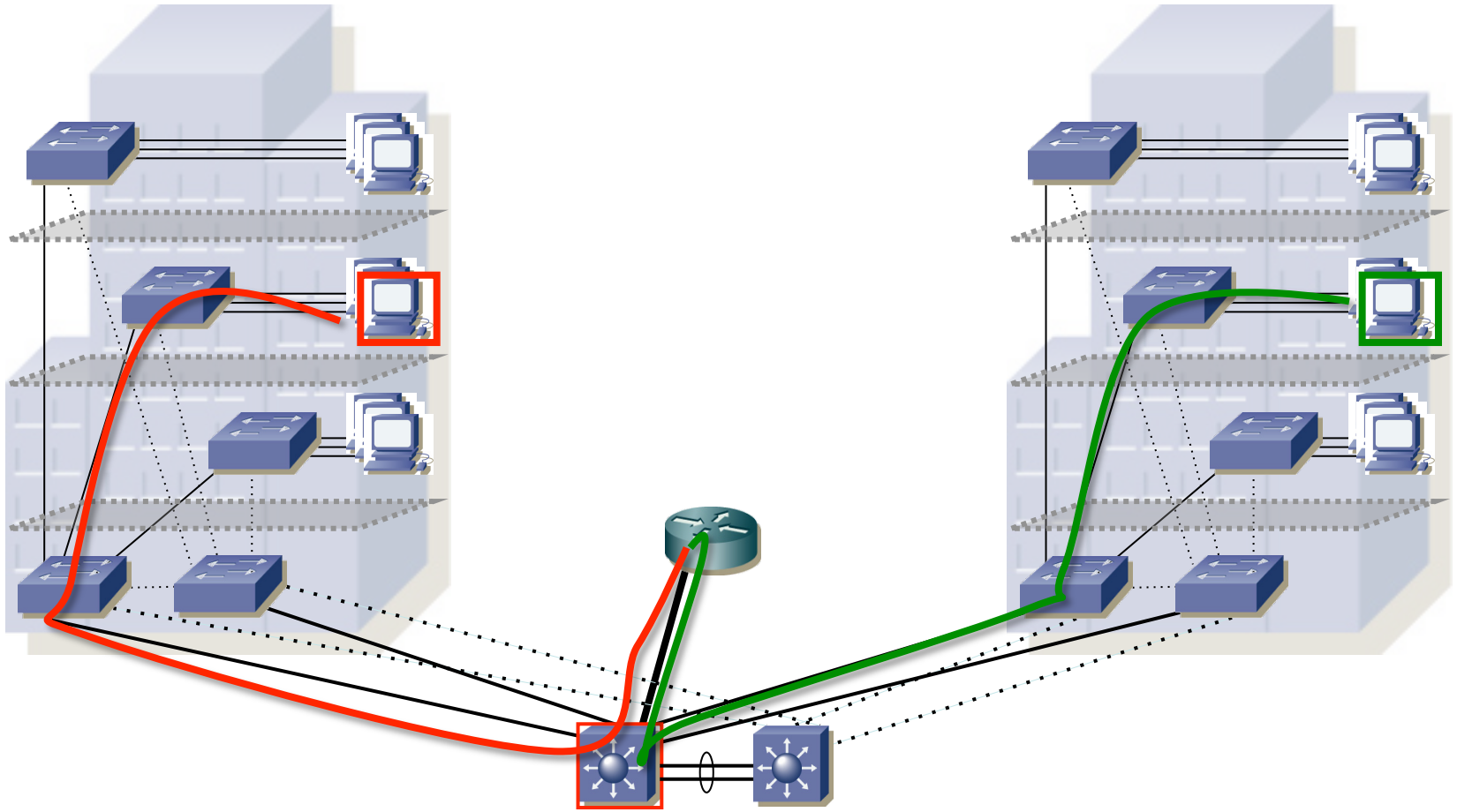
Enrutamiento

- Por ejemplo en el caso de un CST y con un router dedicado
- Por ejemplo un enlace troncal con todas las VLANs (...)



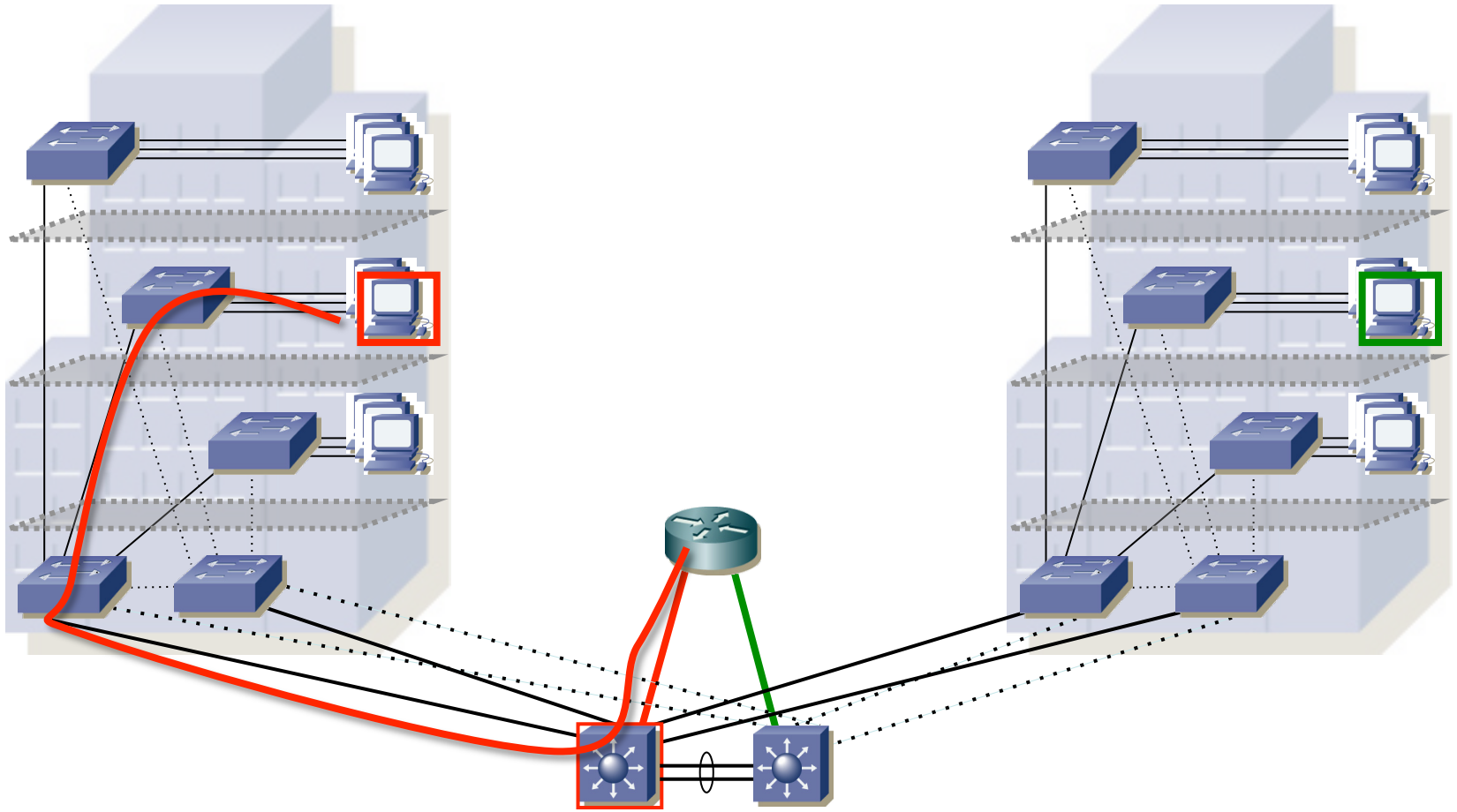
Enrutamiento

- Por ejemplo en el caso de un CST y con un router dedicado
- Por ejemplo un enlace troncal con todas las VLANs (...)



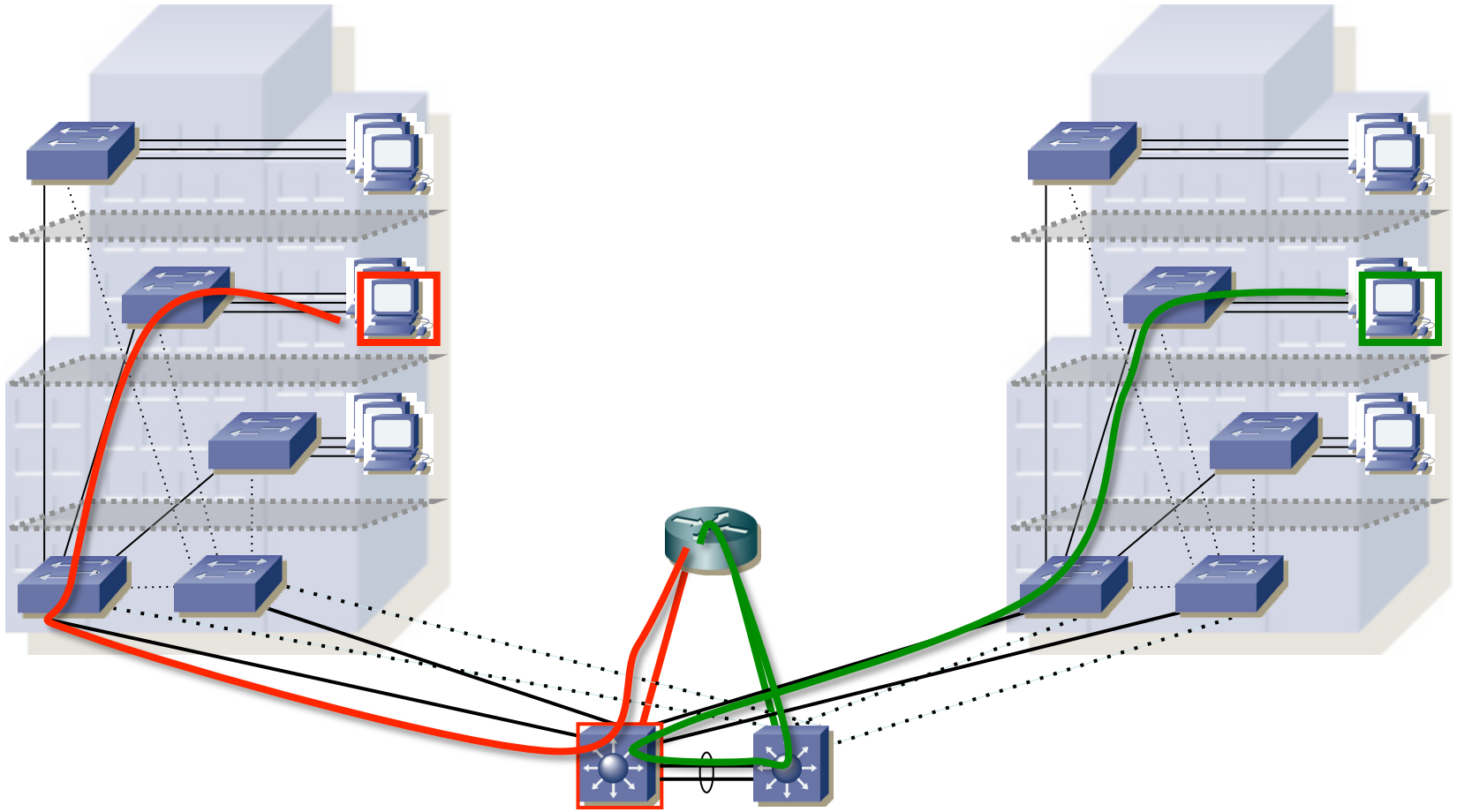
Enrutamiento

- Por ejemplo en el caso de un CST y con un router dedicado
- O dos enlaces, uno en cada VLAN (...)



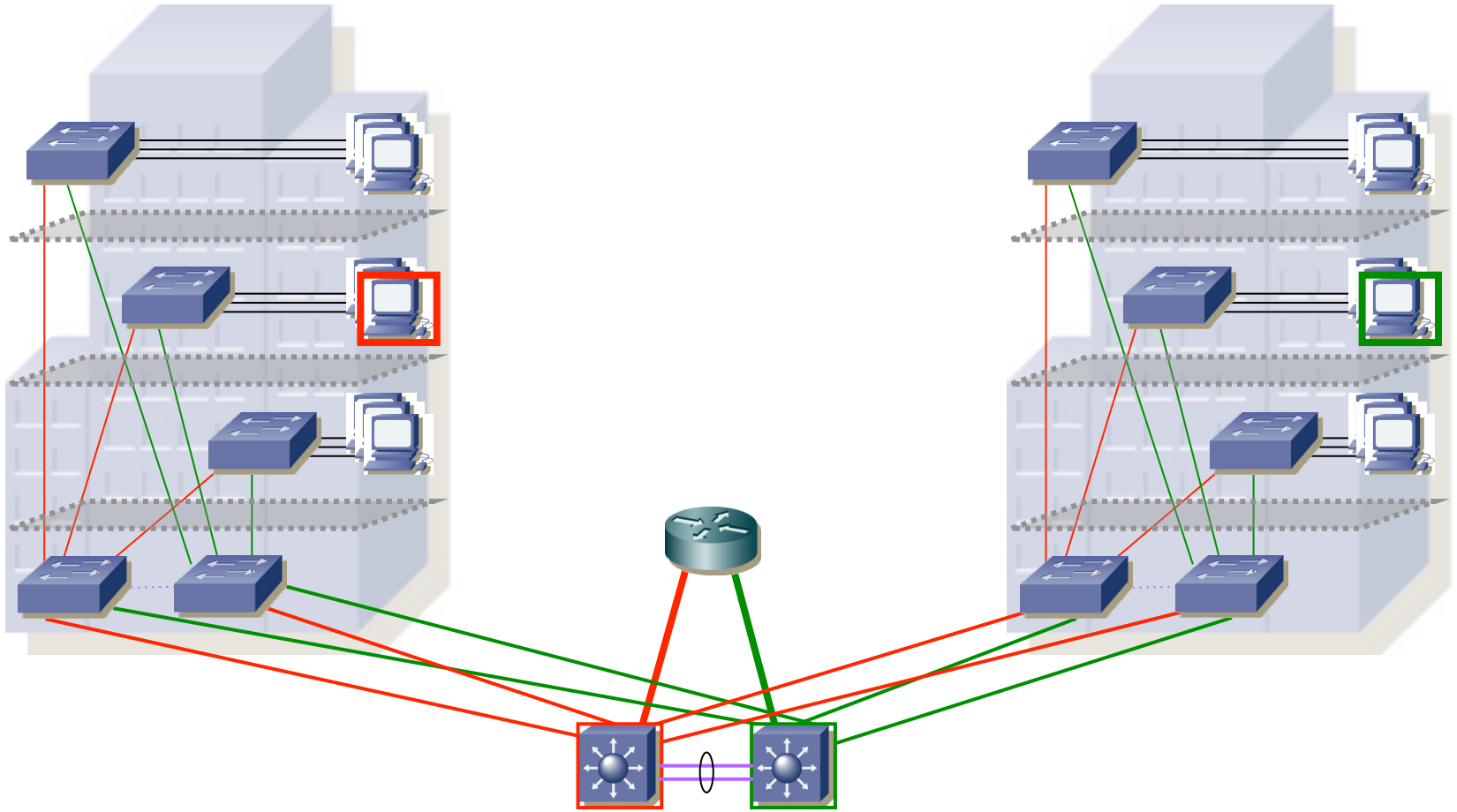
Enrutamiento

- Por ejemplo en el caso de un CST y con un router dedicado
- O dos enlaces, uno en cada VLAN
- Tener dos enlaces a los dos conmutadores del core no parece especialmente rentable



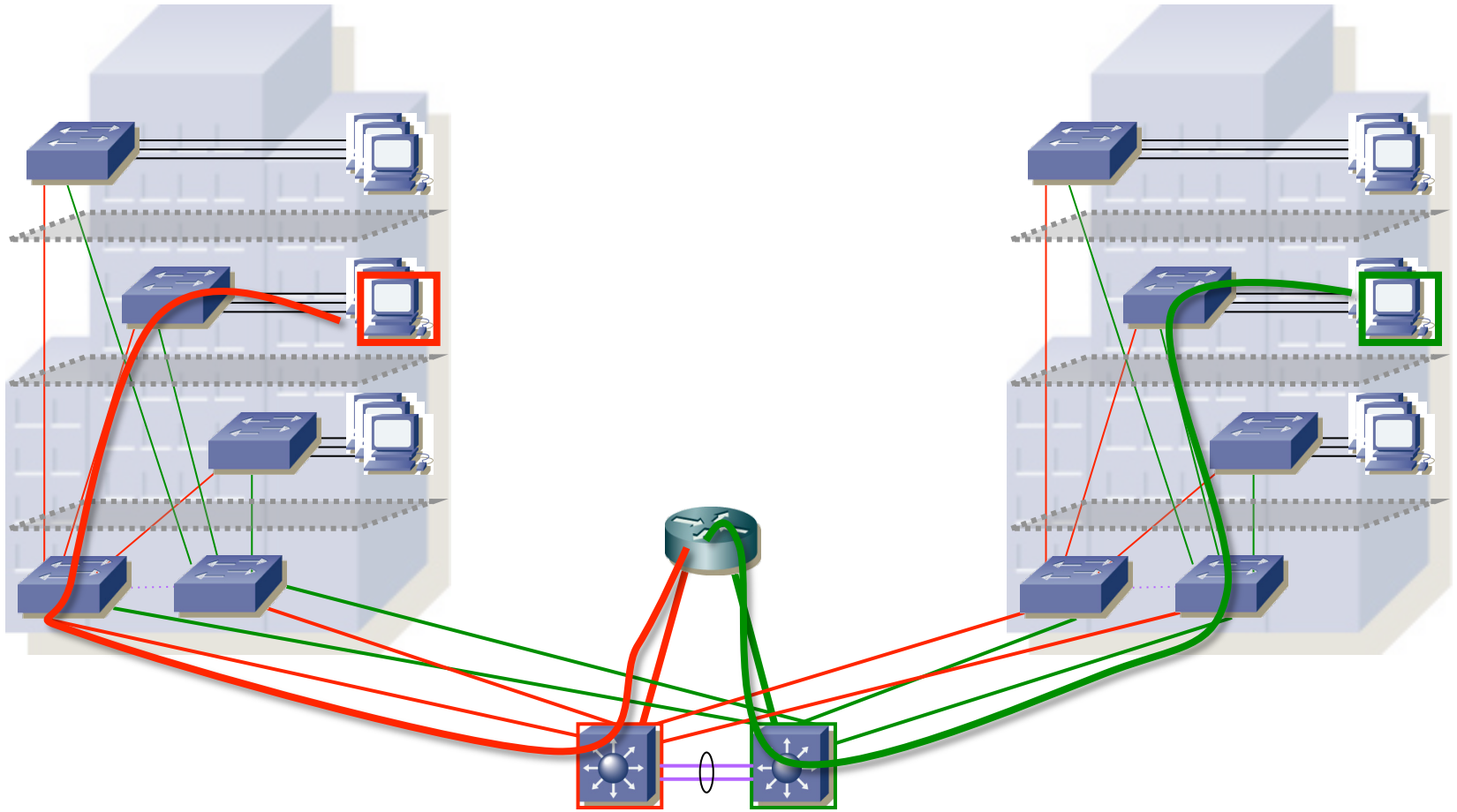
Enrutamiento

- ¿Y con los MSTs? (...)



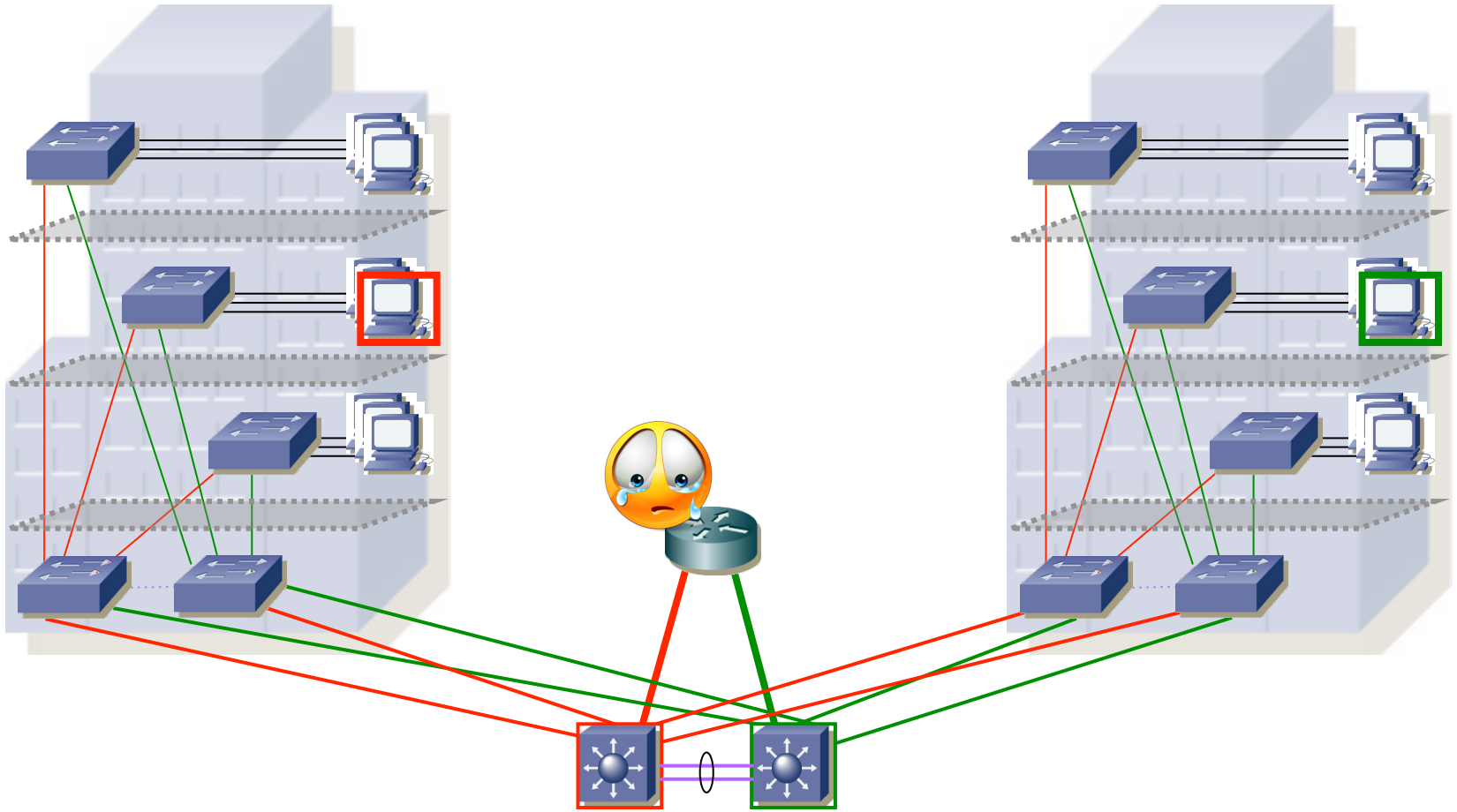
Enrutamiento

- ¿Y con los MSTs?
- Al menos no comparte enlaces el tráfico de una VLAN con el de la otra



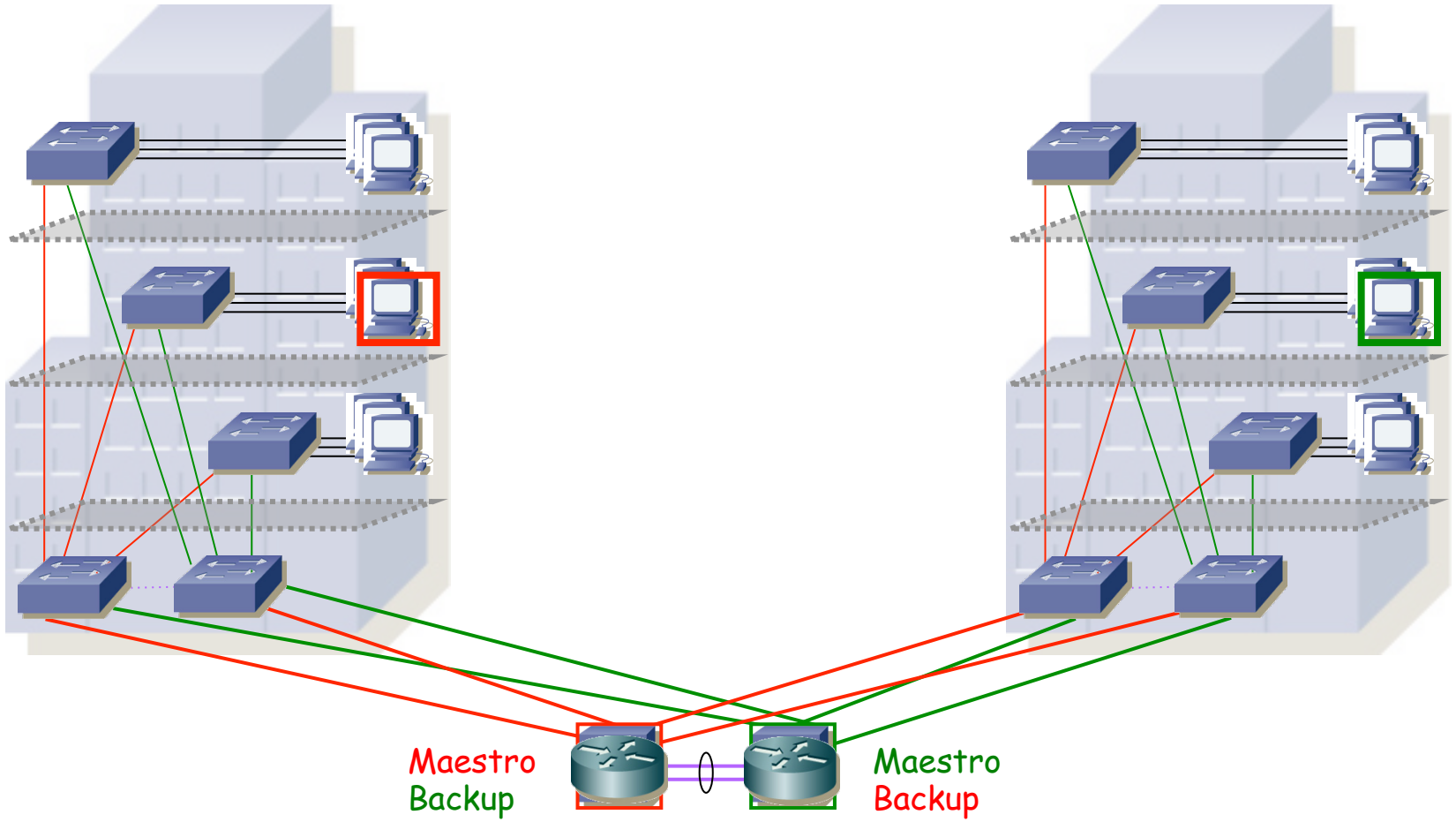
Enrutamiento

- En cualquiera de estos esquemas, no hay redundancia en ese router
- Ni en sus enlaces
- (...)



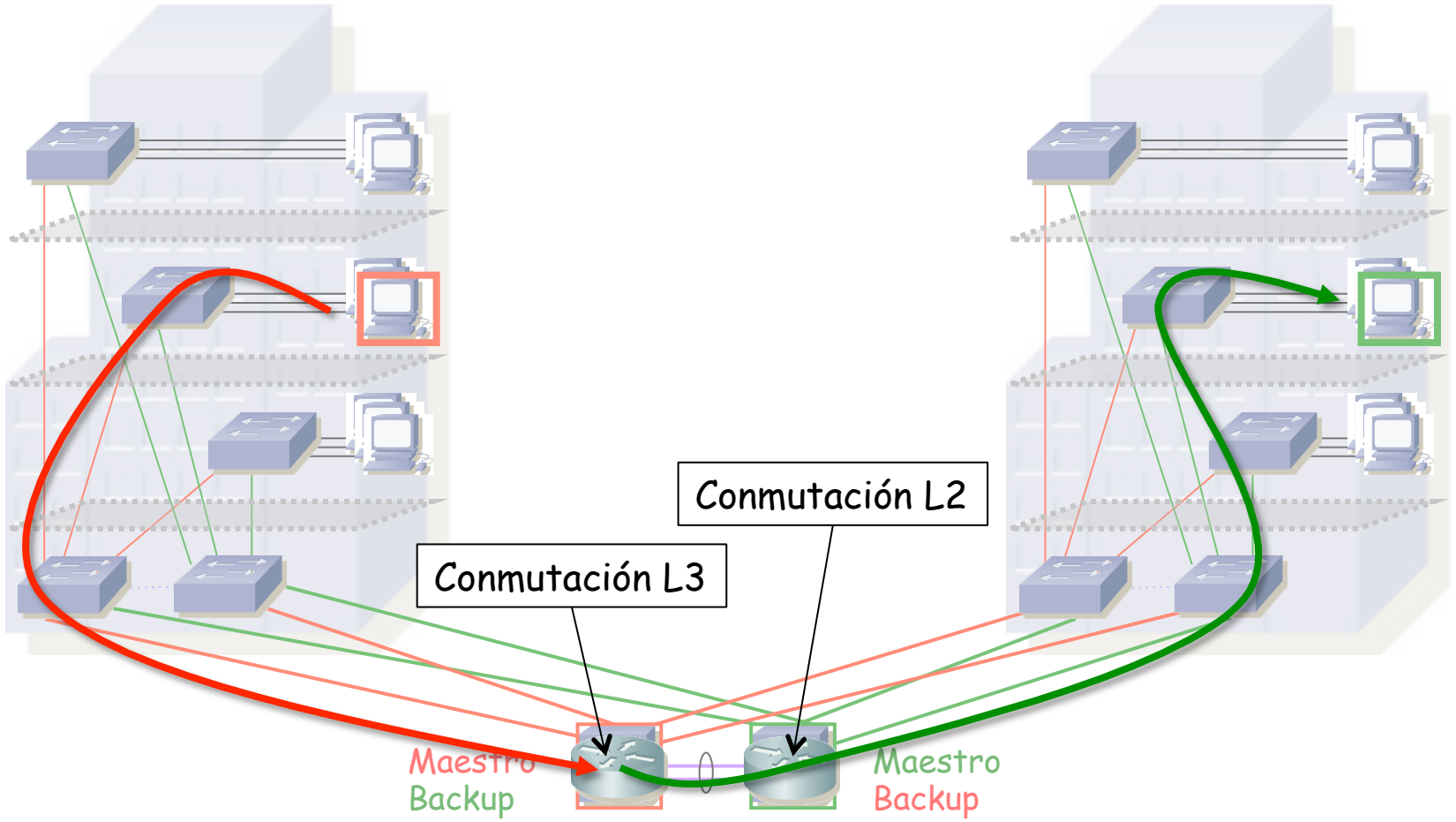
Enrutamiento

- Una solución habitual es que esos conmutadores del core sean capa 2/3 y se encarguen del encaminamiento entre VLANs
- Podemos añadir un FHRP y que se repartan tareas de maestro y backup para diferentes VLANs (...)



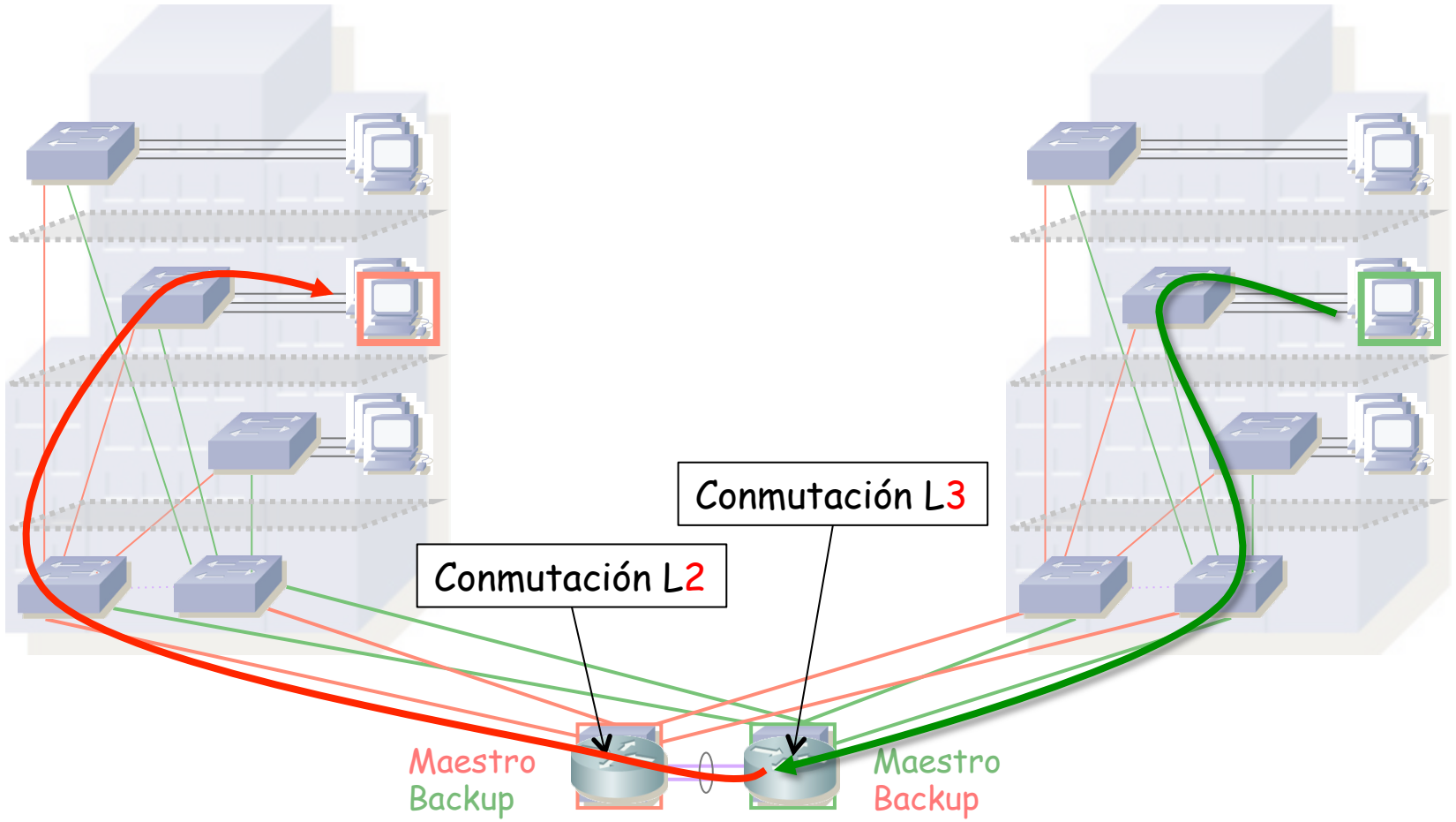
Enrutamiento

- Una solución habitual es que esos conmutadores del core sean capa 2/3 y se encarguen del encaminamiento entre VLANs
- Podemos añadir un FHRP y que se repartan tareas de maestro y backup para diferentes VLANs (...)



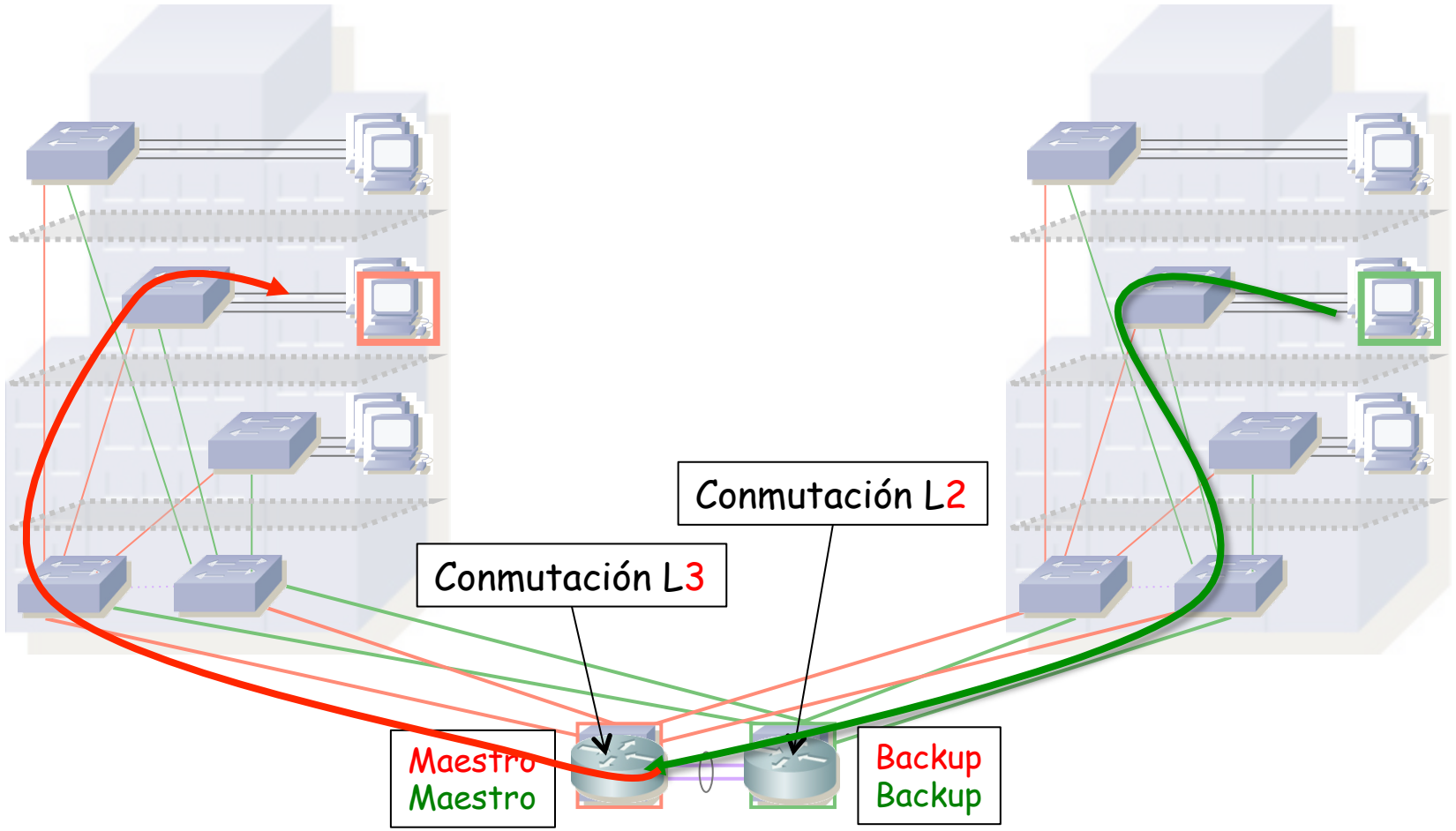
Enrutamiento

- Una solución habitual es que esos conmutadores del core sean capa 2/3 y se encarguen del encaminamiento entre VLANs
- Podemos añadir un FHRP y que se repartan tareas de maestro y backup para diferentes VLANs (...)



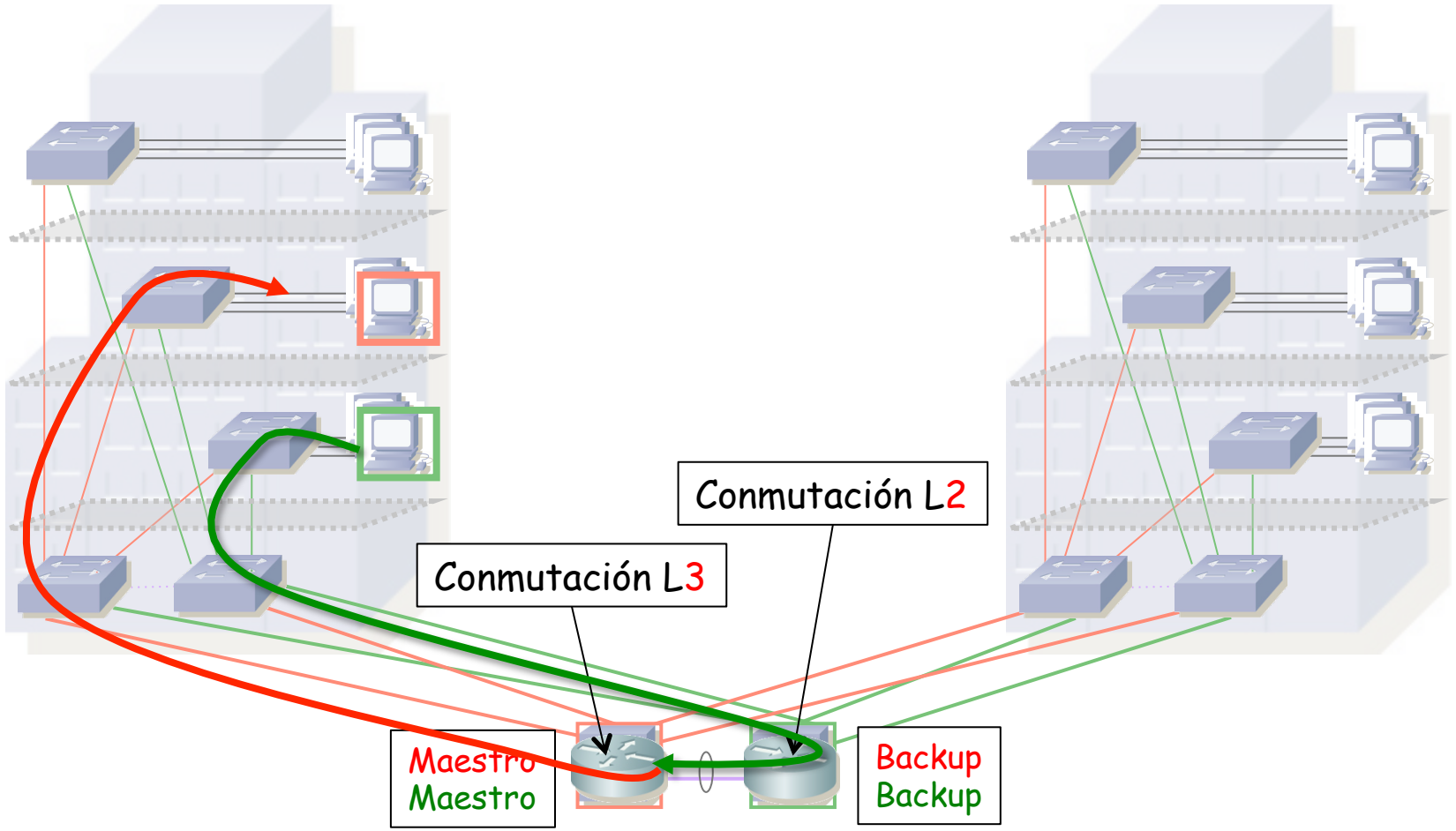
Enrutamiento

- Por simplicidad de gestión puede tener sentido dejar el mismo como maestro en todas las subredes



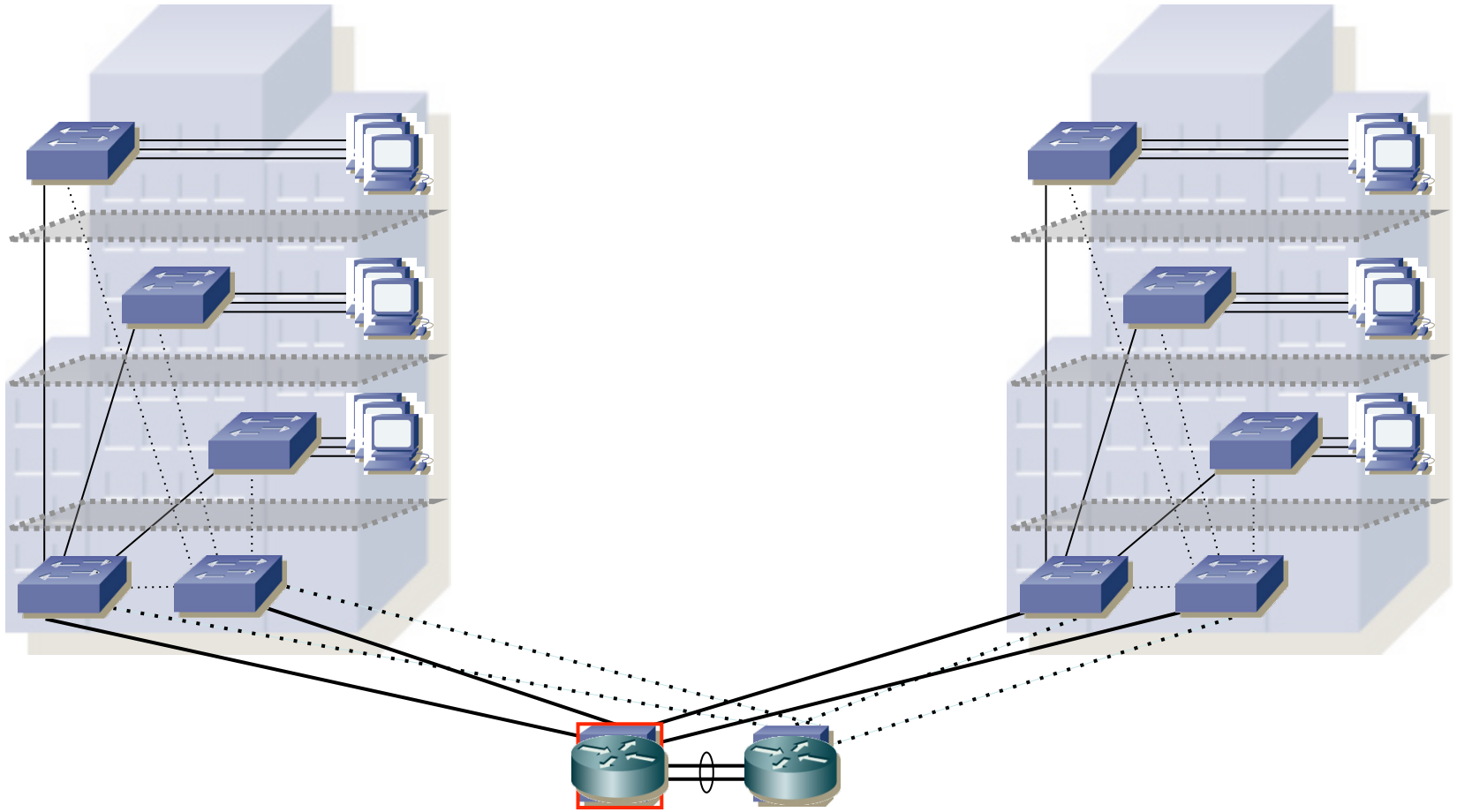
Enrutamiento

- Los dos hosts pueden estar en el mismo edificio



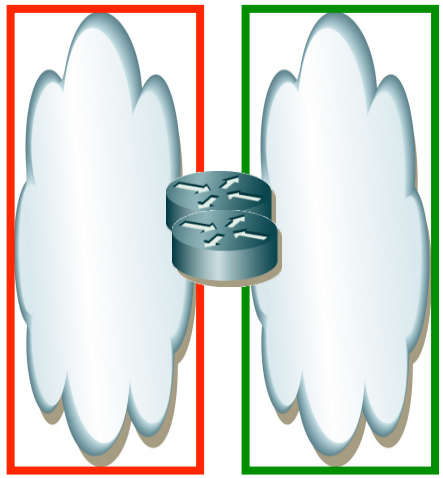
Enrutamiento

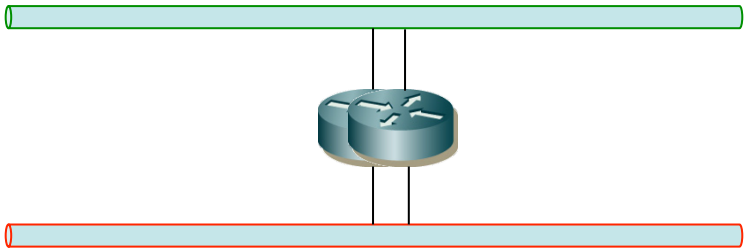
- Y seguramente tampoco compense repartir las VLANs (un CST)
- Con lo que el segundo switch del core queda completamente como backup
- La mejor forma de utilizarlo es poder crear un switch virtual con el otro



Enrutamiento

- Al final en capa 3 se quedaría simplemente en esto

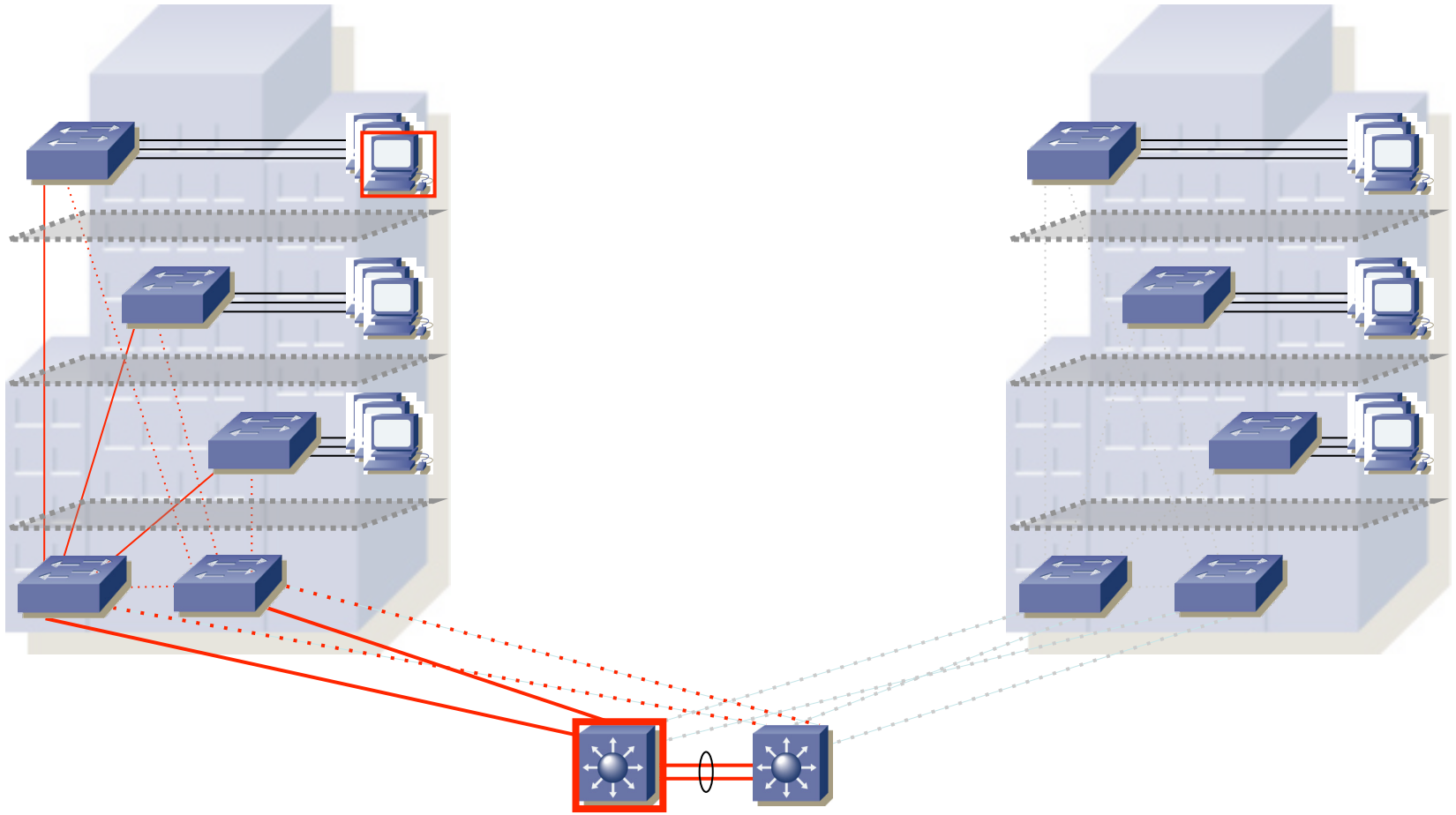




Enrutamiento con VLANs restringidas

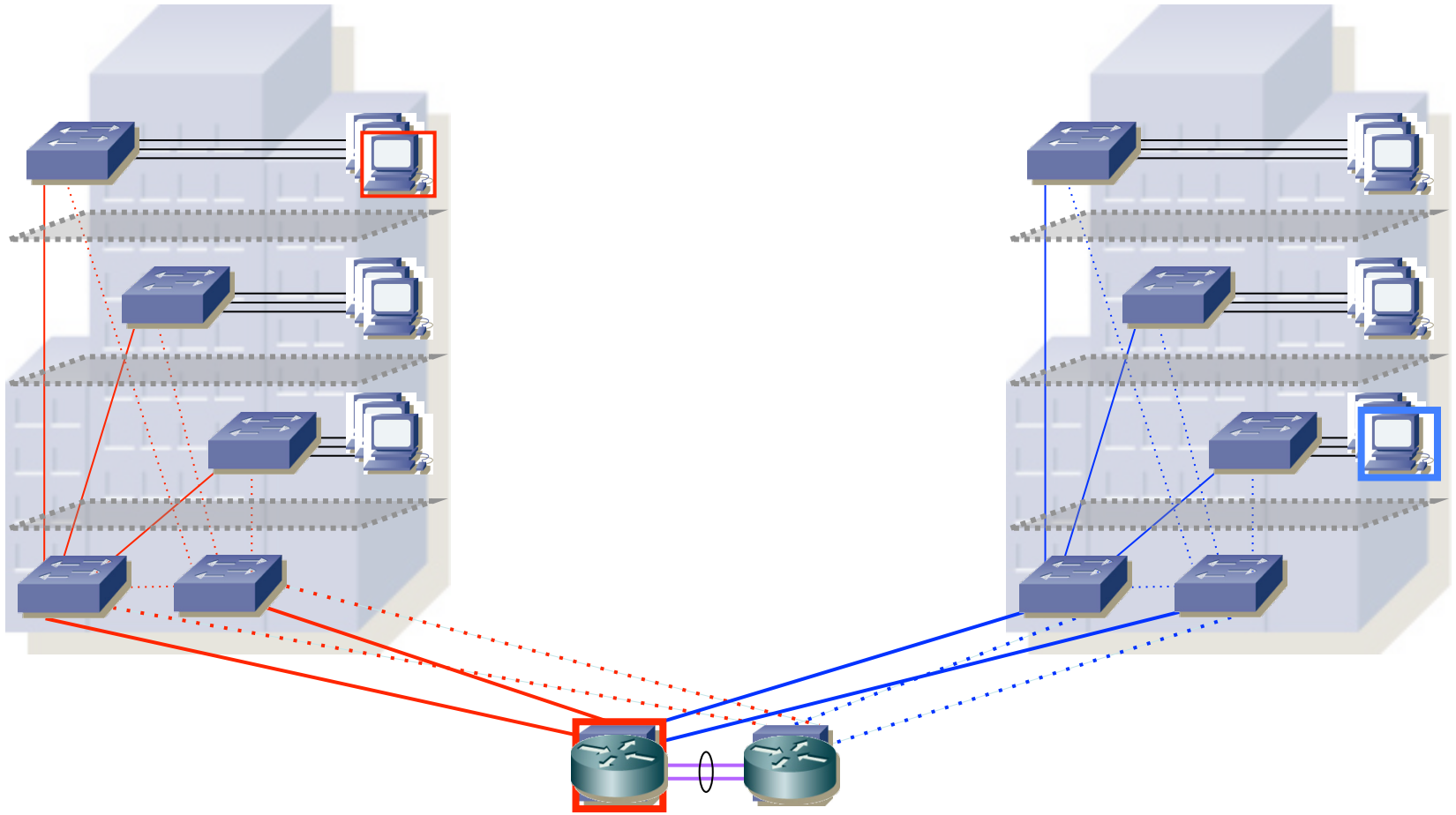
VLANs restringidas

- Campus-wide VLANs poco recomendadas para red grande
- Sin ellas, tenemos VLANs localizadas en cada *distribution block*
- En este caso, en cada edificio
- Deben extenderse hasta el core si el router es un switch del mismo



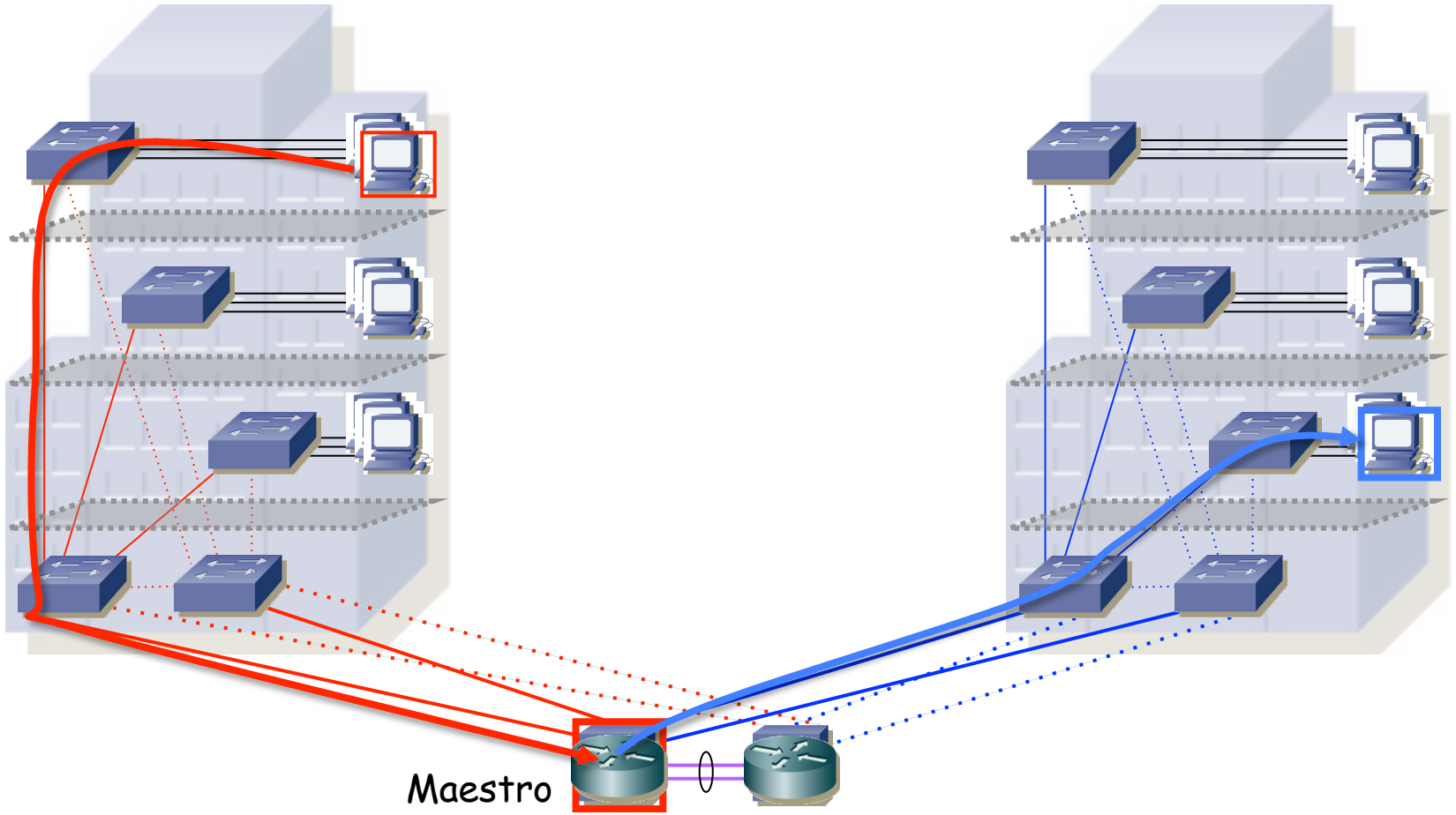
Enrutamiento

- Si el *root bridge* es el mismo en las VLANs de edificios diferentes puede interesar que el primario del FHRP sea el mismo *root bridge* (...)



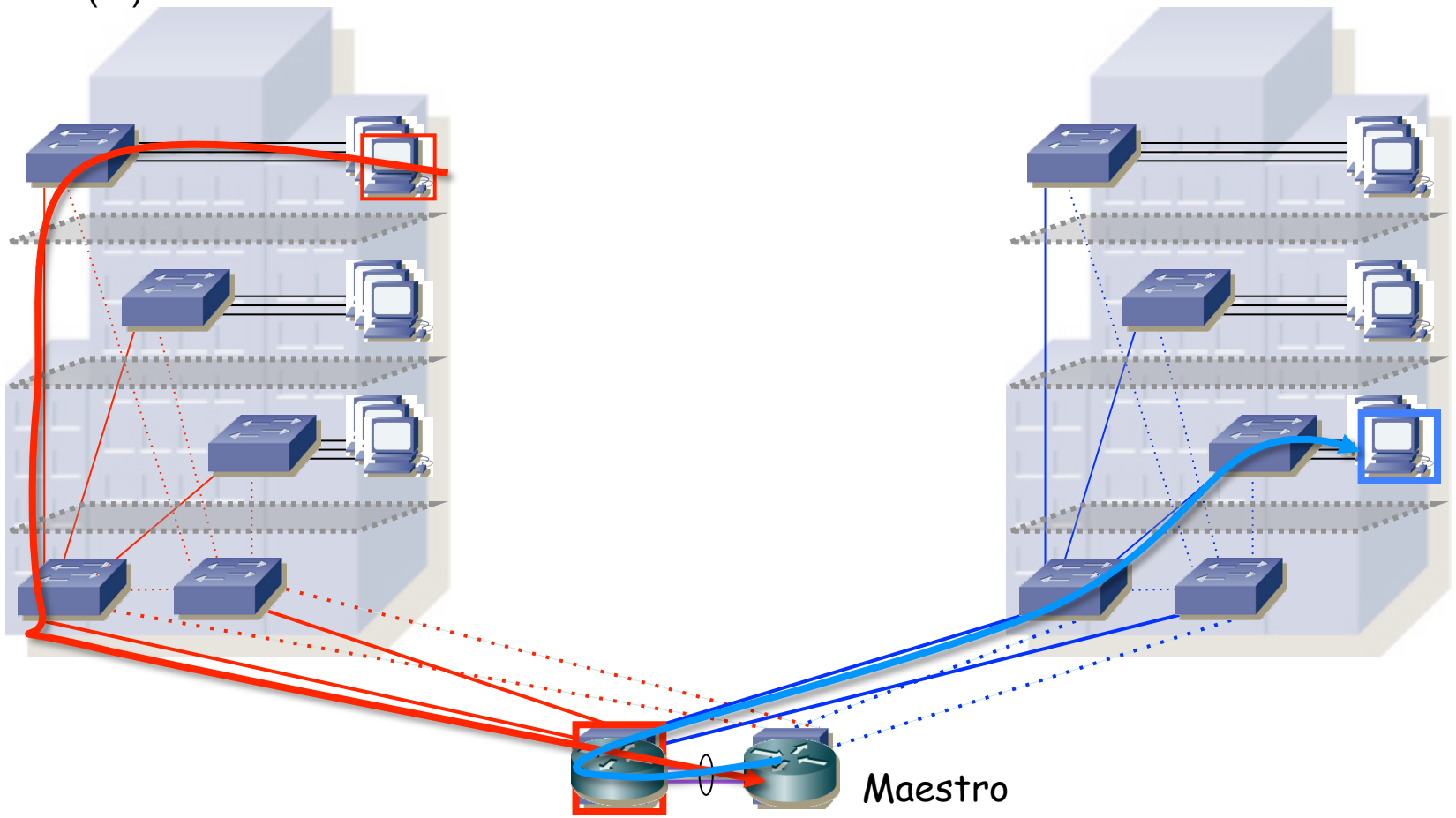
Enrutamiento

- Si el *root bridge* es el mismo en las VLANs de edificios diferentes puede interesar que el primario del FHRP sea el mismo *root bridge*
- Si no (...)



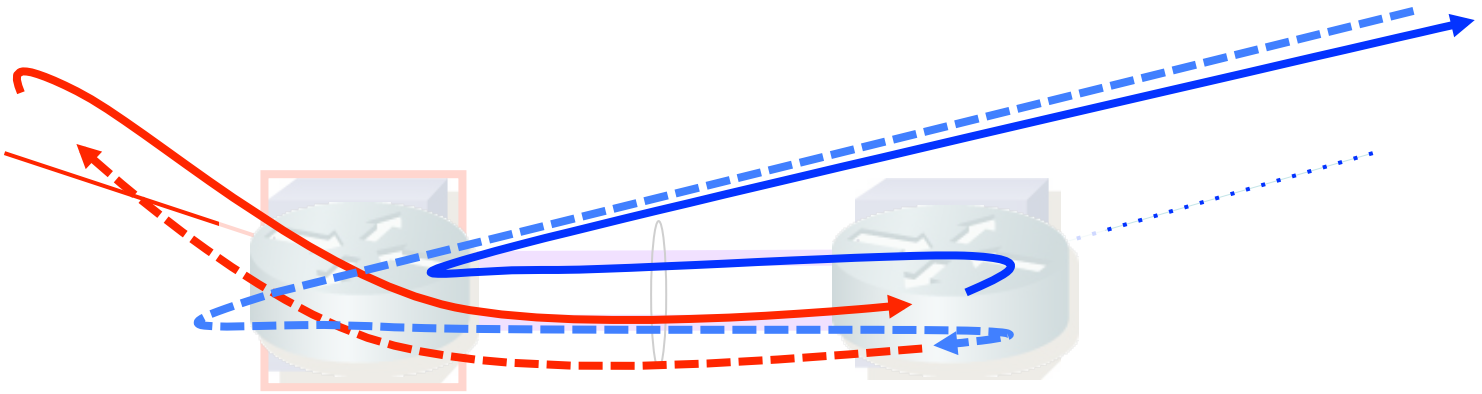
Enrutamiento

- Si el *root bridge* es el mismo en las VLANs de edificios diferentes puede interesar que el primario del FHRP sea el mismo *root bridge*
- Si no pasaría por el enlace entre los conmutadores del core
- No es un problema en sí pero si el flujo es bidireccional coinciden en ese enlace (...)



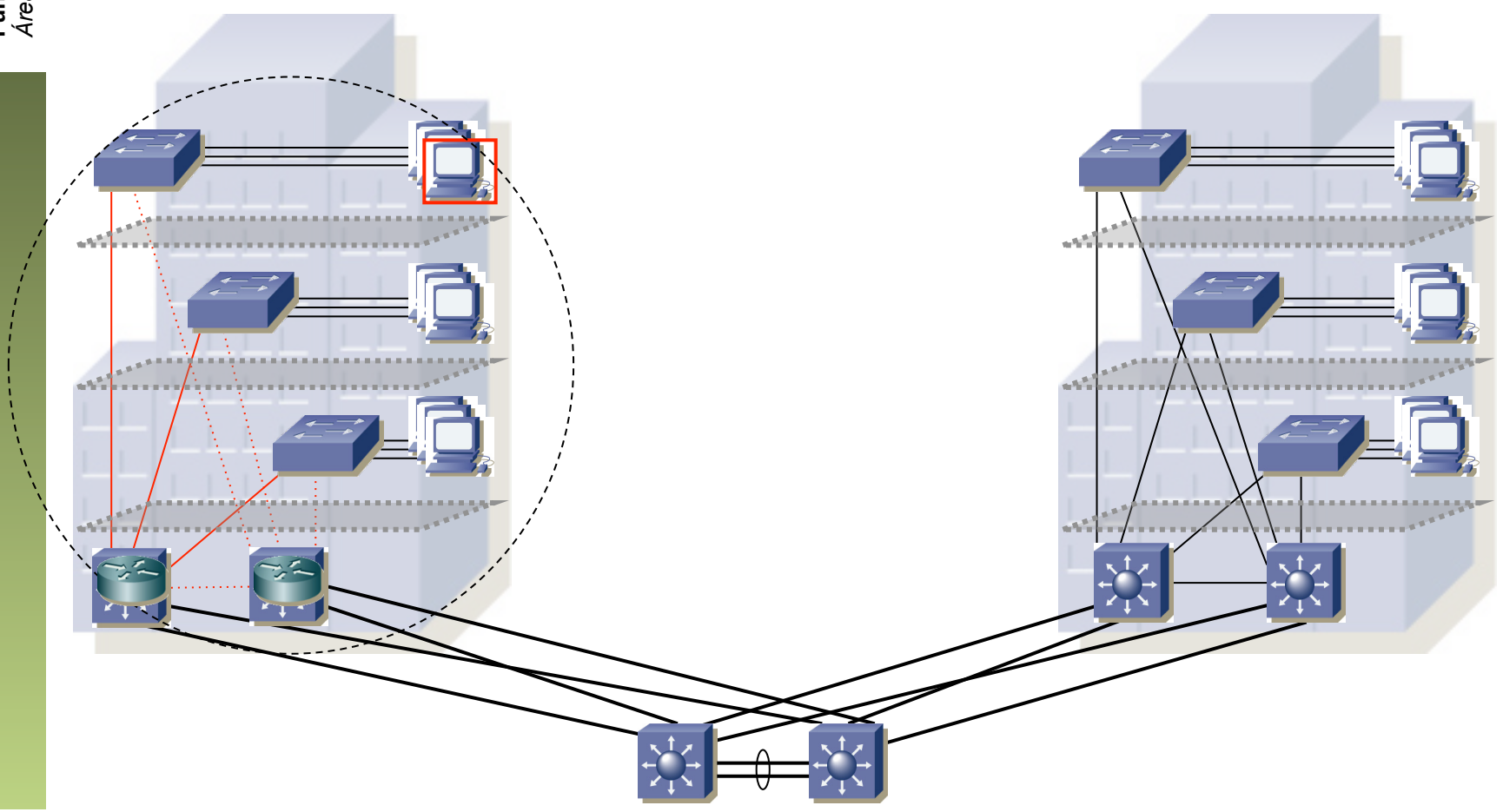
Enrutamiento

- Si el *root bridge* es el mismo en las VLANs de edificios diferentes puede interesar que el primario del FHRP sea el mismo *root bridge*
- Si no, pasaría por el enlace entre los conmutadores del core
- No es un problema en sí pero si el flujo es bidireccional coinciden en ese enlace
- En el enlace entre los conmutadores coincide el tráfico en un sentido con el tráfico en el otro (¡ menos mal que tenemos un LAG !)
- Eso no sucedía con la otra alternativa
- De cara a reducir errores de configuración y entender la red de cara al *troubleshooting* nos interesa la solución más simple



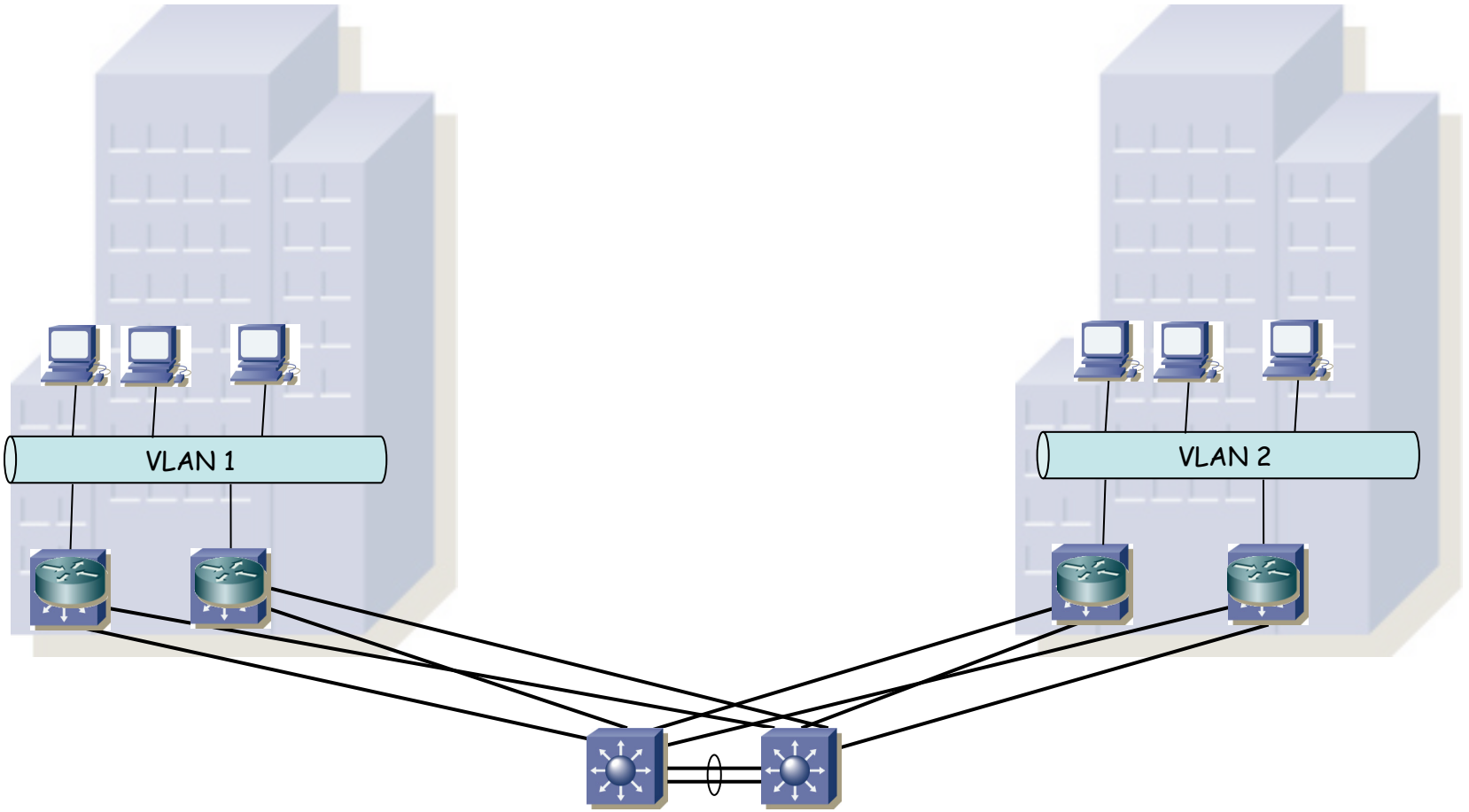
Capa 3 en distribución

- La siguiente alternativa es tener conmutadores capa 2/3 en la distribución
- Ahora sí que las VLANs están restringidas al sistema de distribución
- Habrá que enrutar en ese sistema de distribución
- Y ya que nos ponemos, que sea con redundancia (FHRP) (…)



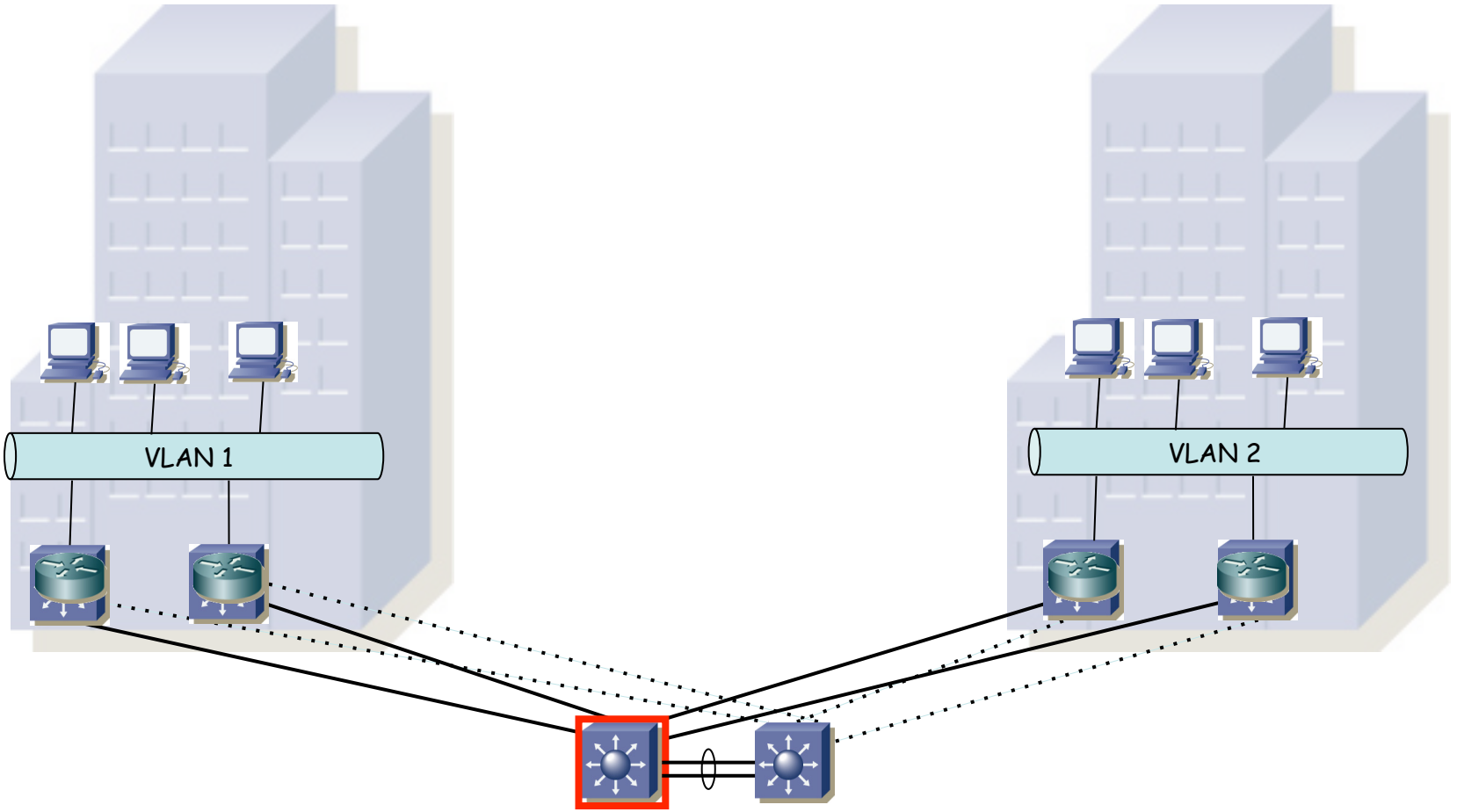
Capa 3 en distribución

- ¿Y cómo gestionamos la interconexión con el core?
- (…)



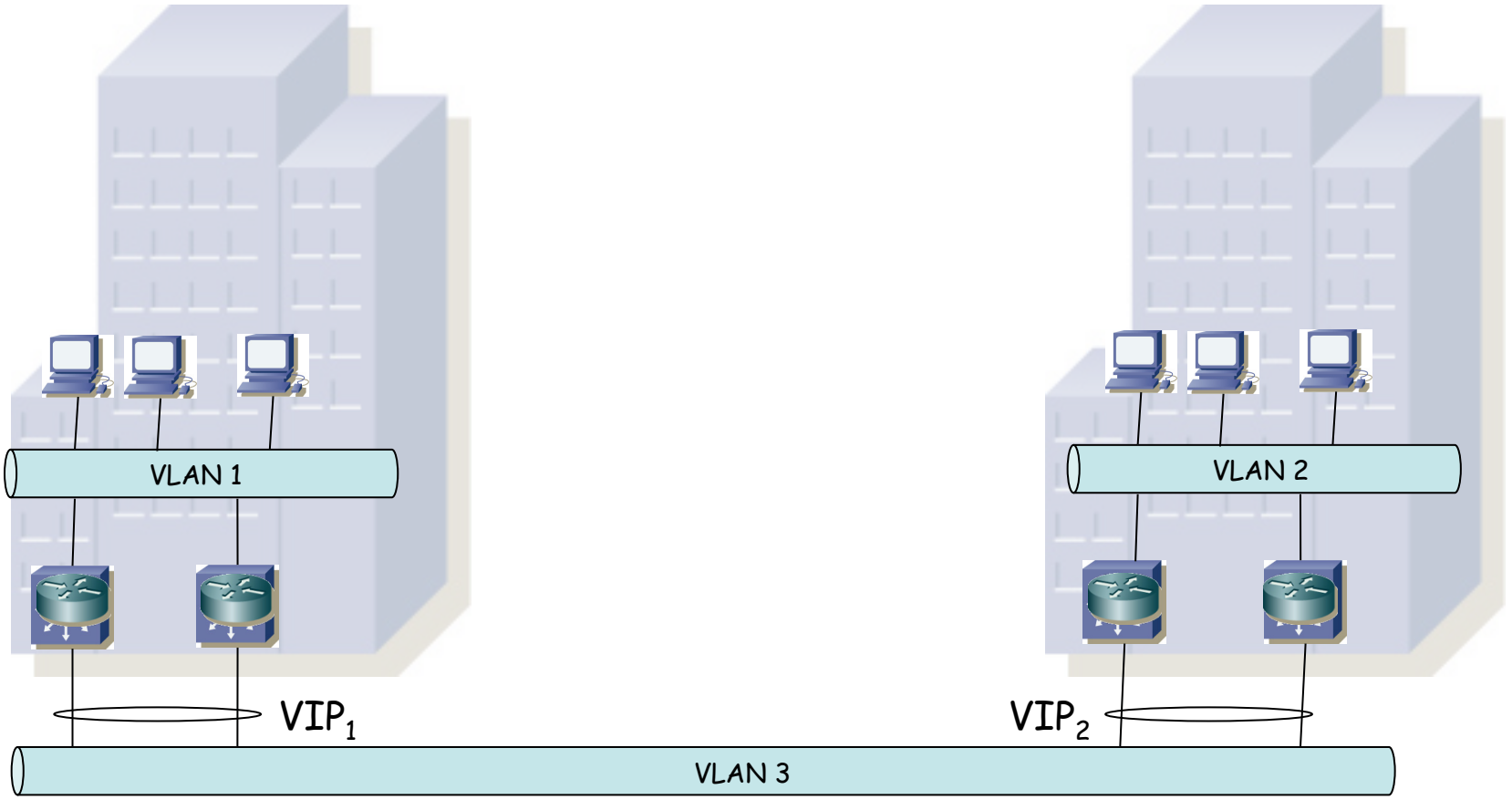
Capa 3 en distribución

- ¿Y cómo gestionamos la interconexión con el core?
- De nuevo podemos hacerlo en capa 2 (STP), por ejemplo con un FHRP (…)



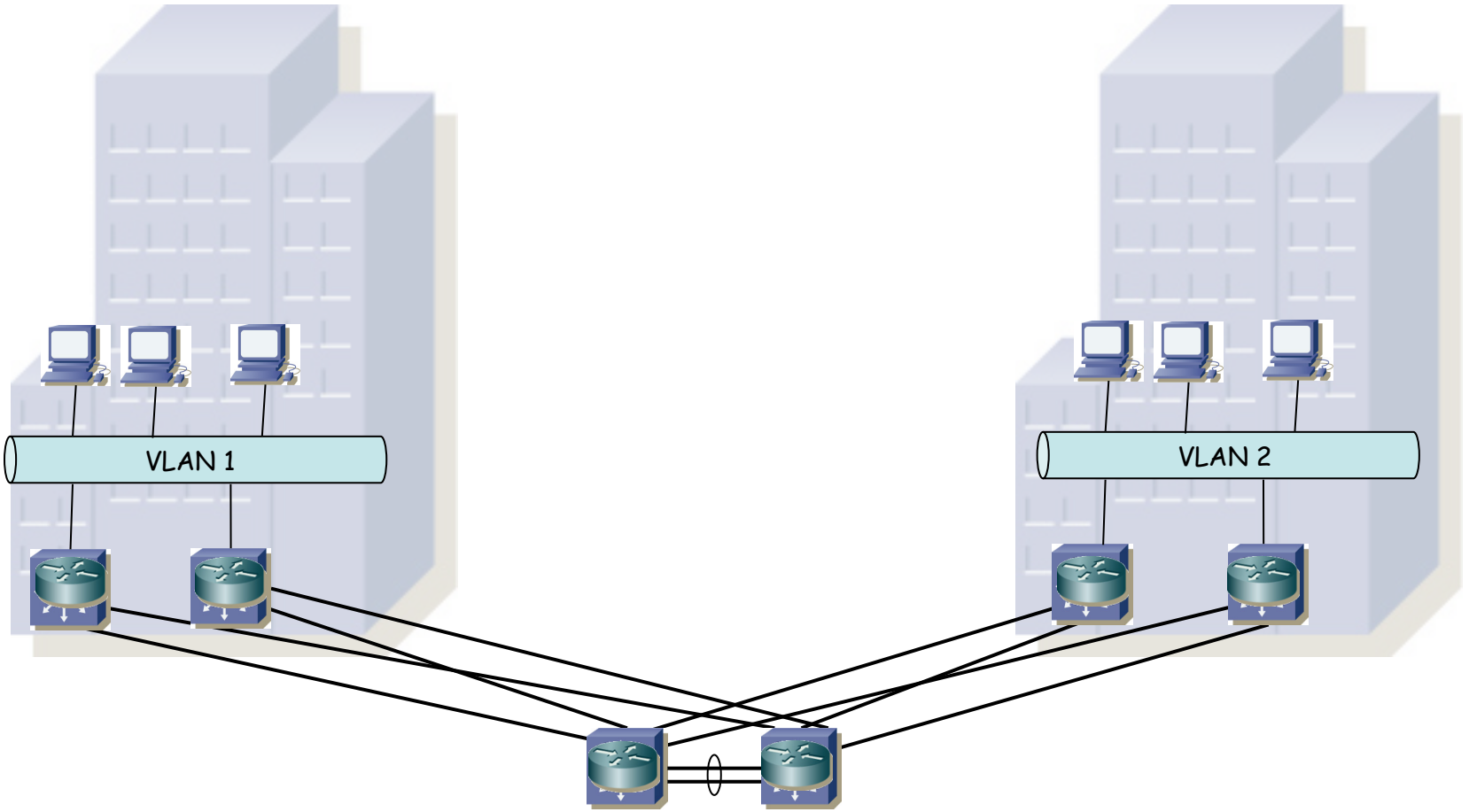
Capa 3 en distribución

- ¿Y cómo gestionamos la interconexión con el core?
- De nuevo podemos hacerlo en capa 2 (STP), por ejemplo con un FHRP
- (…)



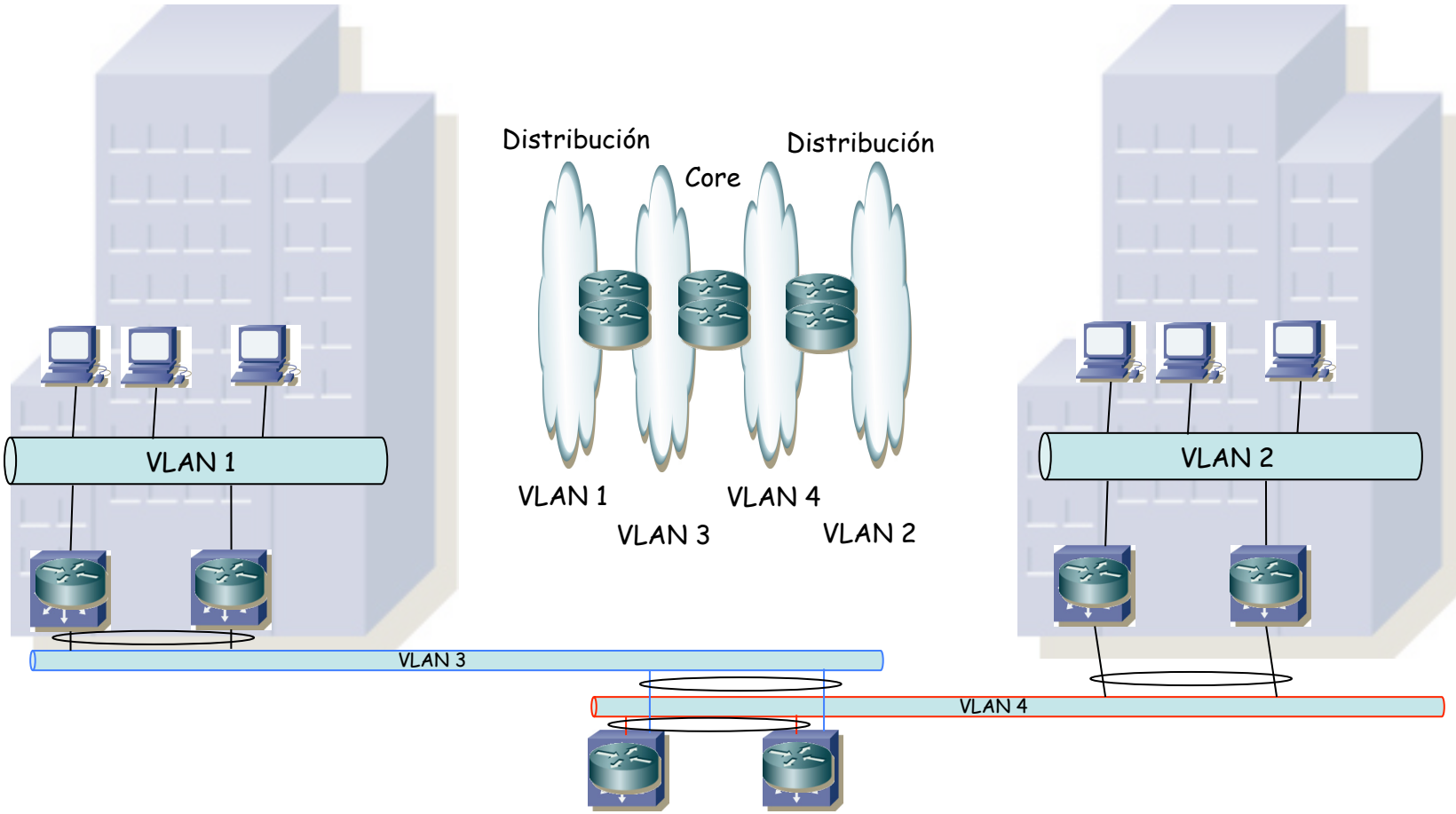
Capa 3 en distribución

- ¿Y cómo gestionamos la interconexión con el core?
- De nuevo podemos hacerlo en capa 2 (STP), por ejemplo con un FHRP
- O en capa 3, también con un FHRP (…)



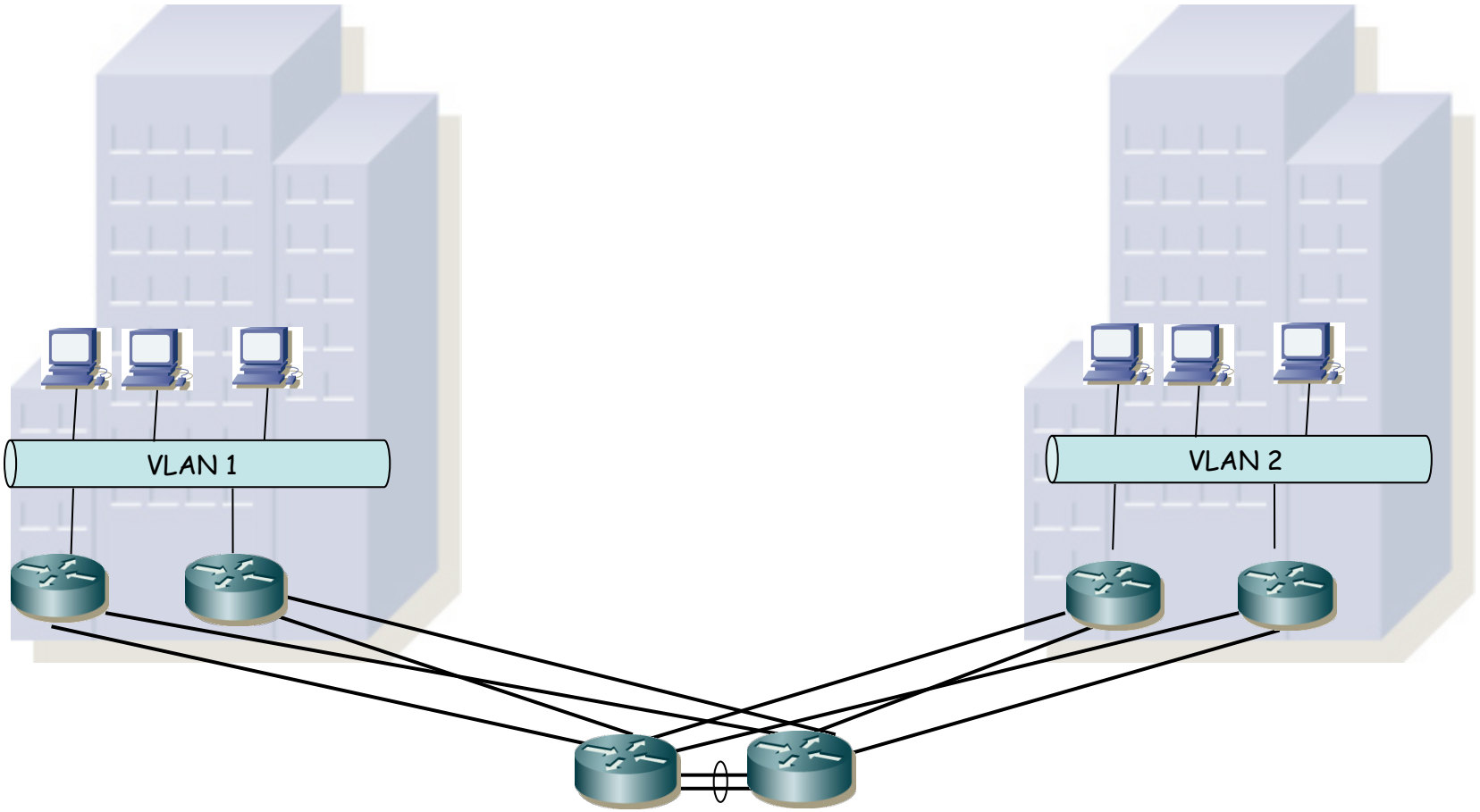
Capa 3 en distribución

- ¿Y cómo gestionamos la interconexión con el core?
- De nuevo podemos hacerlo en capa 2 (STP), por ejemplo con un FHRP
- O en capa 3, también con un FHRP
- (…)



Capa 3 en distribución

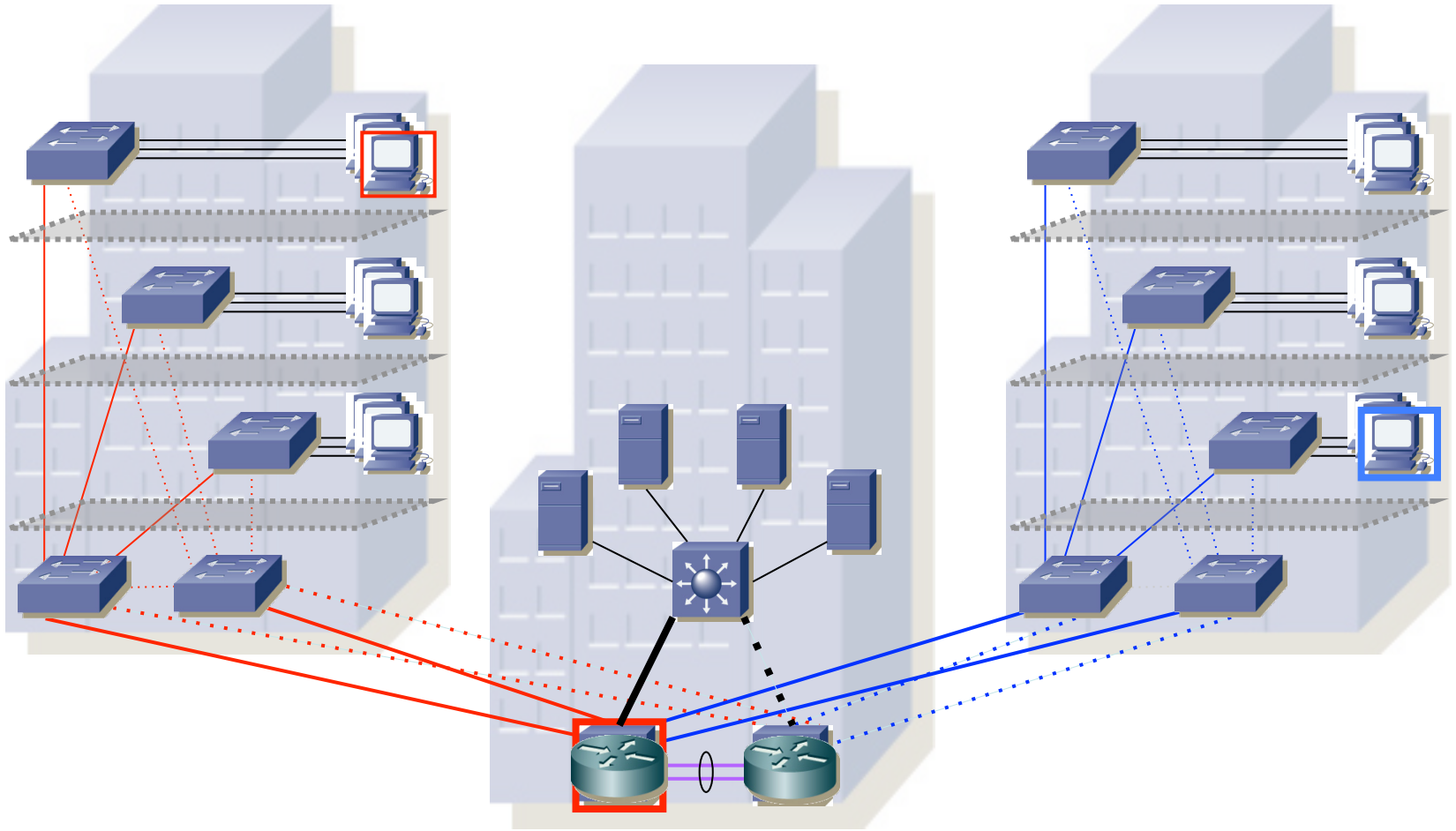
- ¿Y cómo gestionamos la interconexión con el core?
- De nuevo podemos hacerlo en capa 2 (STP), por ejemplo con un FHRP
- O en capa 3, también con un FHRP
- O todo en capa 3 y emplear un protocolo de encaminamiento



Servidores y exterior

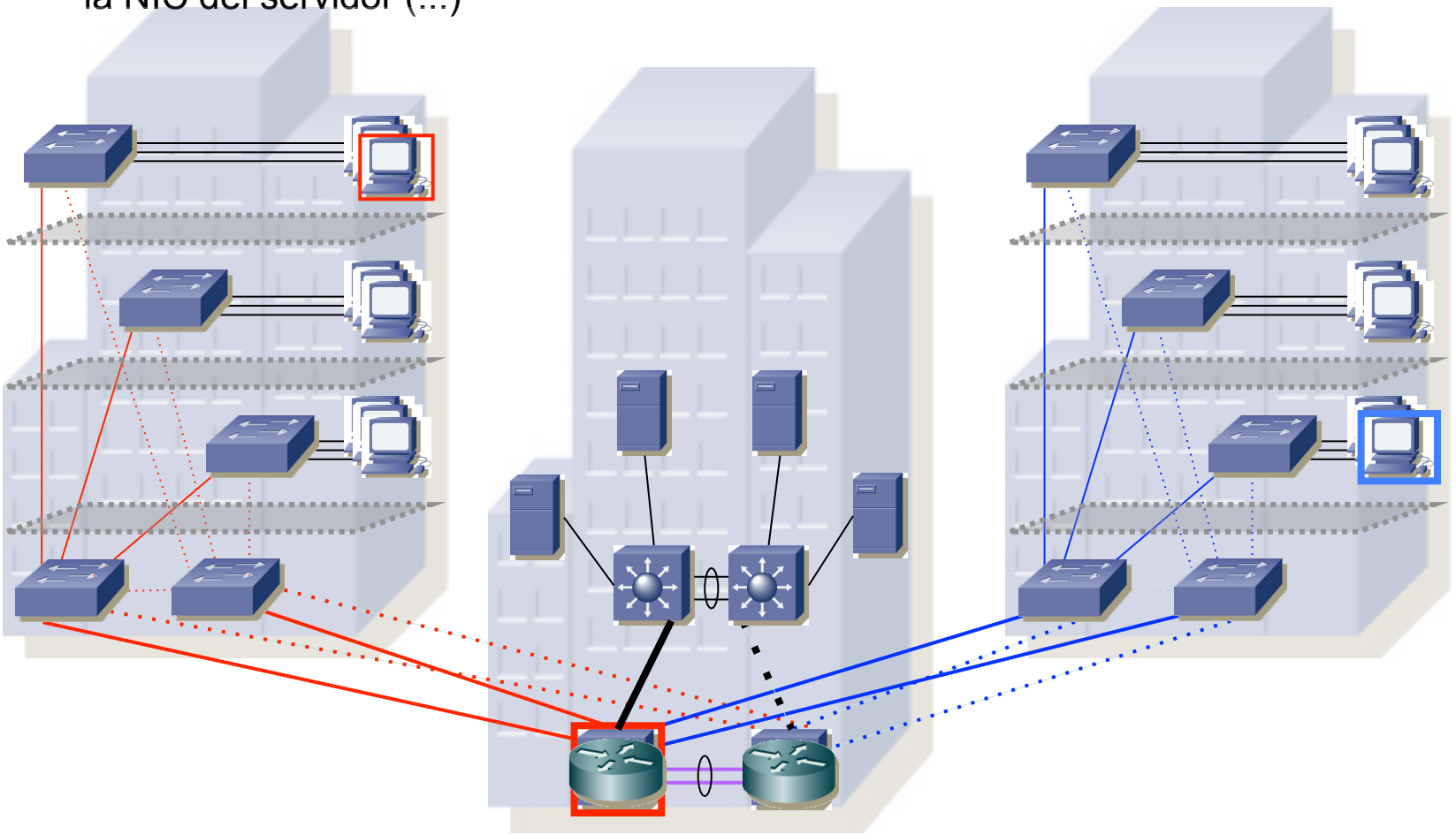
Centralización de servidores

- Podemos tener una VLAN con servidores centralizados
- Pero con esto hay un punto de fallo en ese nuevo conmutador
- (...)



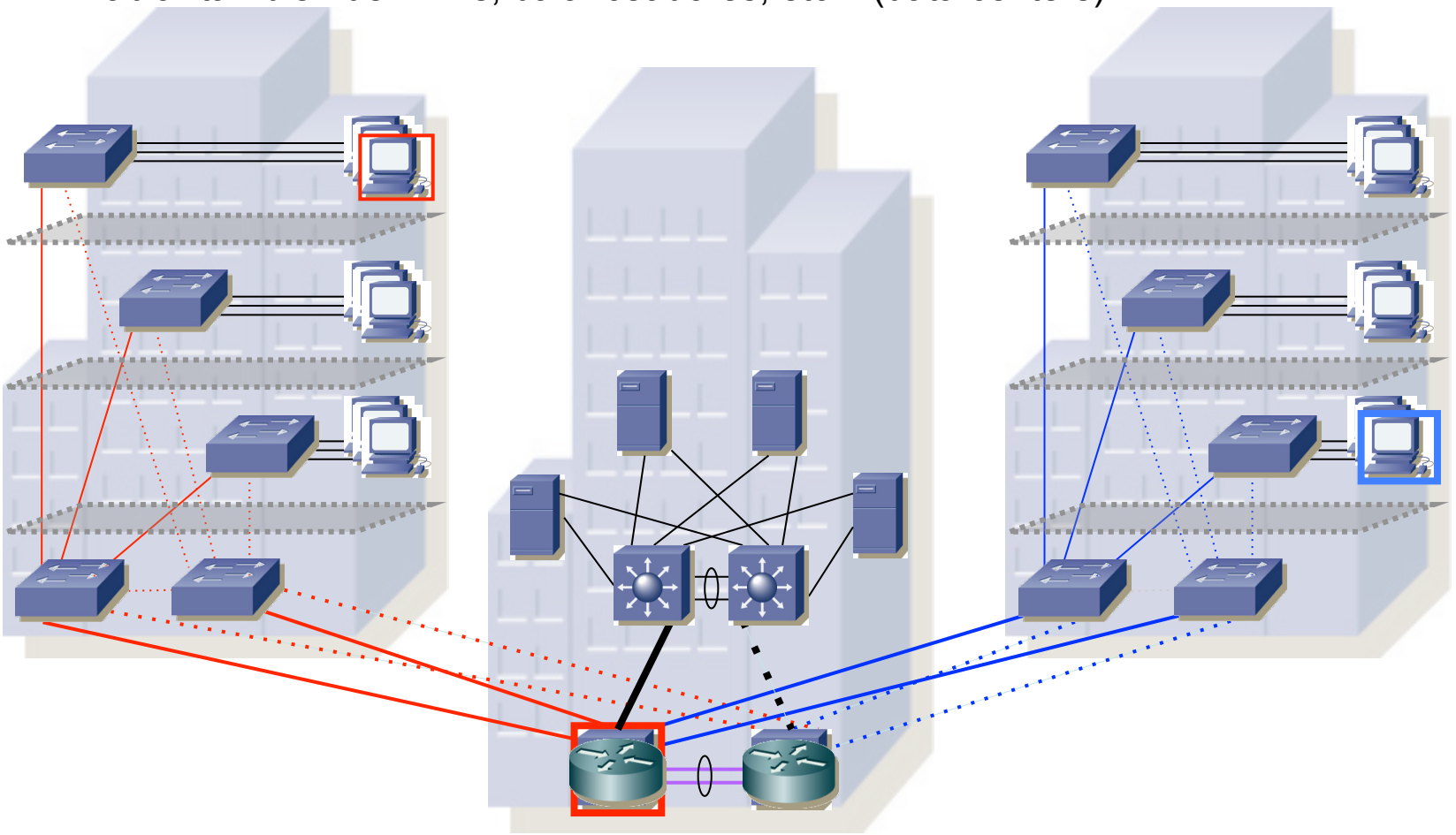
Centralización de servidores

- Podemos tener una VLAN con servidores centralizados
- Pero con esto hay un punto de fallo en ese nuevo conmutador
- Podemos duplicarlo pero ¿qué hacemos con los servidores?
- ¿Todos a uno? ¿Repartirlos? En cualquier caso queda un punto de fallo que es la NIC del servidor (...)



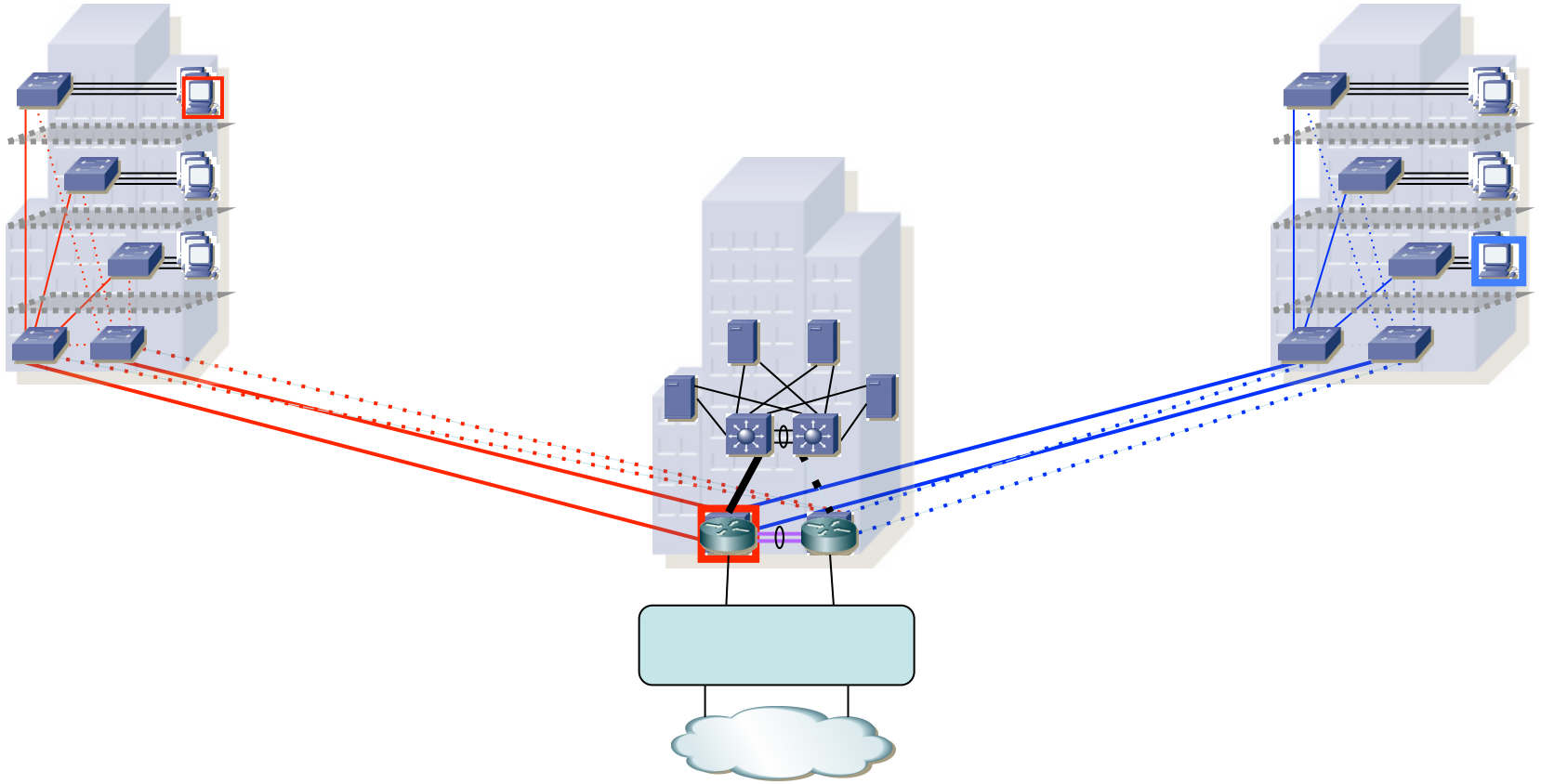
Centralización de servidores

- Podemos duplicar la NIC y repartirlas entre los dos conmutadores
- Cómo emplear esas NICs (una u otra o las dos a la vez) suele ser dependiente de la solución del fabricante de la NIC
- No vamos a entrar en esto pues llegando a los servidores tendríamos que hablar también de NATs, balanceadores, etc... (data centers)



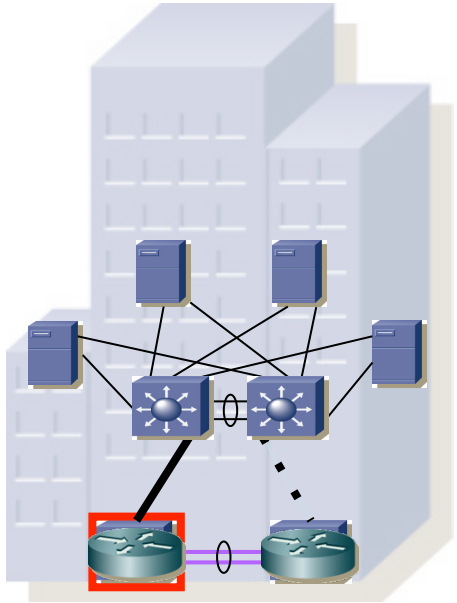
Acceso a WAN

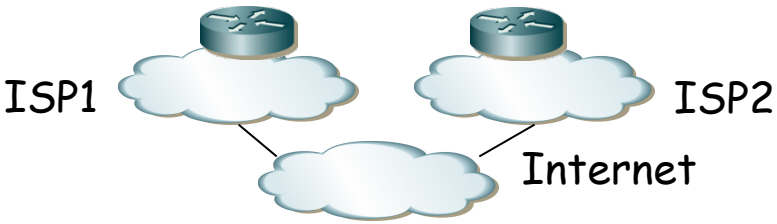
- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- (...)



Acceso a WAN

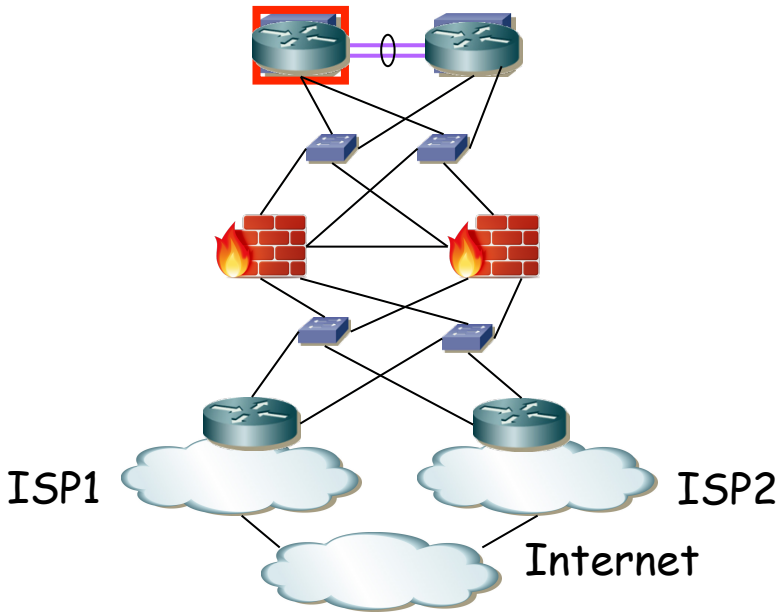
- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- El acceso a WAN/Internet puede ser por uno o dos ISPs
- (...)





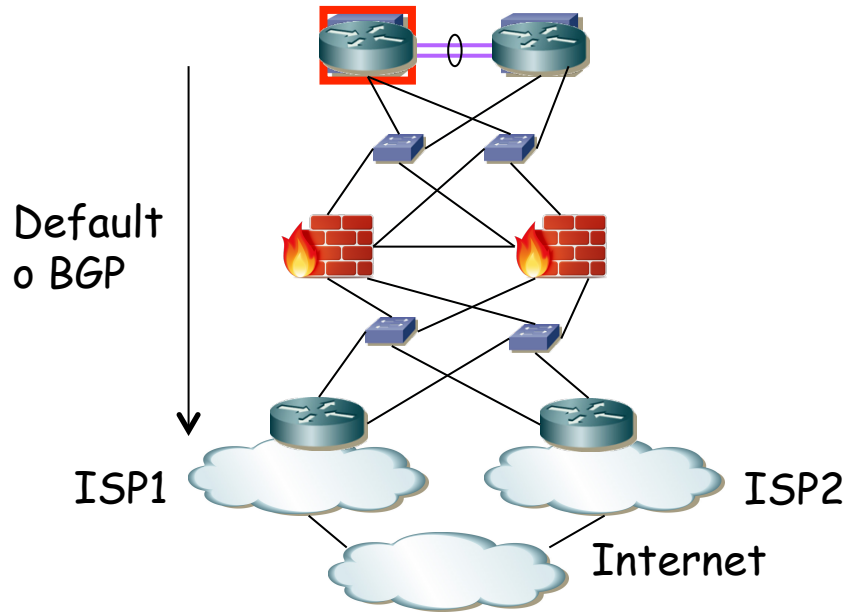
Acceso a WAN

- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- El acceso a WAN/Internet puede ser por uno o dos ISPs
- Aquí entran en juego inevitablemente Firewalls y NATs
- Normalmente en equipos independientes aunque pueden ser módulos en un chasis, por ejemplo de un conmutador del core
- La interconexión puede hacerse con VLANs o emplear equipos de conmutación independientes
- Con todo tipo de redundancia de enlaces, equipos, un FHRP en cada LAN, encaminamiento dinámico, protocolos propietarios, etc



Acceso a WAN: Routing

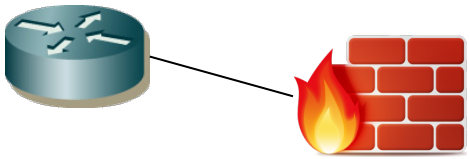
- Hacia el exterior es frecuente trabajar con una ruta por defecto
- Salvo que empecemos a hablar de sedes remotas, VPNs, etc
- Se puede emplear BGP para aprender las rutas a Internet y repartir tráfico entre los dos ISPs



VLANs vs Subredes IP vs STP

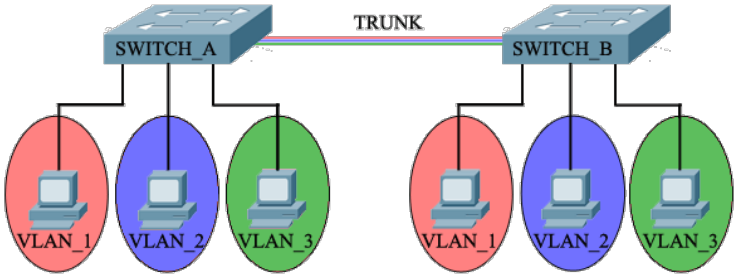
VLANs

- Dependen mucho de las necesidades de la red
- Conmutar en capa 3 nos permite implementar seguridad con Firewalls
- Limitamos el broadcast
  - Evitamos que un host que envíe sin control congestione a todos los hosts (un fallo en la NIC)
  - Aunque aún puede congestionar enlaces compartidos
  - Limitamos coste de procesado de broadcasts (aunque esto no es un problema para el hardware moderno)



VLANs

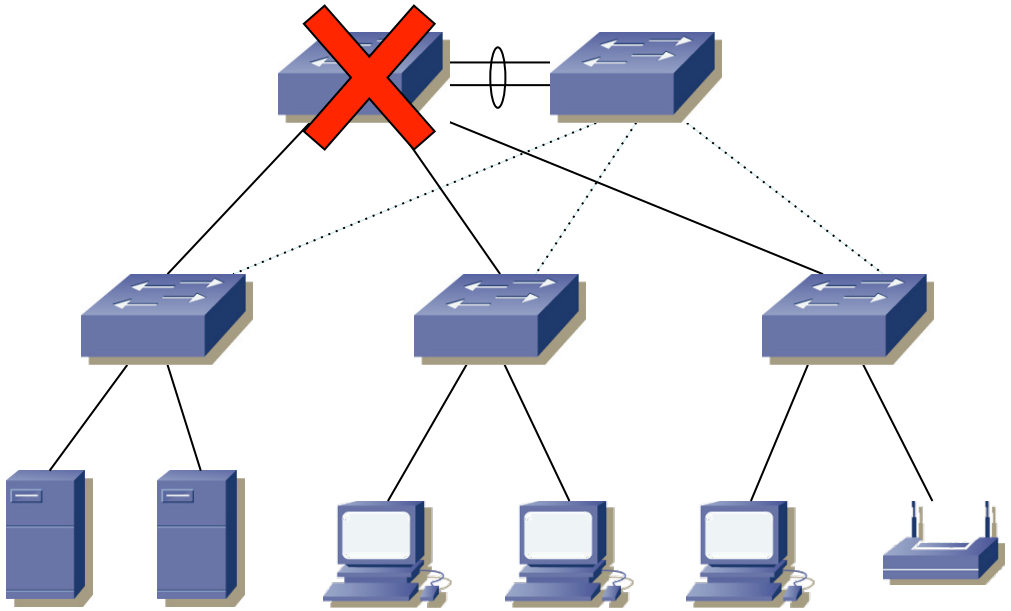
- Típicas:
  - Usuarios
  - Servidores, impresoras
  - VoIP
  - WiFi
  - WiFi pública
  - Gestión
  - VLAN por puertos desconectados



- Puede ser conveniente limitar el número de MACs por un puerto
  - Evita un ataque de saturación de la CAM
- También es conveniente limitar el envío de respuestas DHCP
- Pero esto ya es hablar de seguridad …

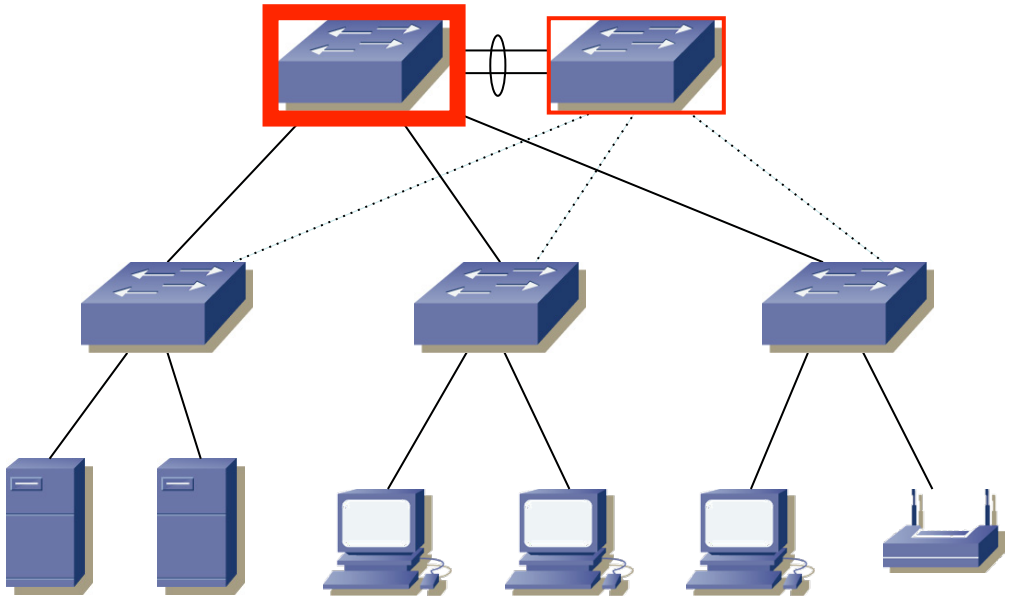
STP

- Convergencia
  - STP 802.1D original convergencia en 30-60s
  - Timers que se deberían ajustar para diámetro de red grande
  - Hoy en día RSTP, convergencia en 2-3s
  - Mejor actualizar los conmutadores si se hace un gran uso de STP
  - RSTP es compatible con STP
  - En caso de dominios de broadcast pequeños aún es útil STP en puerto a usuario por protección



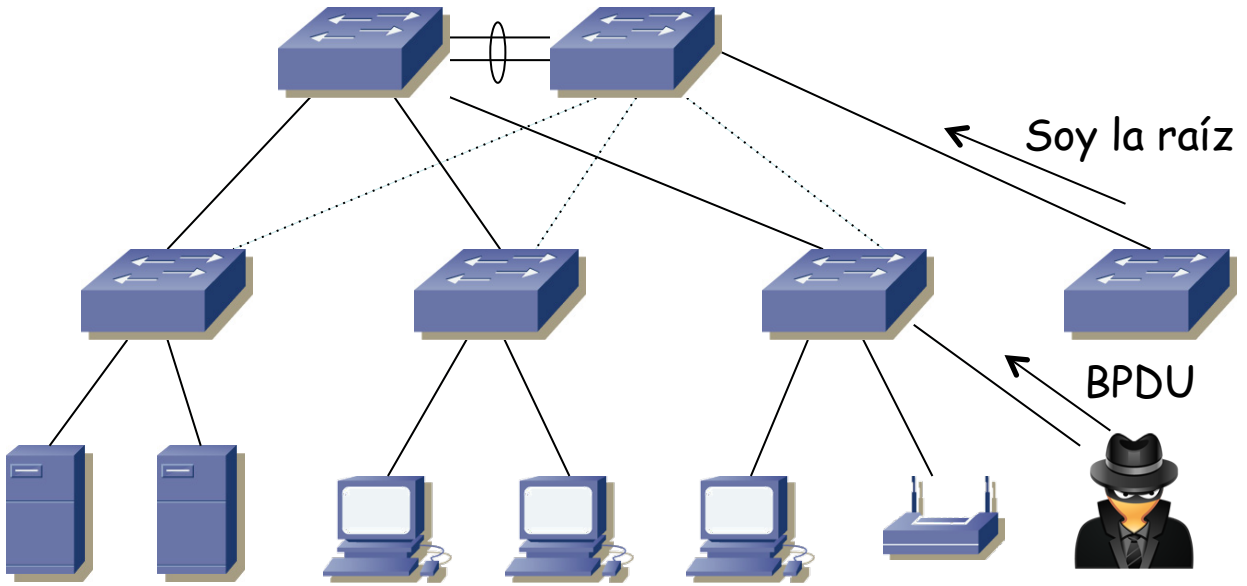
STP

- Topología
  - Mejor seleccionar el *root bridge* y un *backup*
  - Si no, será el conmutador más viejo (menor MAC, esto es en el fondo bueno pues evita que conectemos uno nuevo y cambie)
- ¿MSTP?
  - Conlleva las mejoras de RSTP
  - Compromiso entre aprovechar enlaces bloqueados y sencillez en la red



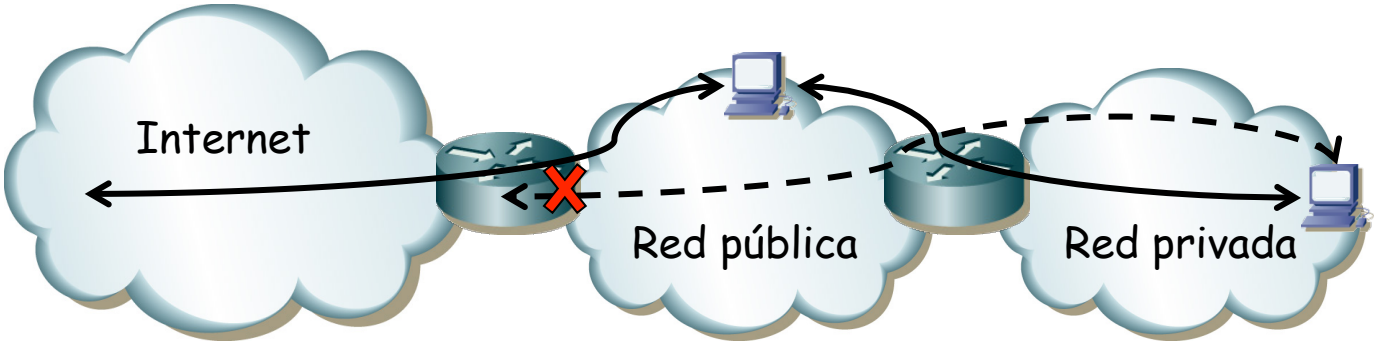
STP

- Técnicas adicionales de protección
  - No aceptar BPDU en puertos hacia hosts (¿alguien ha conectado ahí un switch?)
  - Protección ante cambio de *root bridge* (¿conexión accidental de switch mal configurado?)



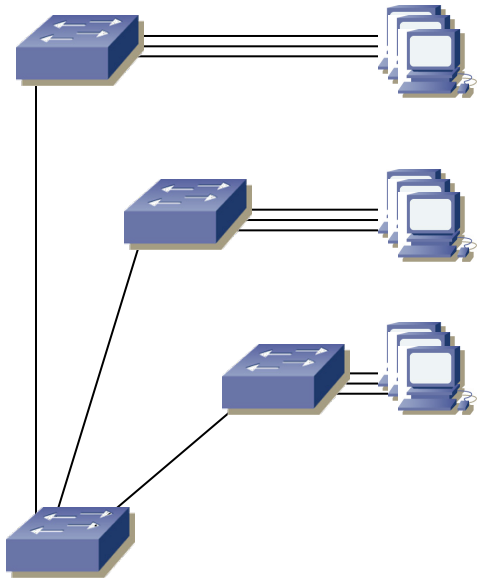
Direccionamiento

- Decidir el tamaño del espacio de direcciones requerido
- Reservar direcciones para futuro crecimiento
- ¿ Direccionamiento privado ?
  - Gran espacio de direcciones
  - No comunicación con exterior
  - Direccionamiento público para máquinas con comunicación al exterior (servidores)
  - Posibilidad de usar NAT (empleando varias IPs públicas o mediante *overload*)
  - Posible comunicación interna pública-privada



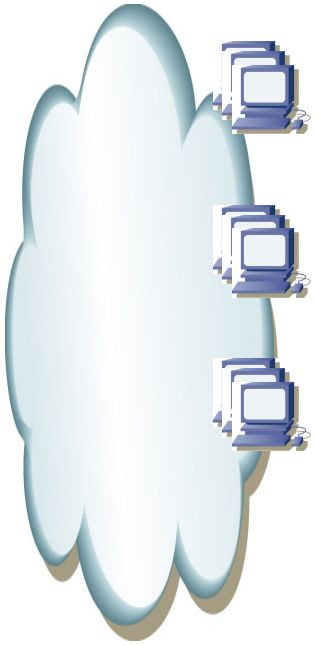
Subredes IP vs VLANs

- Una subred IP implica una dirección de red y una máscara, un bloque de direcciones IP
- Esas máquinas se supone que tienen conectividad L2
- Es decir, normalmente una subred IP está toda ella en una LAN
- Y por lo tanto en una VLAN
- (...)



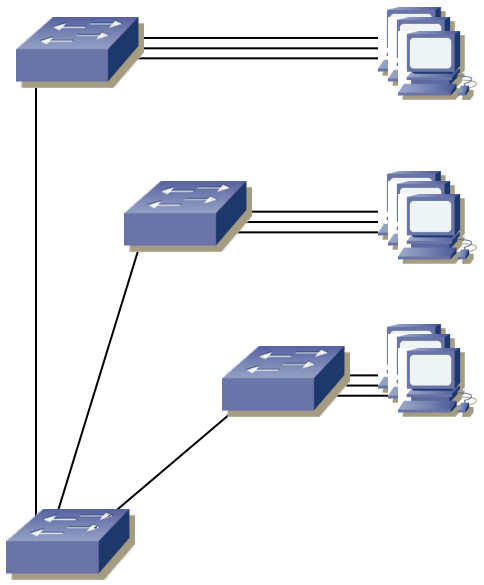
VLAN 1

172.17.1.128/26

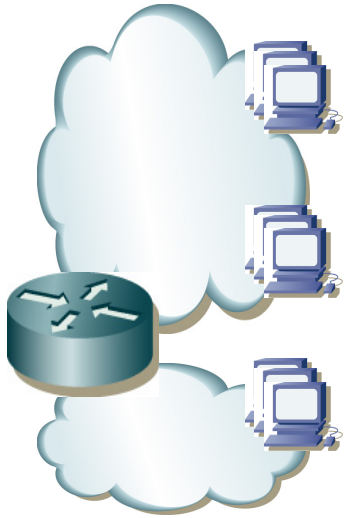


Varias subredes en la LAN

- Pero esto no impide que en una misma LAN/VLAN haya más de una subred IP
- Esas máquinas en realidad tienen conectividad L2 pero no lo saben
- A la hora de comunicarse entre las subredes necesitan un router (...)



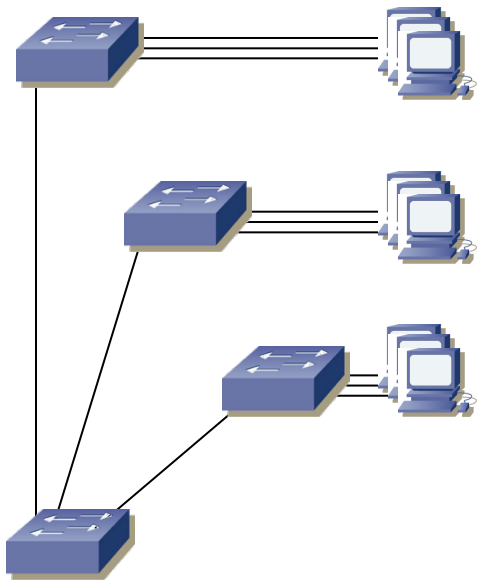
VLAN 1

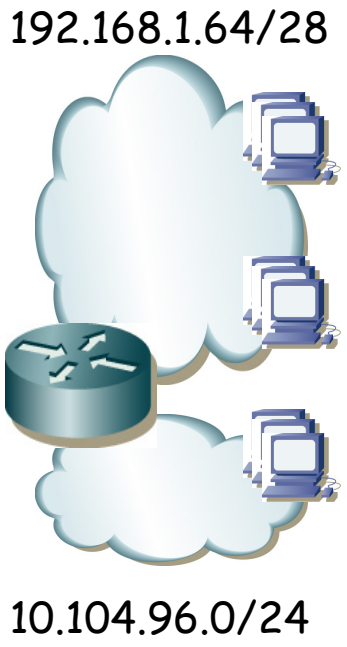


Varias subredes en la LAN

- Ese router tiene los dos interfaces en la misma LAN/VLAN pero en diferente subred IP
- (...)

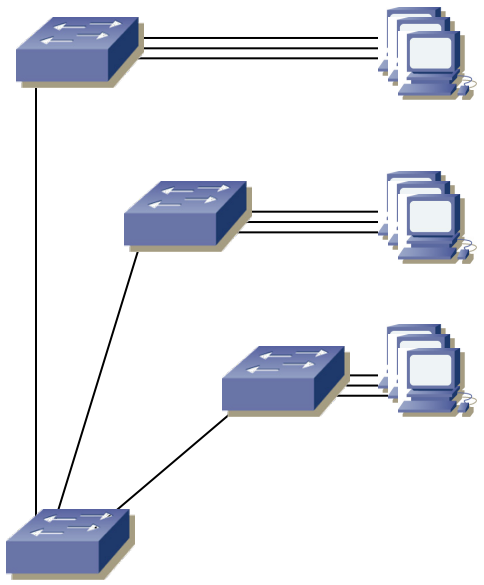
Destino	Next-hop	if
192.168.1.64/28	–	0
10.104.96.0/24	–	0



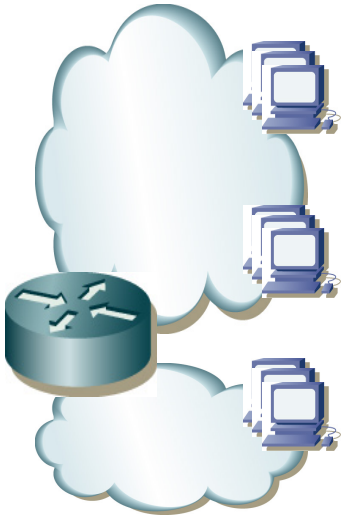


Varias subredes en la LAN

- Un broadcast en la LAN llegará a todos los host, aunque sean de la otra subred
- Por ejemplo un paquete IP a 255.255.255.255 o a 192.168.1.79
- Un ARP request cualquiera también llegará a todos los hosts
- (...)

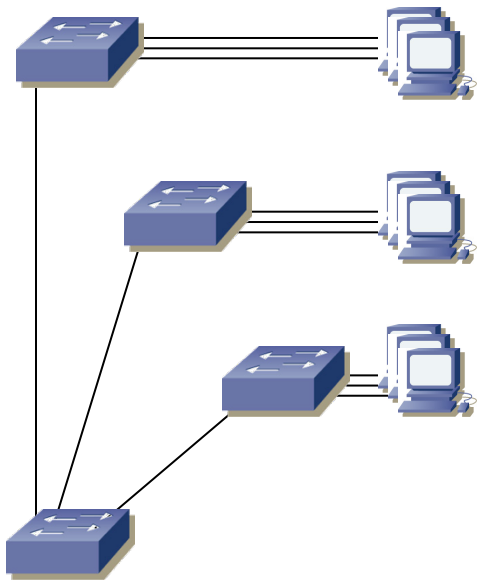


VLAN 1

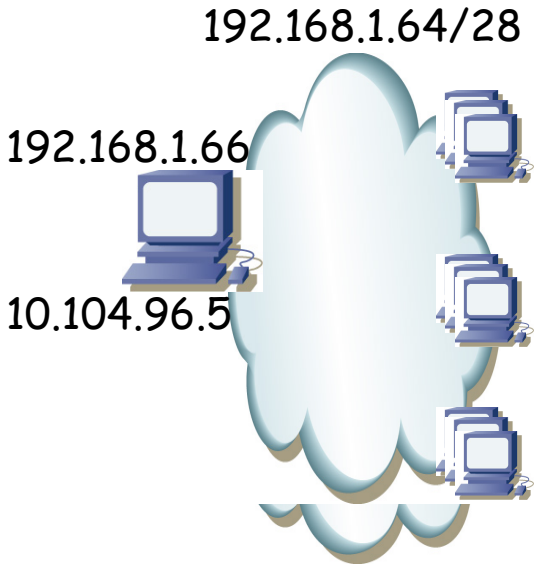


Varias subredes en la LAN

- En realidad los hosts pueden intercambiar paquetes IP
- Solo necesitan resolver la ruta a la otra subred
- Por ejemplo teniendo un segundo interfaz IP (lógico) sobre la misma tarjeta Ethernet configurado con dirección en la otra subred
- Es lo mismo que tenía el router anterior
- O con un solo interfaz y una ruta estática a la otra subred

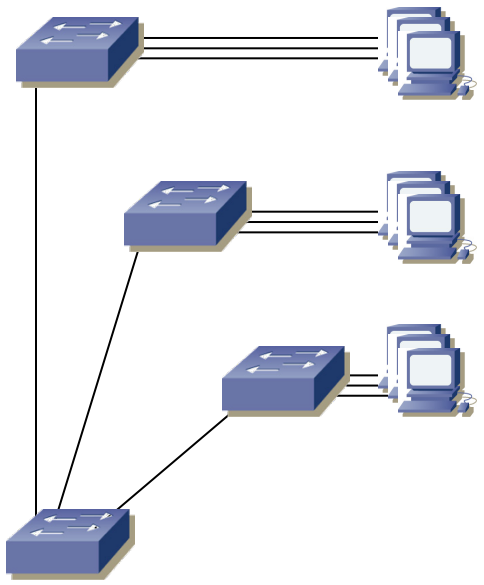


VLAN 1



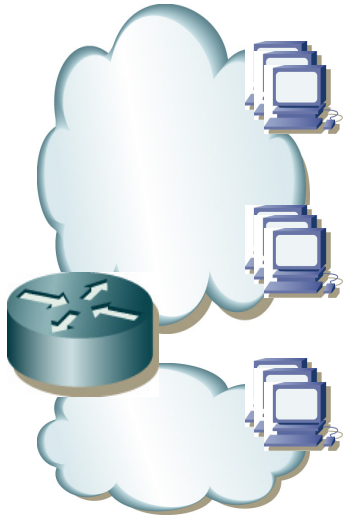
Varias subredes en la LAN

- No es lo habitual pero se puede hacer
- No me atrevería a calificarlo de “mala práctica”
- No es seguro, no aisla broadcast pero puede tener su utilidad
- Por ejemplo una LAN donde los hosts tienen dirección de una subred y los equipos de red dirección de gestión en otra subred, todo sin VLANs (por ejemplo porque no las soporten)



VLAN 1

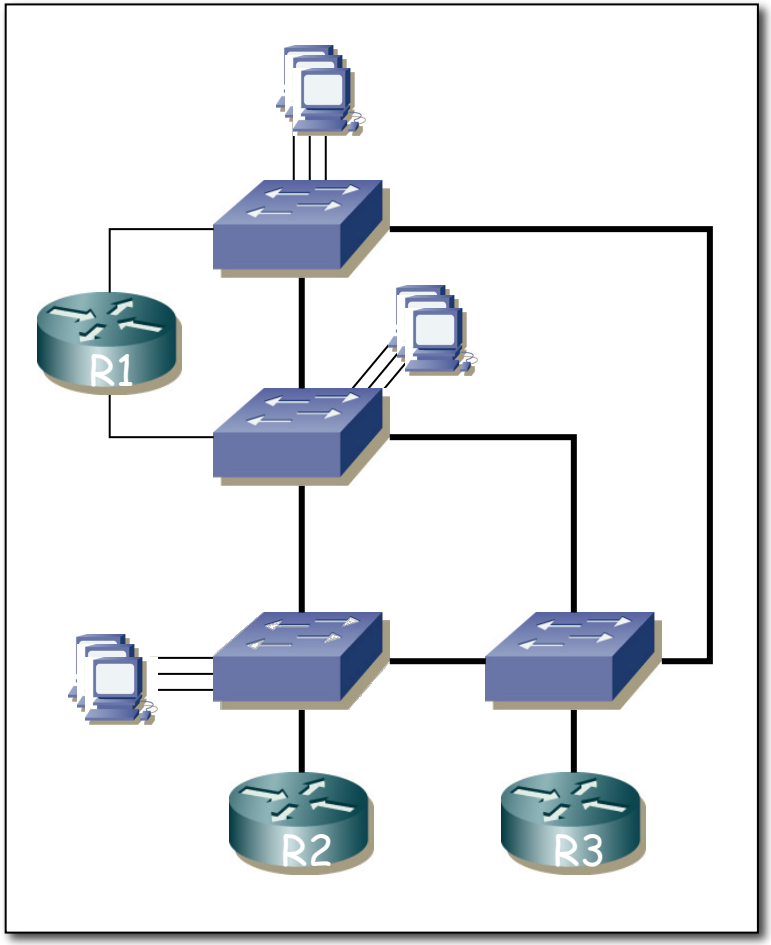
192.168.1.64/28

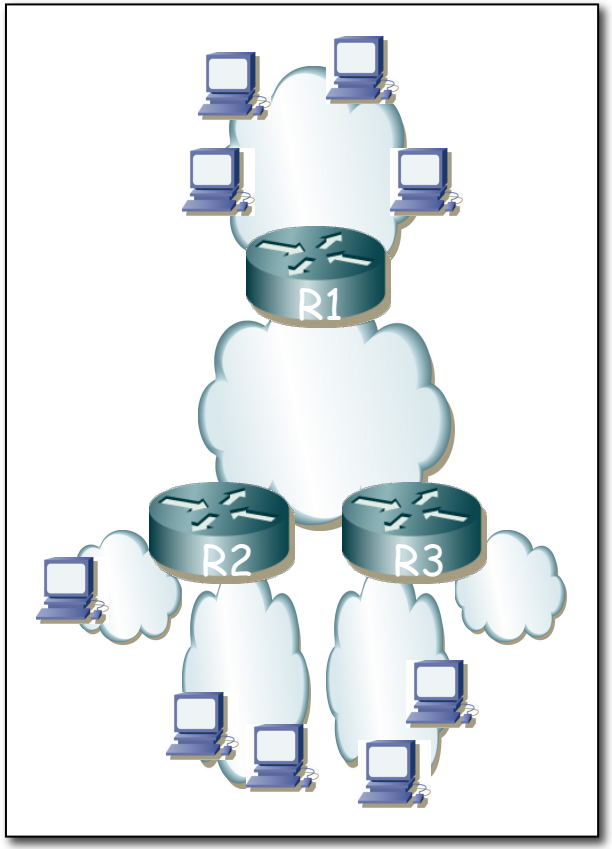


10.104.96.0/24

Topologías de nivel 1-2 y 3

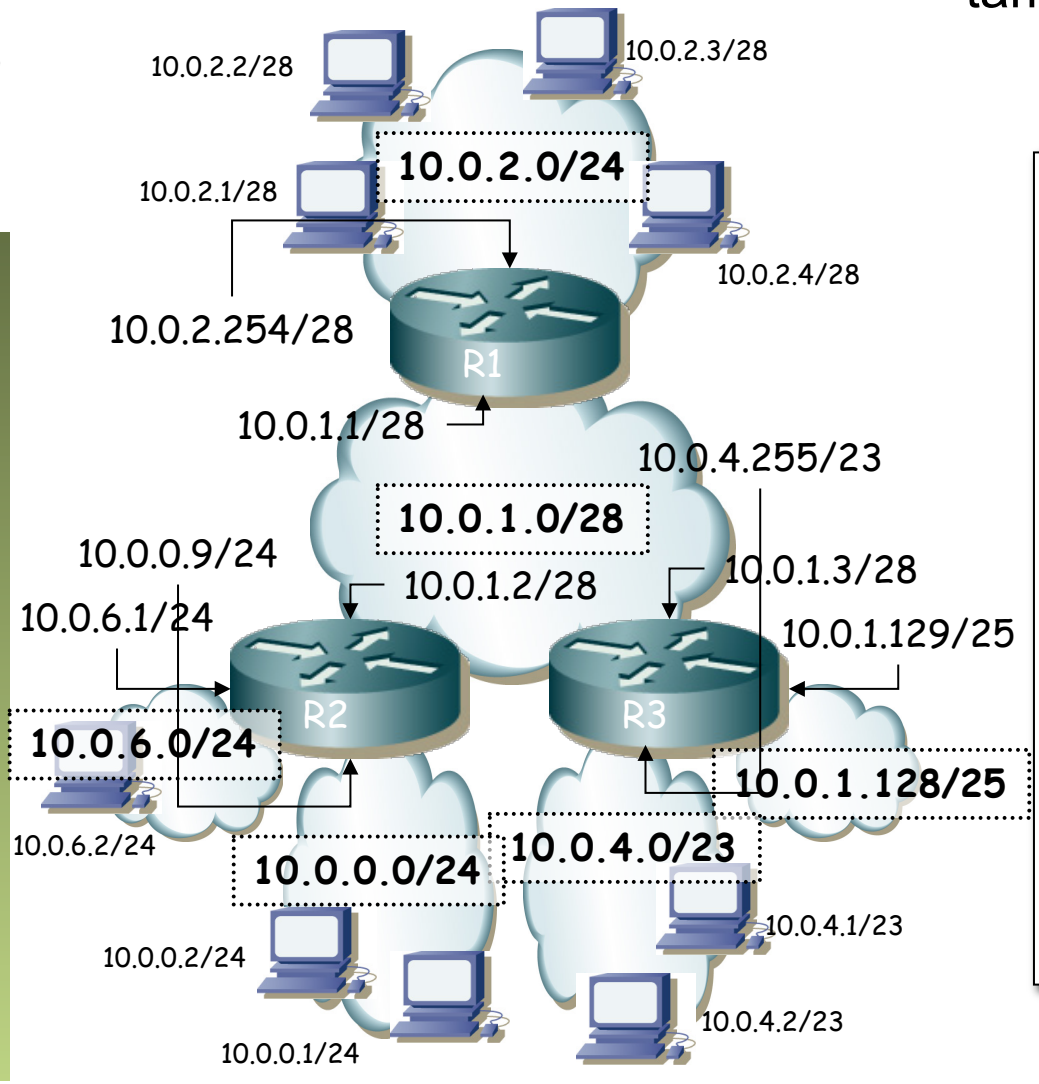
- Con VLANs puede ser difícil reconocer la topología de nivel 3
- Recomendable tener también la visión del nivel 3

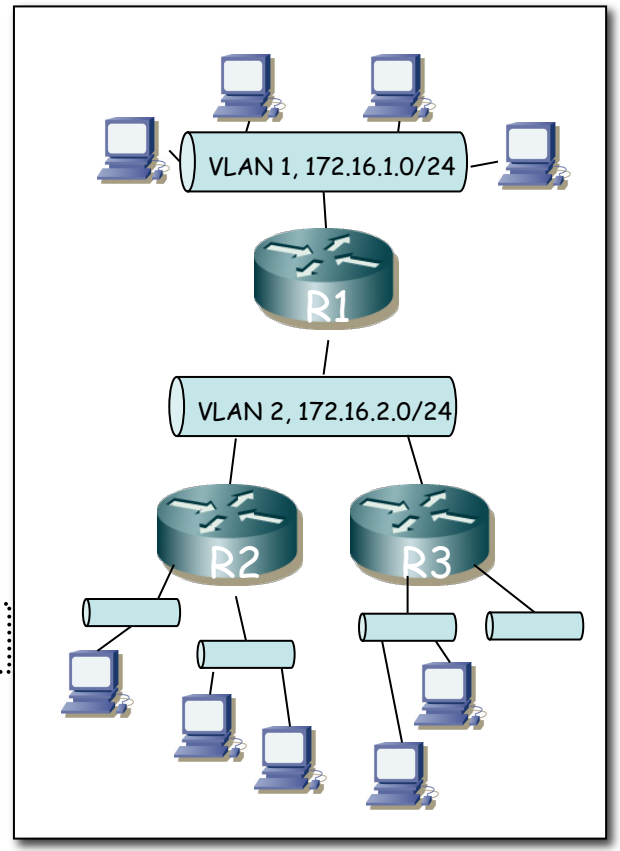




Topologías de nivel 1-2 y 3

- Incluido el direccionamiento
- Recomendable tener también la visión del nivel 3





Resumen sobre protección

- En el hardware del host
  - NICs dobles
- En el hardware interno del conmutador
  - Controladora (supervisor module)
  - Fuentes de alimentación
  - Sistemas de refrigeración
- En el hardware de conmutación
  - Equipos replicados y agregados en un conmutador virtual
  - Equipos apilados
  - Redundancia de router (FHRP)
- En la topología física de la VLAN
  - Agregaciones de enlaces
  - Redundancia de caminos (STP)
- En los caminos en capa 3
  - Routing dinámico
  - Balanceo de carga