Diseño de Campus LAN (parte 4)

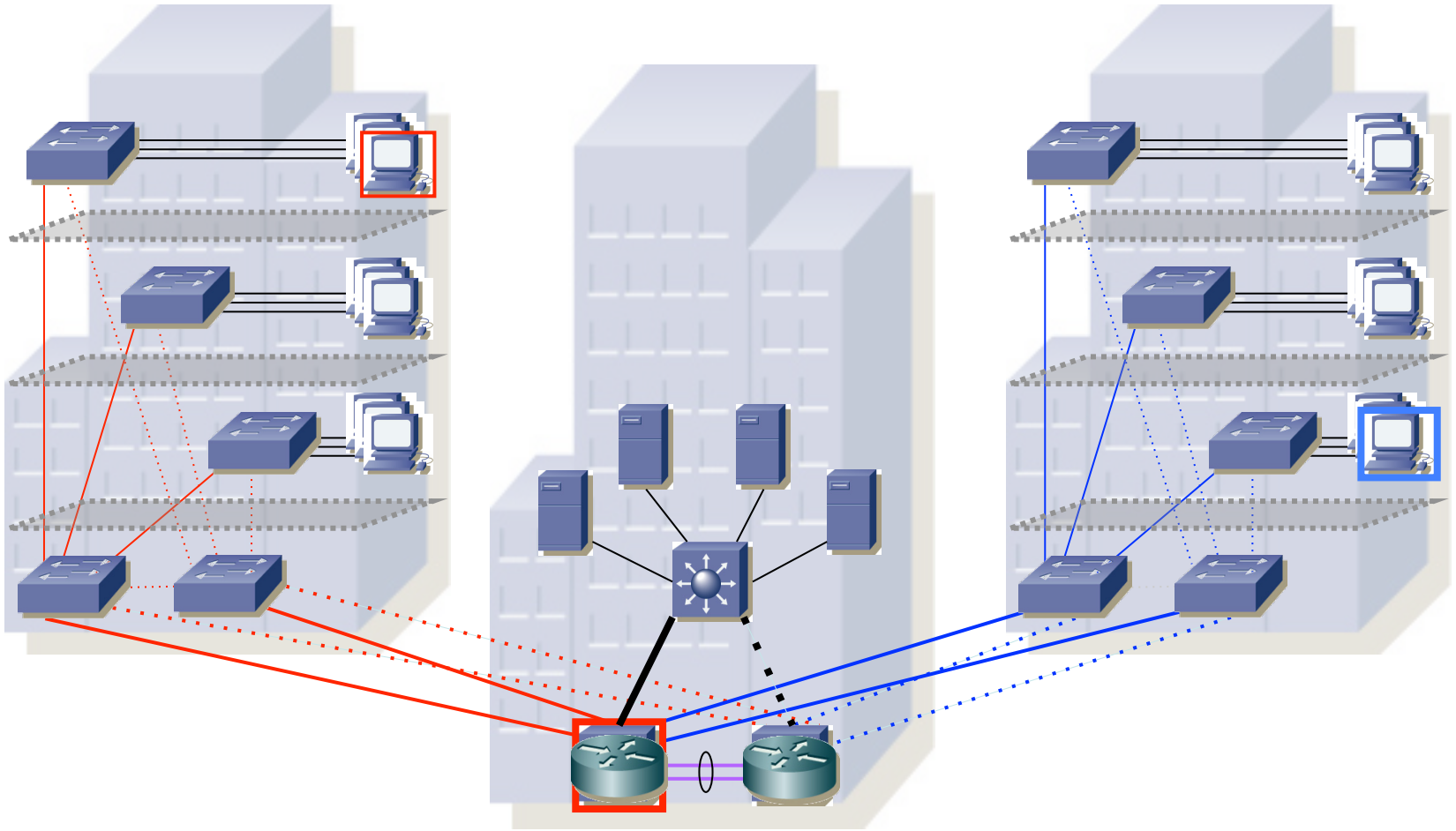
Area de Ingeniería Telemática
http://www.tlm.unavarra.es

Grado en Ingeniería en Tecnologías de Telecomunicación, 3º

Servidores y exterior

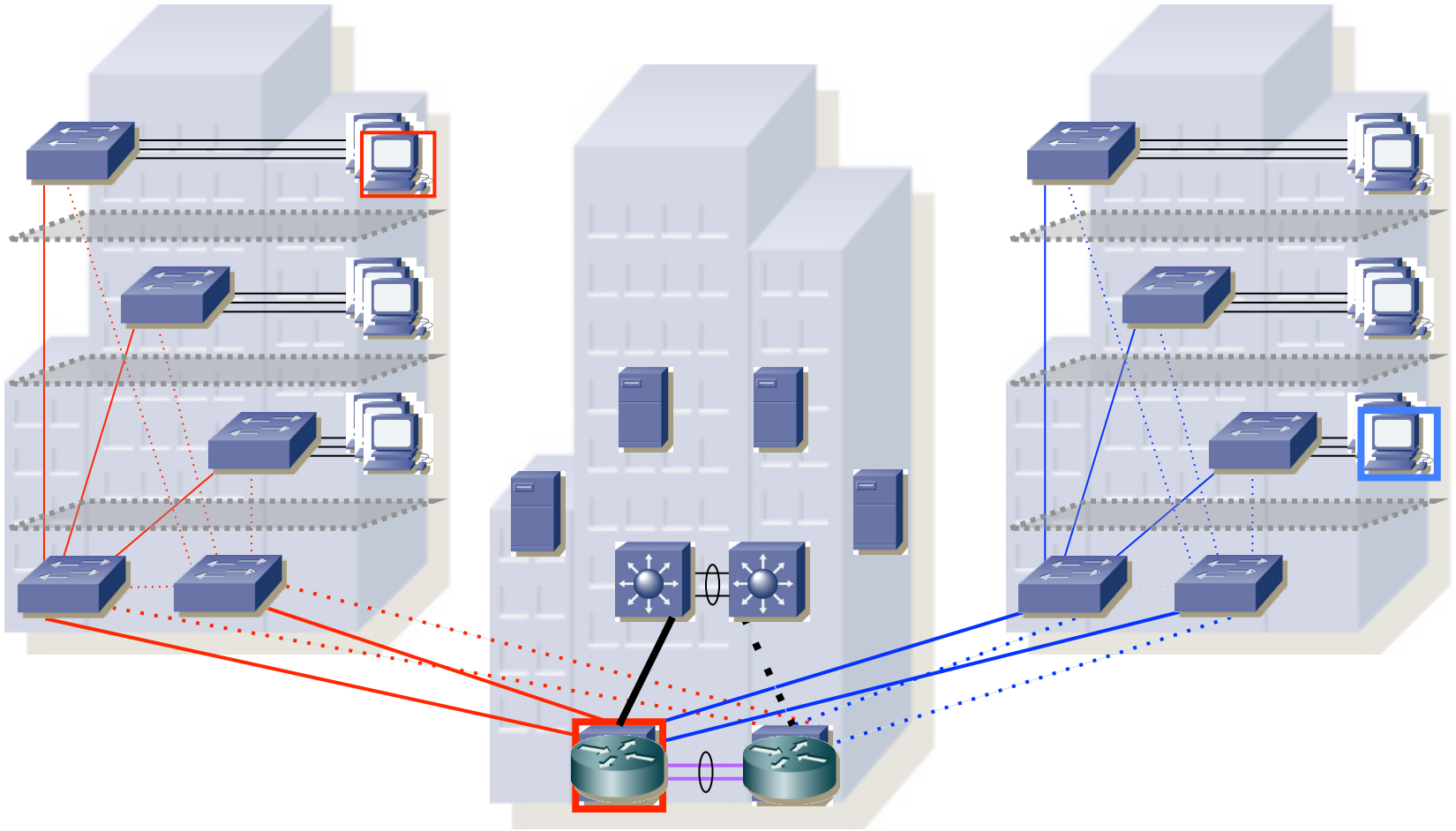
Centralización de servidores

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



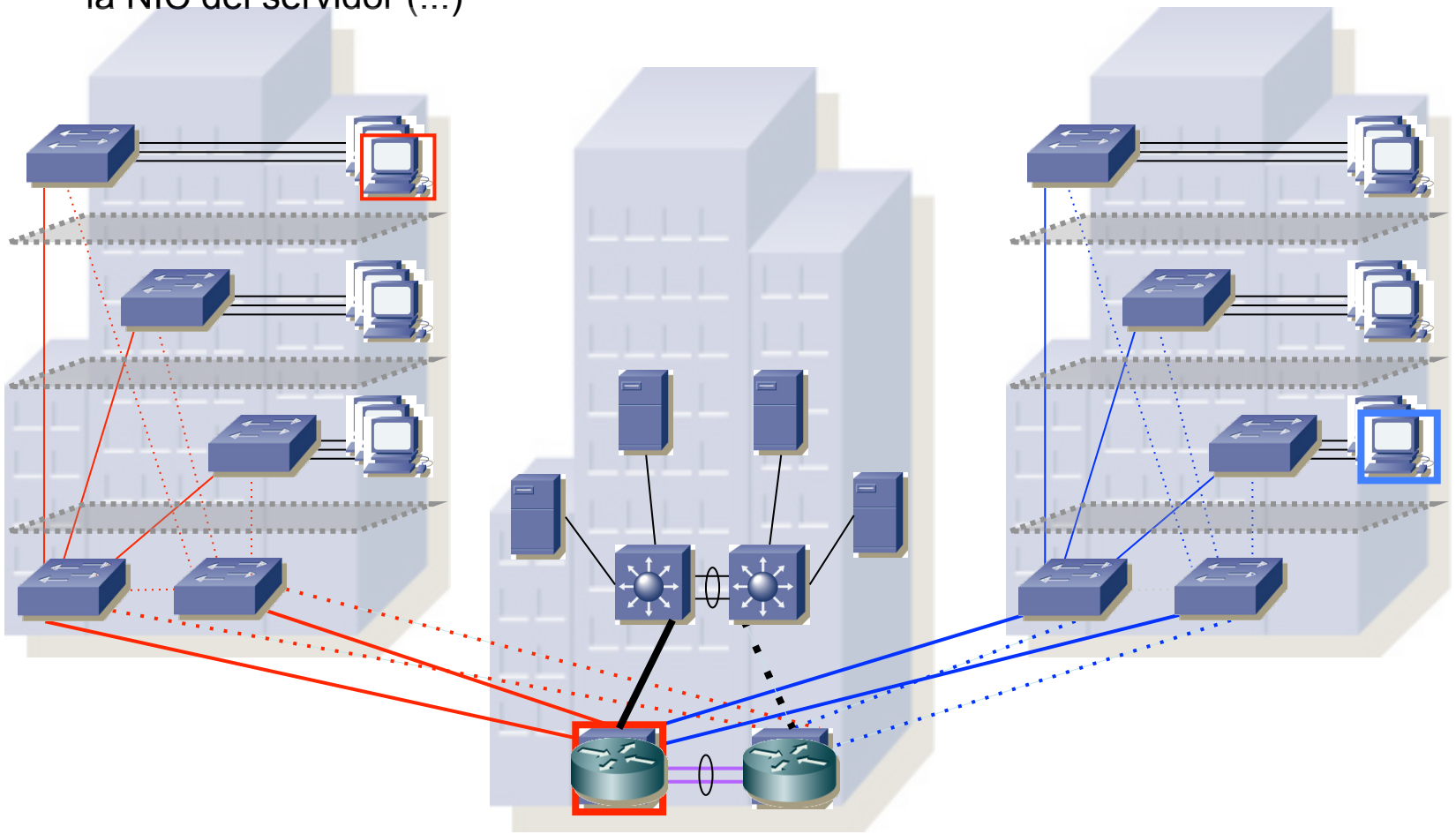
Centralización de servidores

- 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? (...)



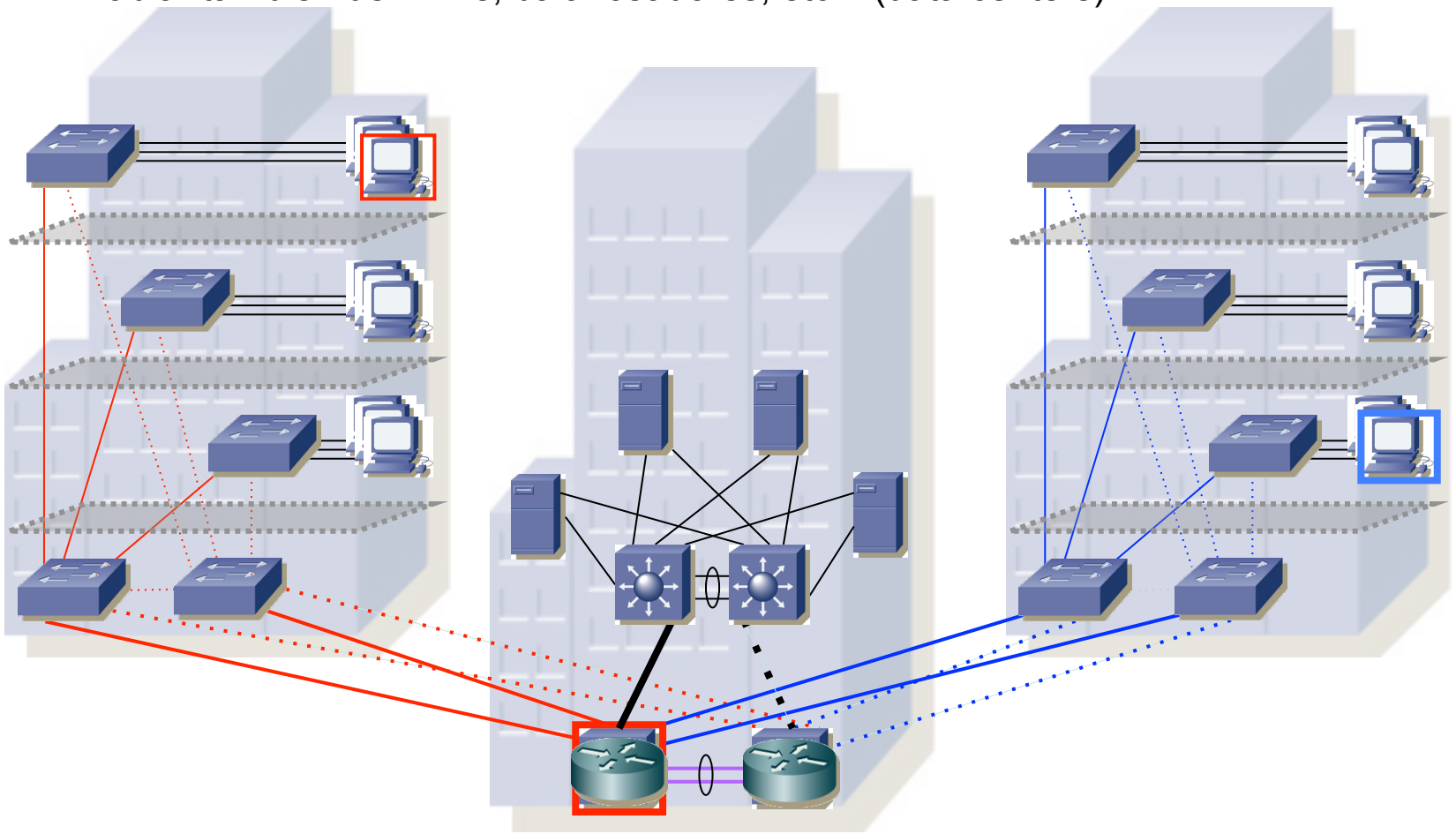
Centralización de servidores

- 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 (...)



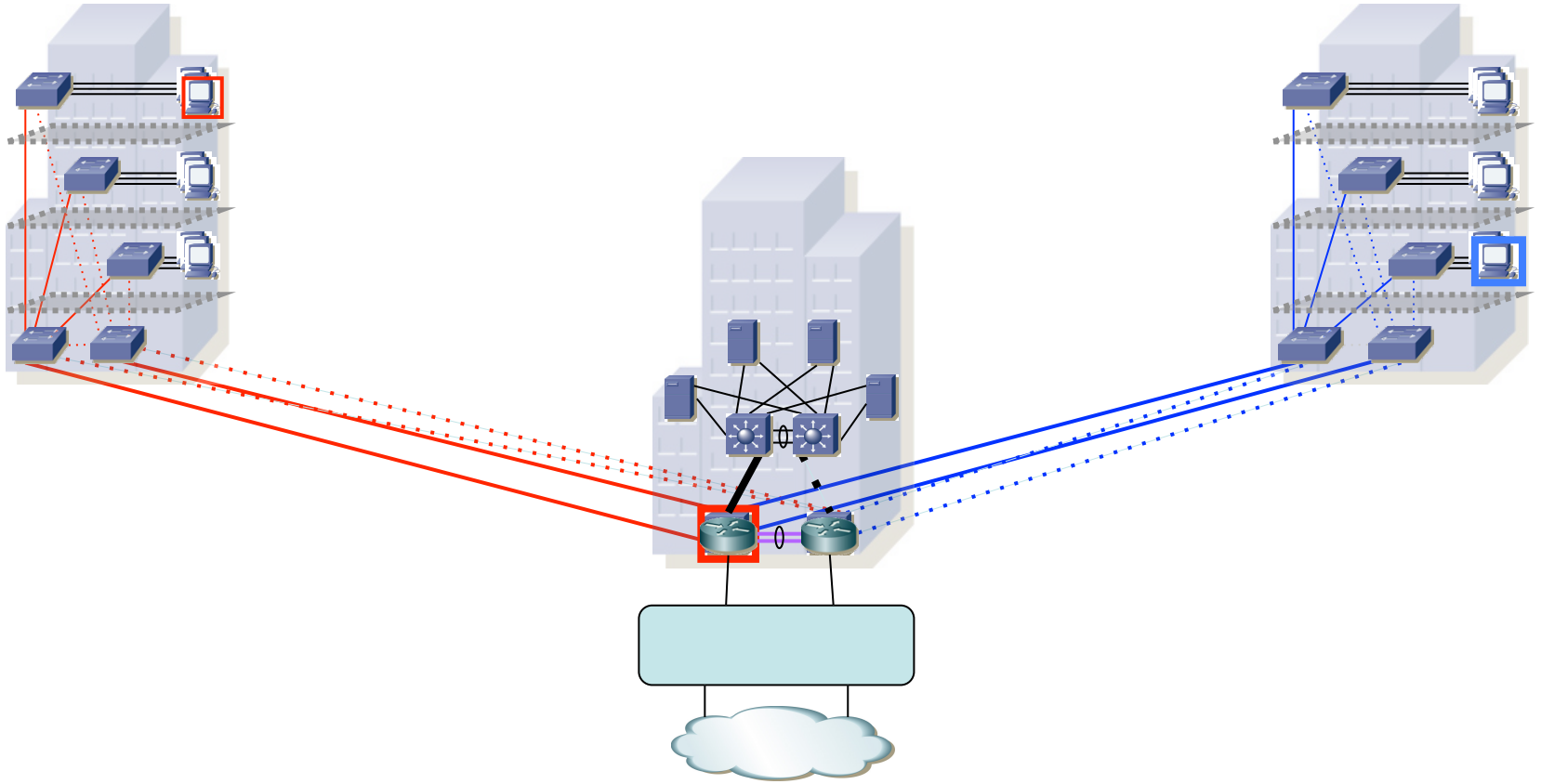
Centralización de servidores

- 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)



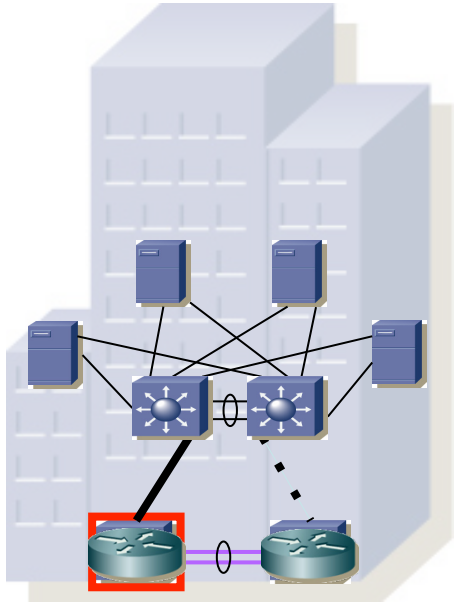
Acceso a WAN

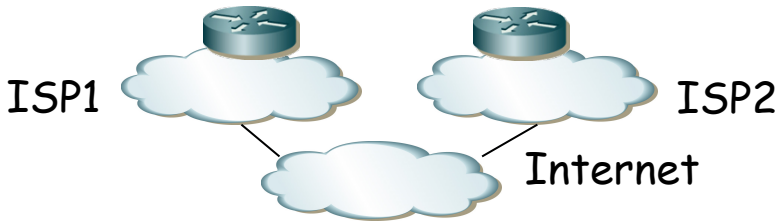
- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- (...)



Acceso a WAN

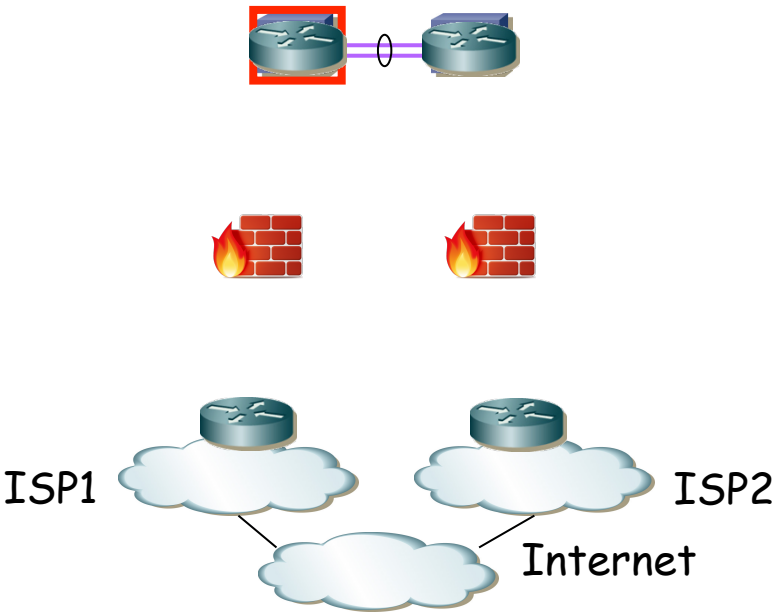
- Falta la conexión con el exterior
- Normalmente desde el core, como otro bloque de distribución
- El acceso a WAN/Internet puede ser por uno o dos ISPs
- (...)





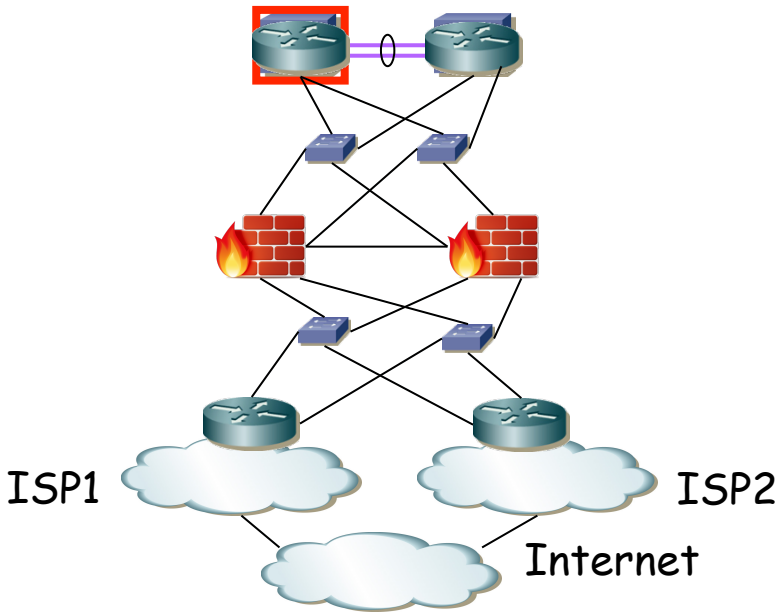
Acceso a WAN

- 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
- (...)



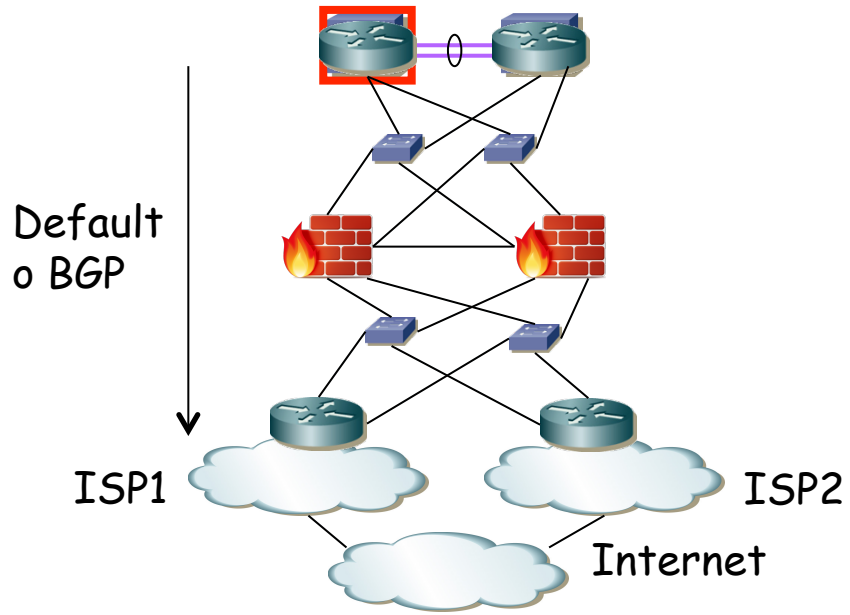
Acceso a WAN

- 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

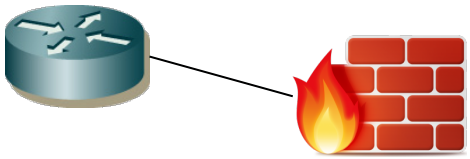
- Hacia el exterior es frecuente trabajar con una ruta por defecto
- Salvo que empecemos a hablar de sedes remotas, VPNs, etc
- Se puede emplear BGP para aprender las rutas a Internet y repartir tráfico entre los dos ISPs



VLANs vs Subredes IP vs STP

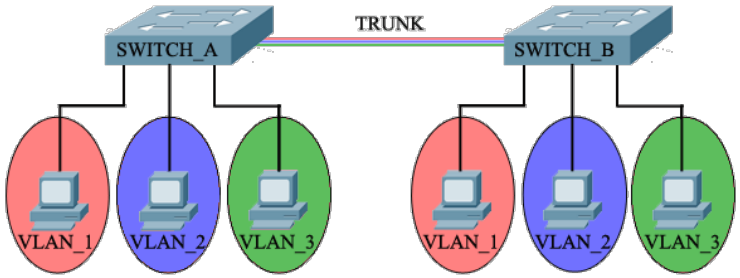
VLANs

- 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

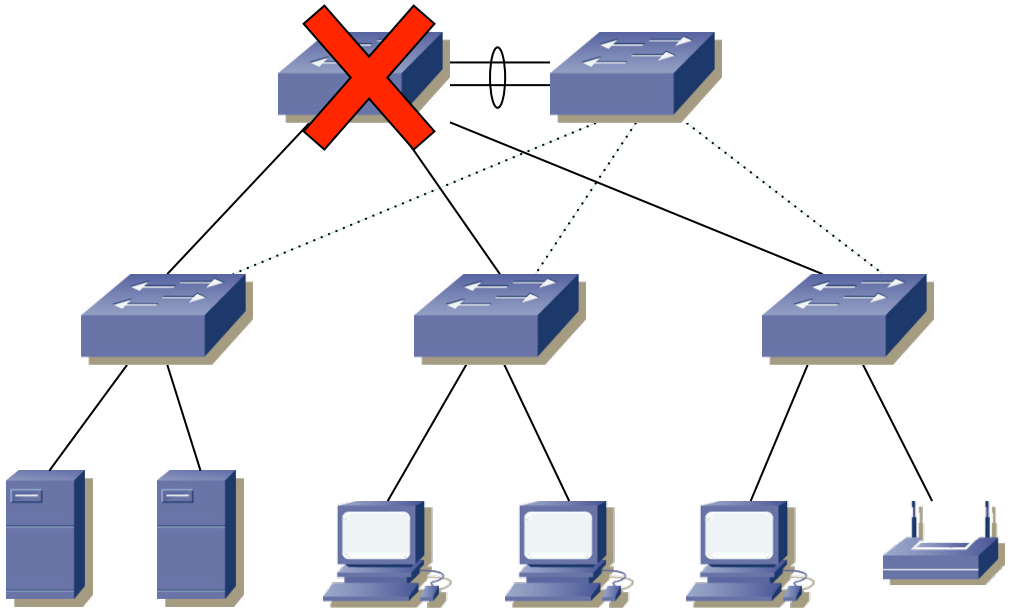
- Típicas:
  - Usuarios
  - Servidores, impresoras
  - VoIP
  - WiFi
  - WiFi pública
  - Gestión
  - VLAN por puertos desconectados



- 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 …

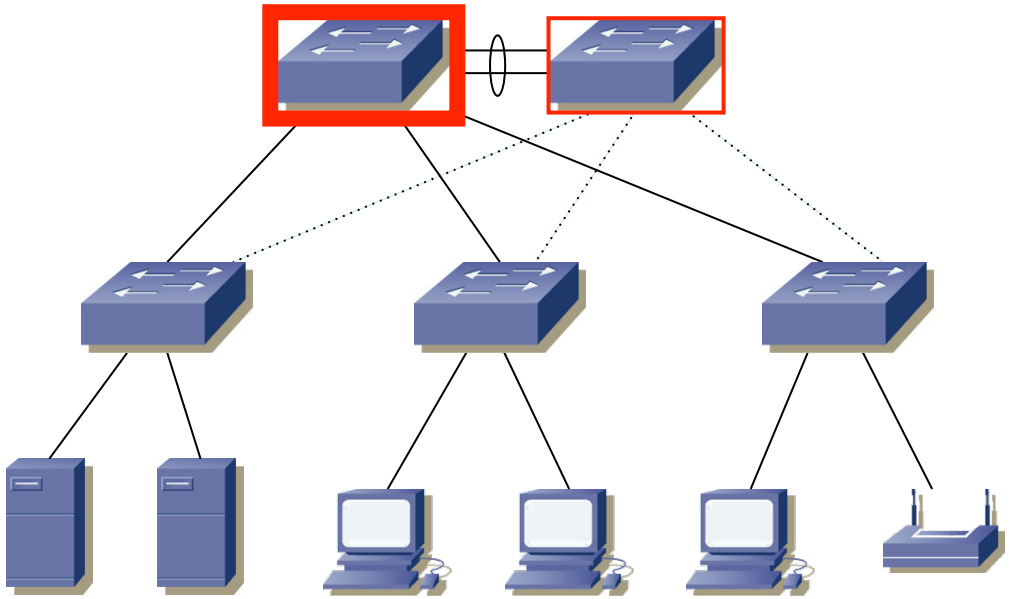
STP

- 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



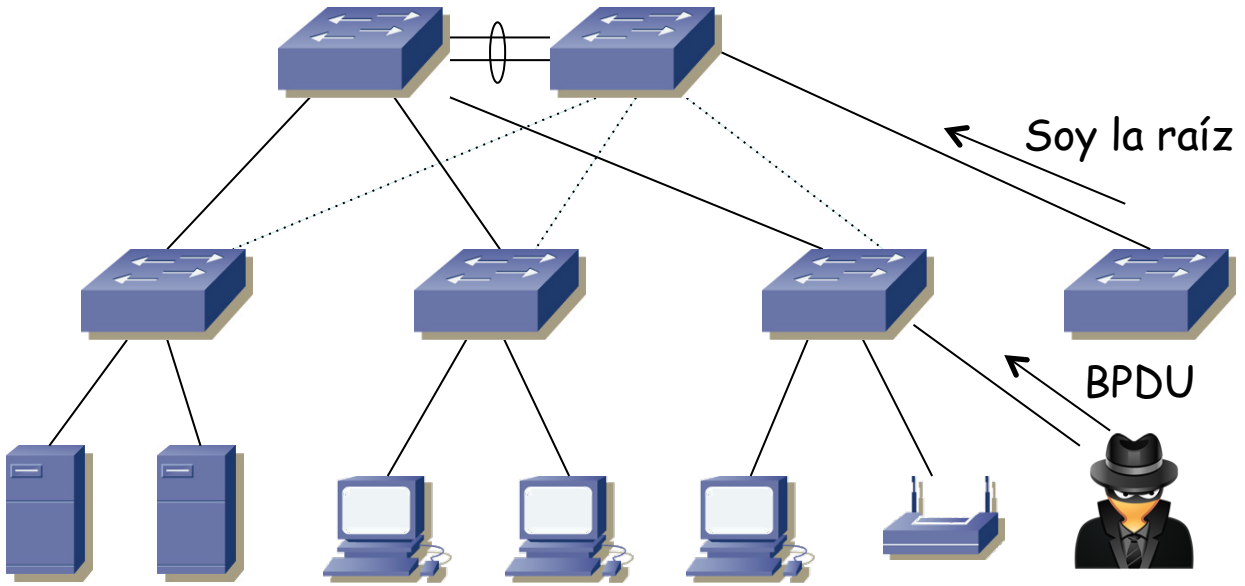
STP

- 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



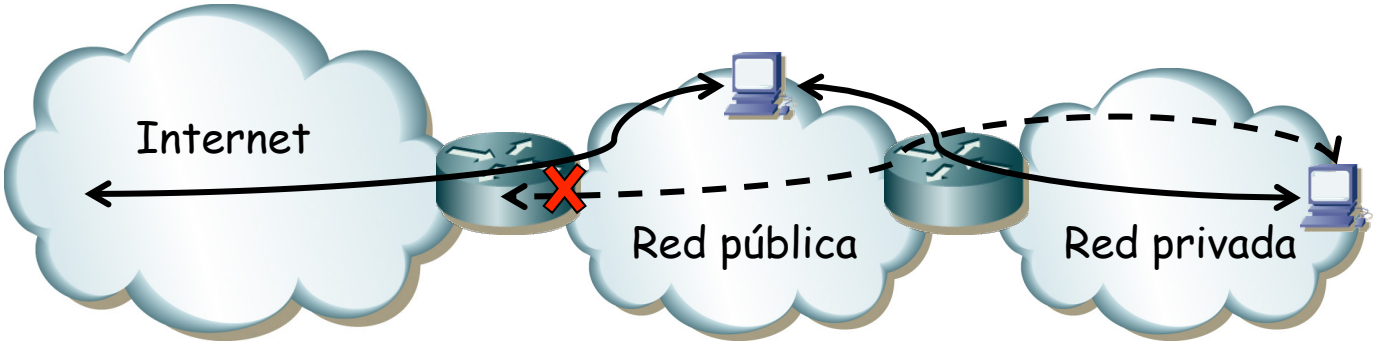
STP

- 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?)



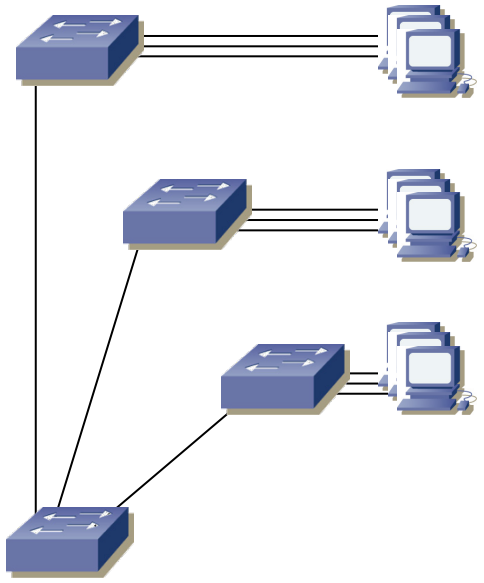
Direccionamiento

- 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



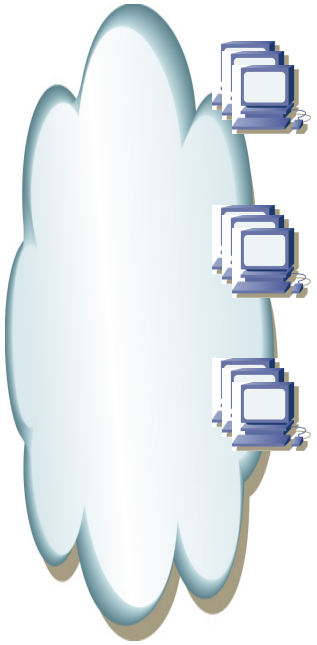
Subredes IP vs VLANs

- 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
- (...)



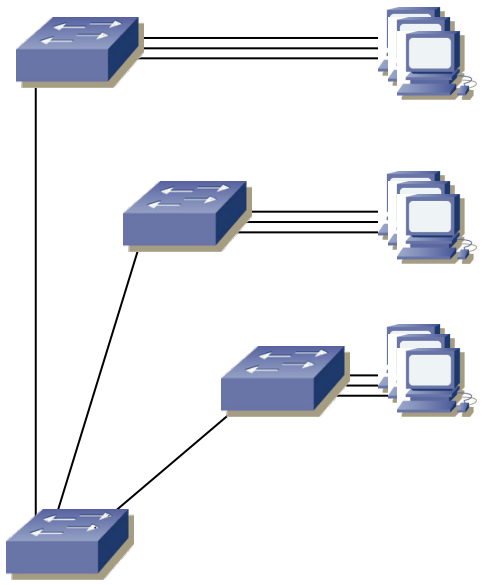
VLAN 1

172.17.1.128/26

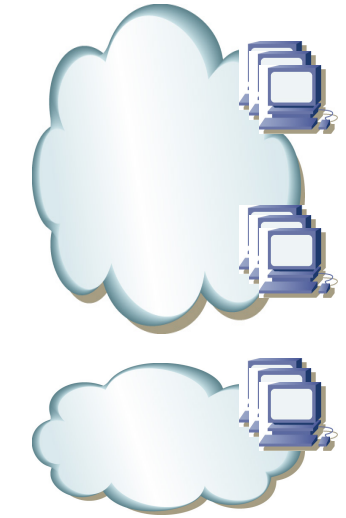


Varias subredes en la LAN

- 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 (...)

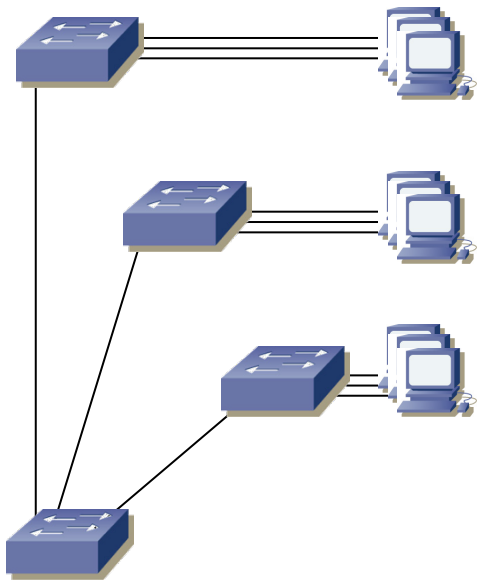


VLAN 1

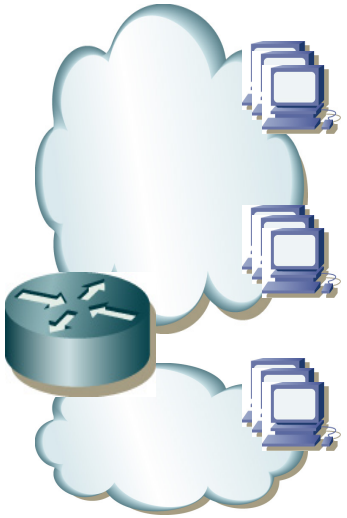


Varias subredes en la LAN

- 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 (...)



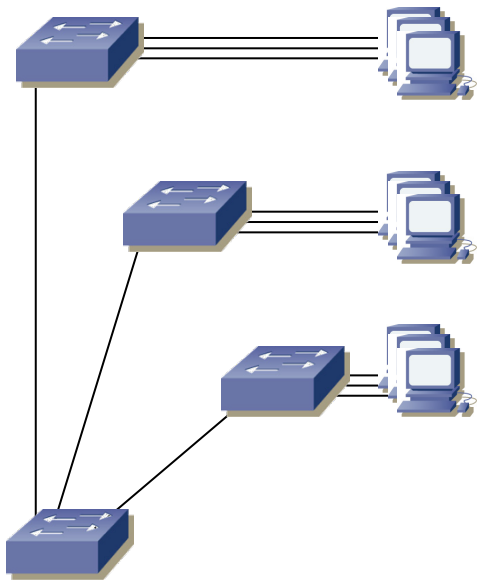
VLAN 1

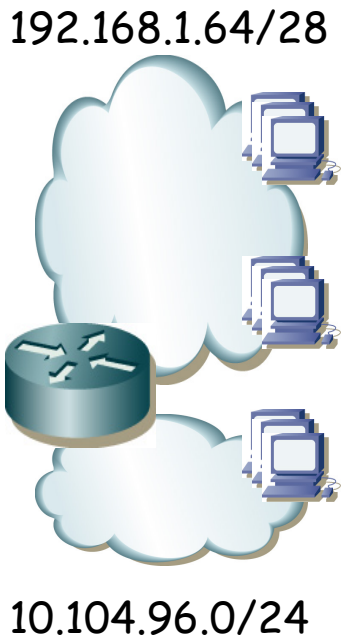


Varias subredes en la LAN

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

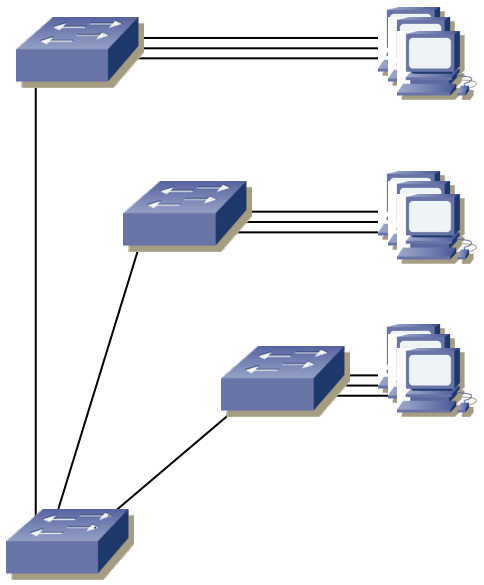
Destino	Next-hop	if
192.168.1.64/28	–	0
10.104.96.0/24	–	0





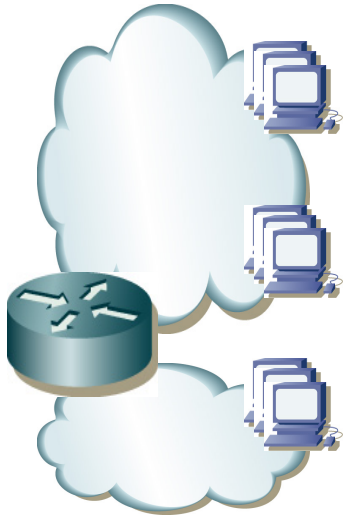
Varias subredes en la LAN

- 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

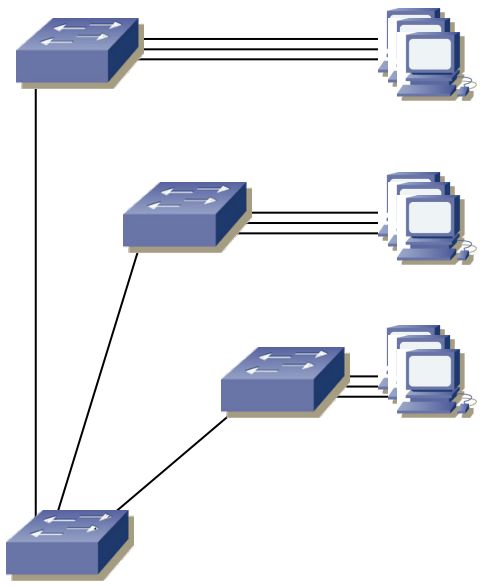
192.168.1.64/28



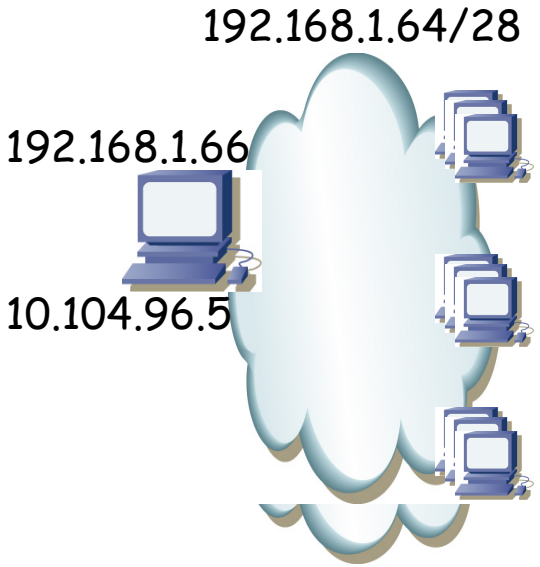
10.104.96.0/24

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

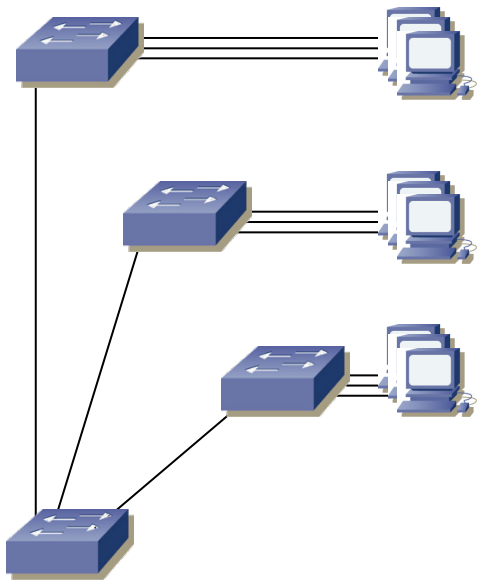


VLAN 1



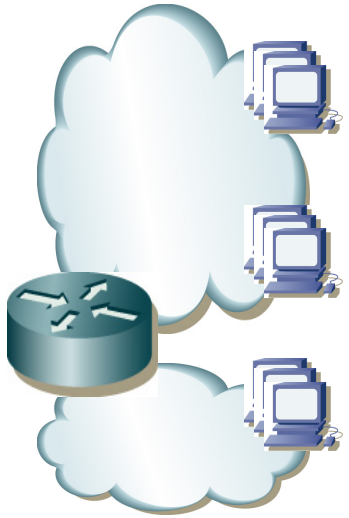
Varias subredes en la LAN

- 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

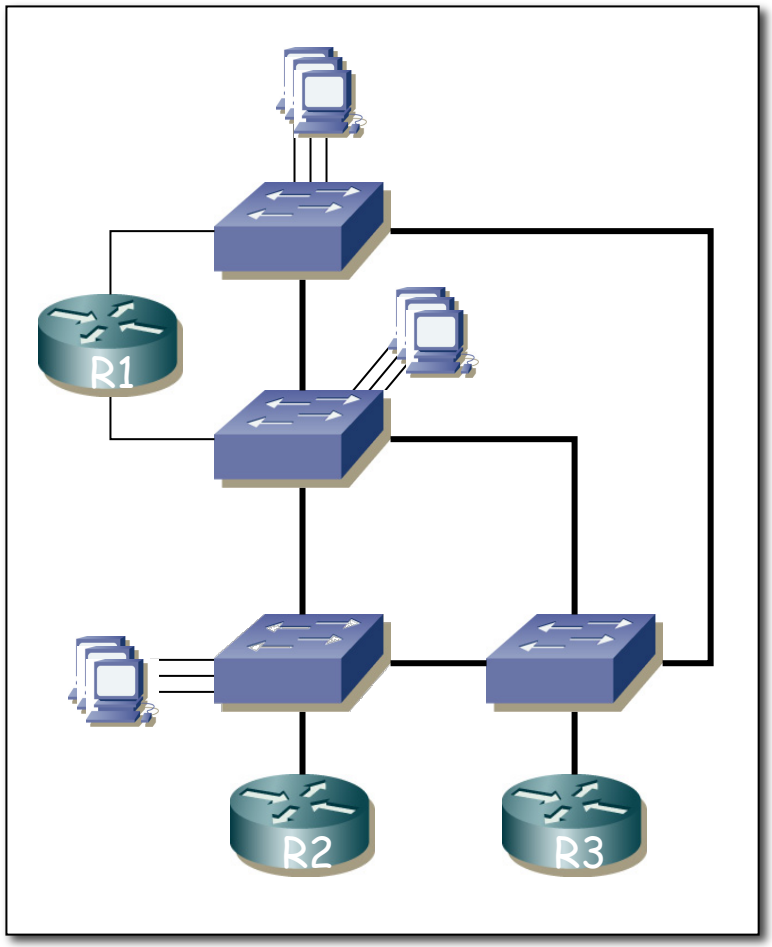
192.168.1.64/28

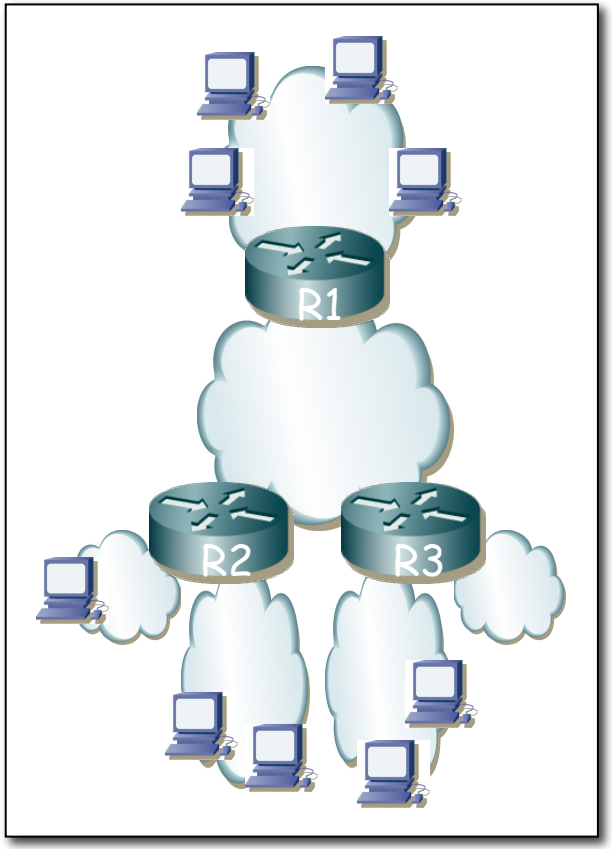


10.104.96.0/24

Topologías de nivel 1-2 y 3

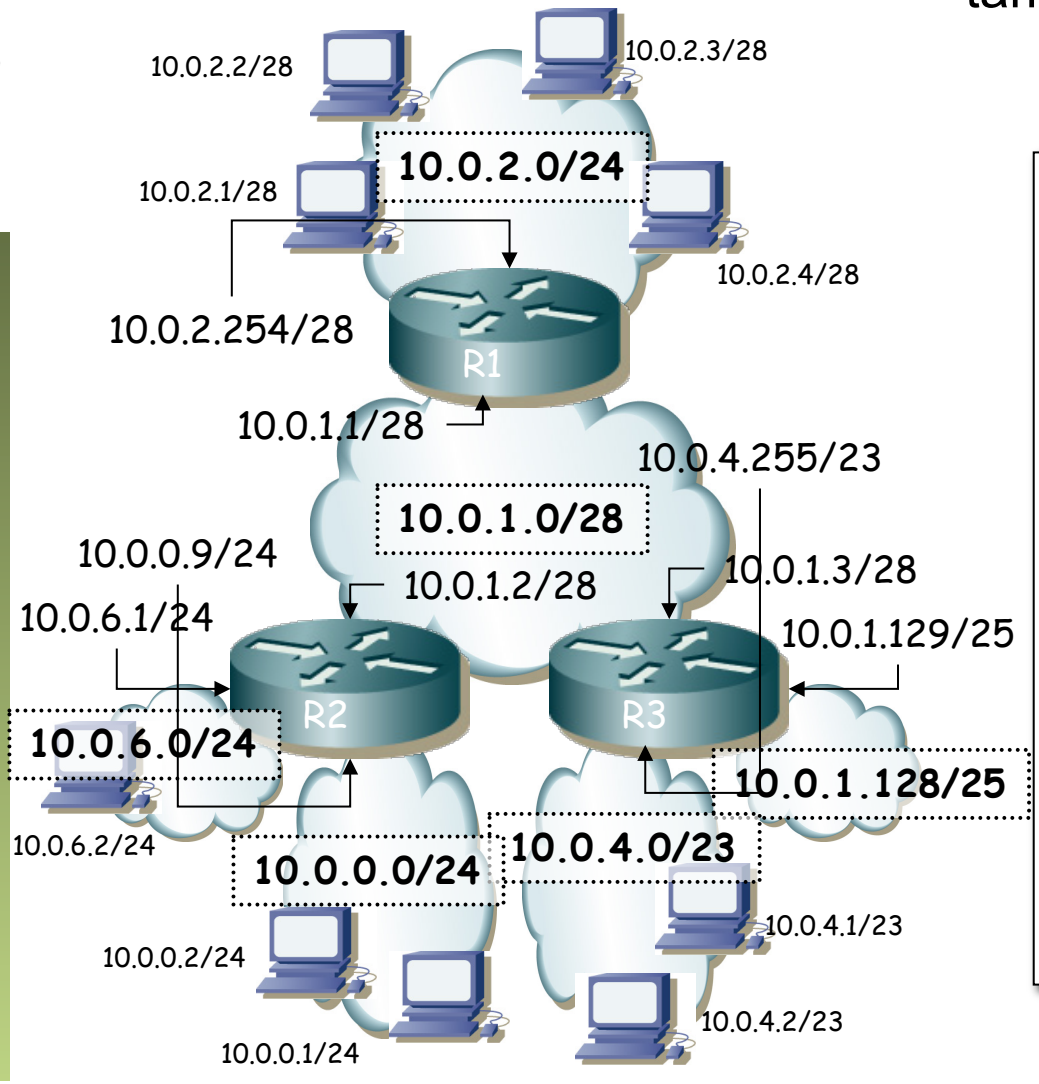
- Con VLANs puede ser difícil reconocer la topología de nivel 3
- Recomendable tener también la visión del nivel 3

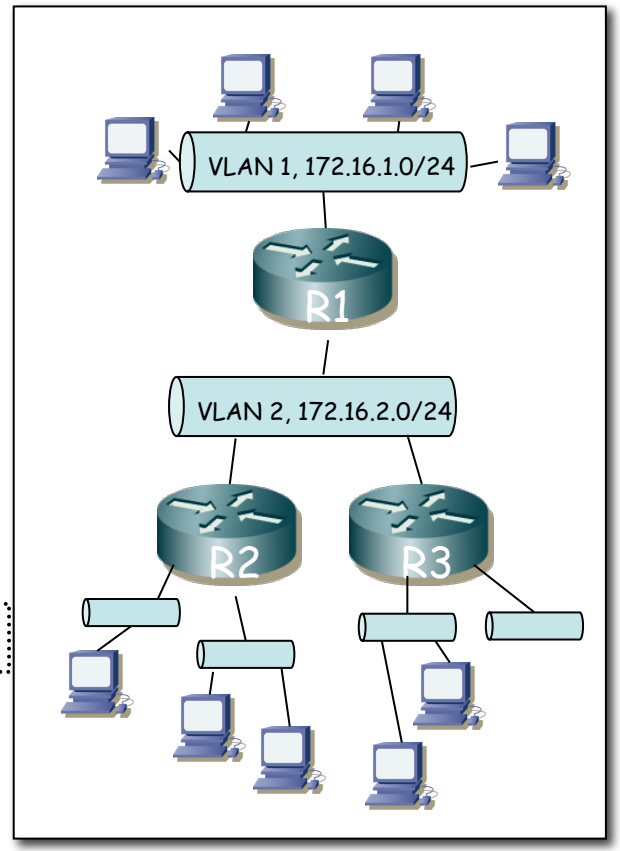




Topologías de nivel 1-2 y 3

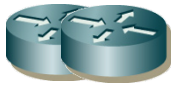
- Incluido el direccionamiento
- Recomendable tener también la visión del nivel 3

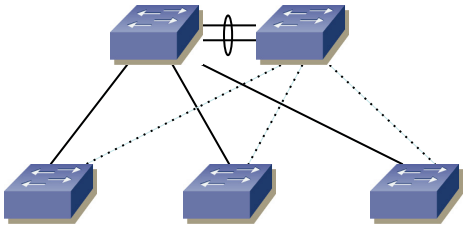


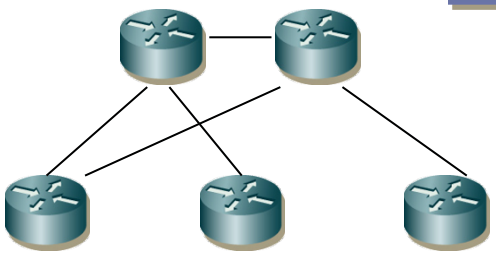


Resumen sobre protección

- 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







Diseño: VLANs y subredes IP

¿ 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