

Diseño de Campus LAN (parte 3)

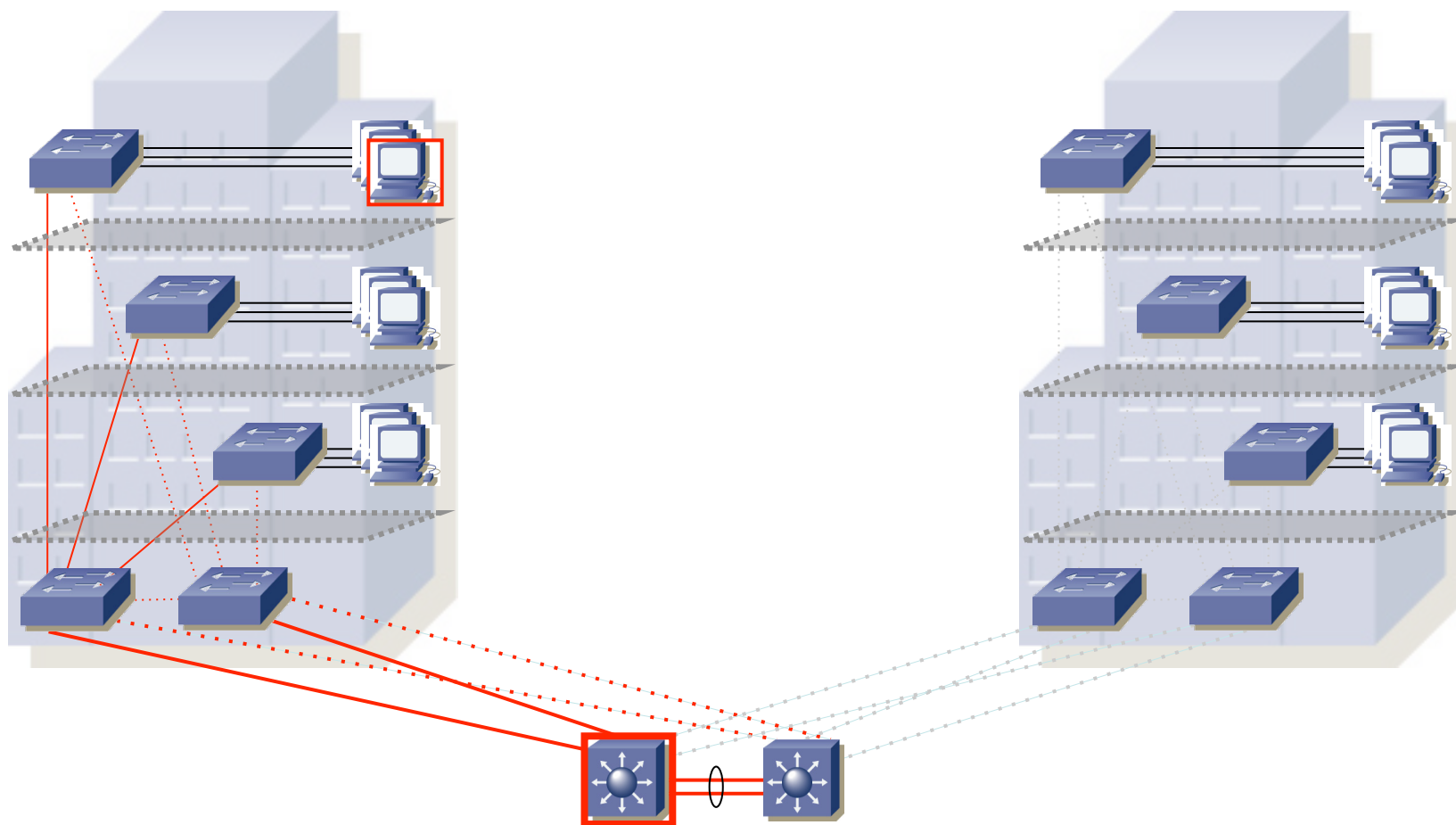
Area de Ingeniería Telemática
<http://www.tlm.unavarra.es>

Grado en Ingeniería en Tecnologías de
Telecomunicación, 3º

Enrutamiento con VLANs restringidas

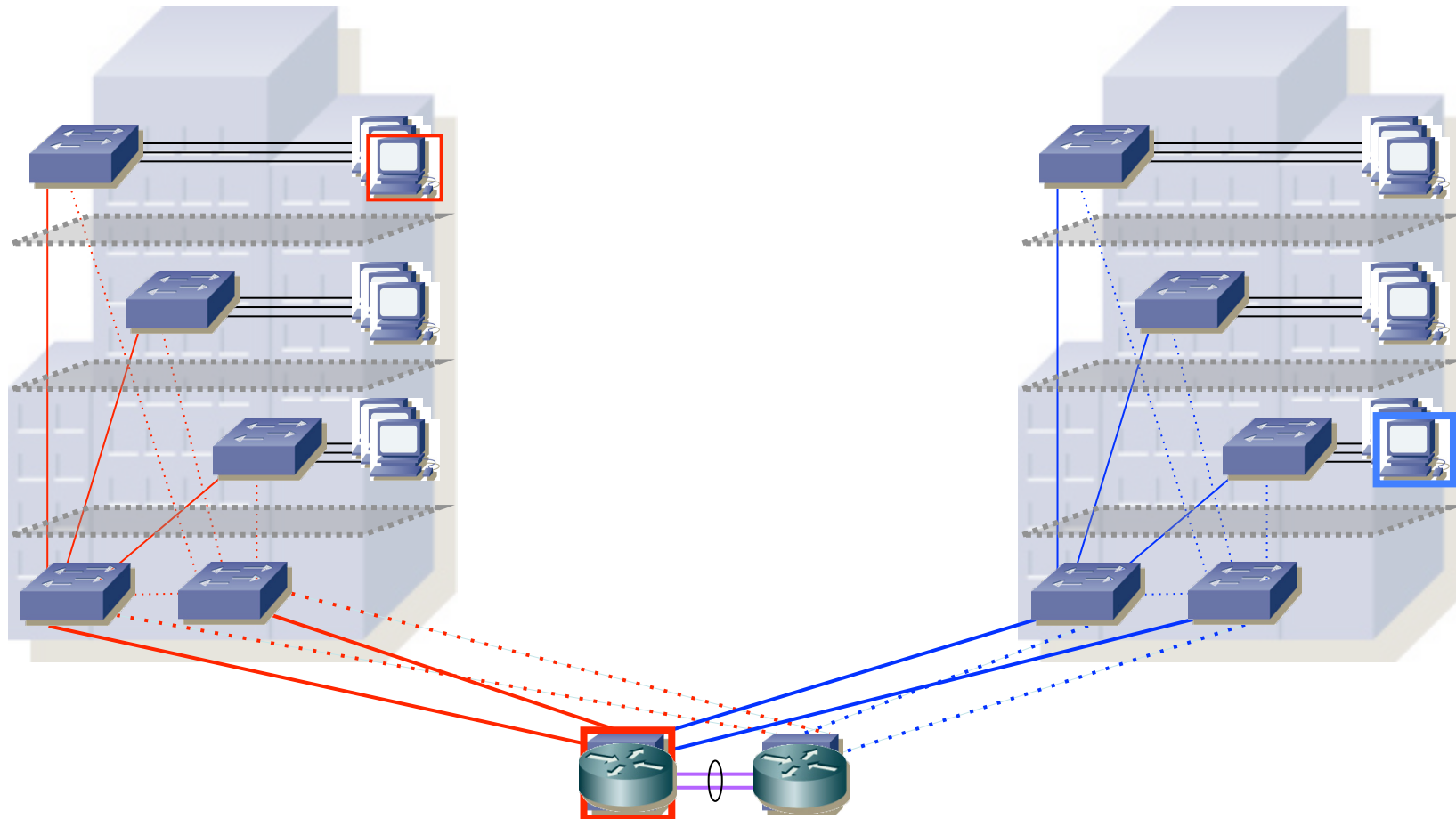
VLANs restringidas

- 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



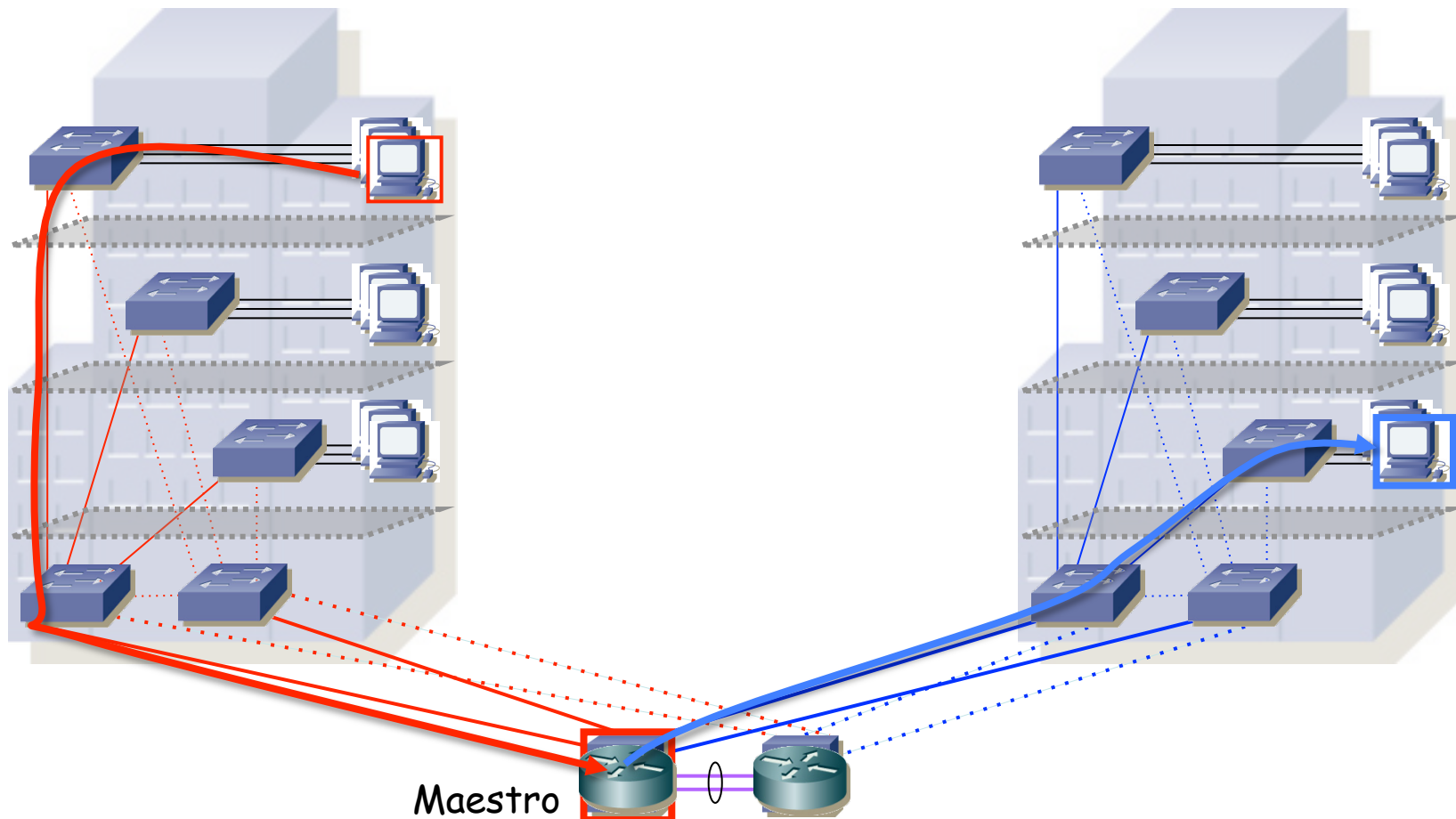
Enrutamiento

- 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* (...)



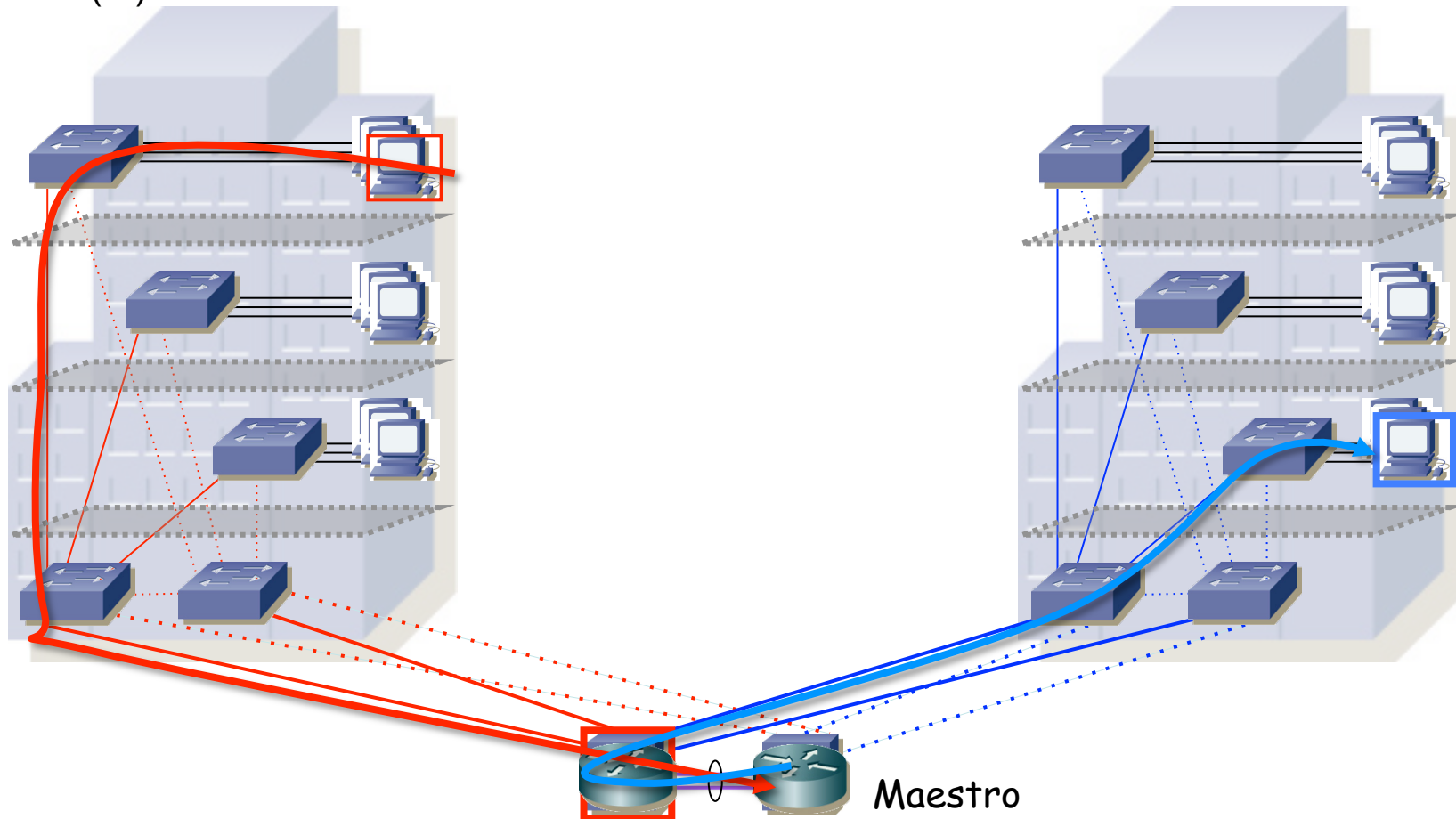
Enrutamiento

- 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 (...)



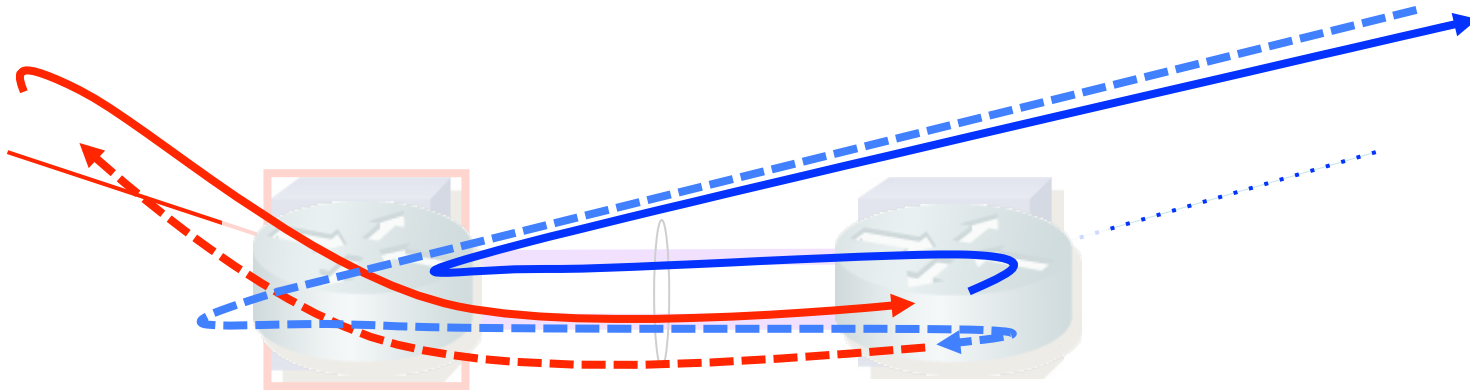
Enrutamiento

- 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 (...)



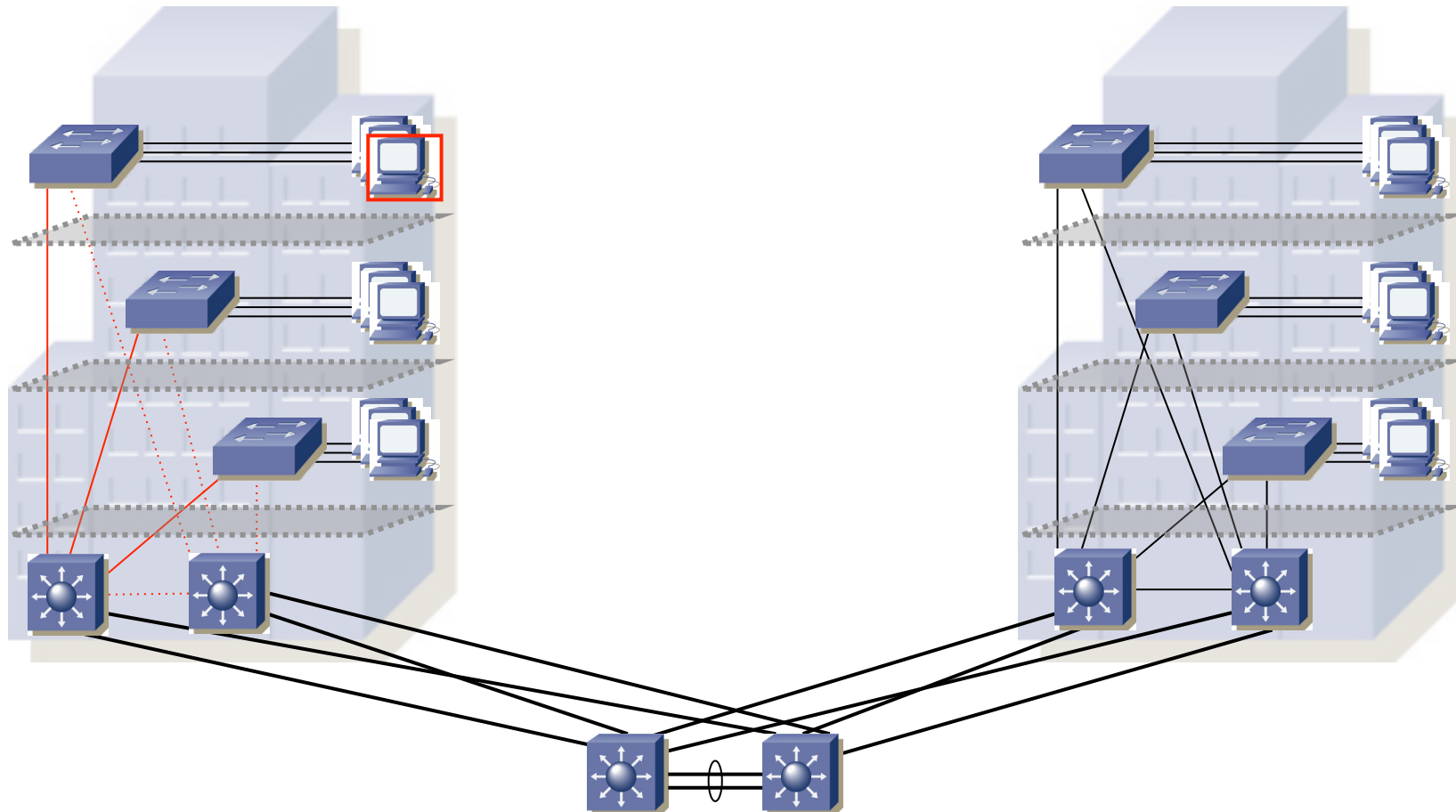
Enrutamiento

- 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



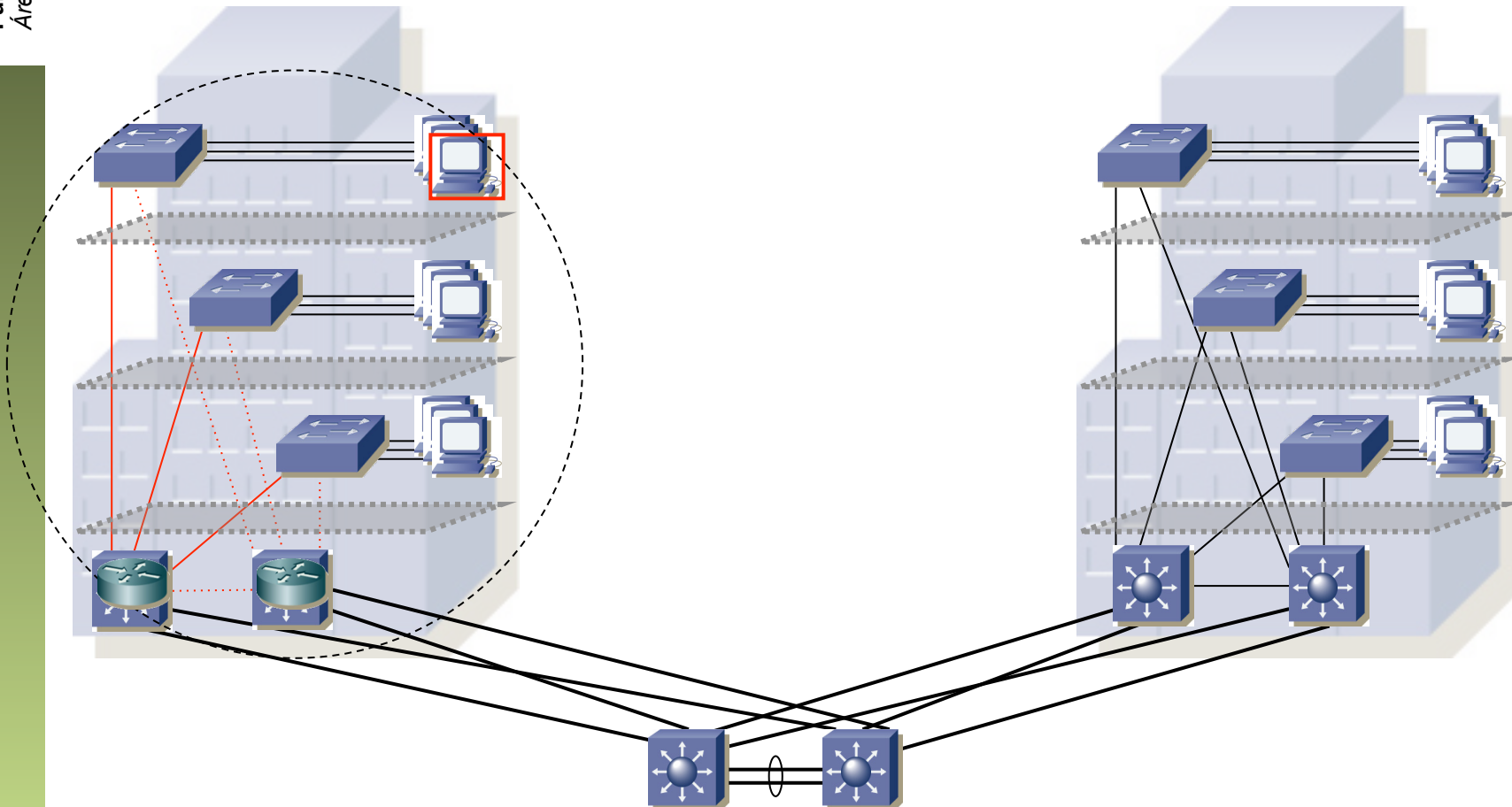
Capa 3 en distribución

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



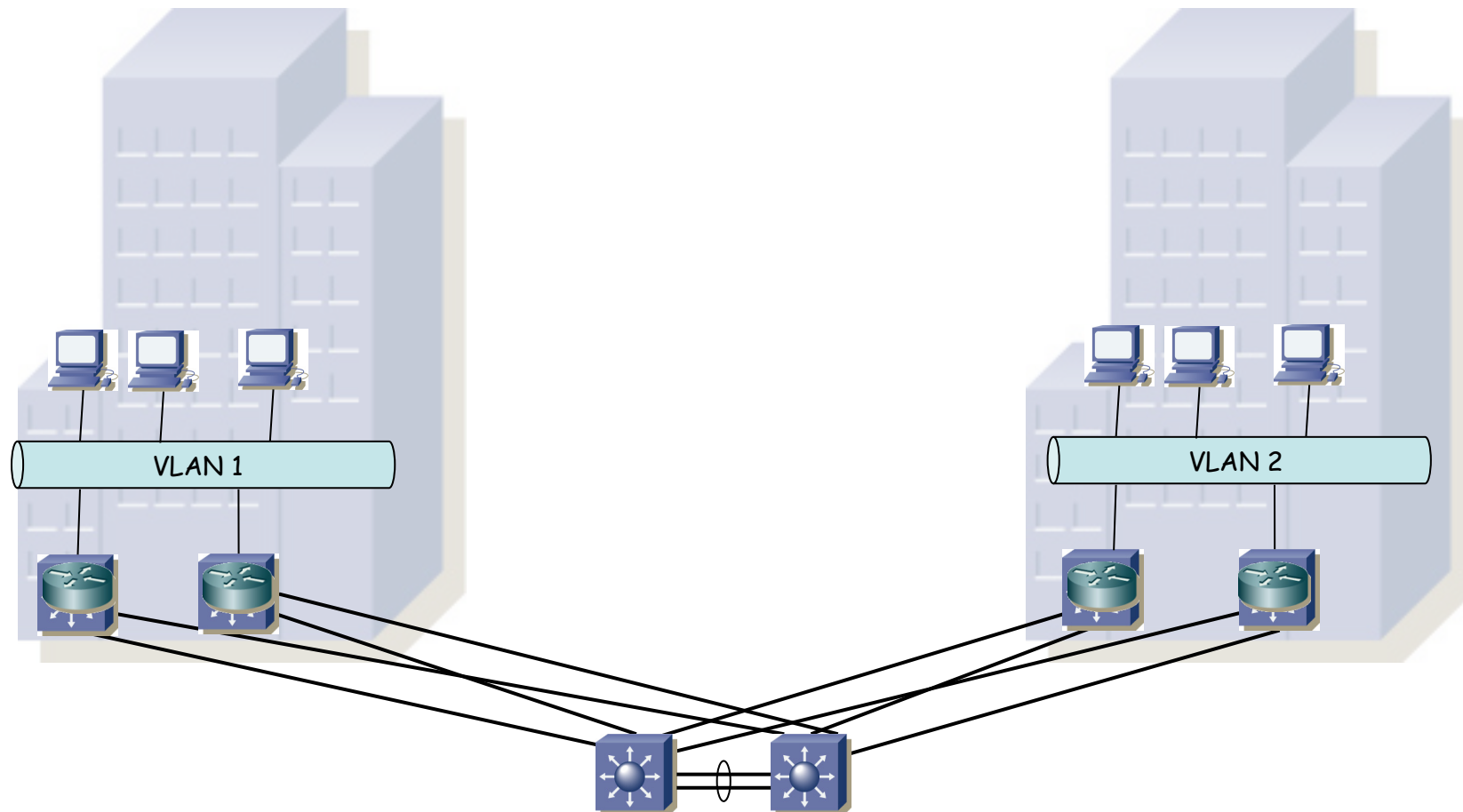
Capa 3 en distribución

- 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) (...)



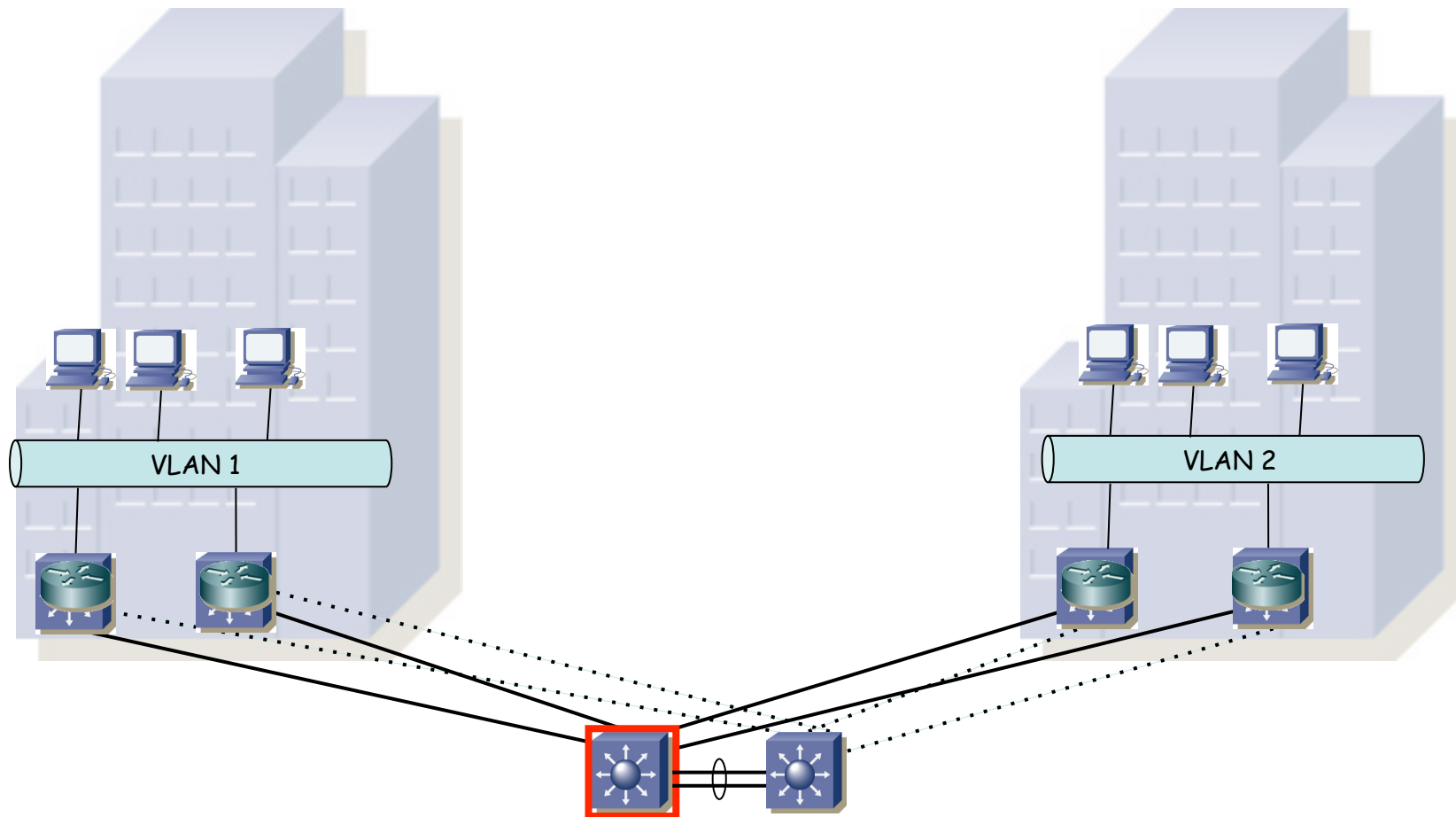
Capa 3 en distribución

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



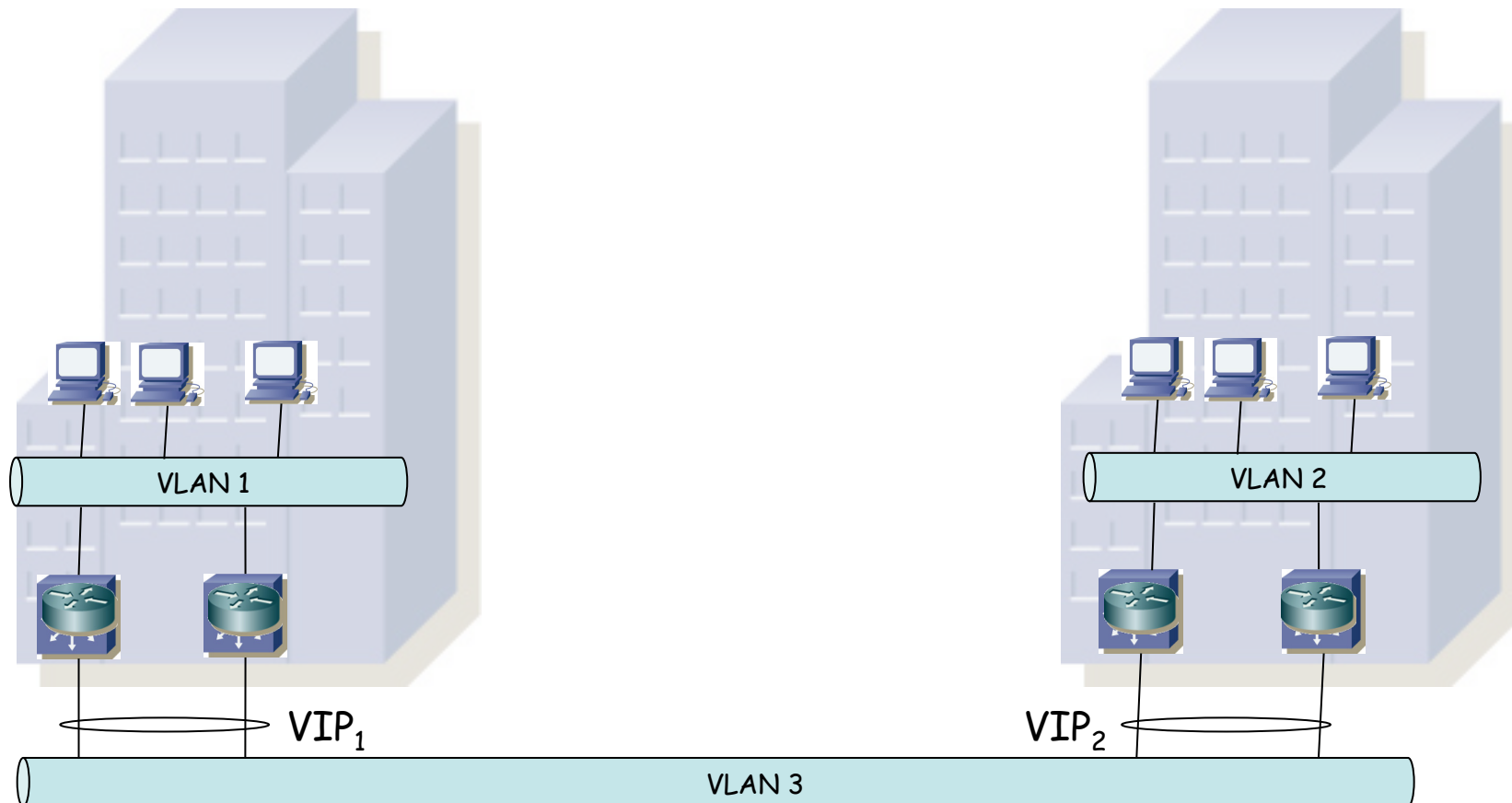
Capa 3 en distribución

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



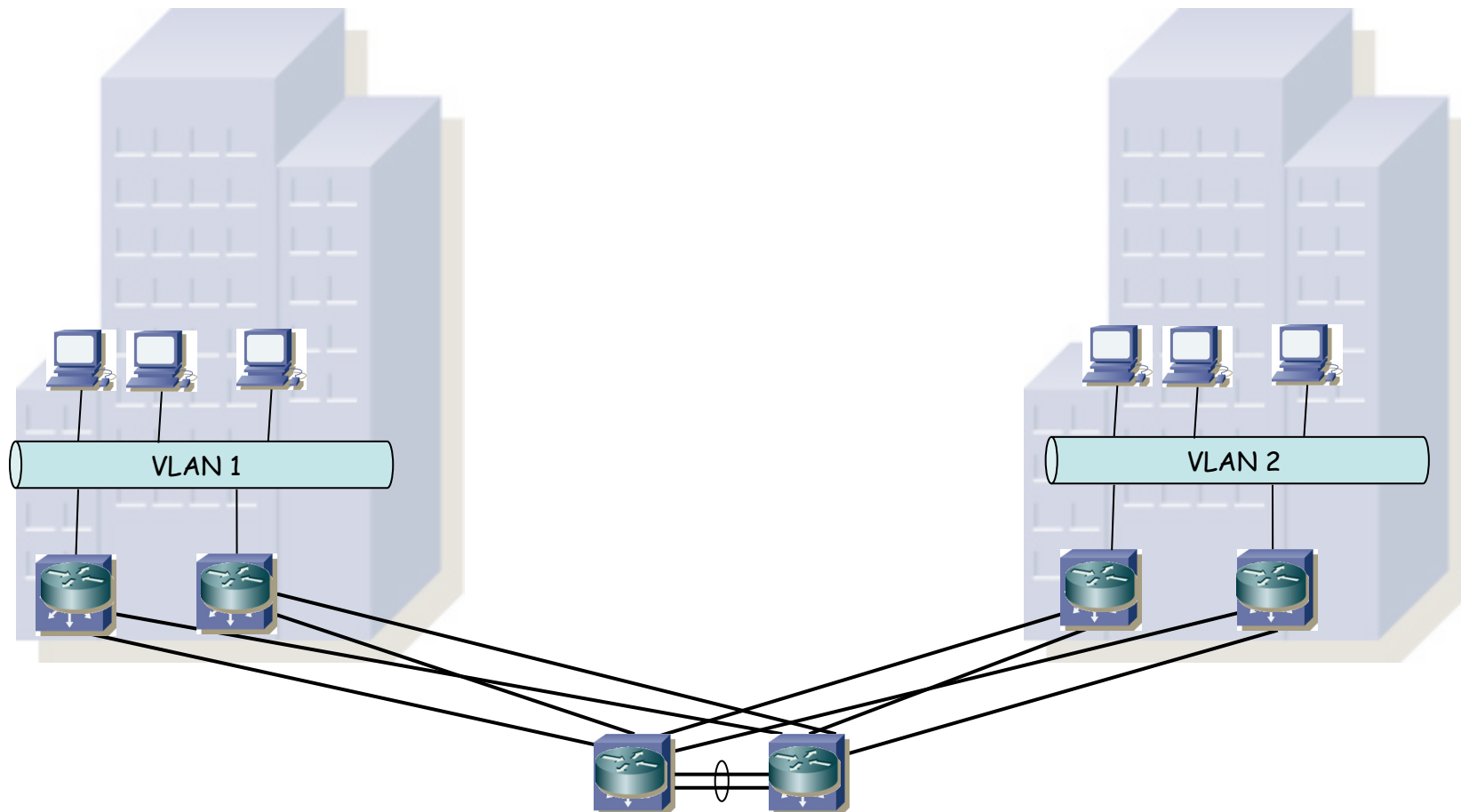
Capa 3 en distribución

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



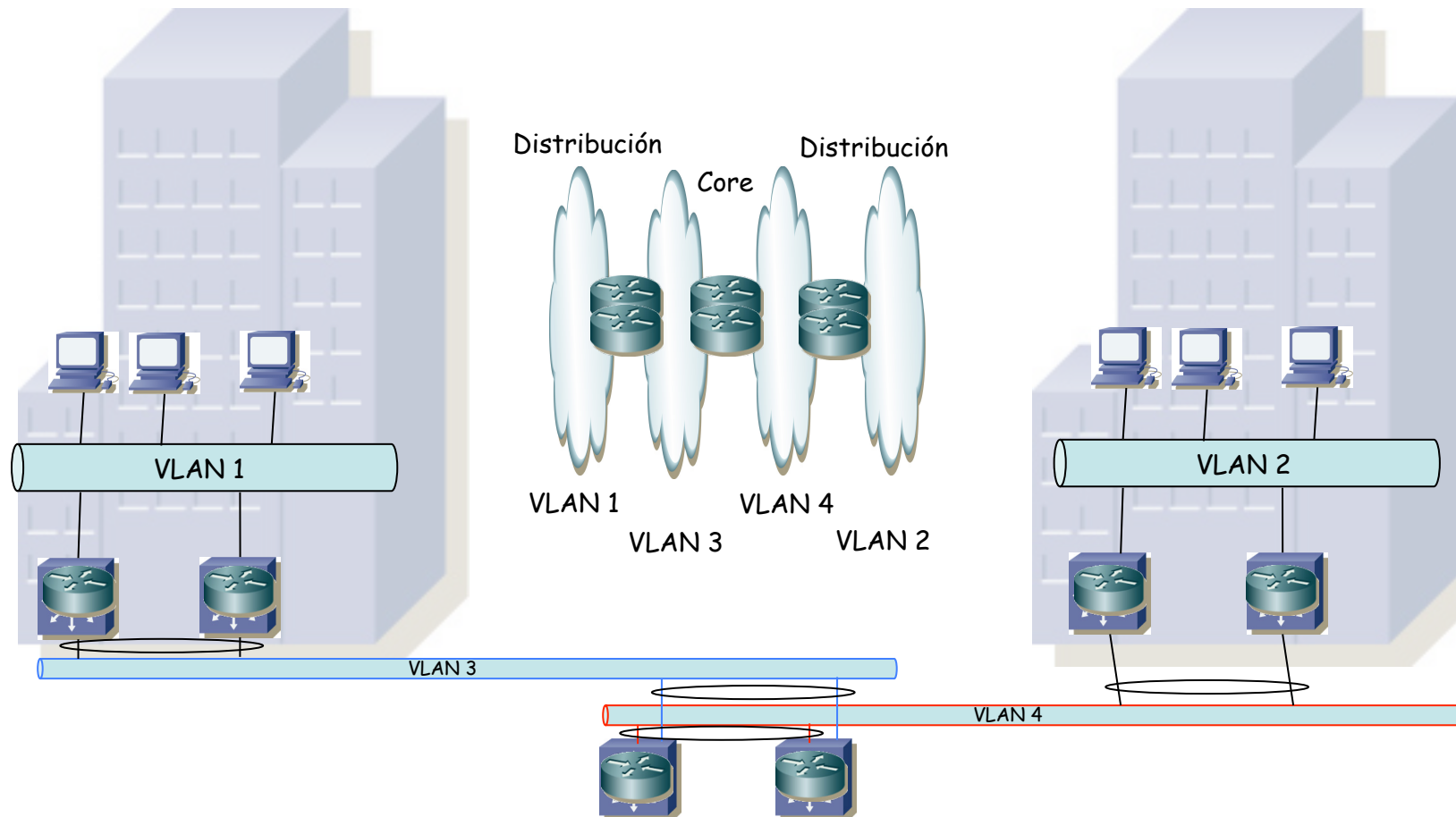
Capa 3 en distribución

- ¿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 (...)



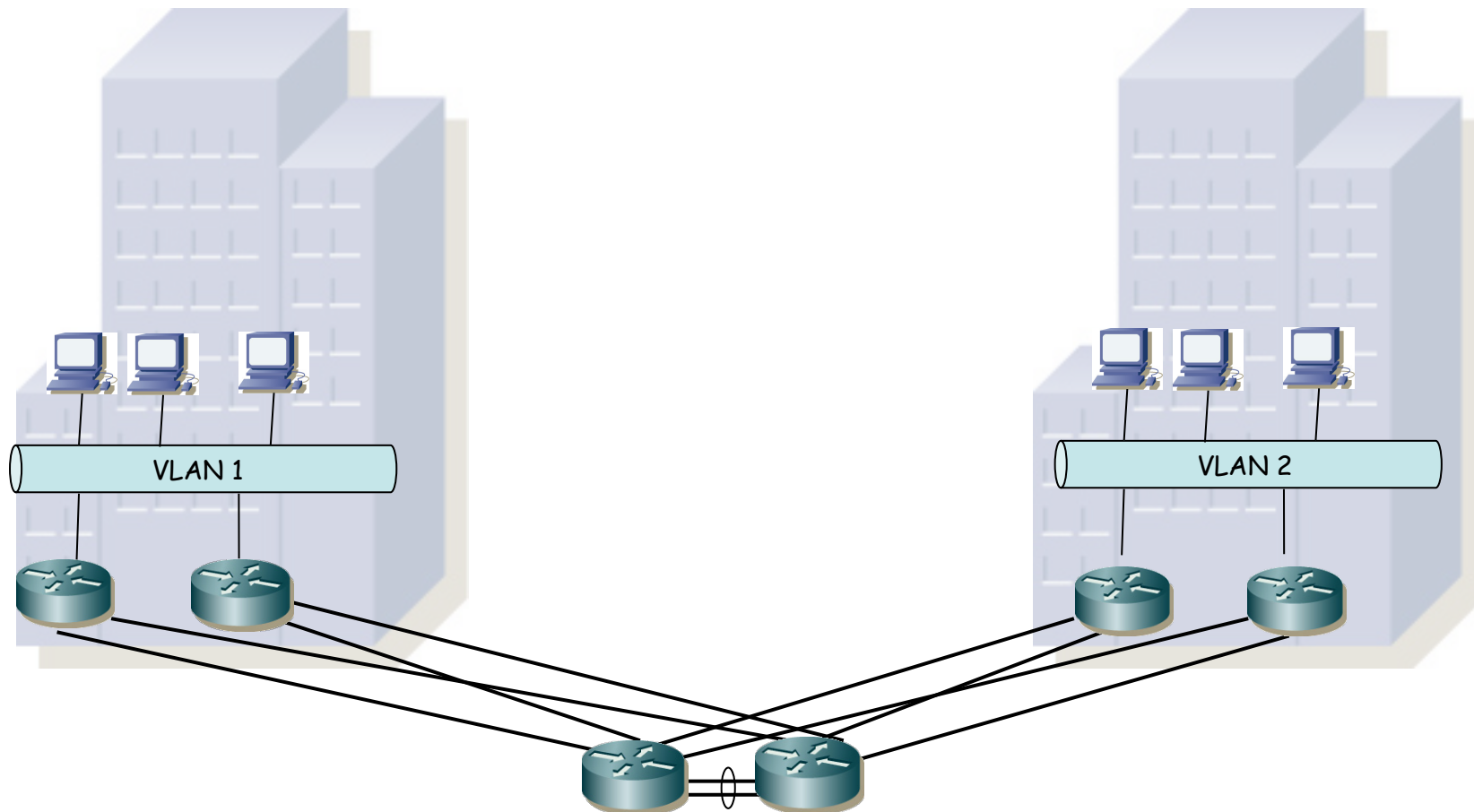
Capa 3 en distribución

- ¿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

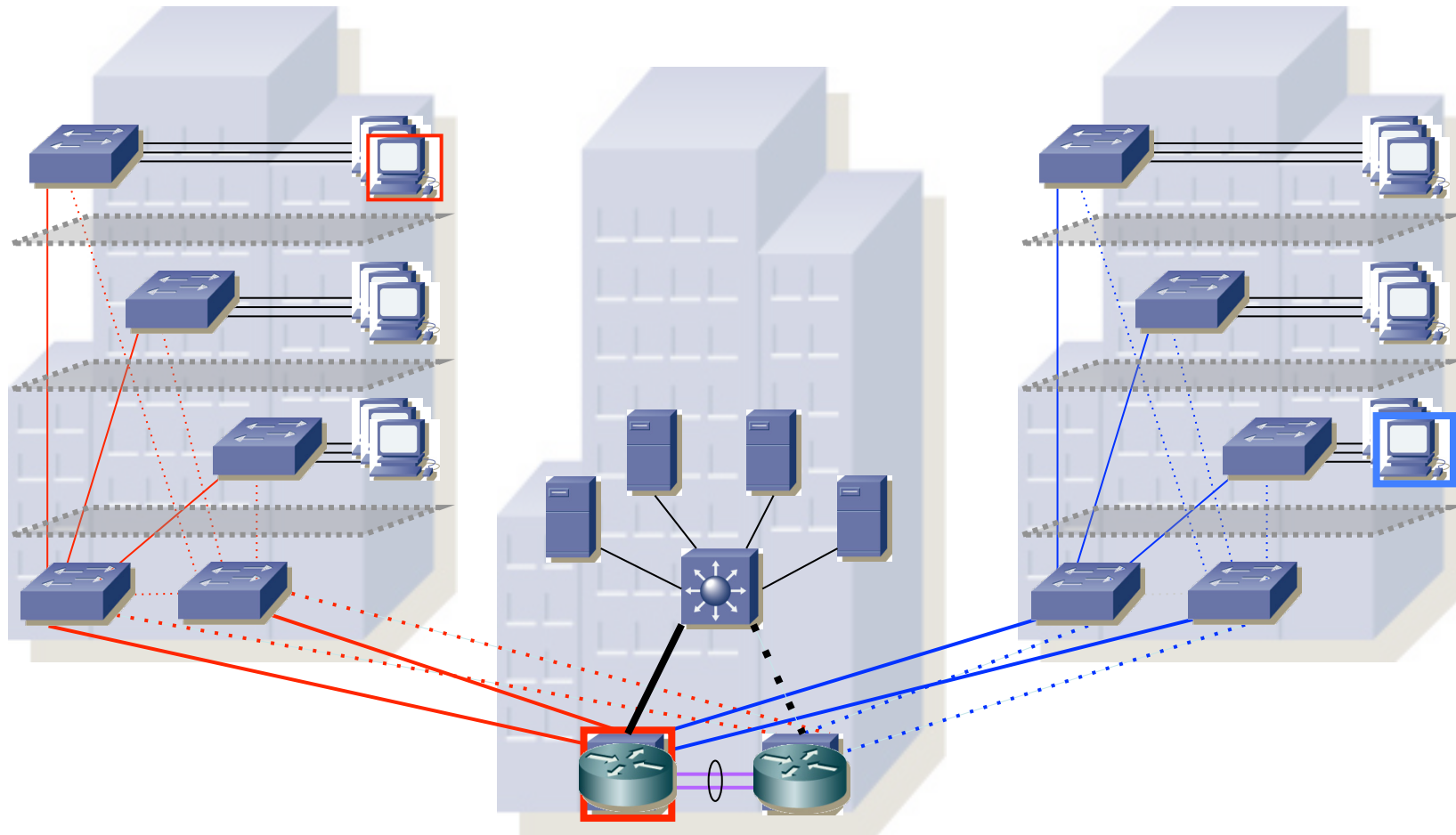
- ¿Y cómo gestionamos la interconexión con el core?
- De nuevo podemos hacerlo en capa 2 (STP), por ejemplo con un FHRP
- O en capa 3, también con un FHRP
- O todo en capa 3 y emplear un protocolo de encaminamiento



Servidores y exterior

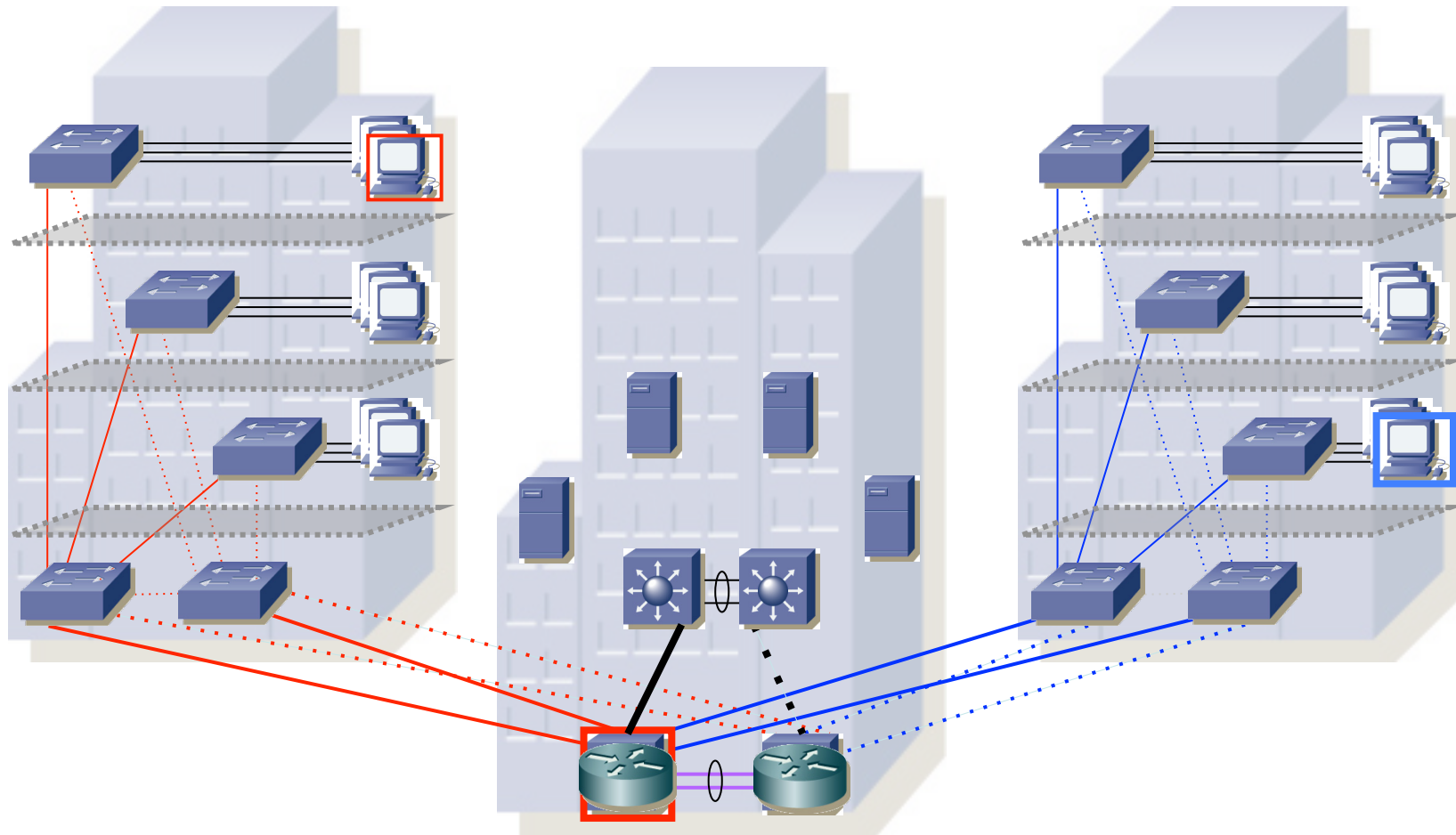
Centralización de servidores

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



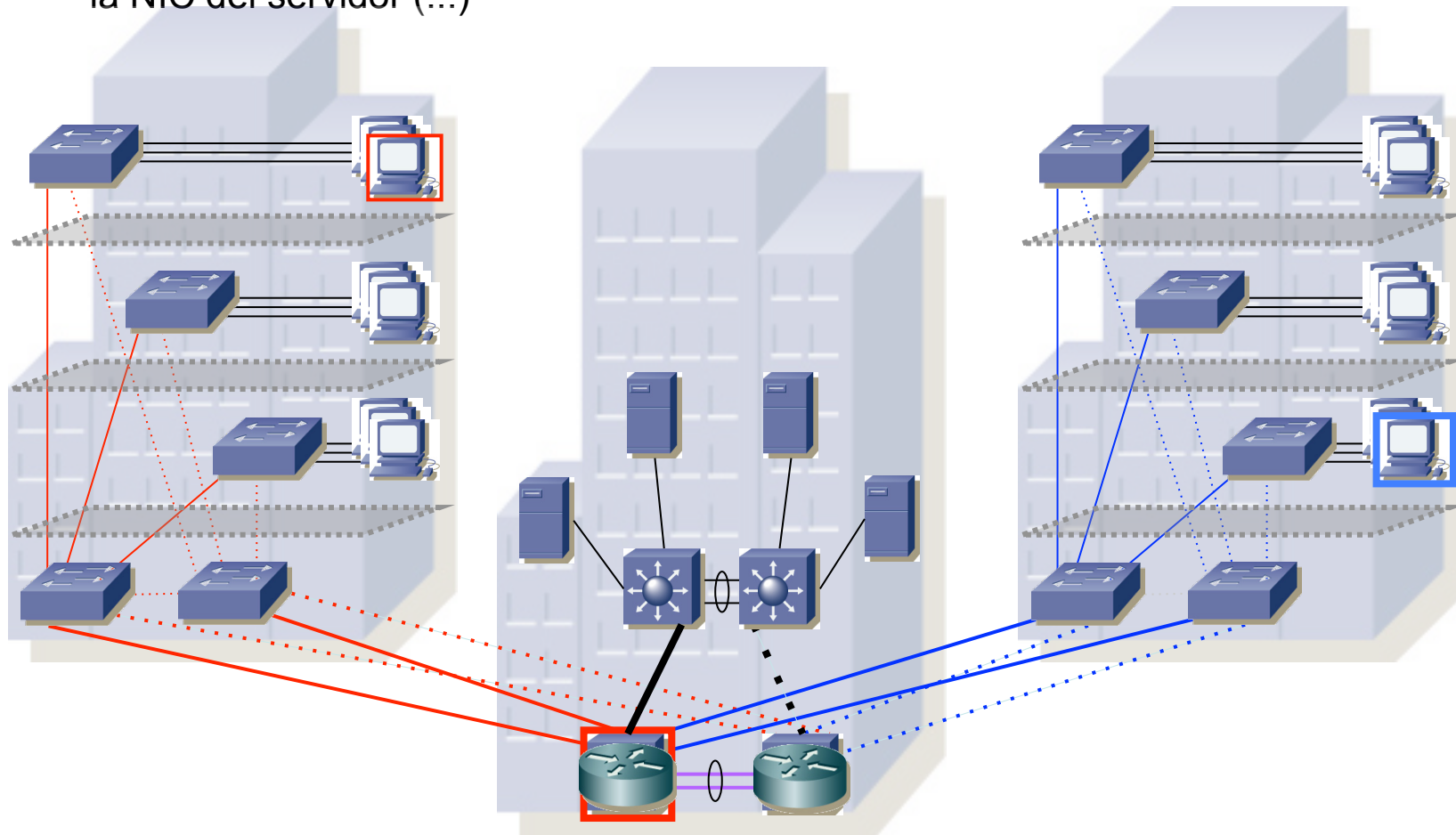
Centralización de servidores

- 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? (...)



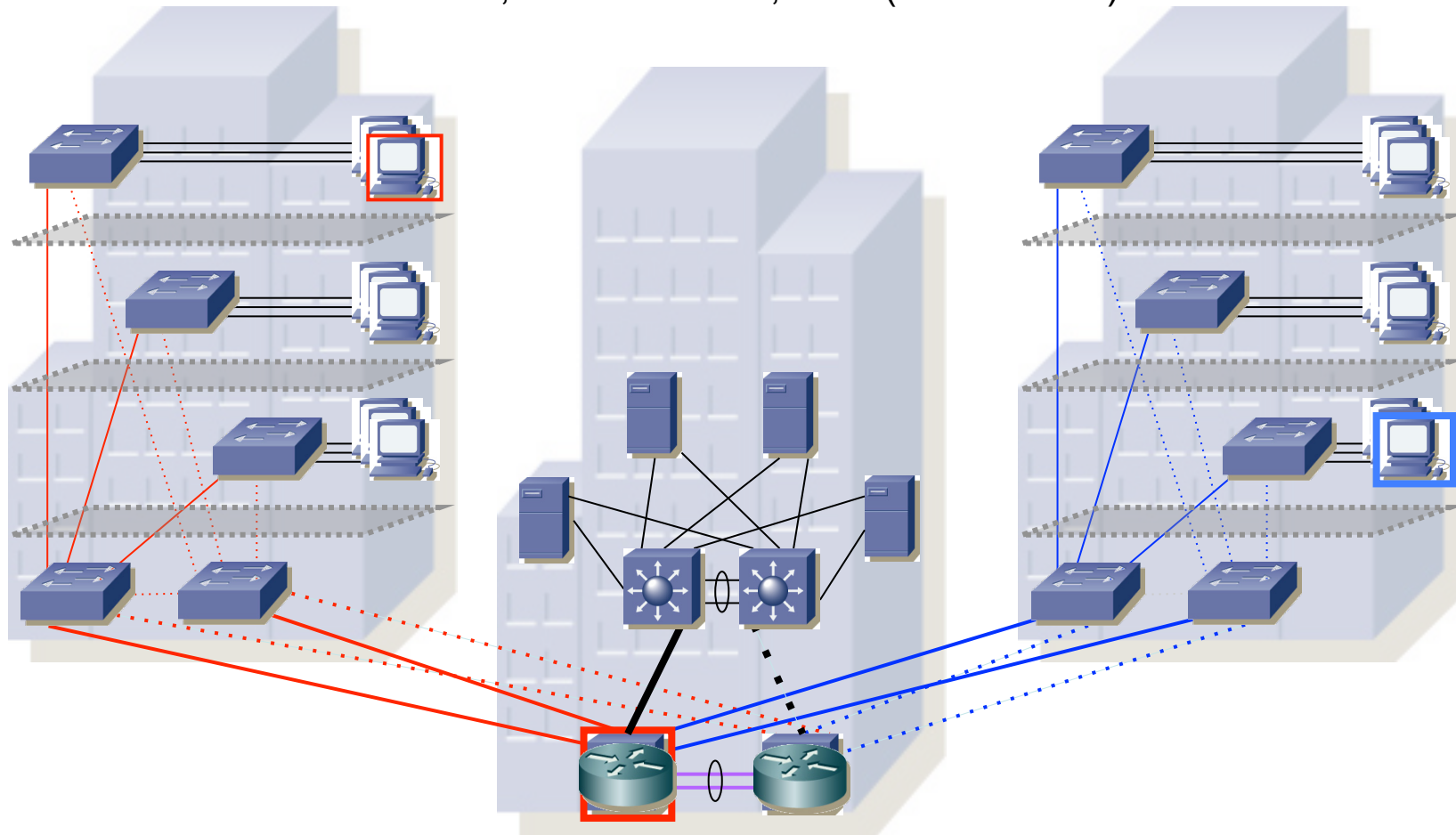
Centralización de servidores

- 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 (...)



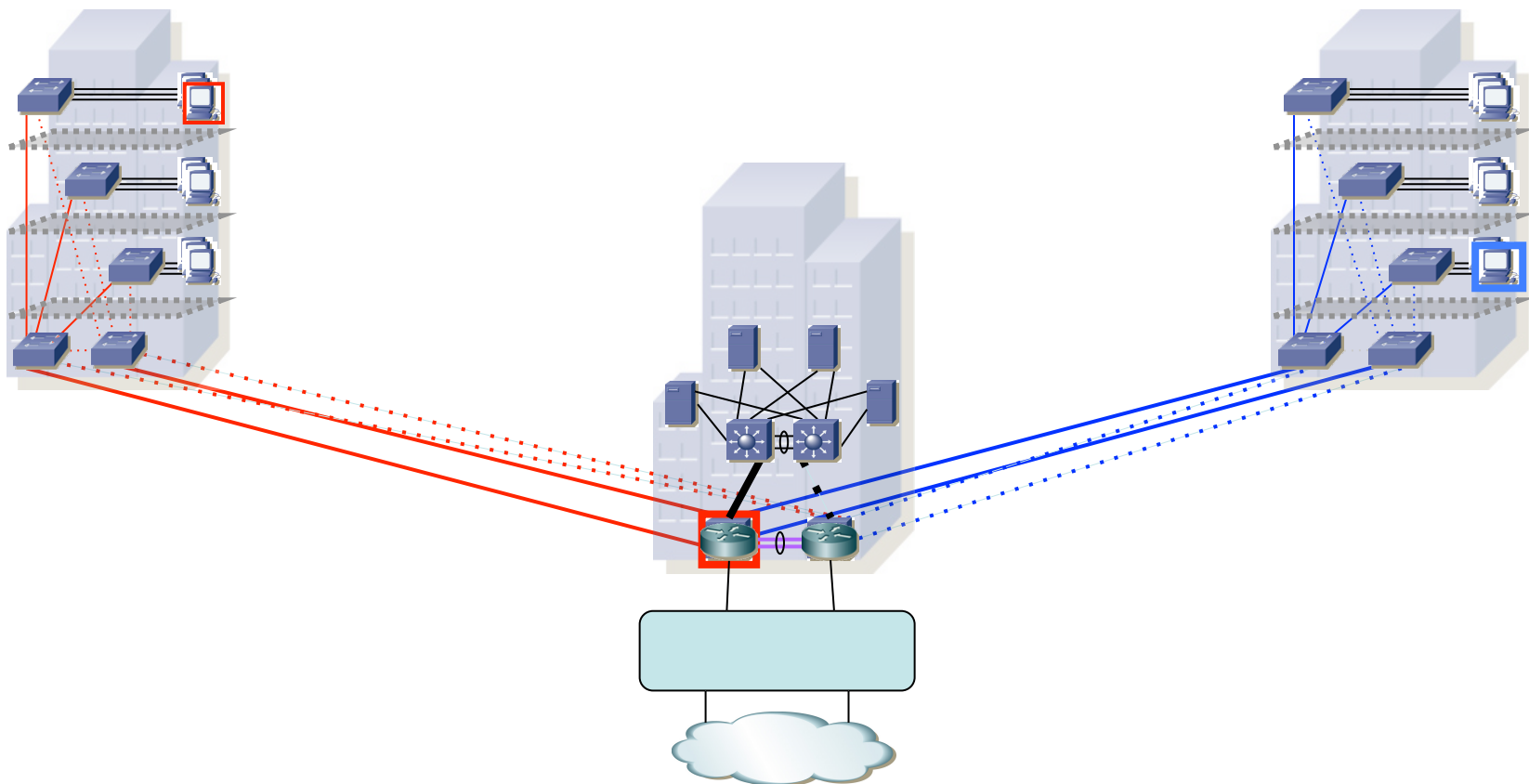
Centralización de servidores

- 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)



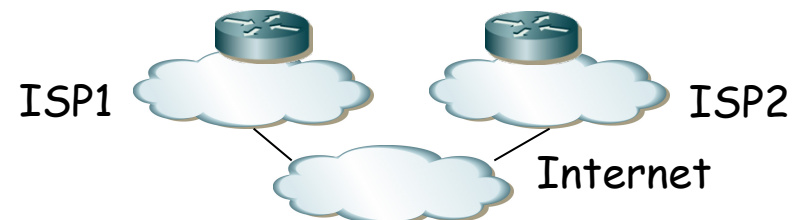
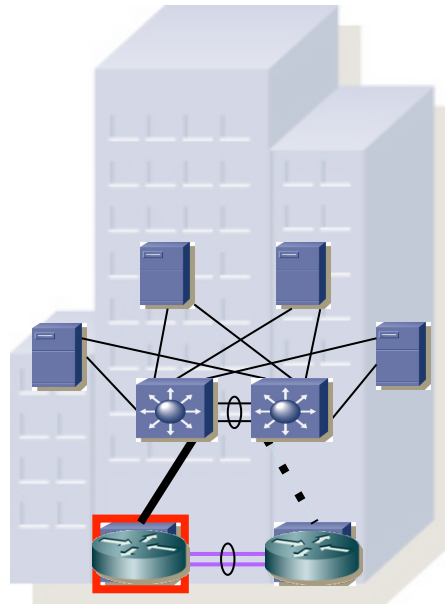
Acceso a WAN

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



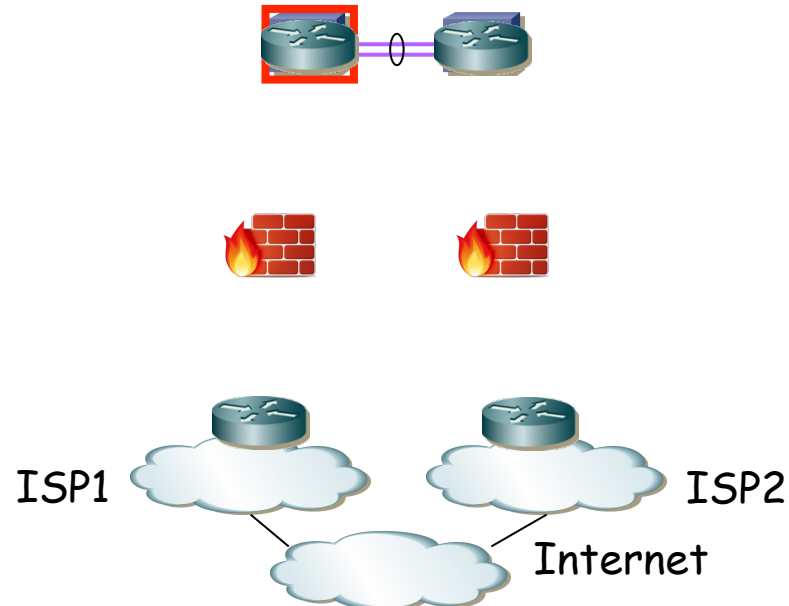
Acceso a WAN

- 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
- (...)



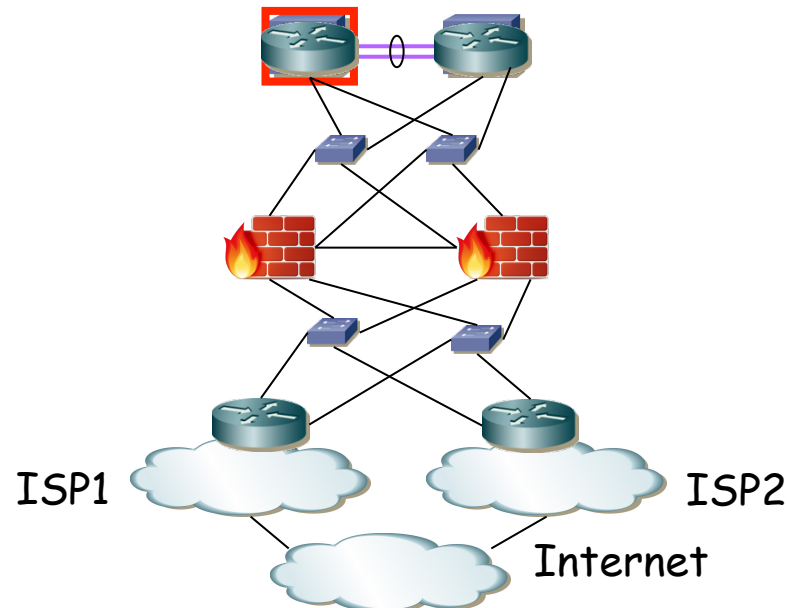
Acceso a WAN

- 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
- (...)



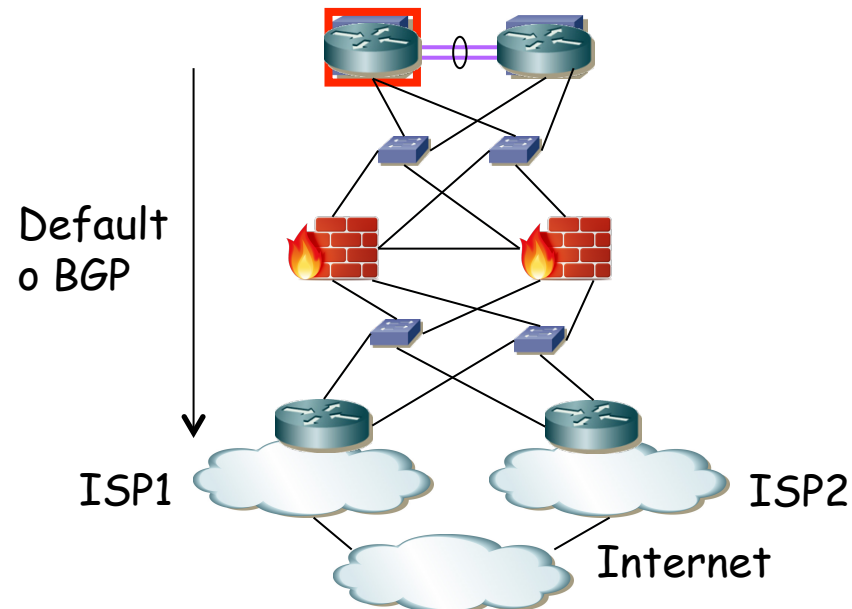
Acceso a WAN

- 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

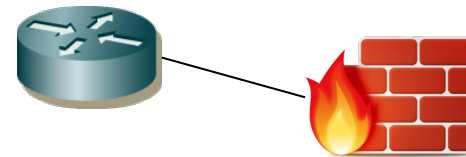
- Hacia el exterior es frecuente trabajar con una ruta por defecto
- Salvo que empecemos a hablar de sedes remotas, VPNs, etc
- Se puede emplear BGP para aprender las rutas a Internet y repartir tráfico entre los dos ISPs



VLANs vs Subredes IP vs STP

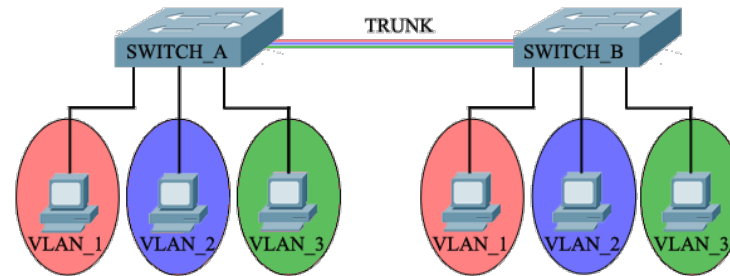
VLANs

- Dependেন 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 procesamiento de broadcasts (aunque esto no es un problema para el hardware moderno)



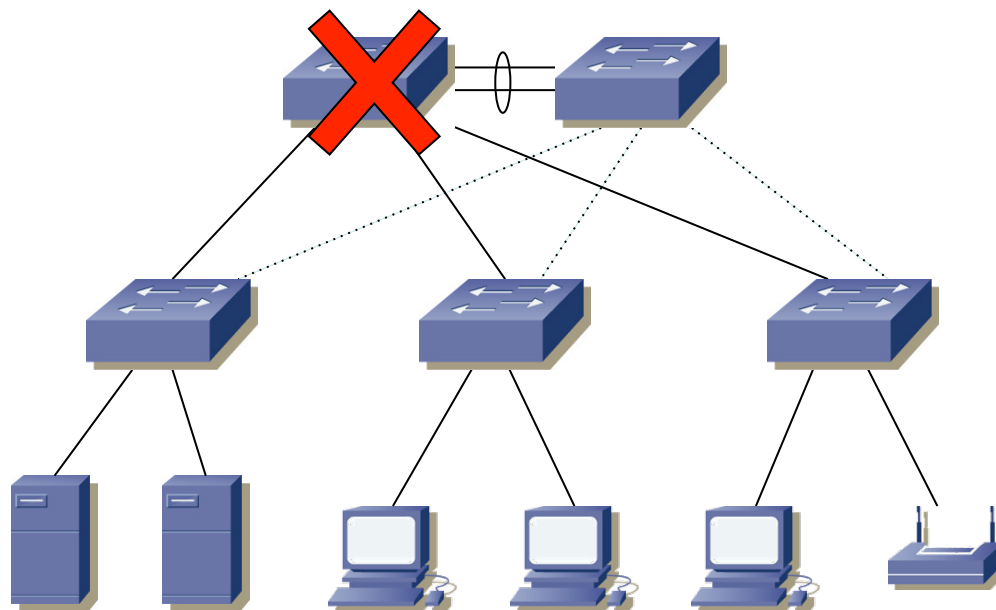
VLANs

- 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 ...



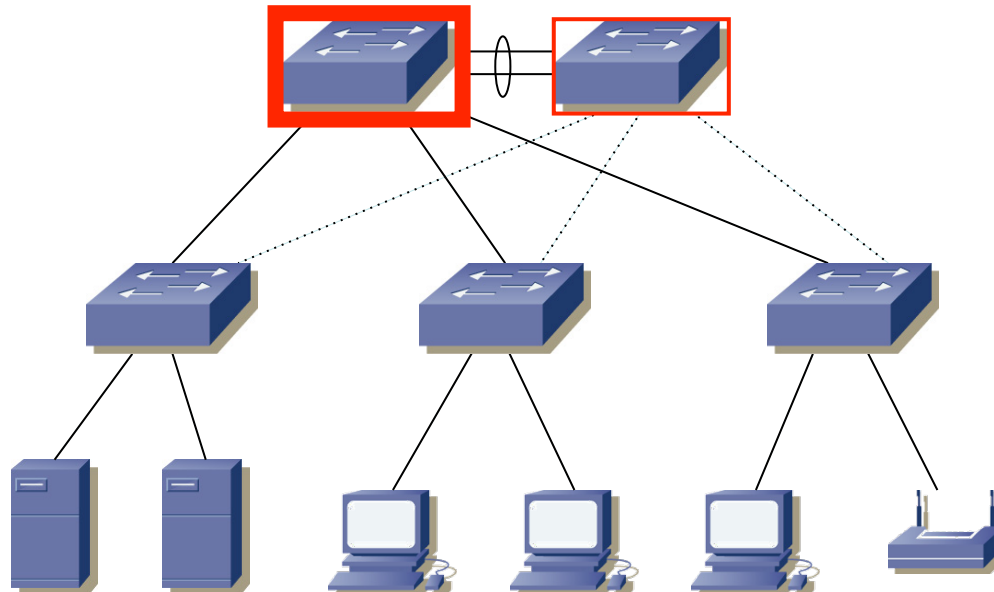
STP

- 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



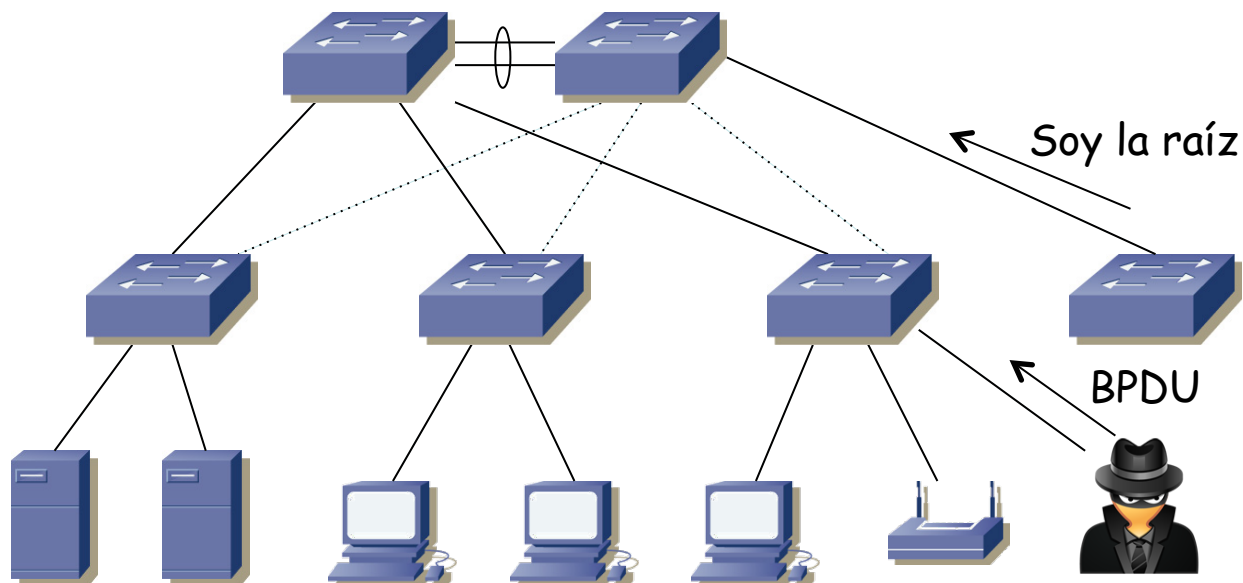
STP

- 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



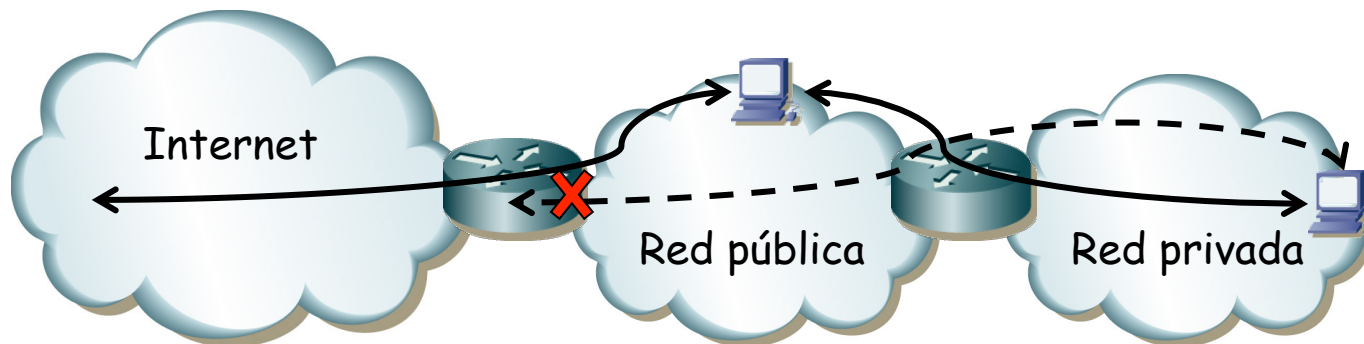
STP

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



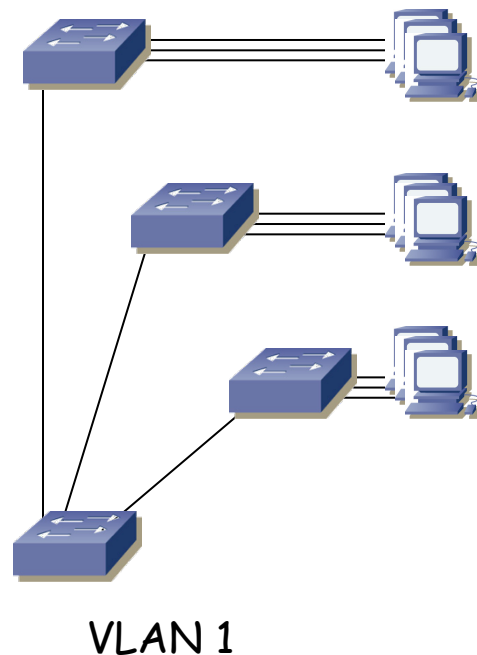
Direccionamiento

- 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

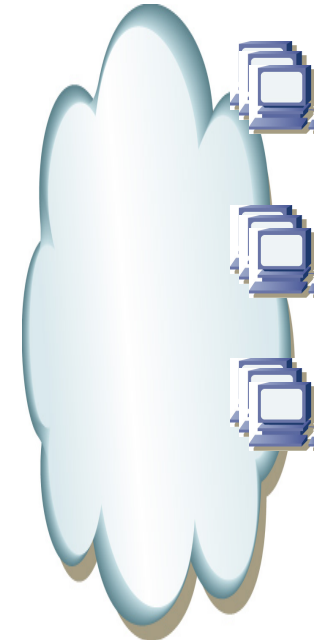


Subredes IP vs VLANs

- 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
- (...)

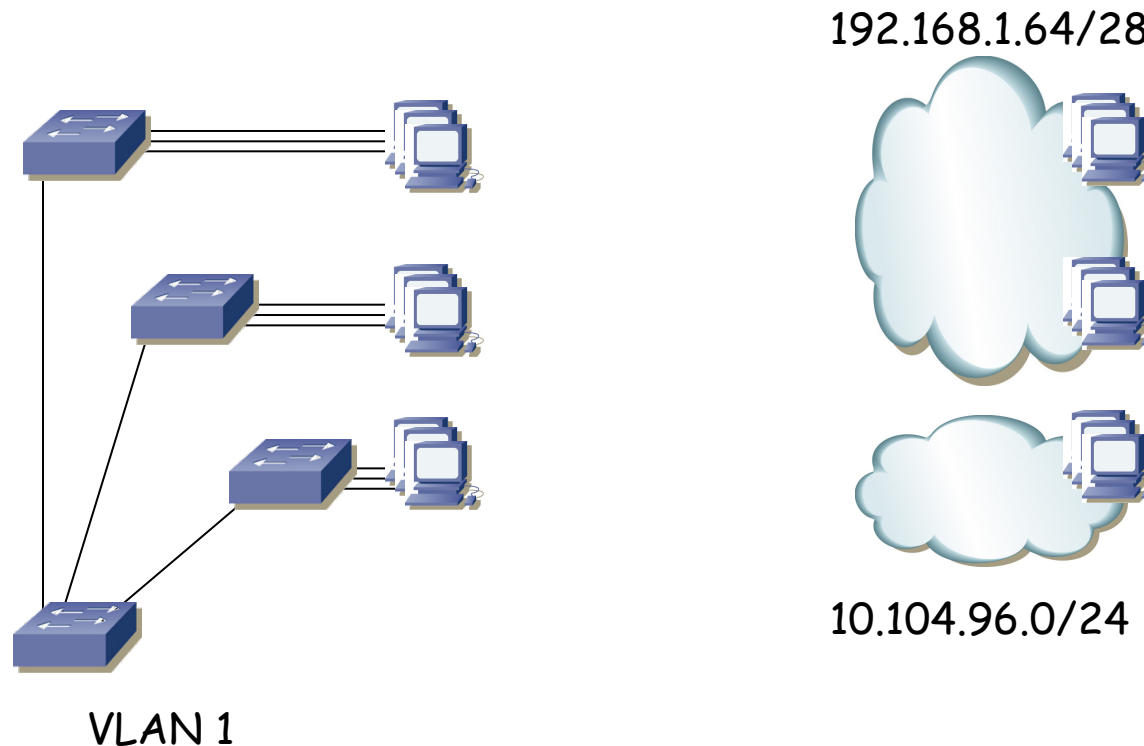


172.17.1.128/26



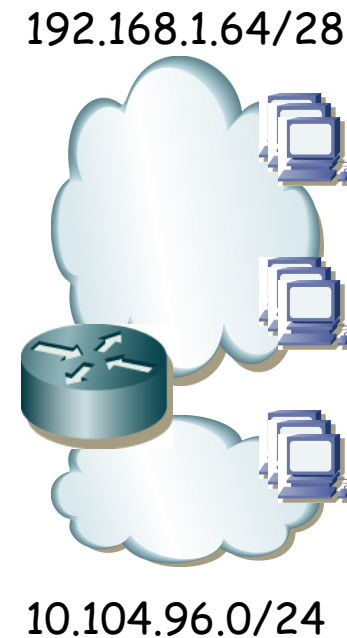
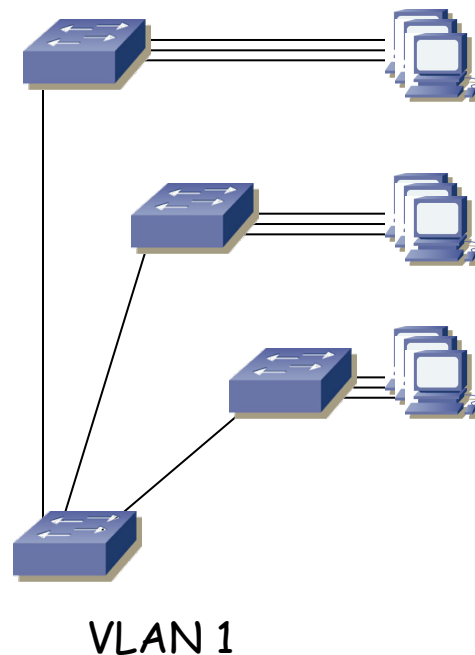
Varias subredes en la LAN

- 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 (...)



Varias subredes en la LAN

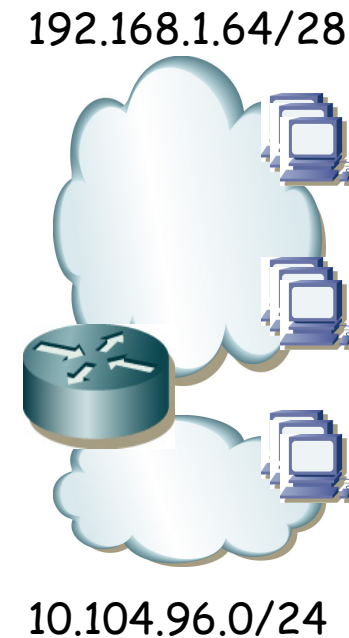
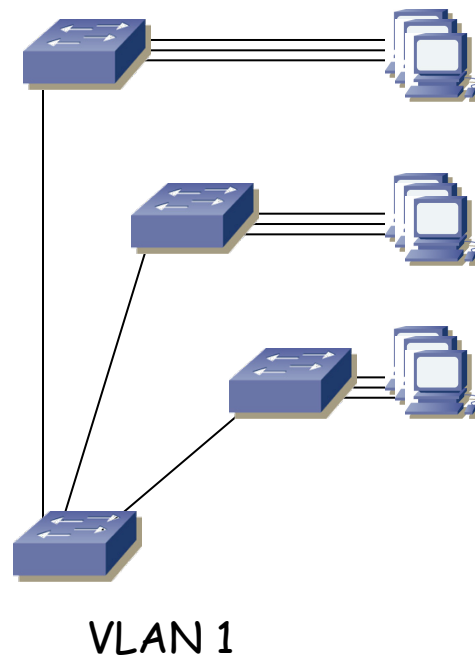
- Pero esto no impide que en una misma LAN/VLAN haya más de una subred IP
- Esas máquinas en realidad tienen conectividad L2 pero no lo saben
- A la hora de comunicarse entre las subredes necesitan un router (...)



Varias subredes en la LAN

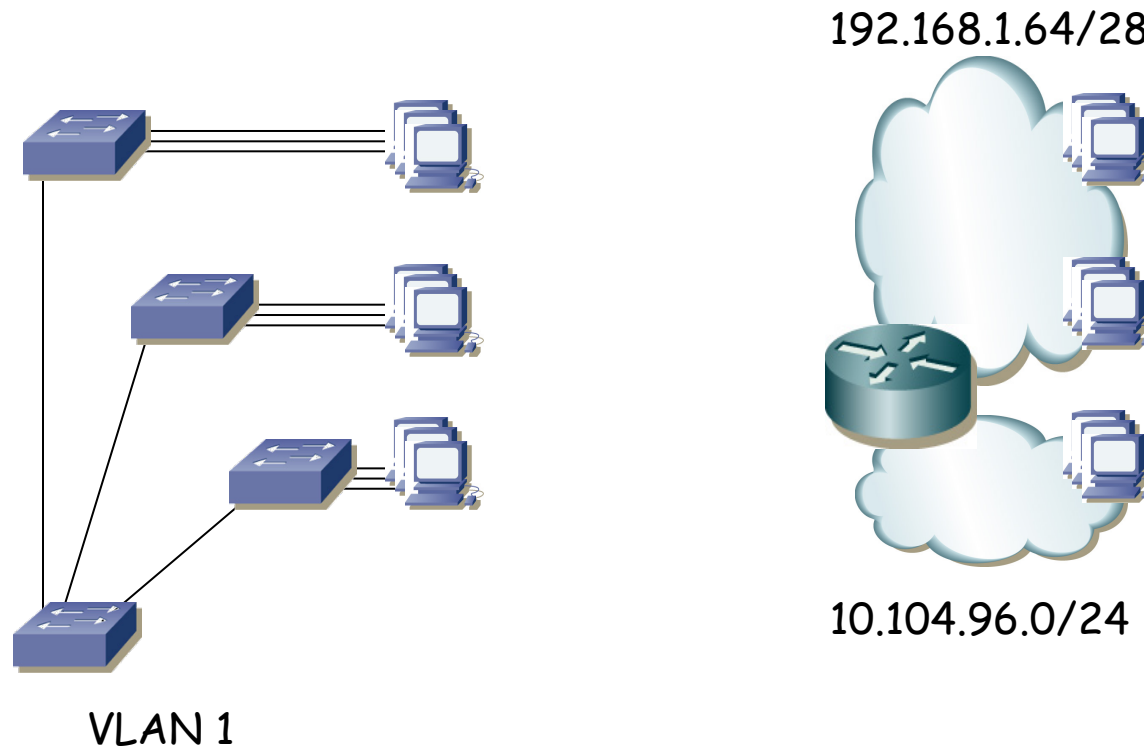
- Ese router tiene los dos interfaces en la misma LAN/VLAN pero en diferente subred IP
- (...)

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



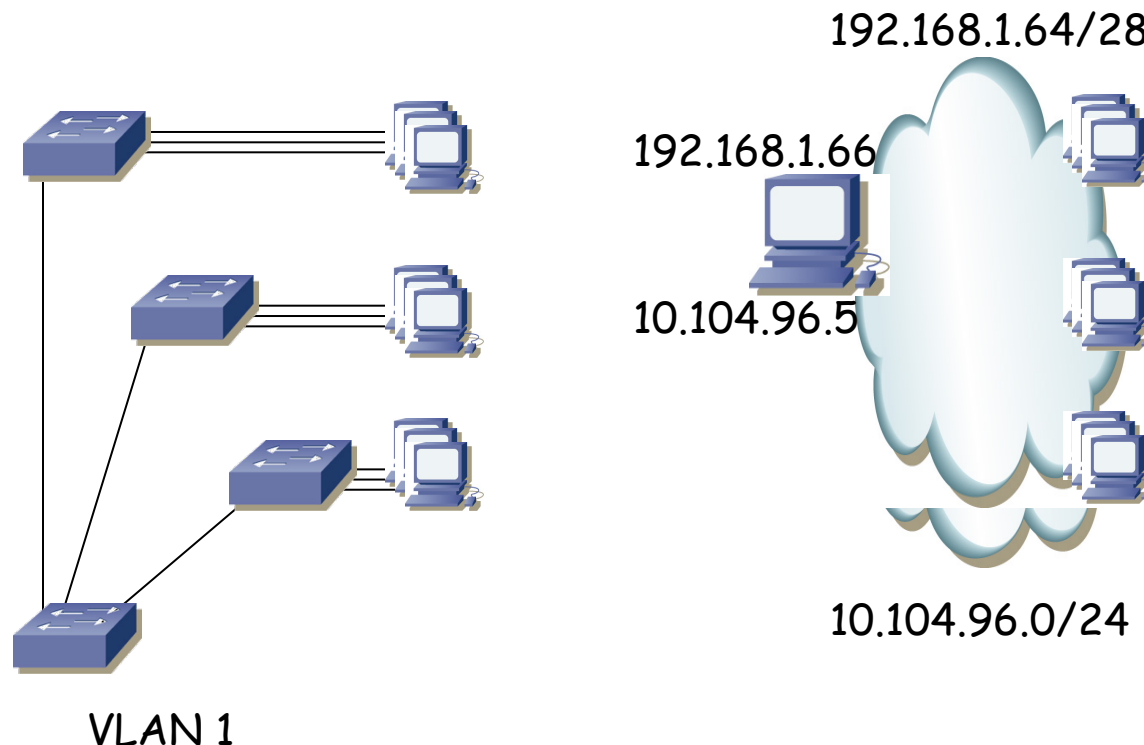
Varias subredes en la LAN

- 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
- (...)



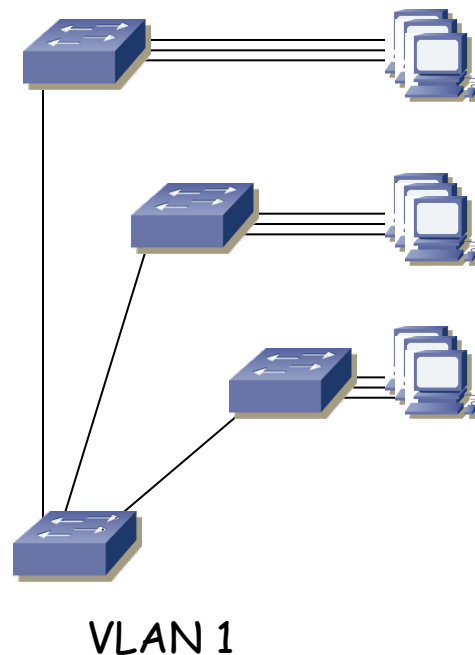
Varias subredes en la LAN

- 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

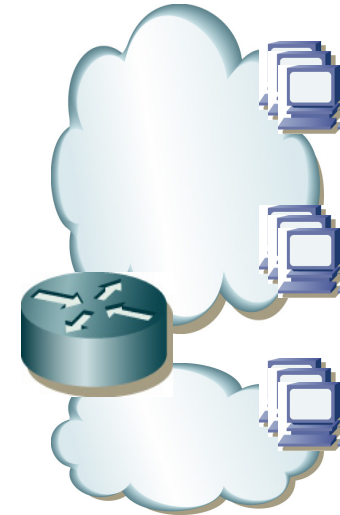


Varias subredes en la LAN

- No es lo habitual pero se puede hacer
- No me atrevería a calificarlo de “mala práctica”
- No es seguro, no aísla 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)



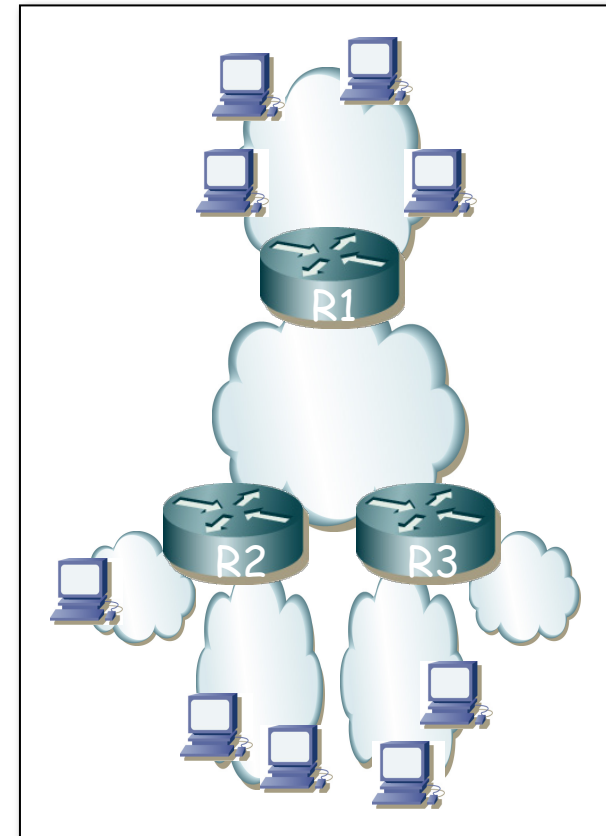
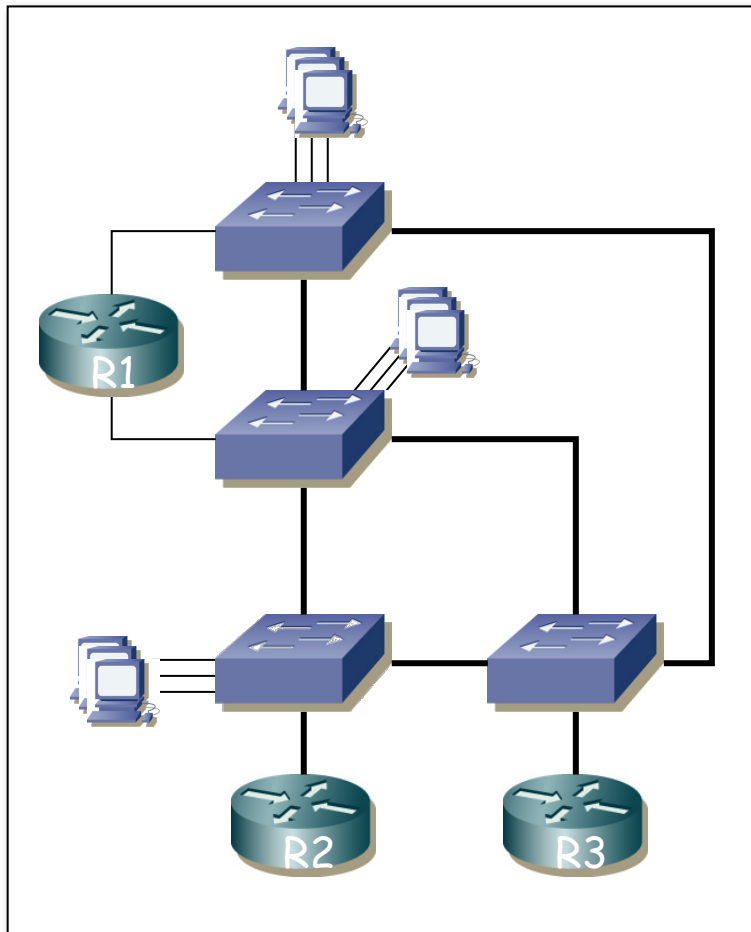
192.168.1.64/28



10.104.96.0/24

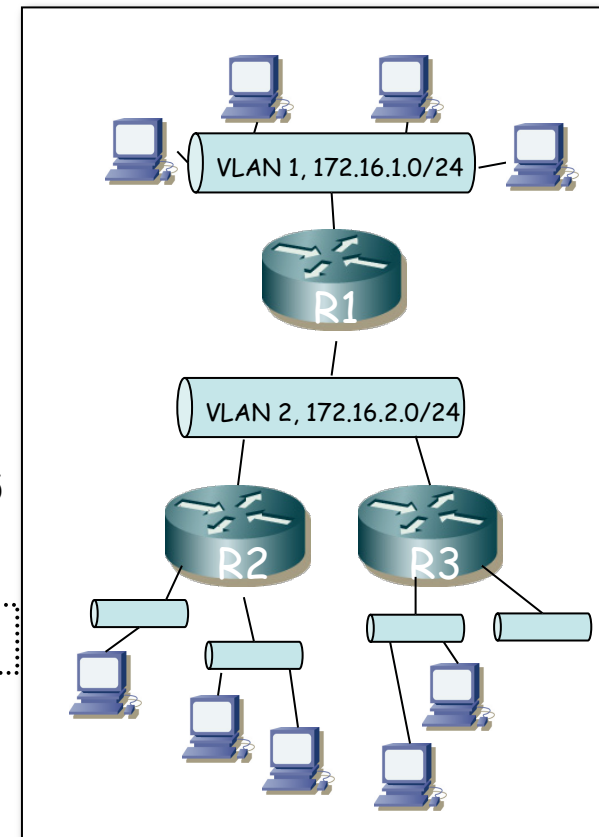
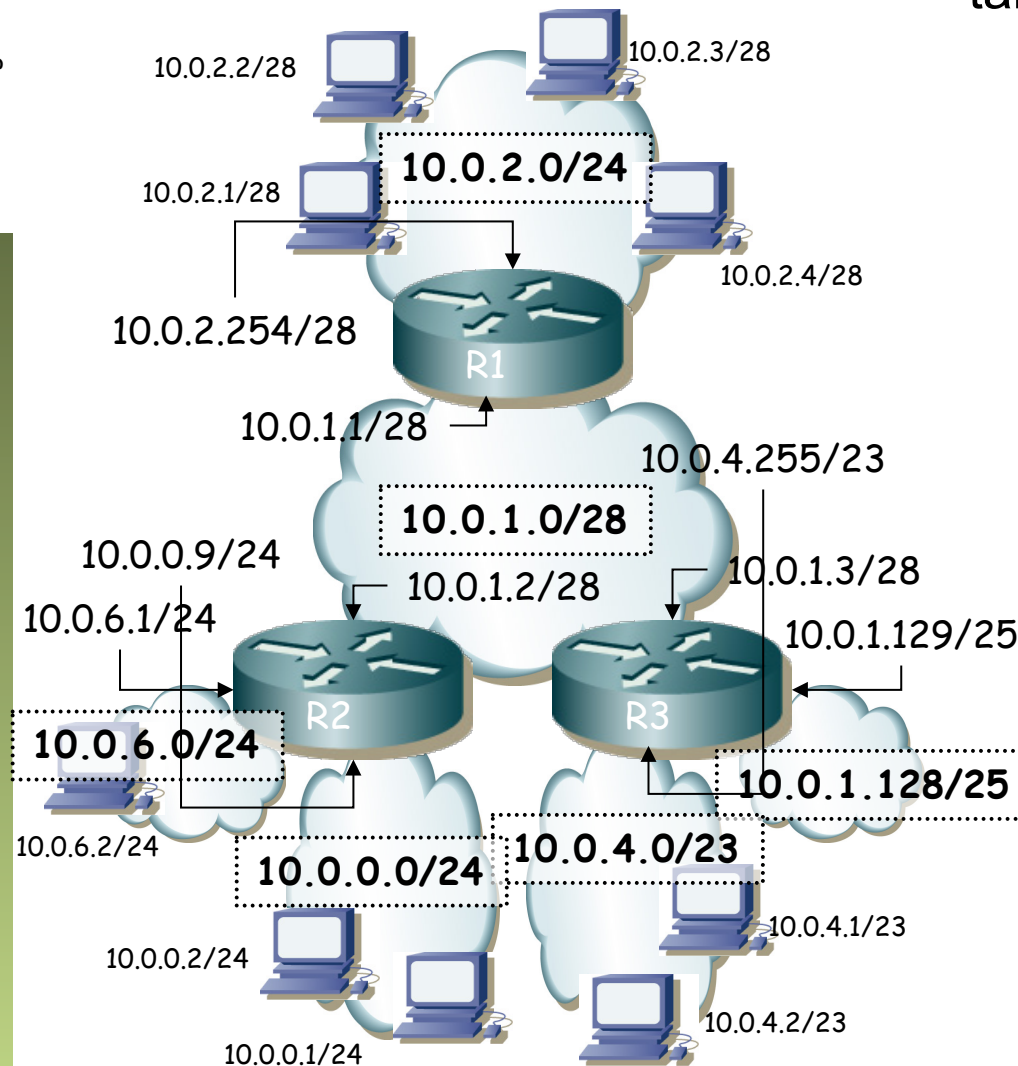
Topologías de nivel 1-2 y 3

- 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

