upna
Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Diseño de Campus LAN
(parte 3)

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

Grado en Ingeniería en Tecnologías de Telecomunicación, 3º

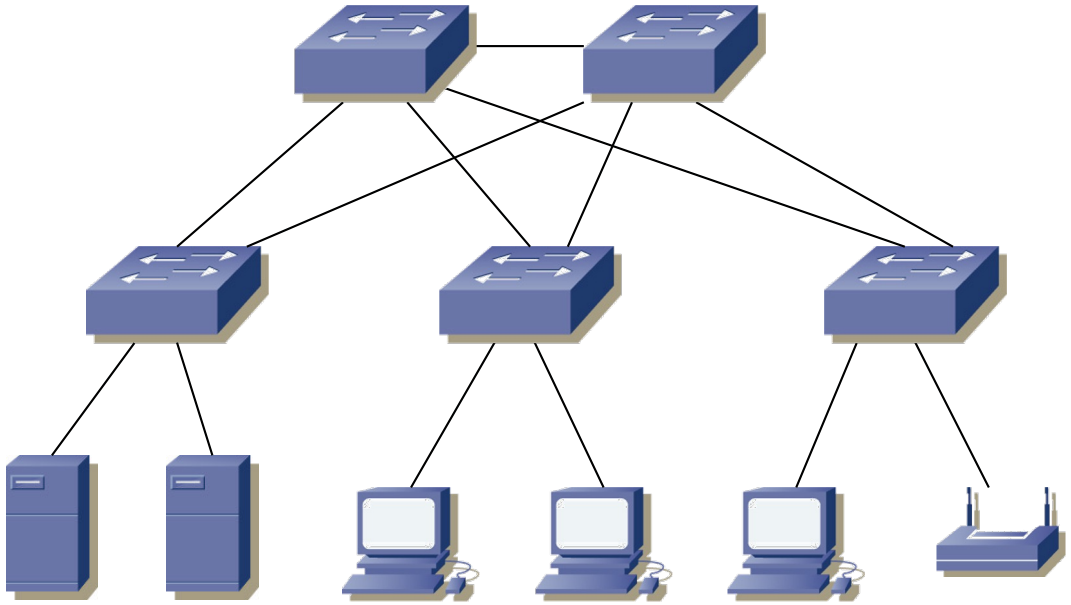
upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

3-tier design

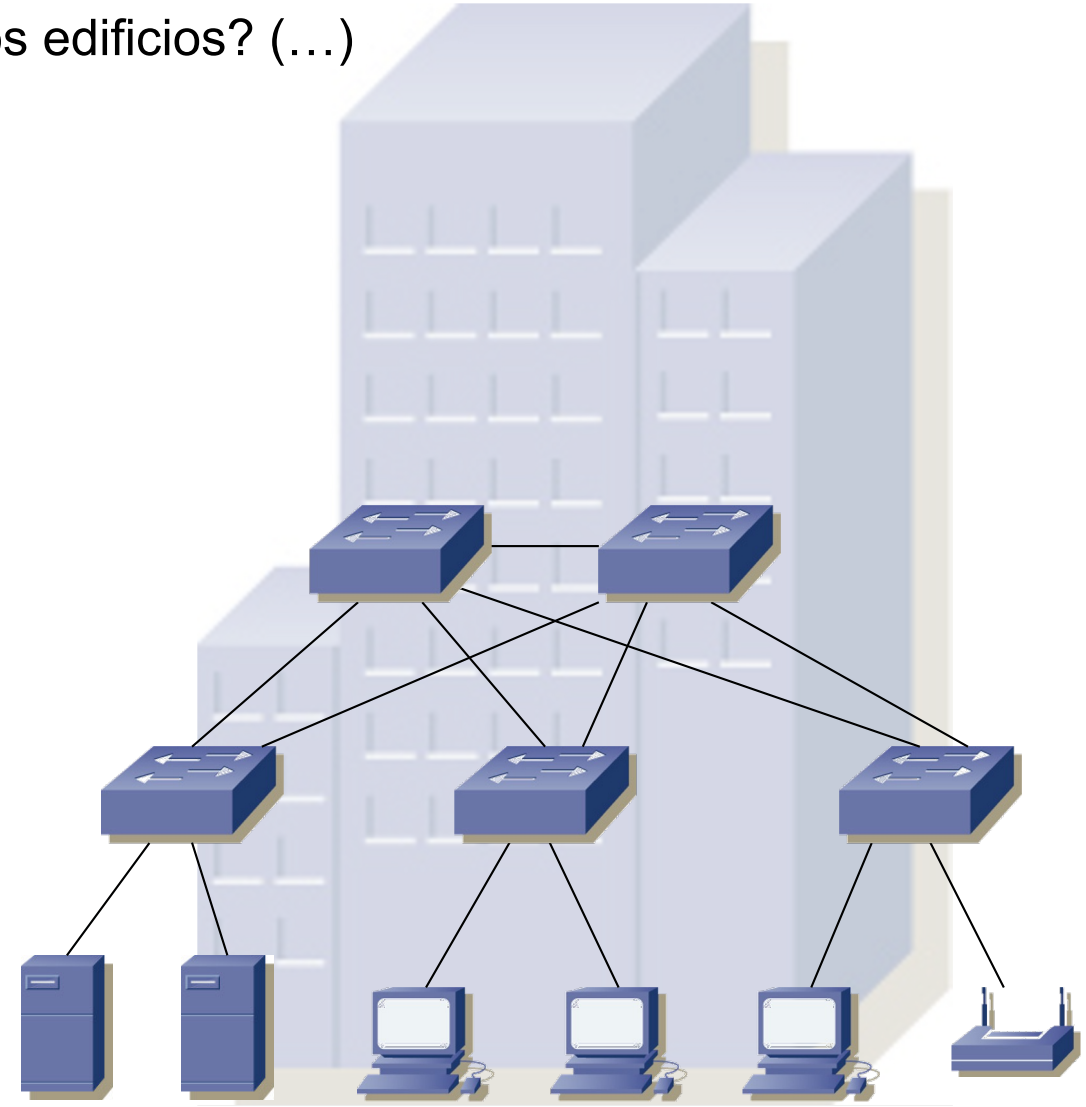
Redes más grandes

- El esquema IDF+MDF (acceso+distribución) sirve hasta una escala
- Por ejemplo cuando está todo contenido en un solo edificio (…)



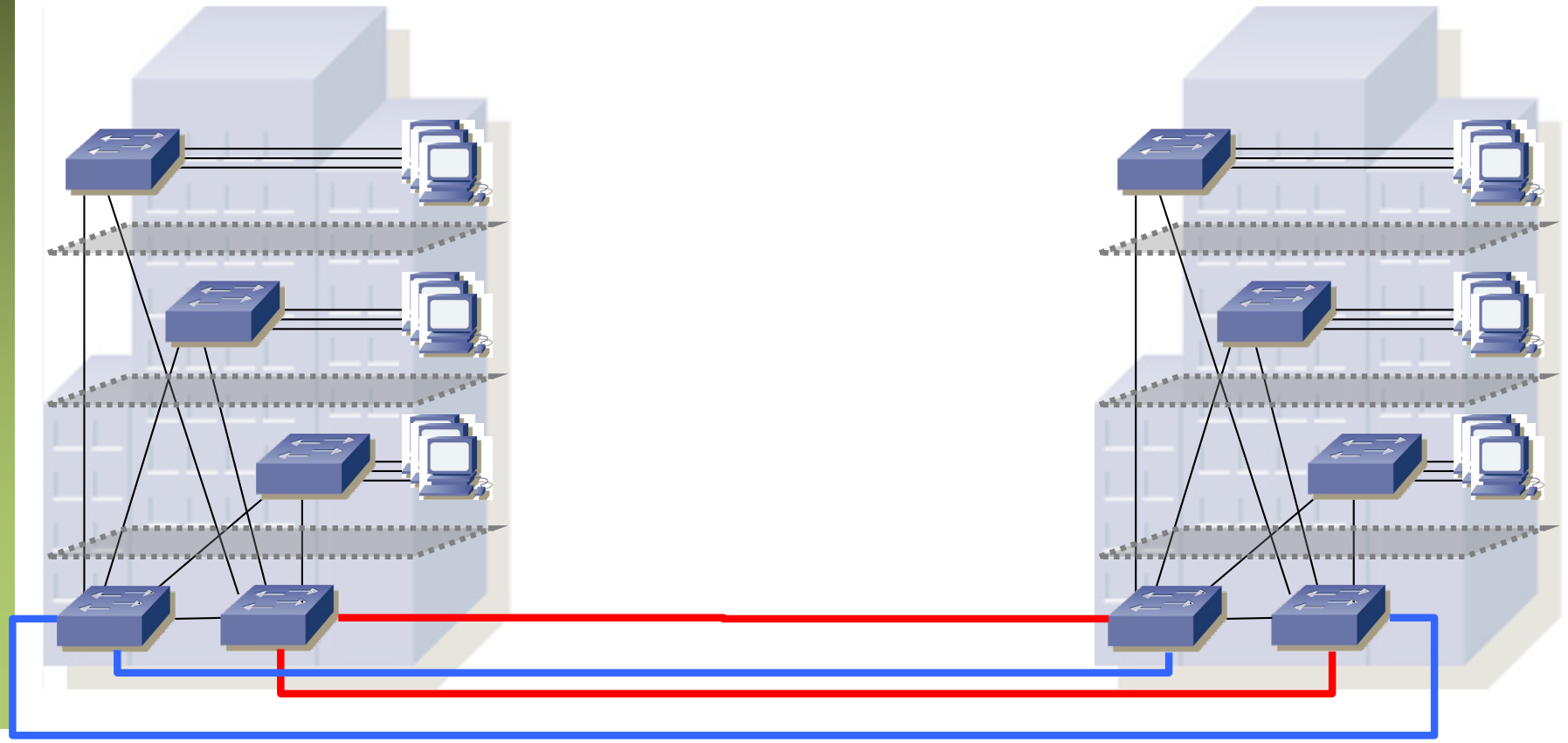
Redes más grandes

- El esquema IDF+MDF (acceso+distribución) sirve hasta una escala
- Por ejemplo cuando está todo contenido en un solo edificio
- ¿Y con varios edificios? (…)



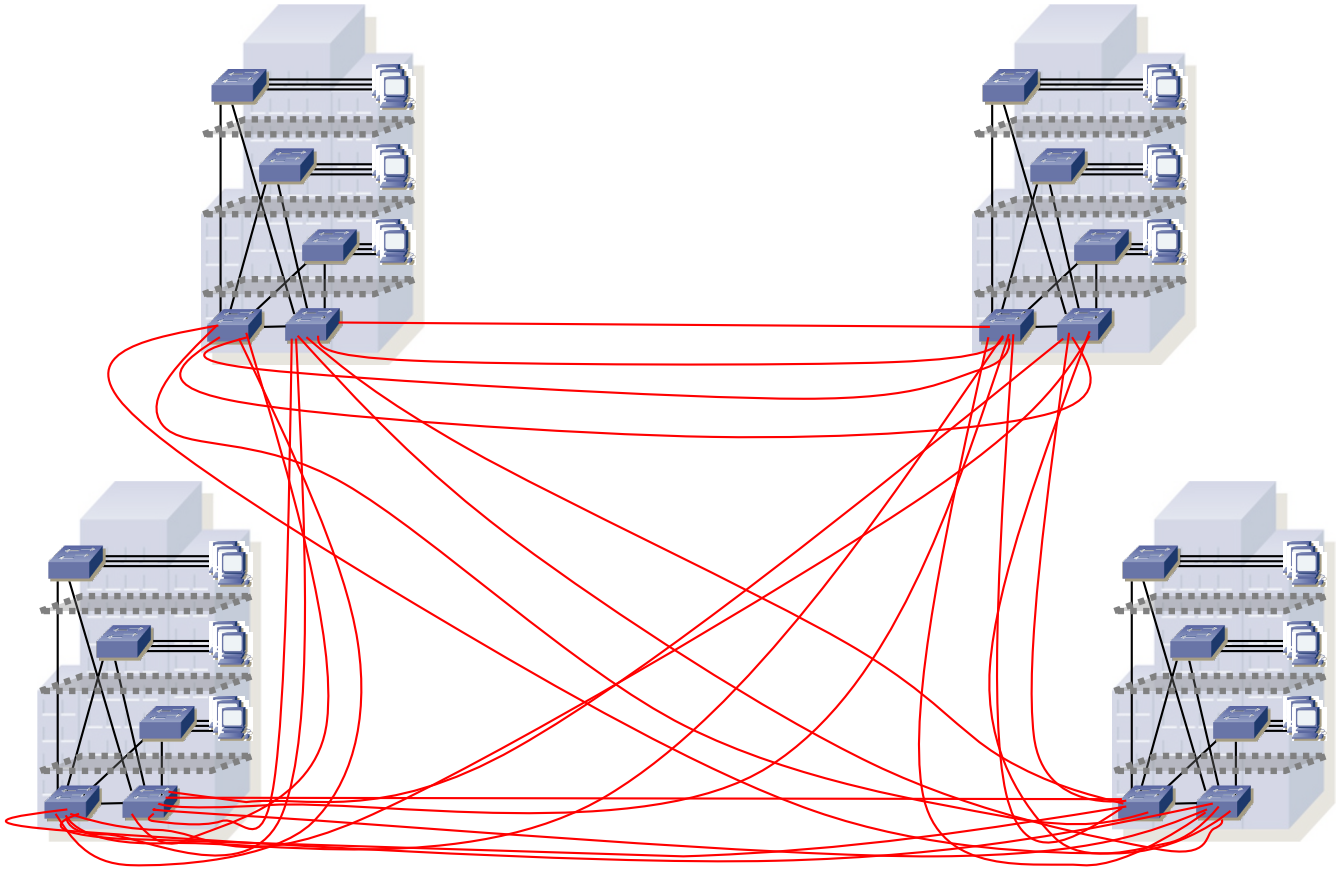
Redes más grandes

- 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 (...)



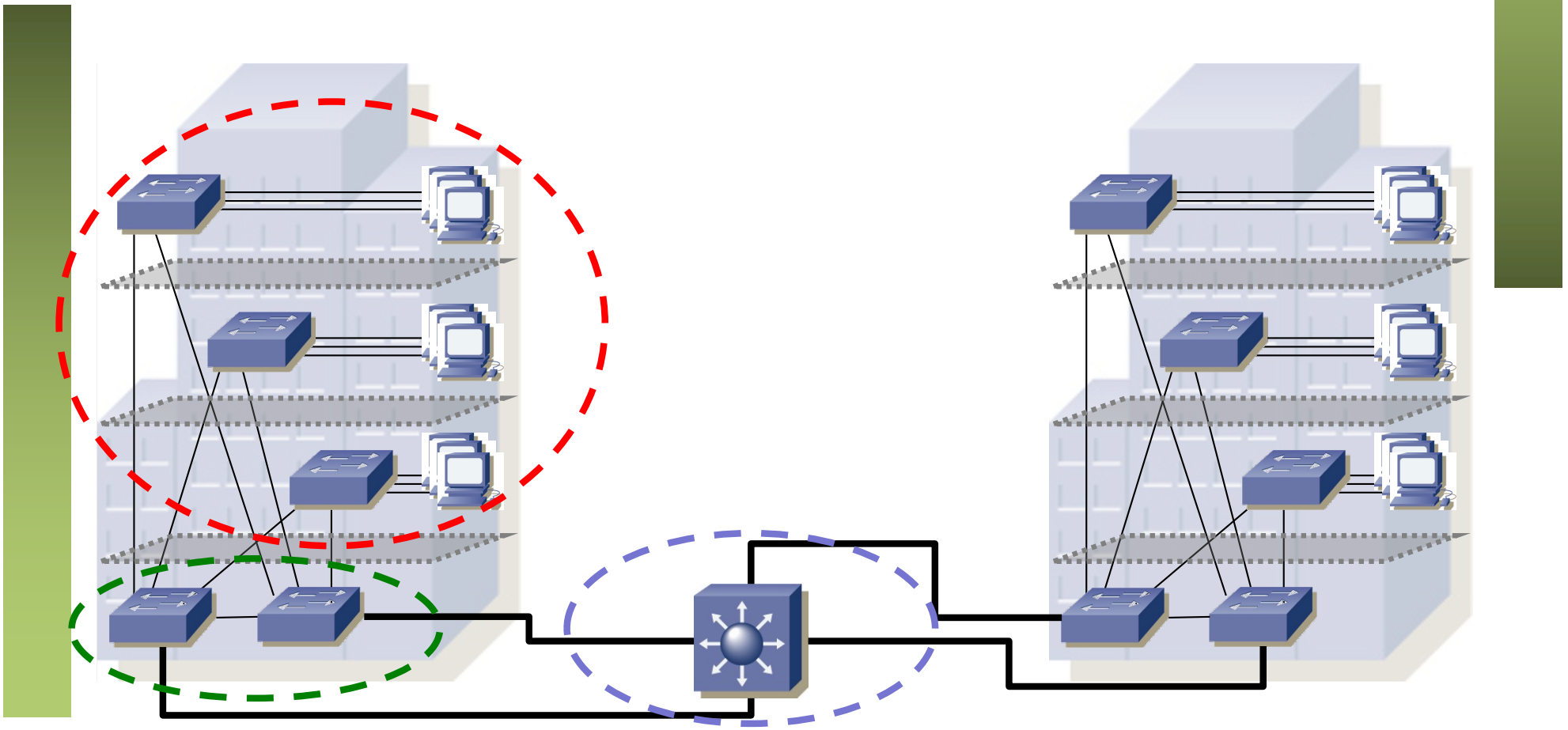
Redes más grandes

- 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



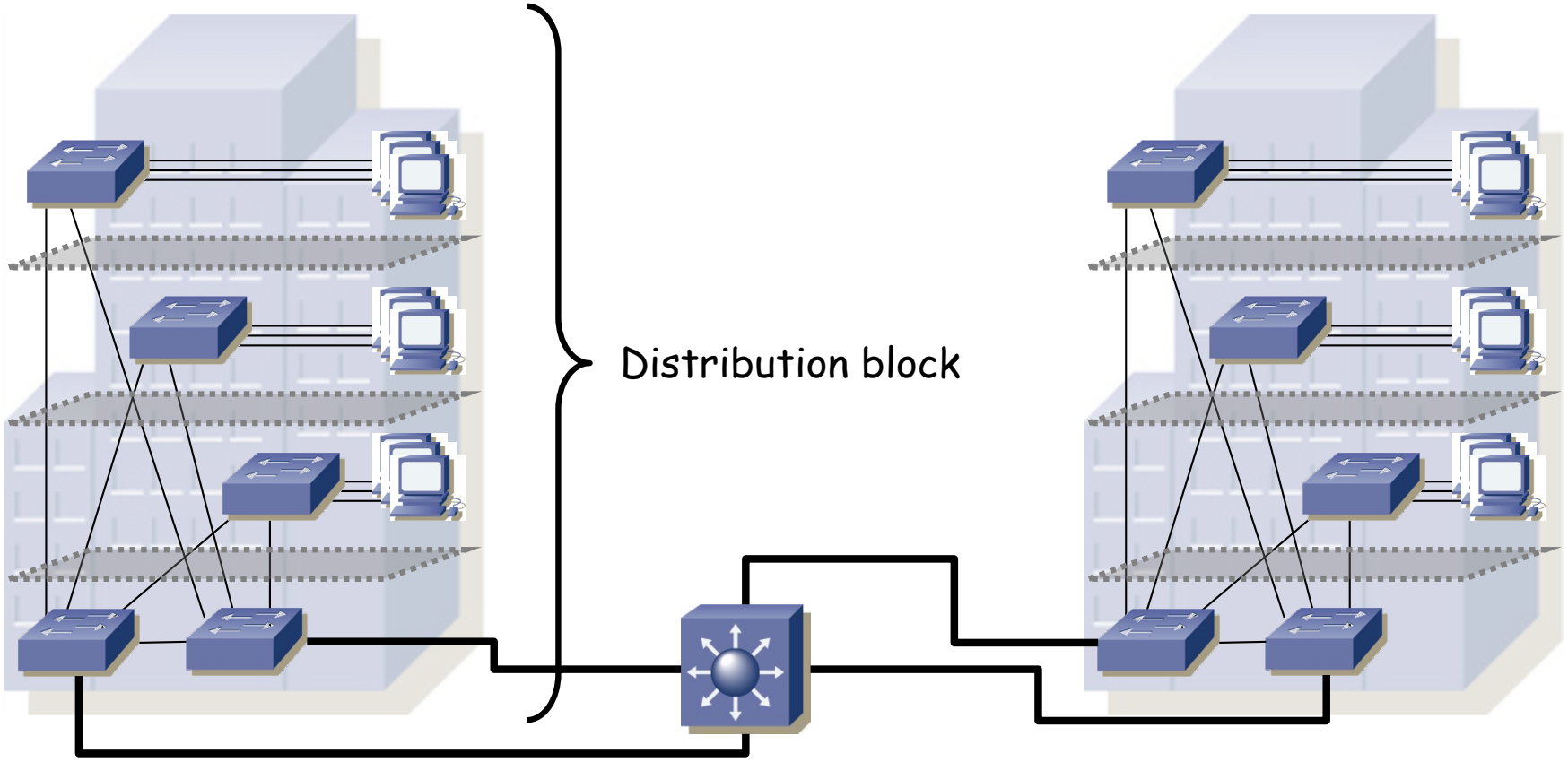
Redes más grandes

- 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)



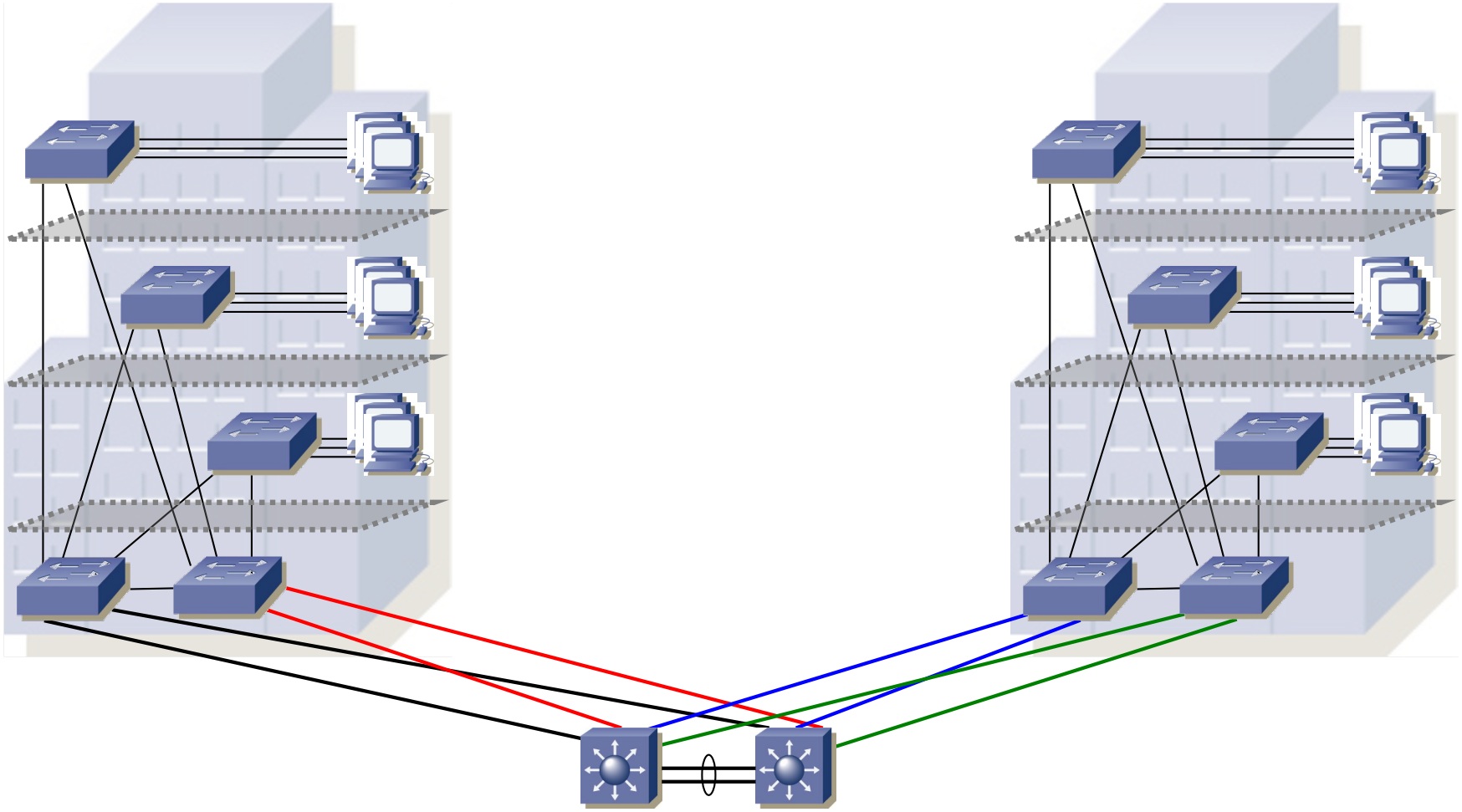
Redes más grandes

- 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)



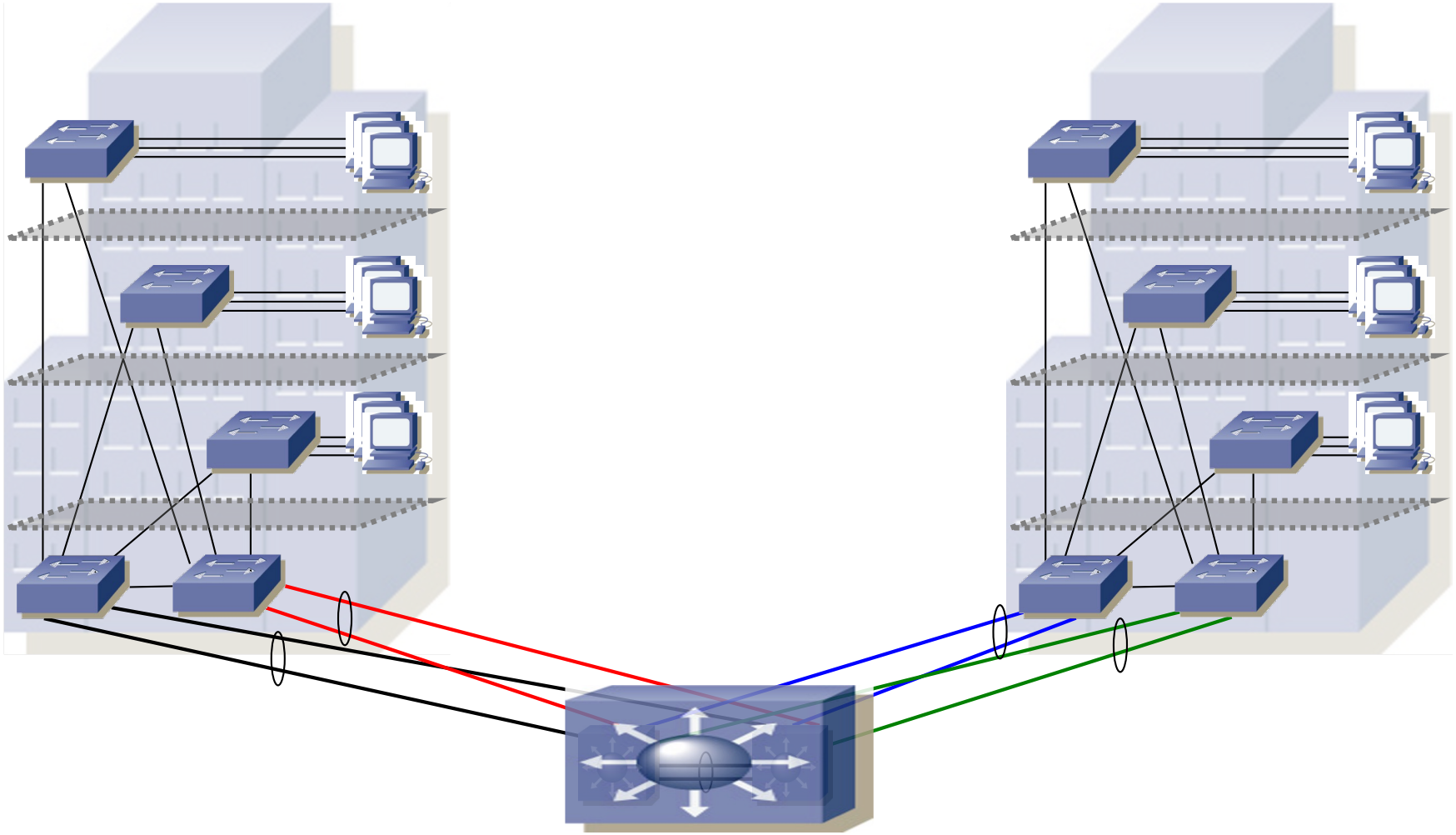
Core

- 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 (...)



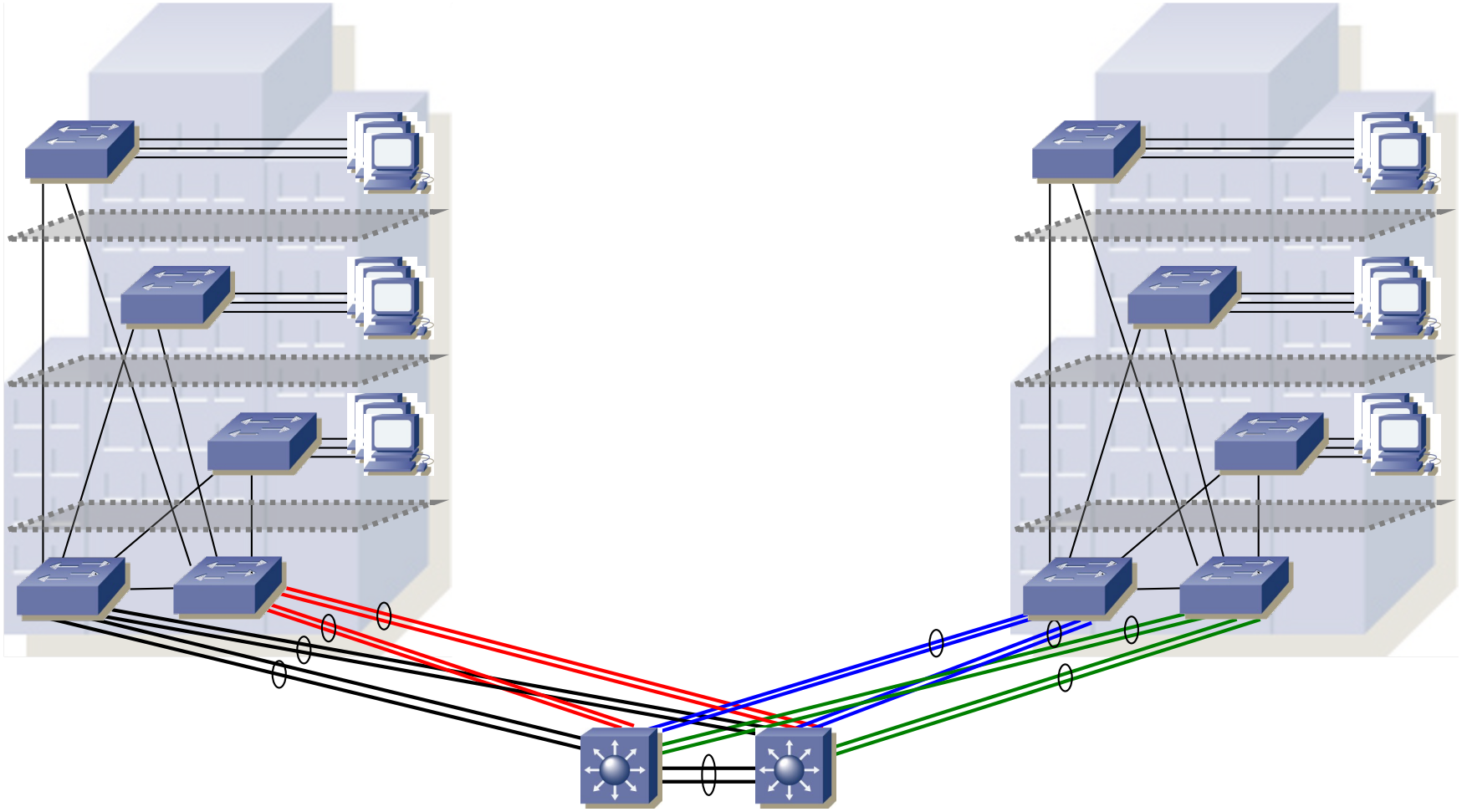
Core

- 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 (...)



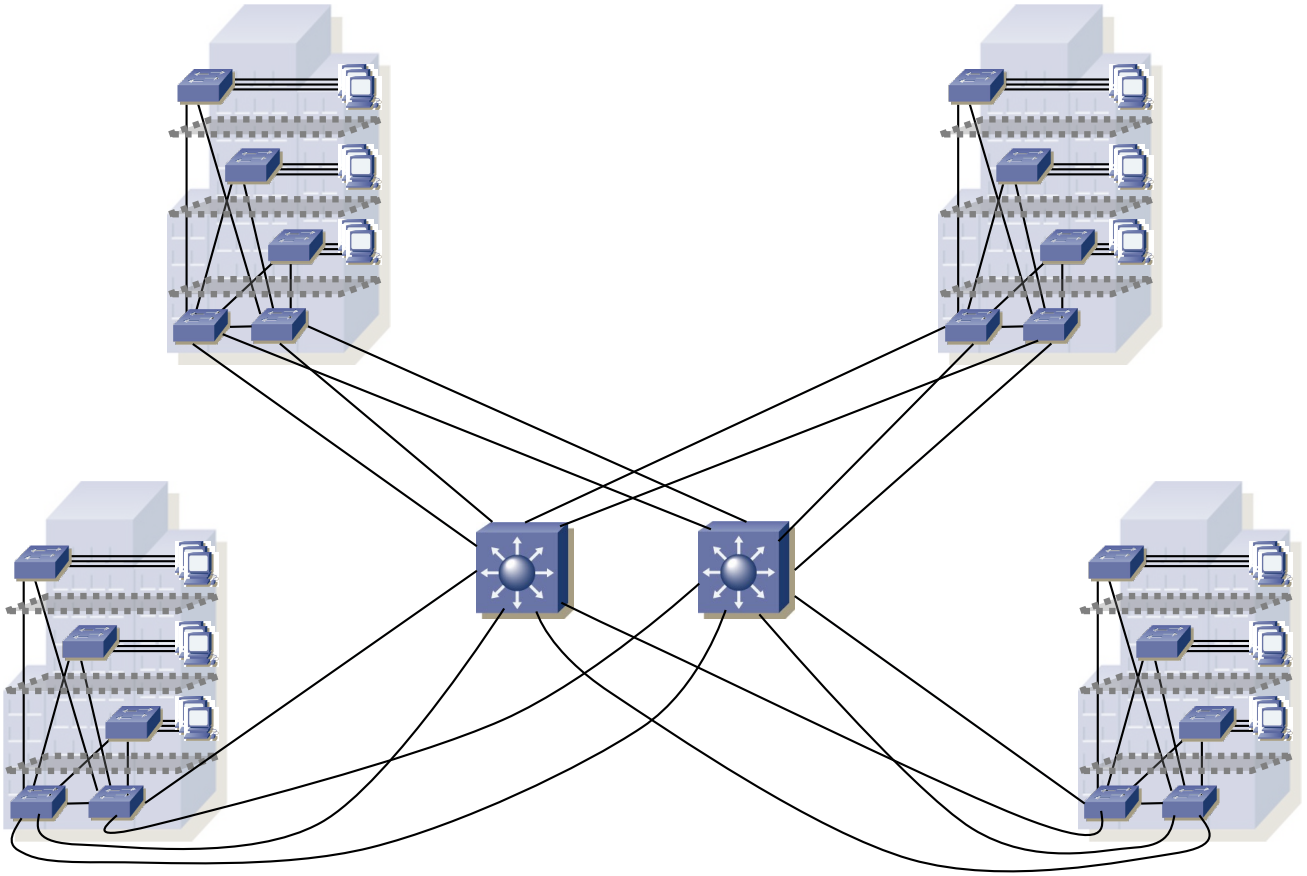
Core

- 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.



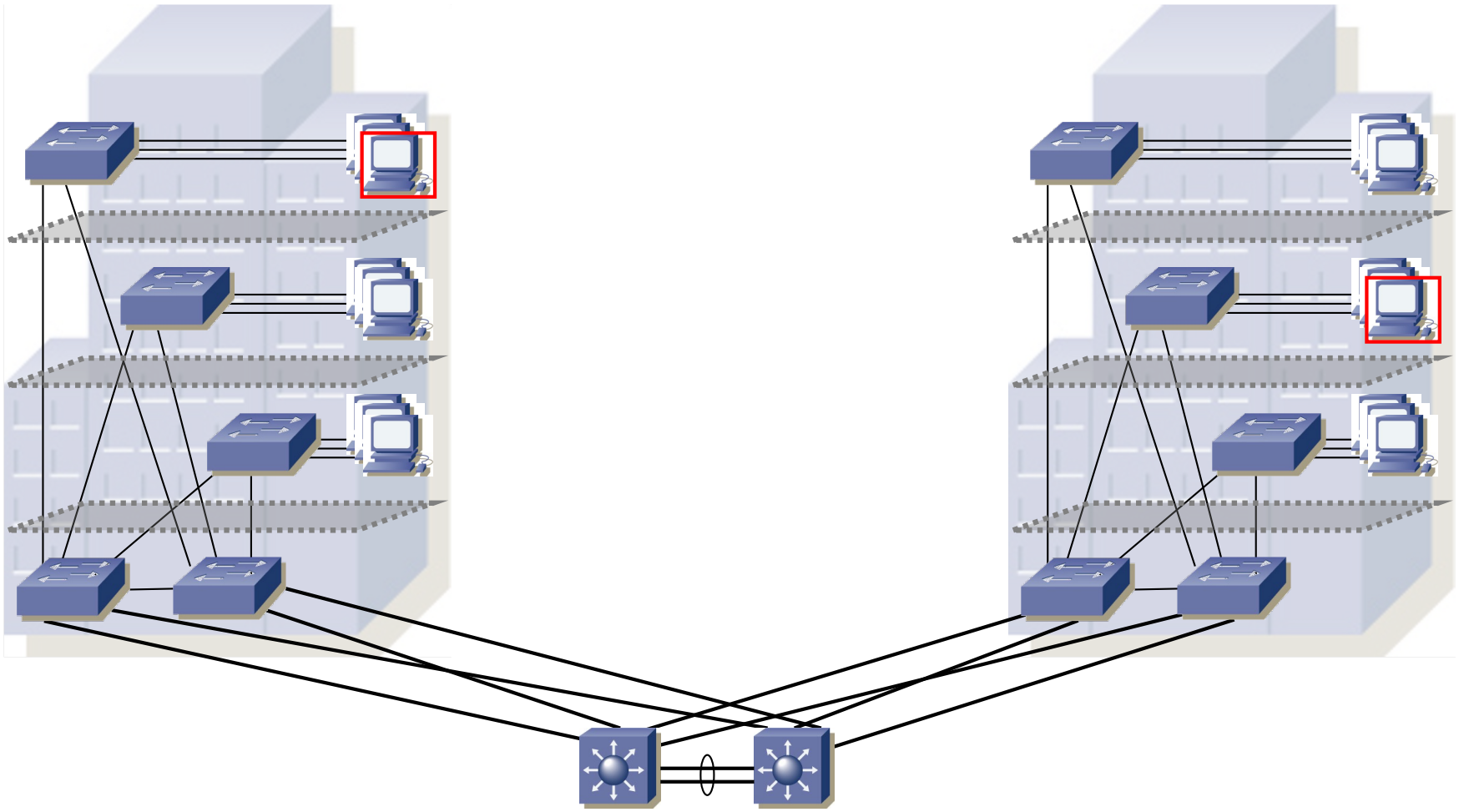
upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Campus-wide VLANs

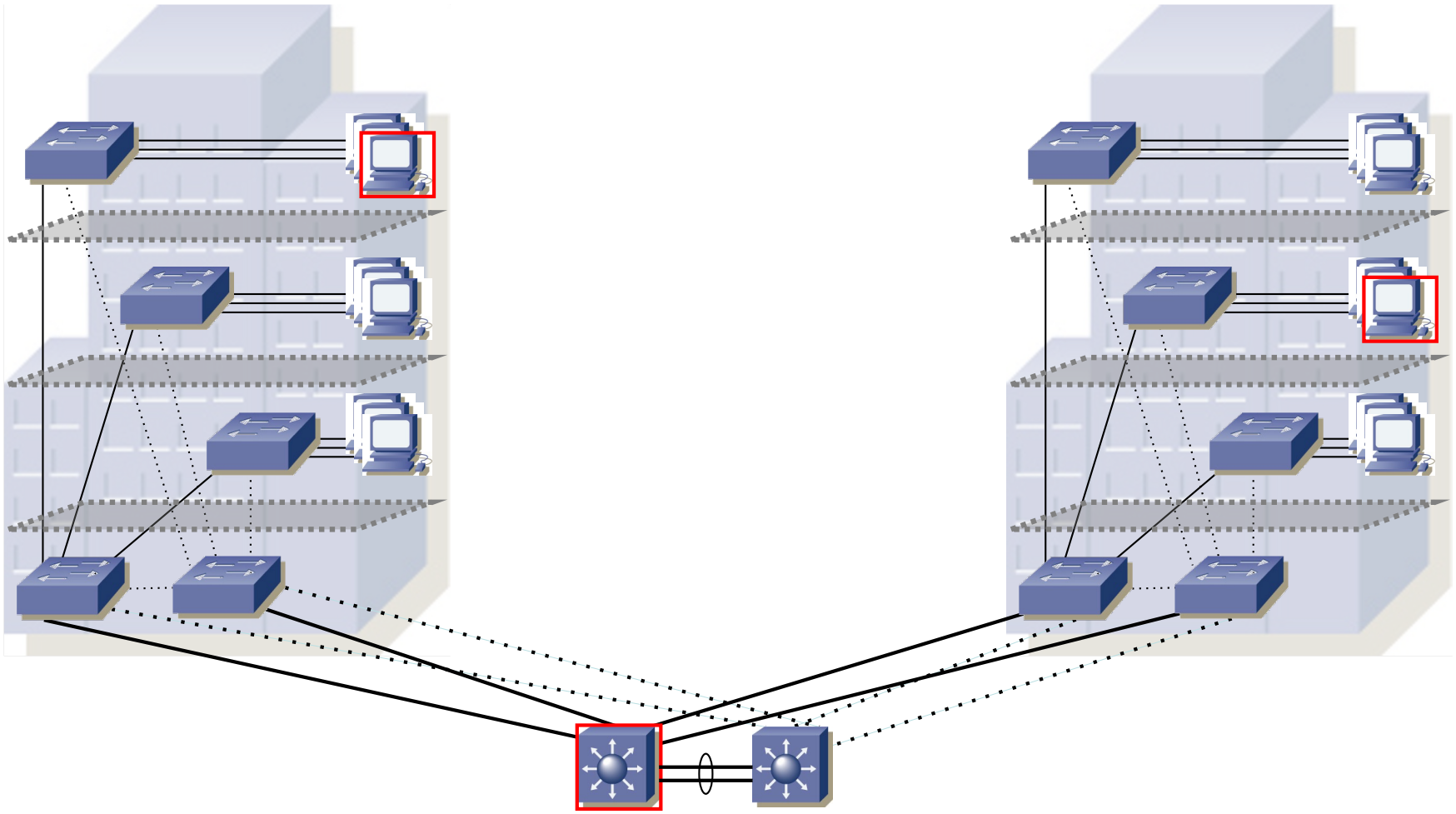
Campus-wide VLANs

- 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



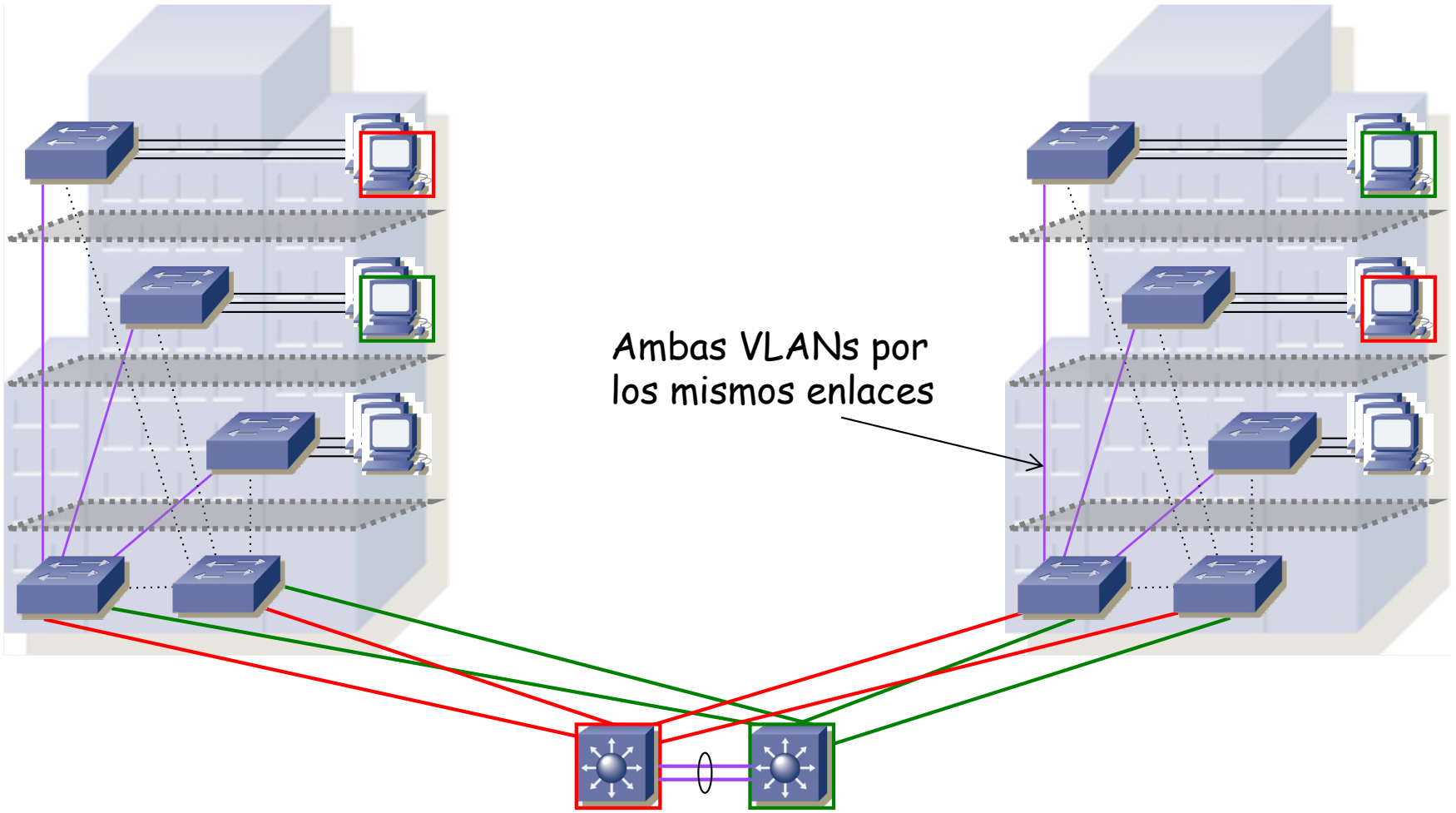
Common Spanning Tree

- En caso de extenderse la VLAN, *root bridge* podría ser del core
- Suponiendo igual coste en los puertos queda este árbol



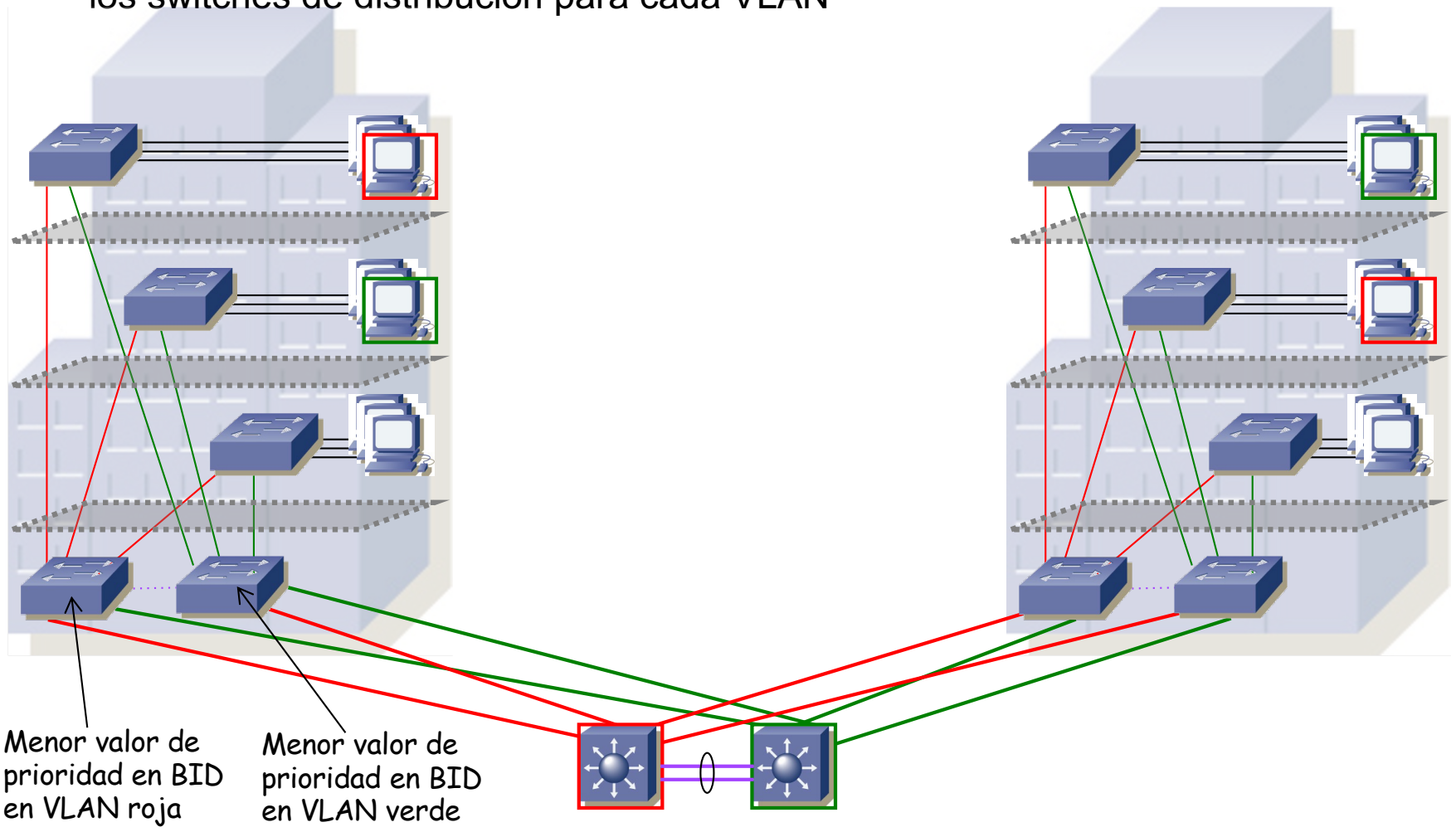
Mutiple Spanning Tree

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



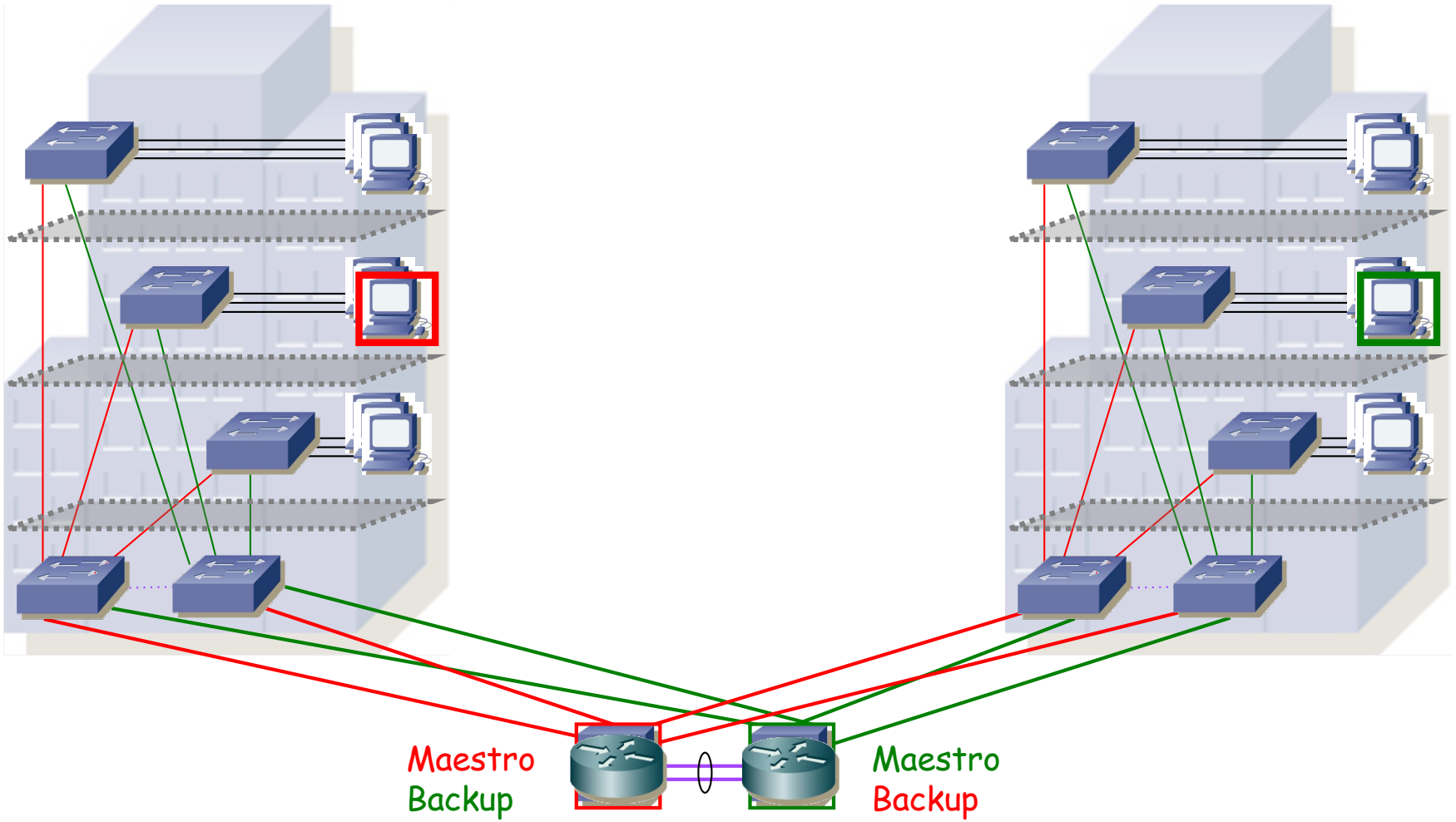
Mutiple Spanning Tree

- 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



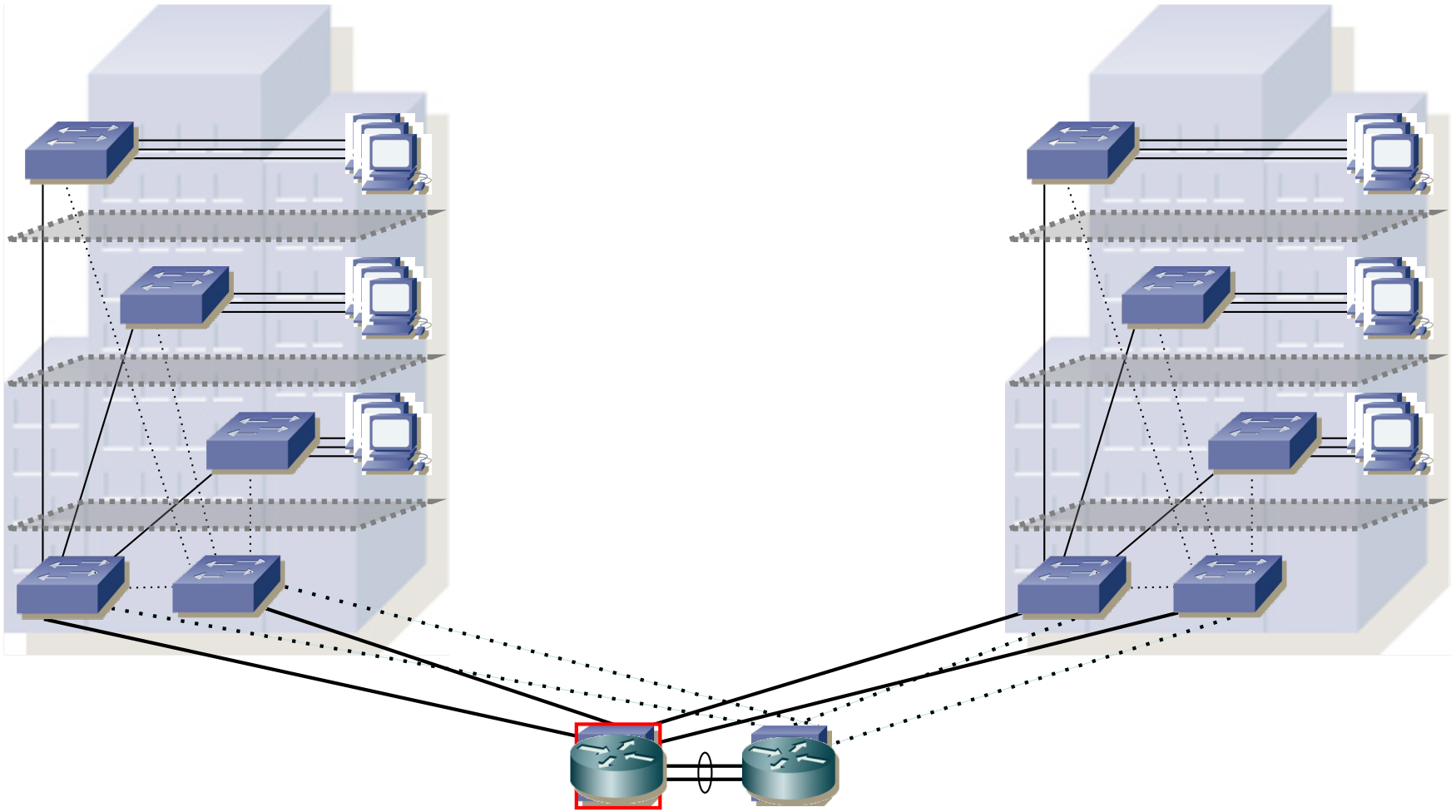
Enrutamiento

- 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 (...)



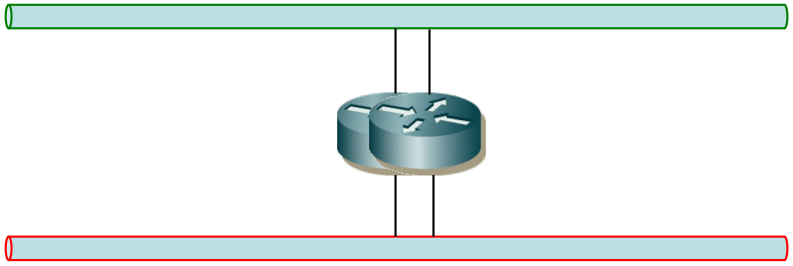
Enrutamiento

- 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 (solo dos subredes/VLANs en el dibujo pero podría haber muchas más)



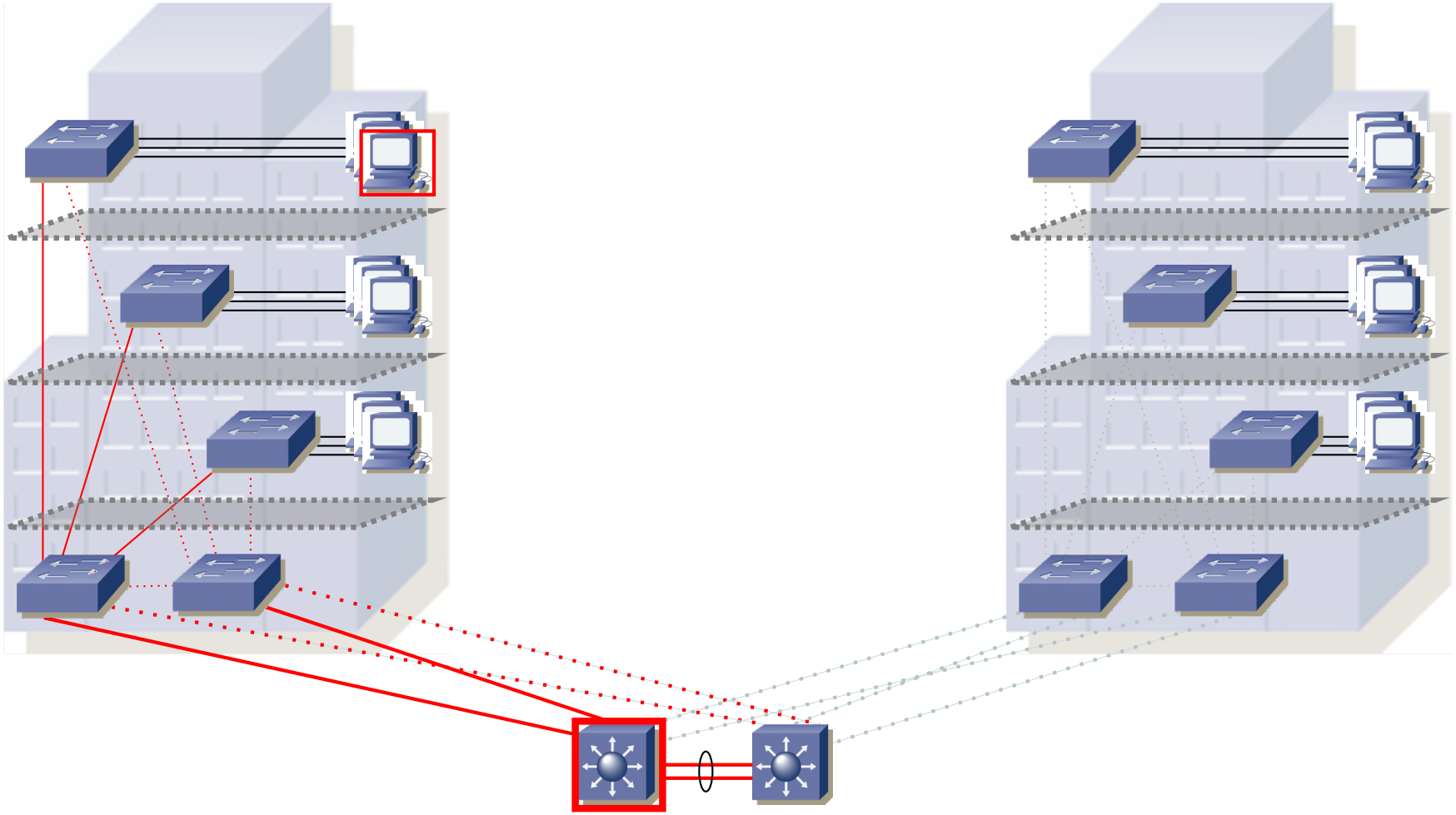
upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Enrutamiento con VLANs restringidas

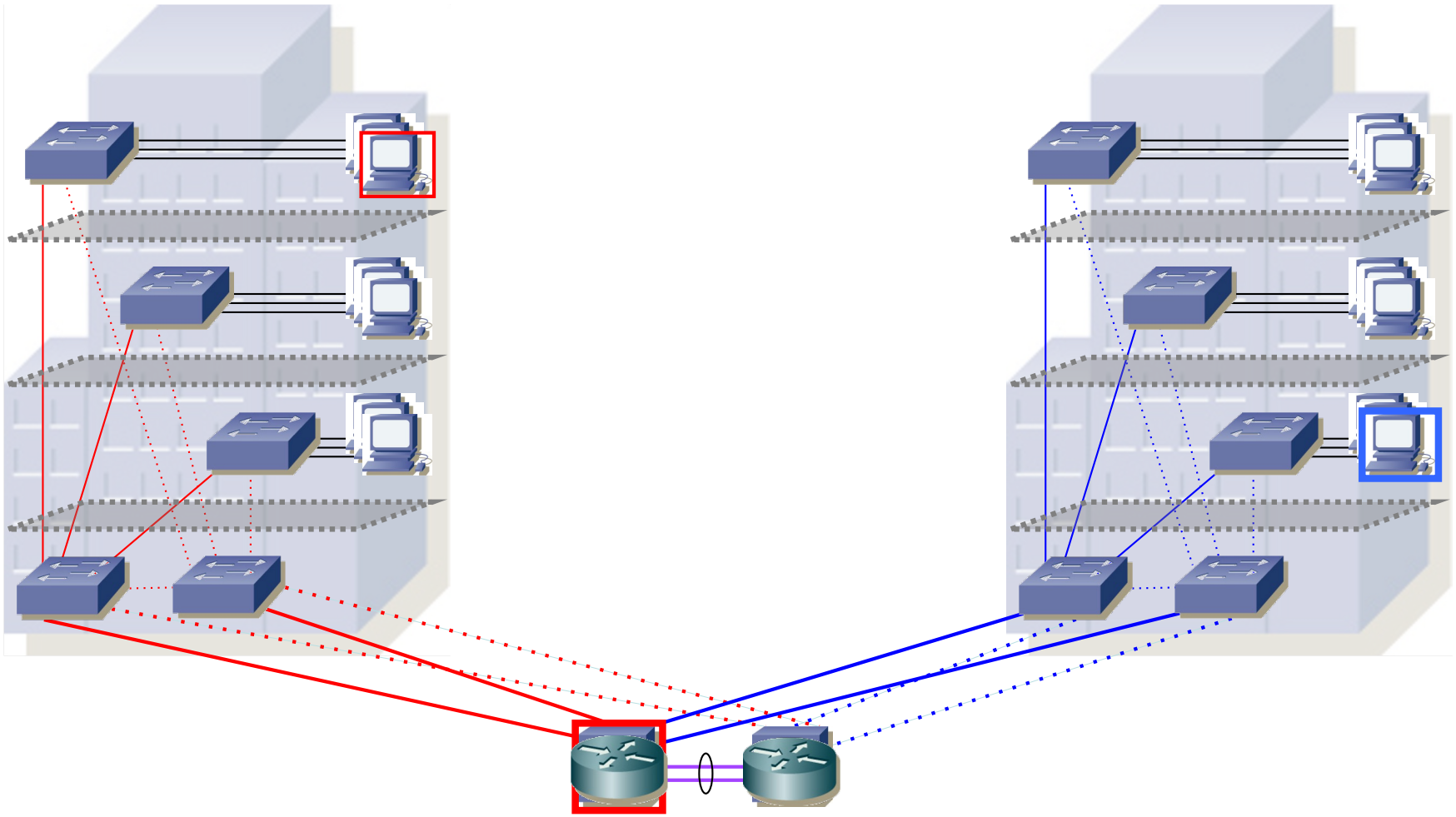
VLANs restringidas

- 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



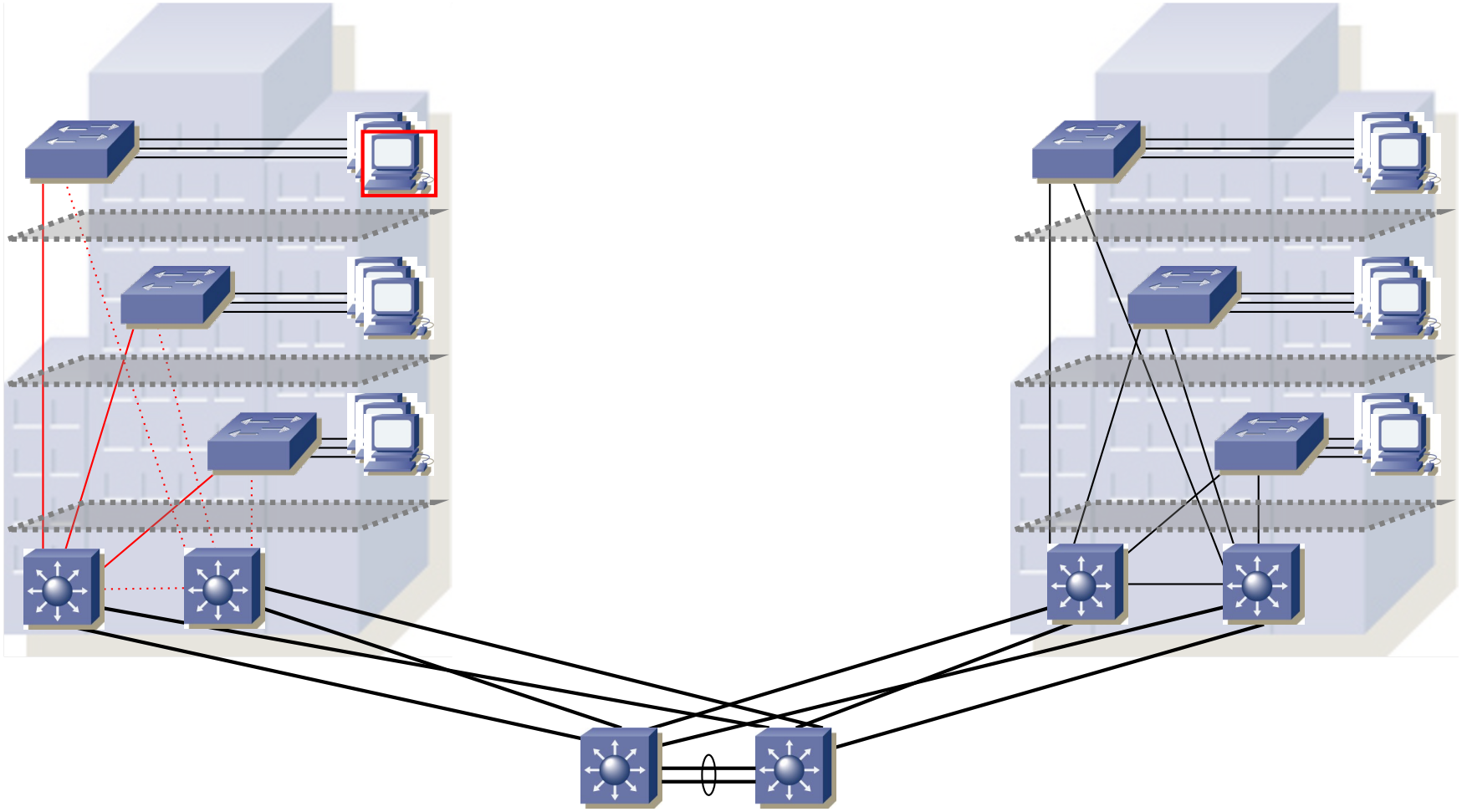
Enrutamiento

- 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* (...)



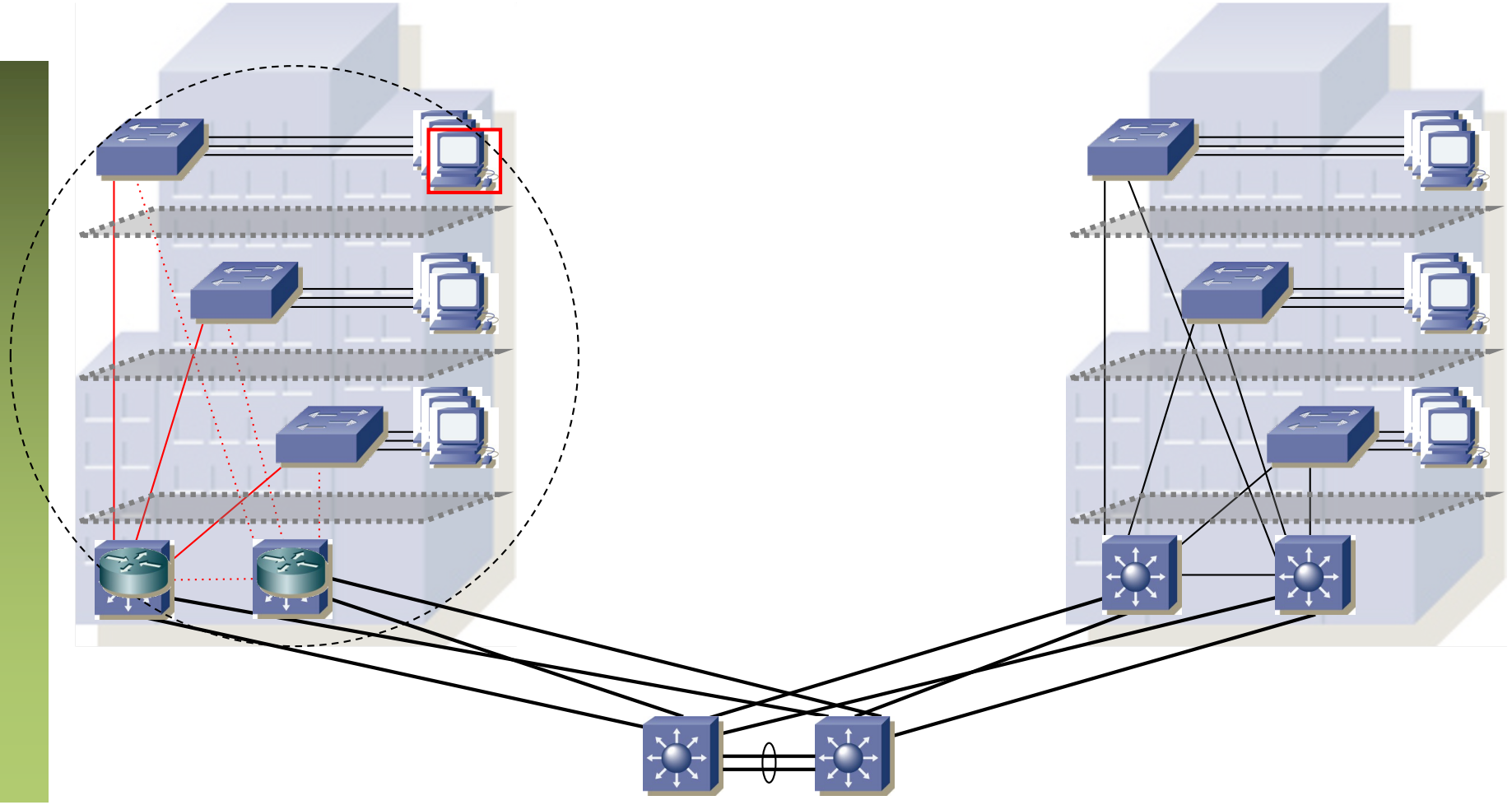
Capa 3 en distribución

- La siguiente alternativa es tener conmutadores capa 2/3 en la distribución
- Ahora sí que las VLANs están restringidas al sistema de distribución
- (…)



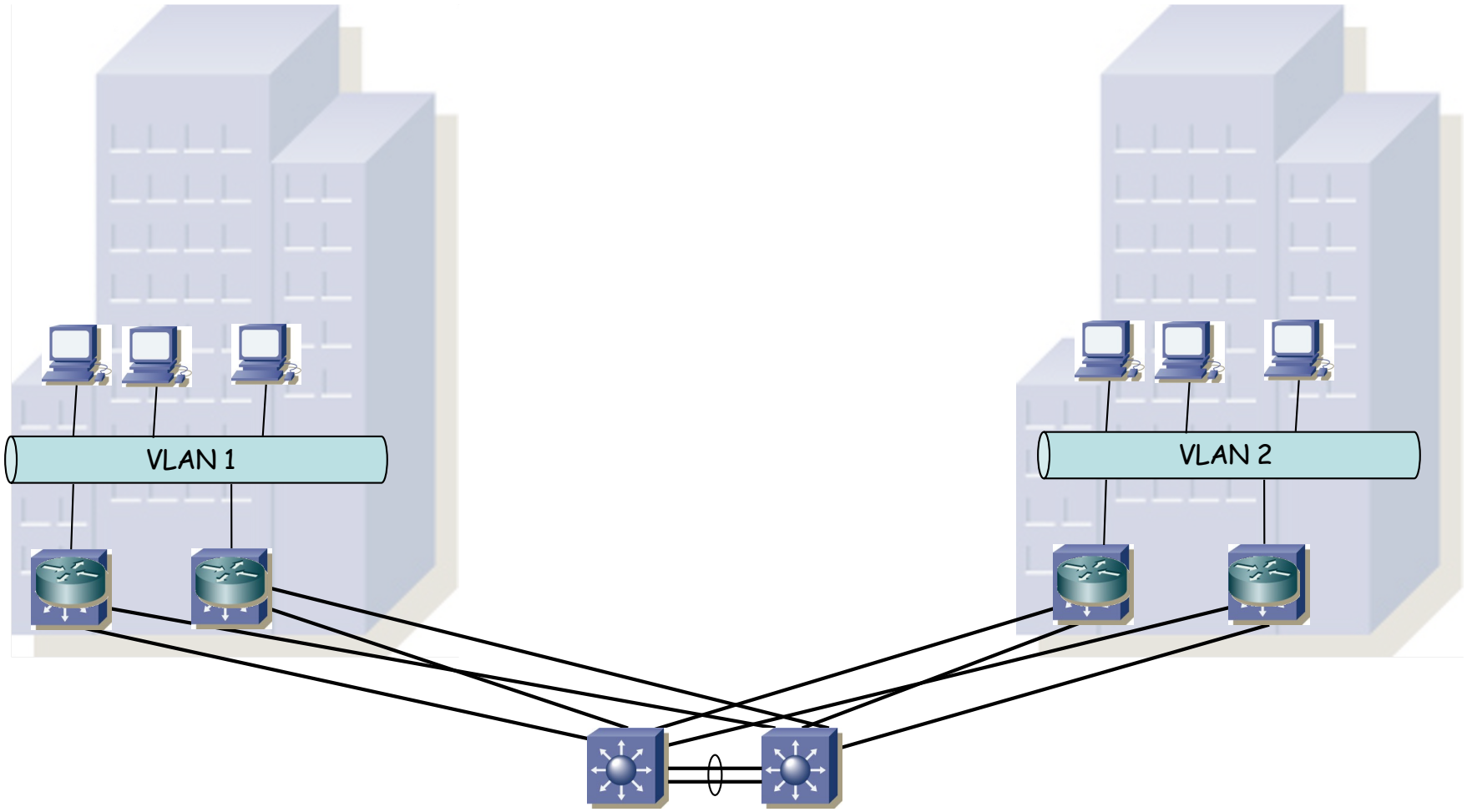
Capa 3 en distribución

- 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) (…)



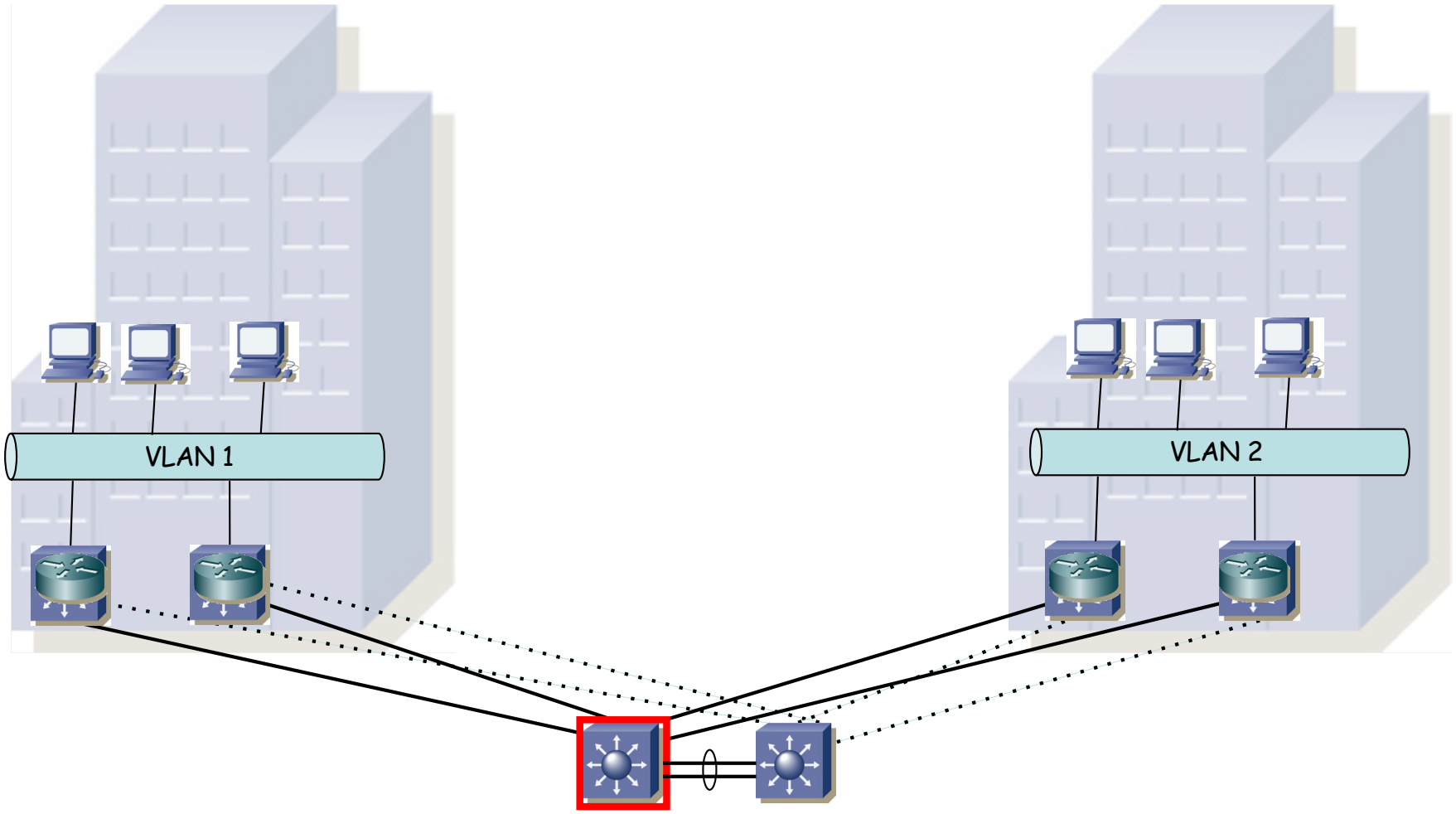
Capa 3 en distribución

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



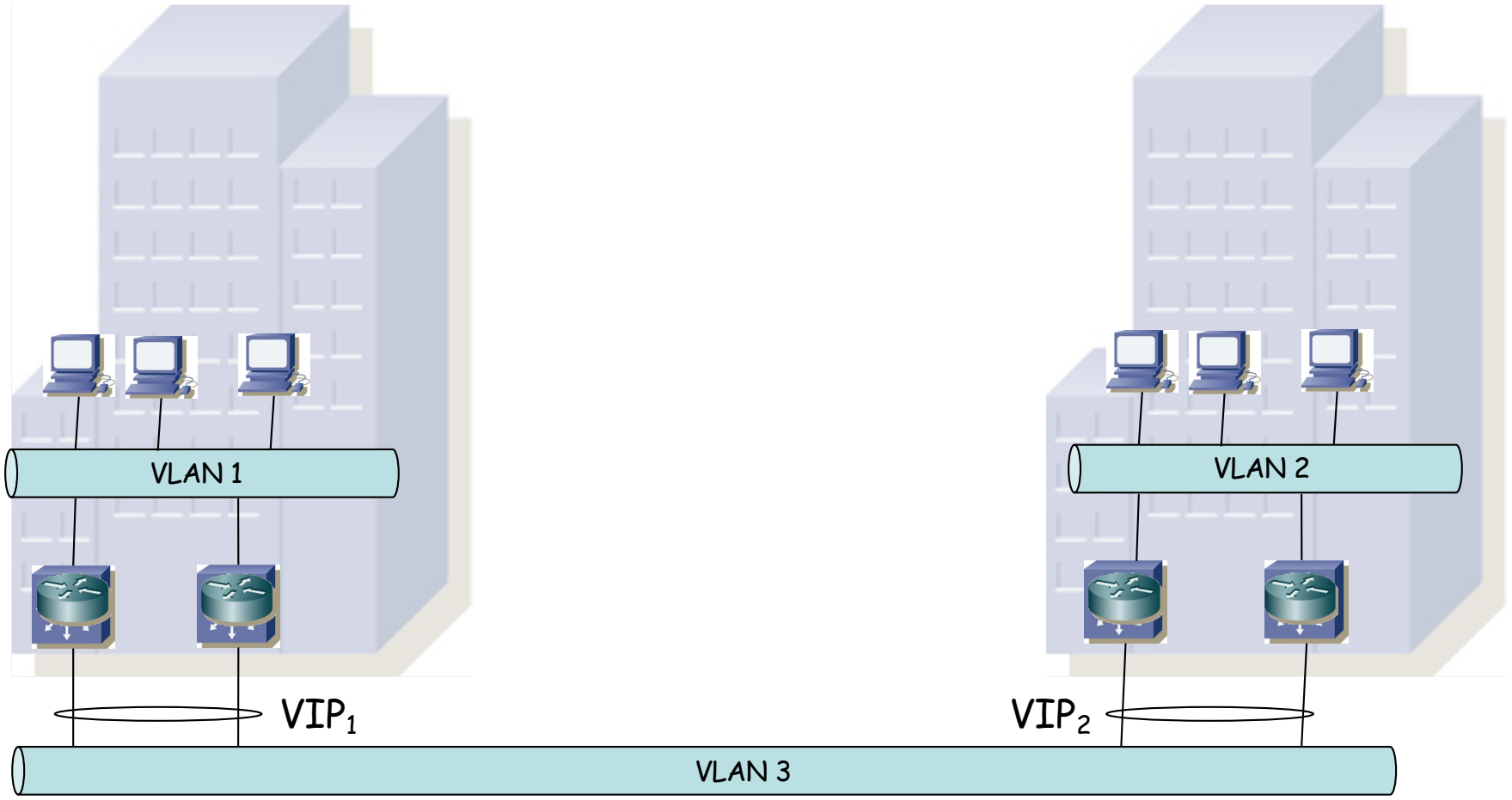
Capa 3 en distribución

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



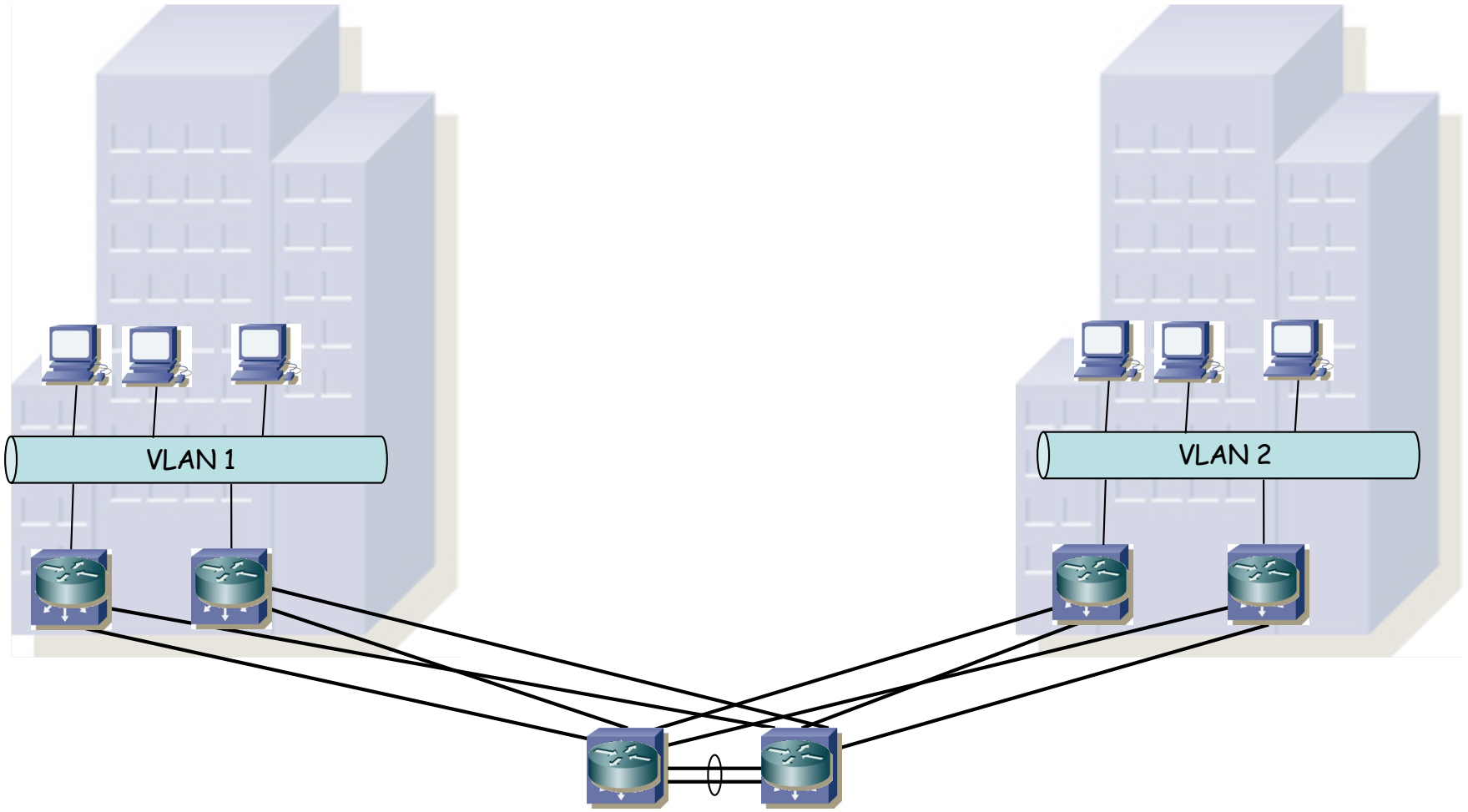
Capa 3 en distribución

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



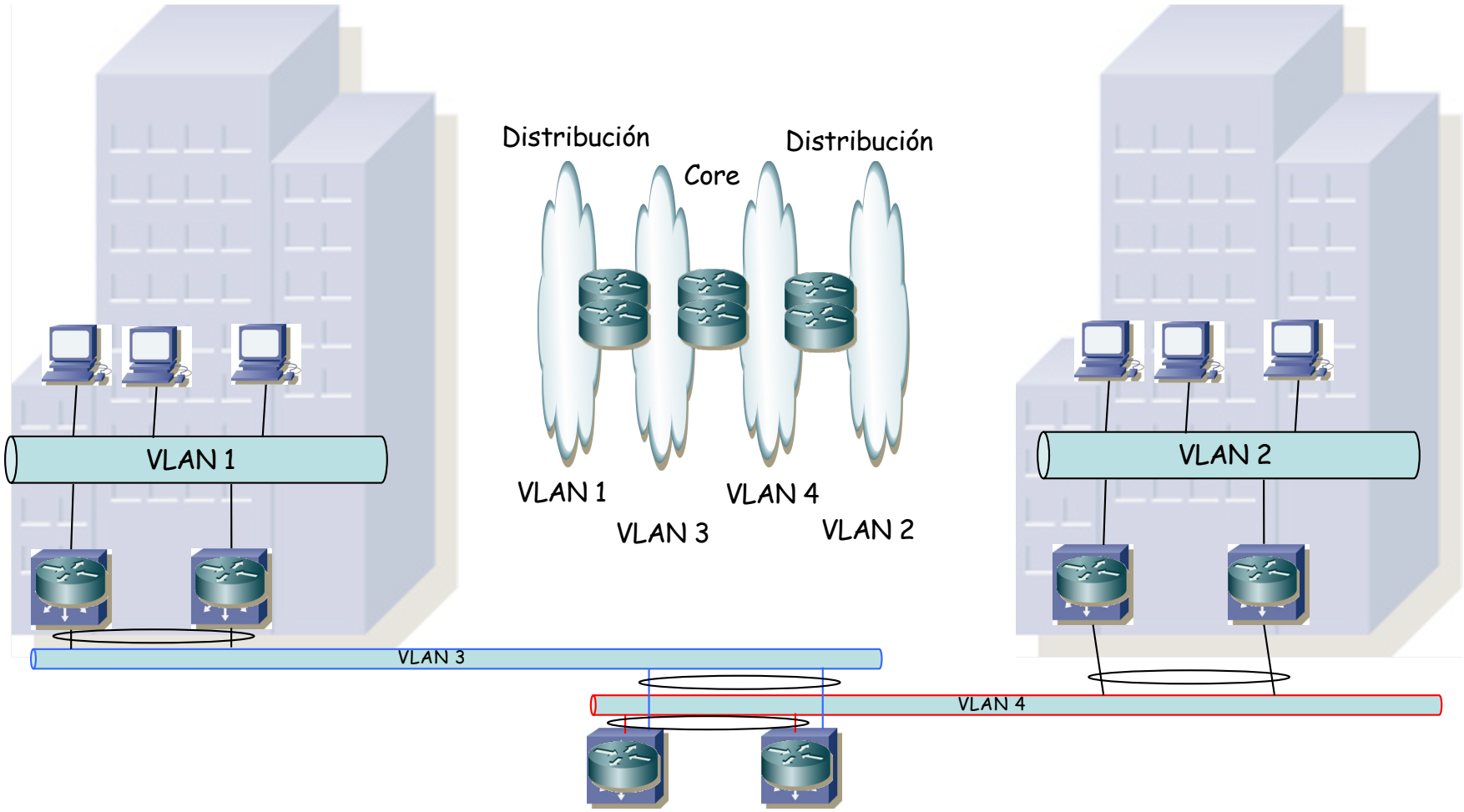
Capa 3 en distribución

- ¿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 (…)



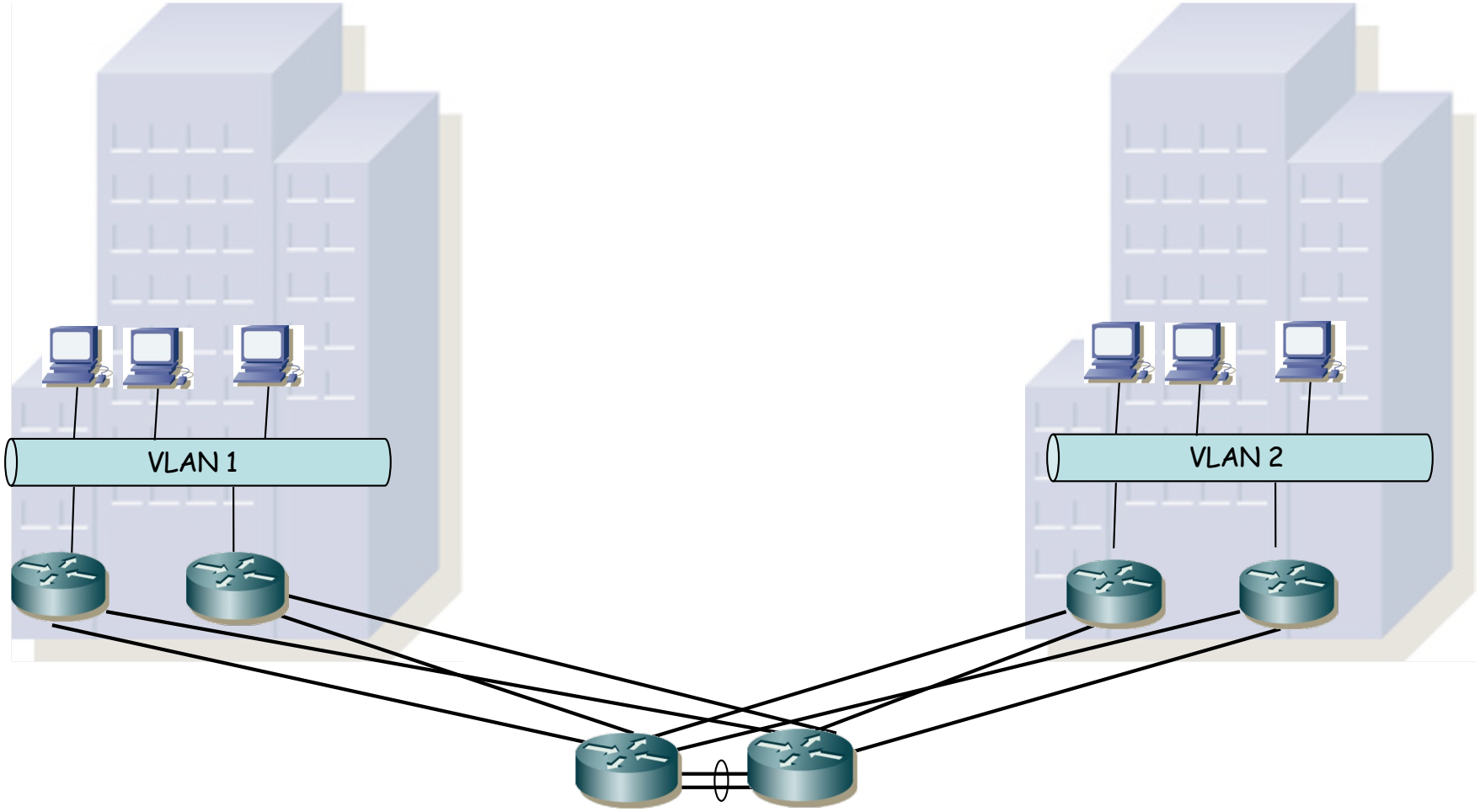
Capa 3 en distribución

- ¿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



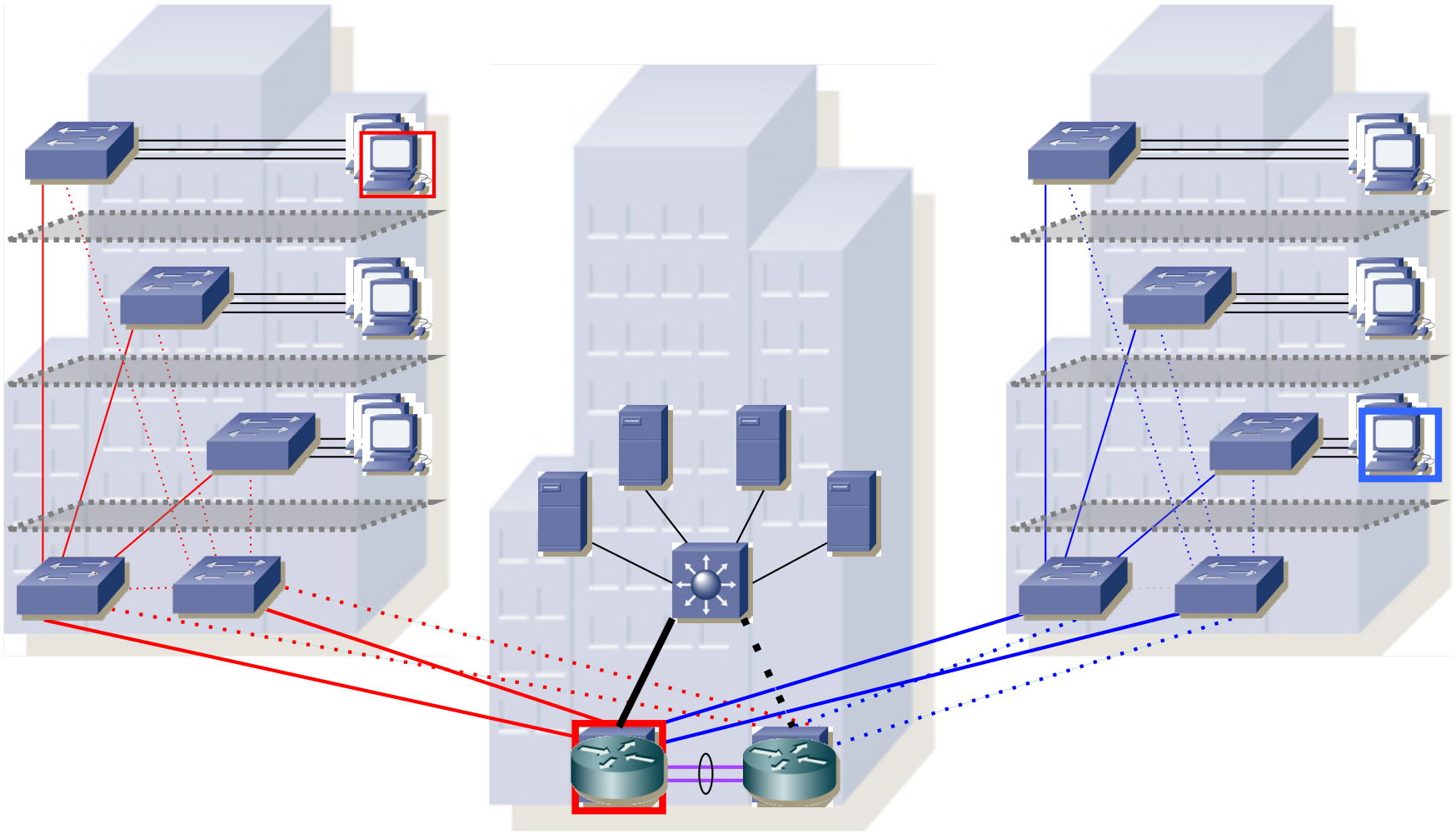
upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Servidores y exterior

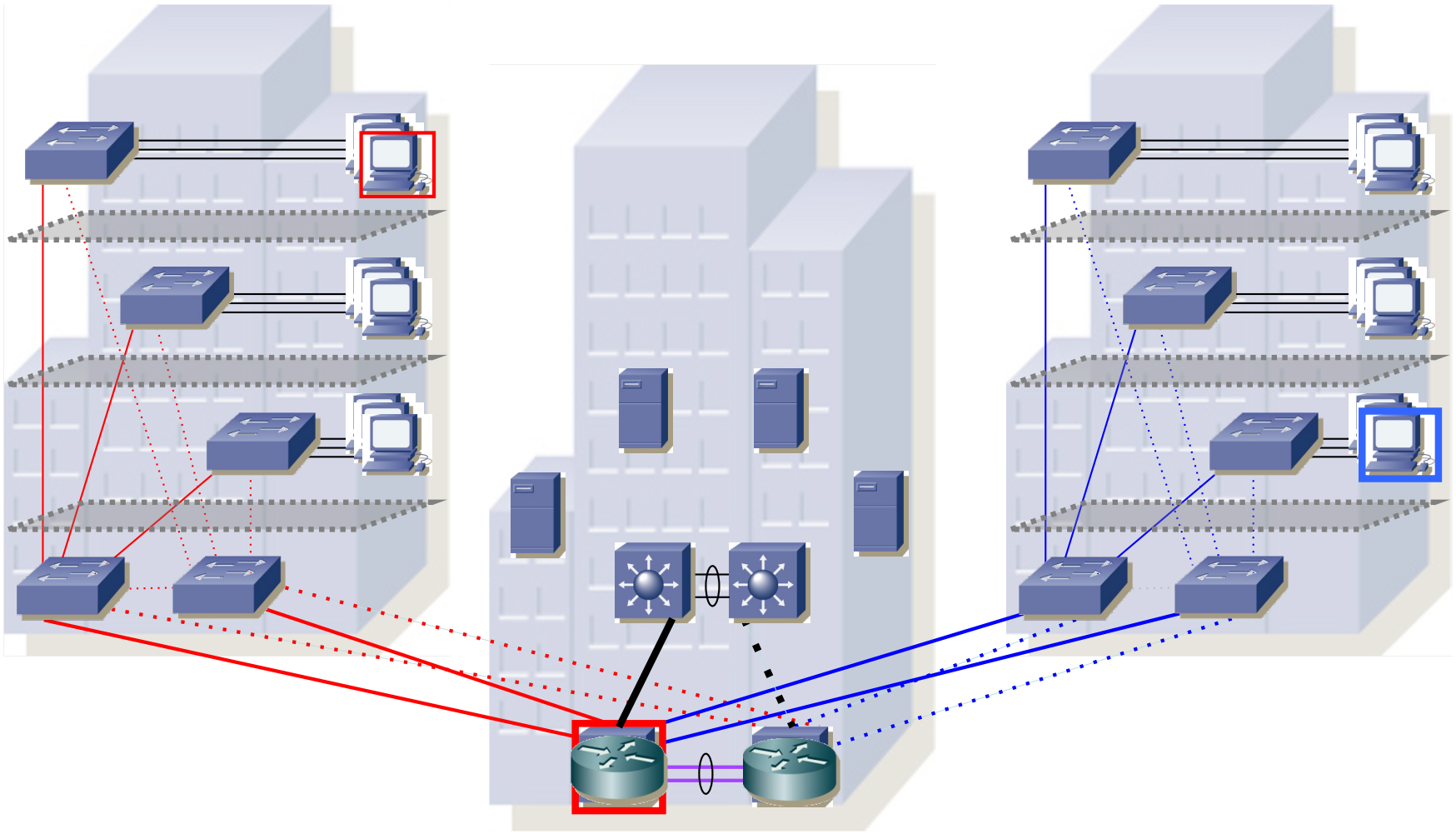
Centralización de servidores

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



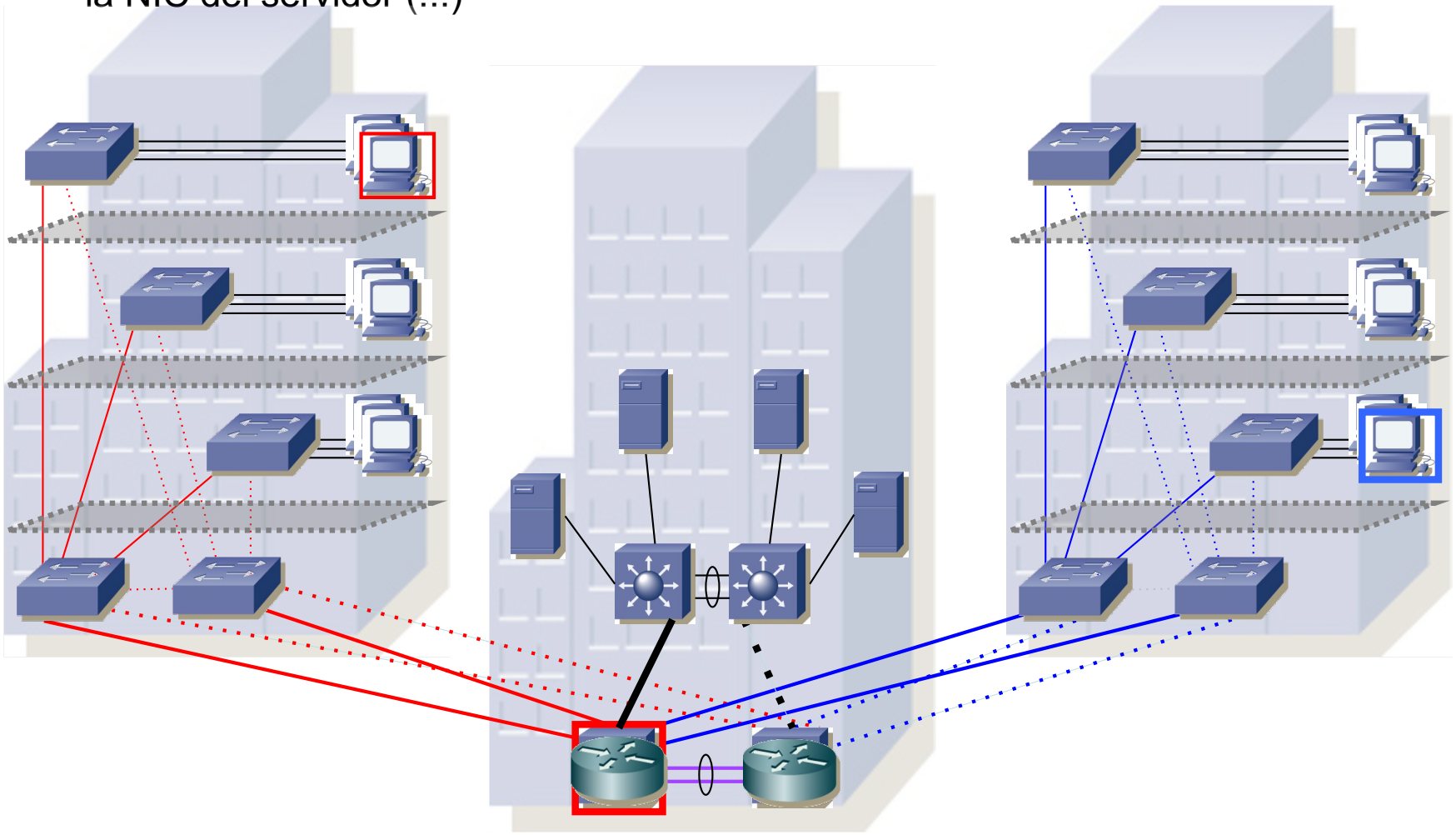
Centralización de servidores

- Podemos tener una VLAN con servidores centralizados o según servicio
- Pero con esto hay un punto de fallo en ese nuevo conmutador
- Podemos duplicarlo pero ¿qué hacemos con los servidores? (...)



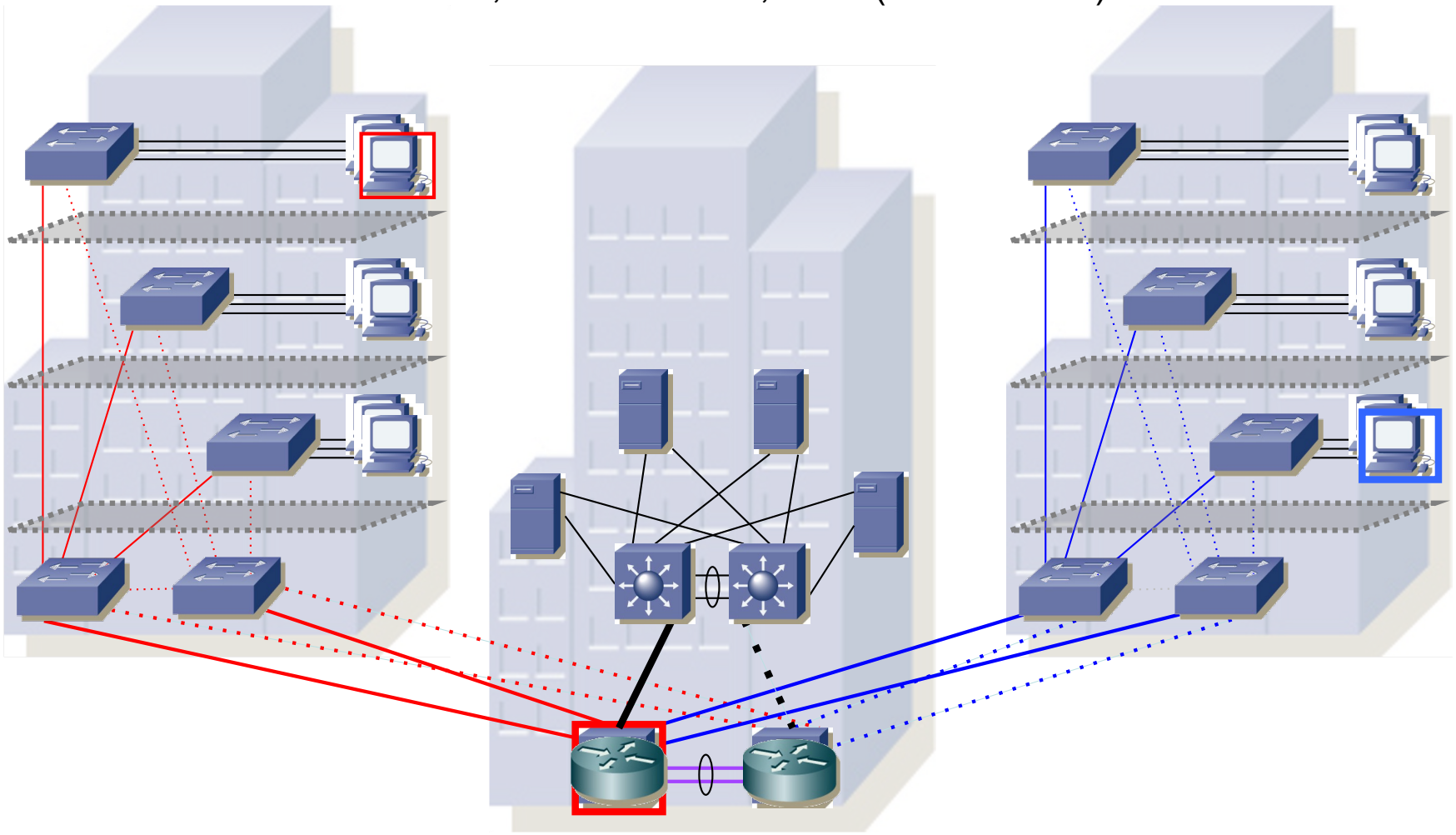
Centralización de servidores

- Podemos tener una VLAN con servidores centralizados o según servicio
- 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 (...)



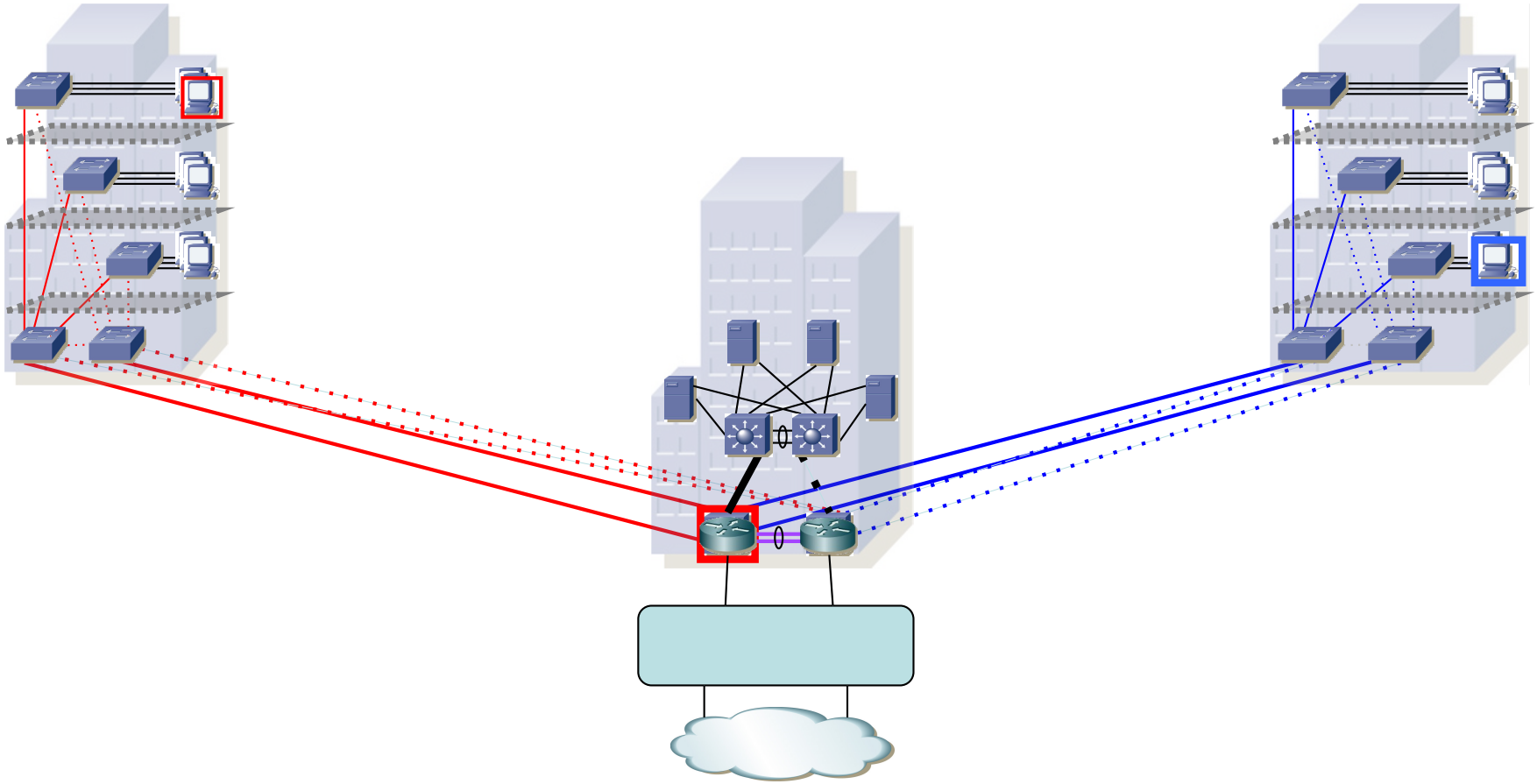
Centralización de servidores

- 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)



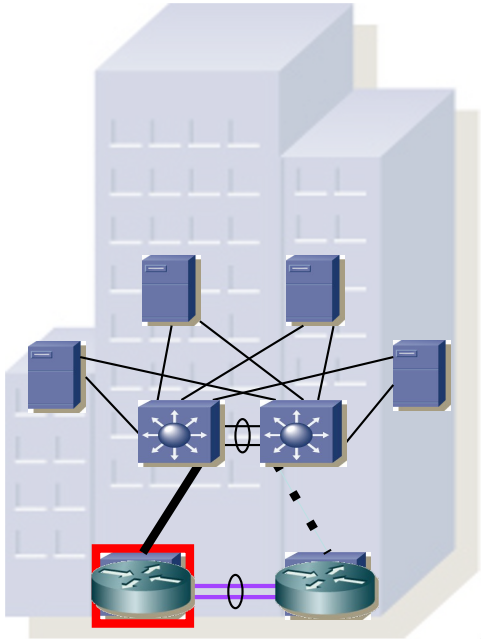
Acceso a WAN

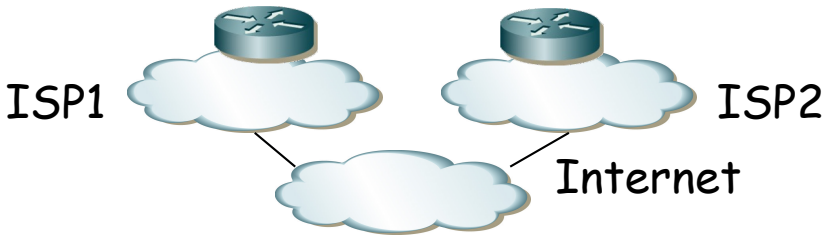
- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- (...)



Acceso a WAN

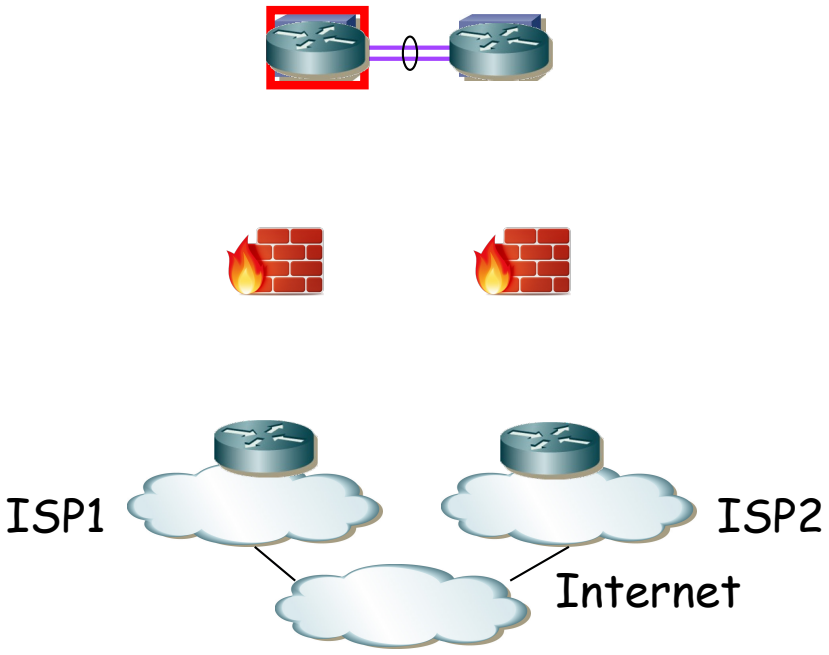
- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- El acceso a WAN/Internet puede ser por uno o dos ISPs
- (...)





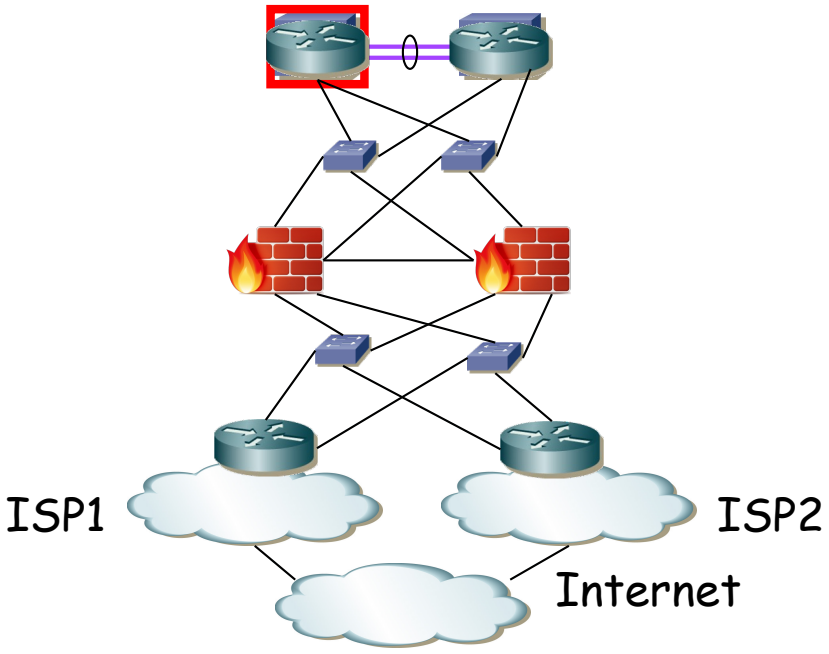
Acceso a WAN

- 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
- (...)



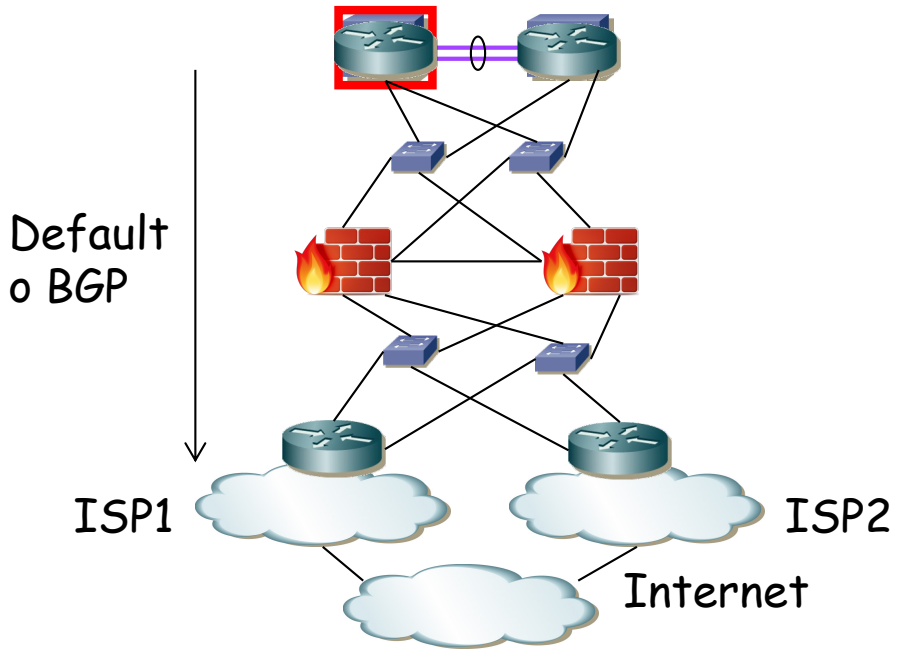
Acceso a WAN

- 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



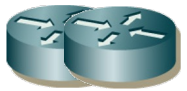
Acceso a WAN: Routing

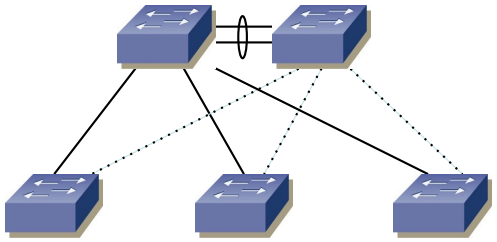
- Hacia el exterior es frecuente trabajar con una ruta por defecto
- Salvo que empecemos a hablar de sedes remotas, VPNs, etc
- Se puede emplear BGP para aprender las rutas a Internet y repartir tráfico entre los dos ISPs

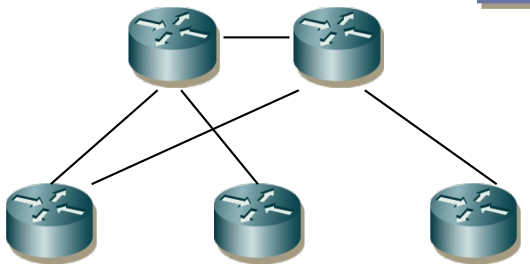


Resumen sobre protección

- 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







¿ Qué no hemos cubierto ?

- **Wireless**: hoy en día frecuente uso de Wireless Controllers
- **Routing**: dinámico, BGP con Internet, OSPF u otros como IGP
- **QoS**: necesario para flujos de voz y vídeo, requiere un servicio extremo a extremo
- Despliegue **VoIP**
- Qué **capacidad**, retardo, jitter me ofrece la red y requieren las aplicaciones/usuarios
- Migración a **IPv6**
- **Seguridad**: Firewalls, VPNs, IDS
- **Gestión**, operación y monitorización de la red
- Relación de la red con arquitectura **multi-tier** de servicios
- Data center, sedes remotas, acceso de usuarios remotos
- Integración con redes **celulares**
- (...)

¿ Qué no hemos cubierto ?

- **Wireless**: hoy en día frecuente uso de Wireless Controllers
- **Routing**: dinámico, BGP con Internet, OSPF u otros como IGP
- **QoS**: necesario para flujos de voz y vídeo, requiere un servicio extremo a extremo
- Despliegue **VoIP**
- Qué **capacidad**, retardo, jitter me ofrece la red y requieren las aplicaciones/usuarios
- Migración a **IPv6**
- **Seguridad**: Firewalls, VPNs, IDS
- **Gestión**, operación y monitorización de la red
- Relación de la red con arquitectura **multi-tier** de servicios
- Data center, sedes remotas, acceso de usuarios remotos
- Integración con redes **celulares**
- Routing, IPv6, NATs, QoS y redes celulares se ven en *Tecnologías Avanzadas de Red*
- Firewalls, ataques, DMZs y VPNs se verán en *Seguridad en Redes y Servicios*
- Prestaciones de la red y servicios/servidores en *Gestión y planificación de redes y servicios*
- Otros temas en el máster: virtualización en la red y en los servidores, balanceadores, arquitectura de CPD, interconexión de CPDs, no-STP, etc.

Diseño de red

- Sencillez hace la red más manejable y entendible
- Redundancia
- En gran medida el diseño es un arte