

Diseño de Campus LAN (parte 1)

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

Grado en Ingeniería en Tecnologías de
Telecomunicación, 3º

Diseño para Campus LANs

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

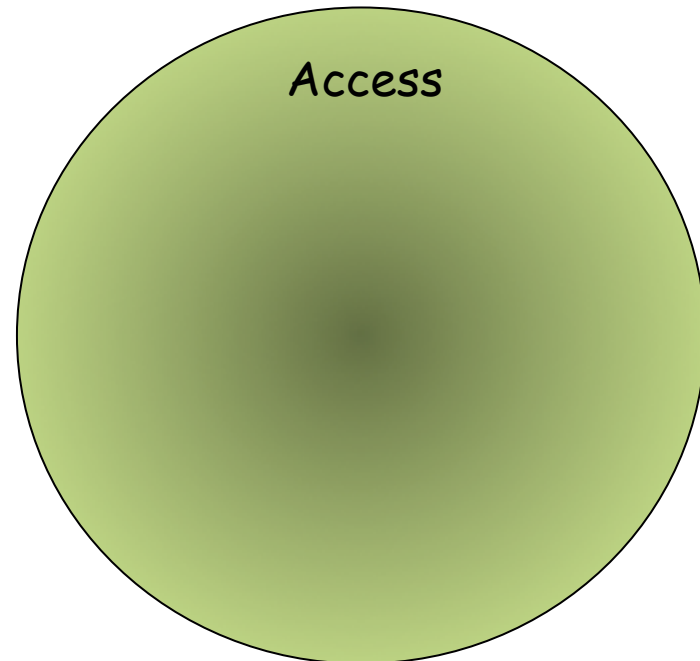


Terminología de 3 capas

Terminología para 3 capas

- **Access**

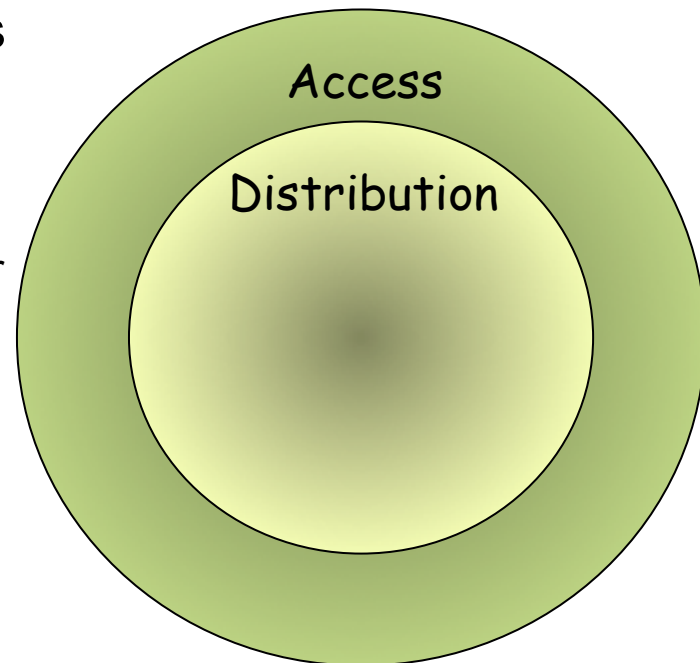
- Acceso de los usuarios a la red
- Usuarios locales o remotos
- Debe dar acceso solo a usuarios autorizados
- IDF (Intermediate Distribution Frame)
- Hay que tener en cuenta:
 - Número de usuarios
 - Aplicaciones
 - Uso de VLANs
 - Redundancia



Terminología para 3 capas

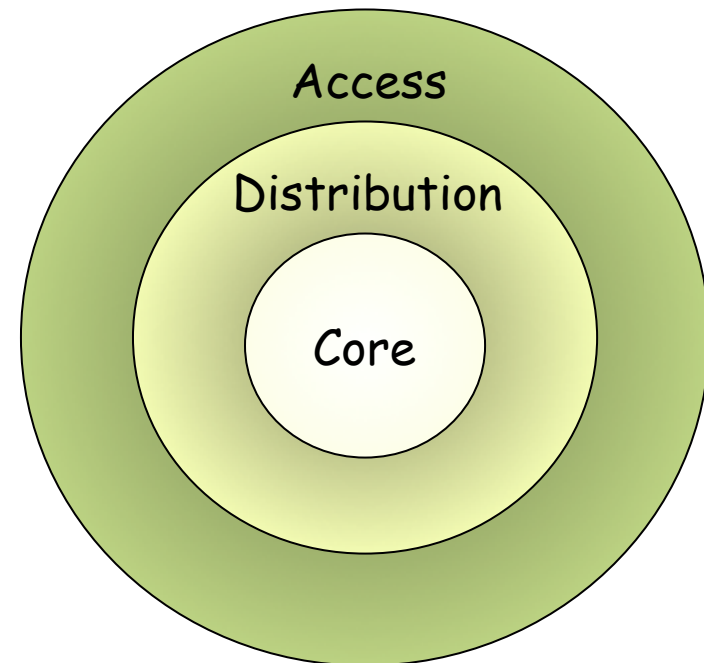
- **Distribution/Agregación**

- 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”



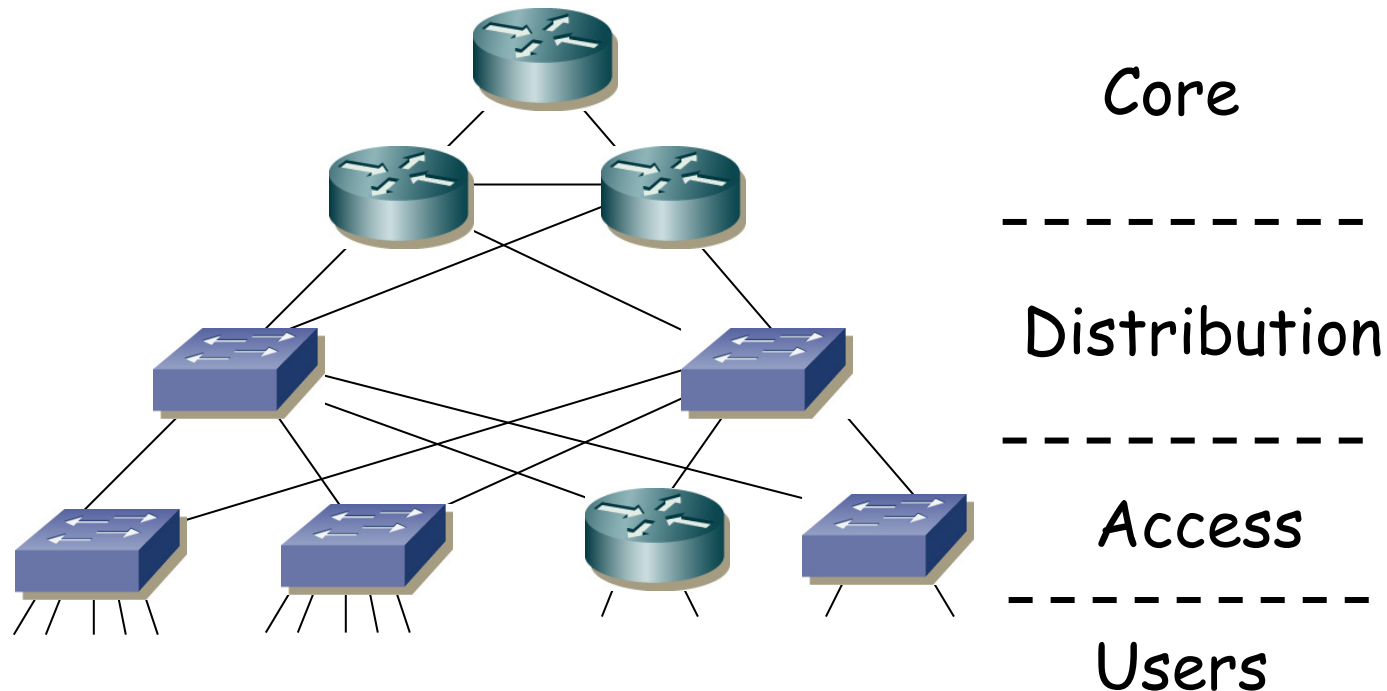
Terminología para 3 capas

- **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

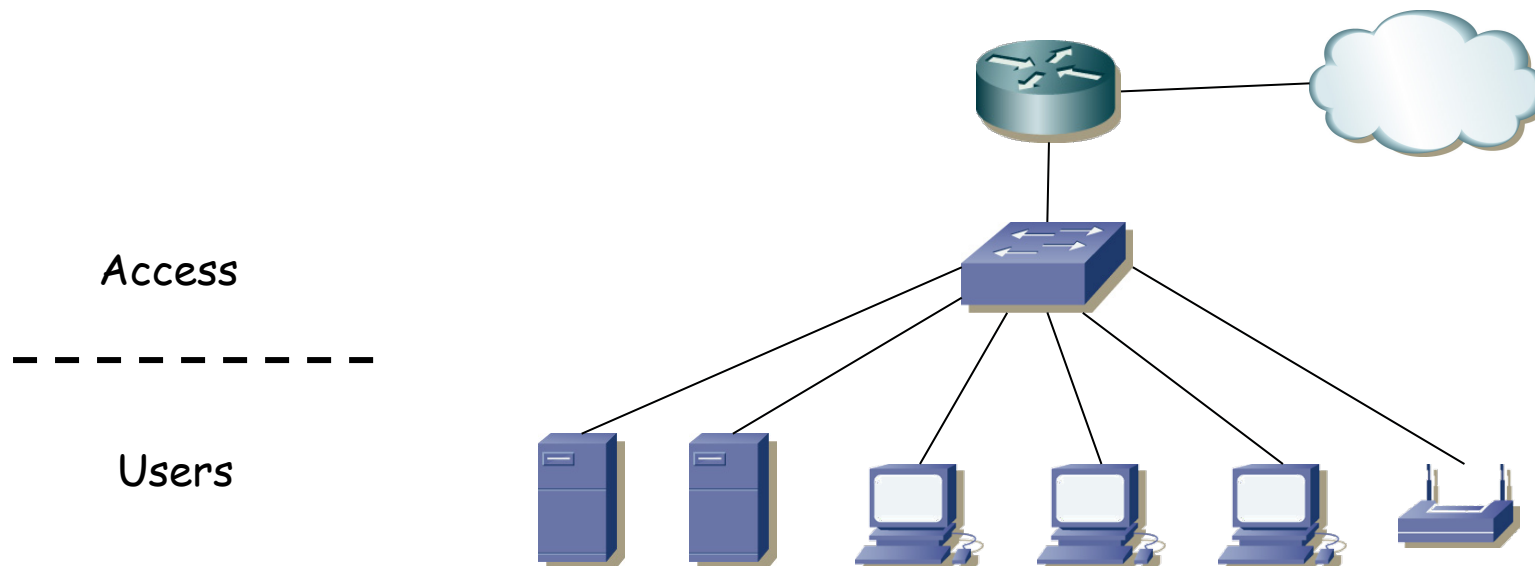
- **Access:** Acceso de los usuarios a la red
- **Distribution:** Conexión entre grupos de trabajo y de ellos al núcleo
- **Core:** Transporte de alta velocidad entre los dispositivos de distribución



Diseño para pequeño número de usuarios

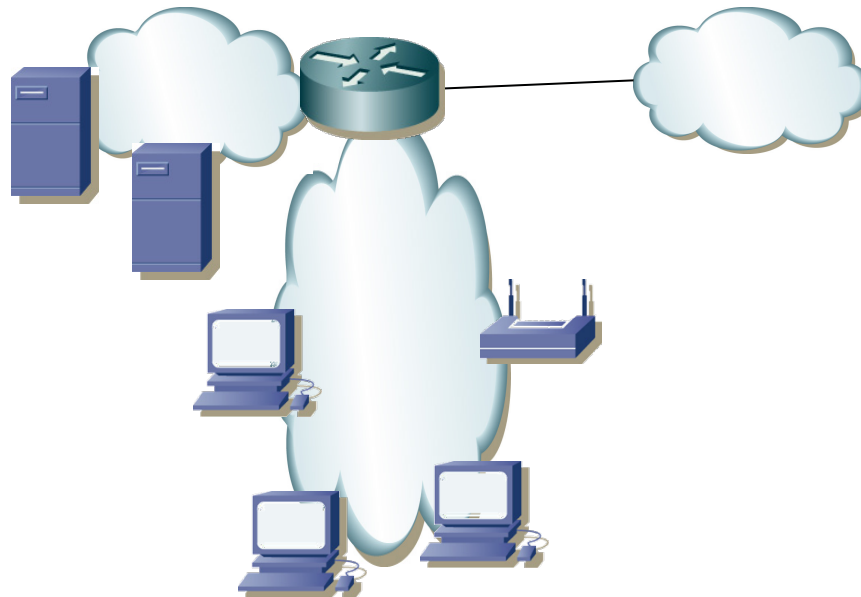
Pocos usuarios

- 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 (...)



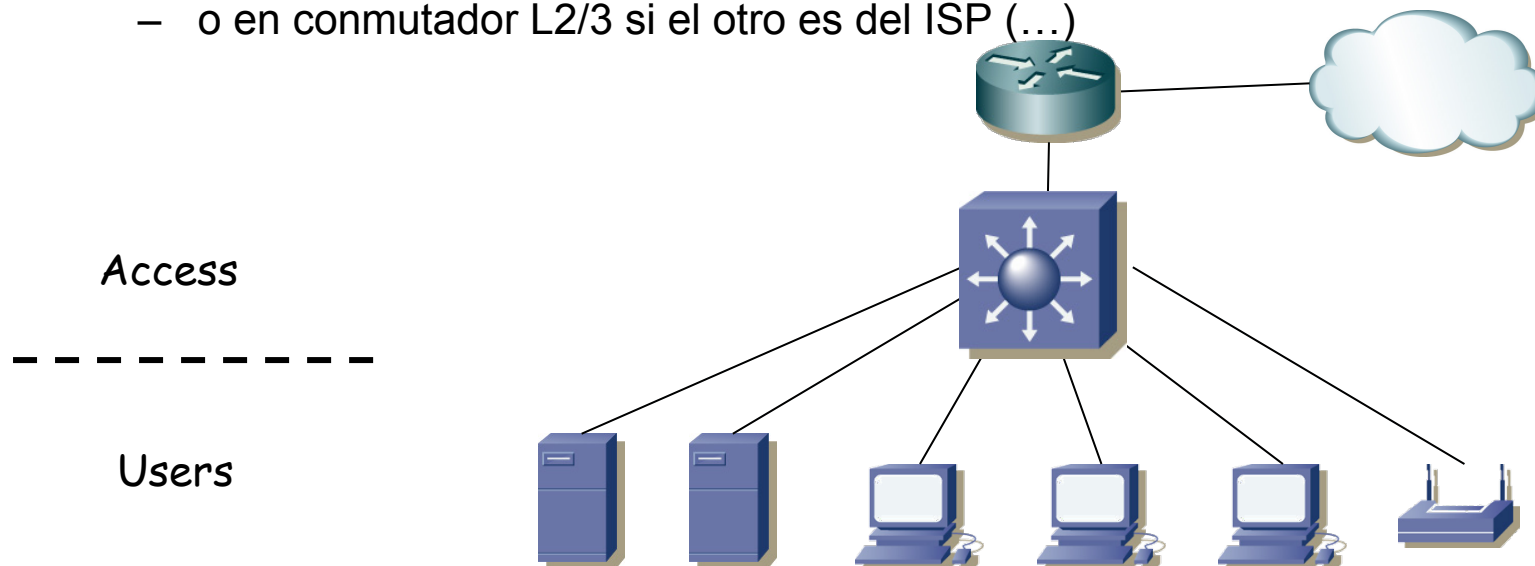
Pocos usuarios

- 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 (...)



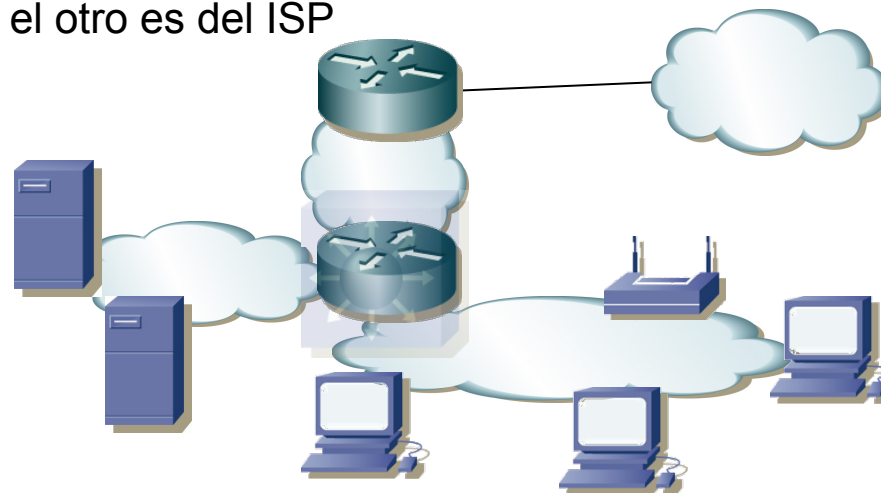
Pocos usuarios

- 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 (...)



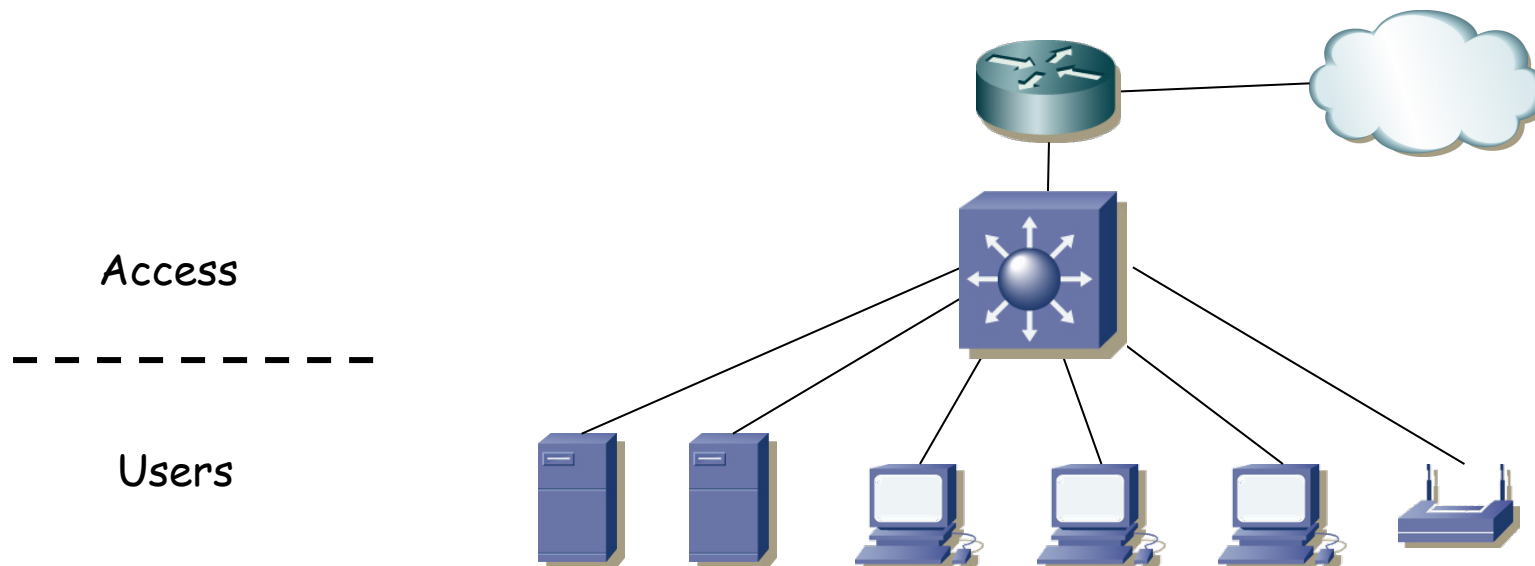
Pocos usuarios

- 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

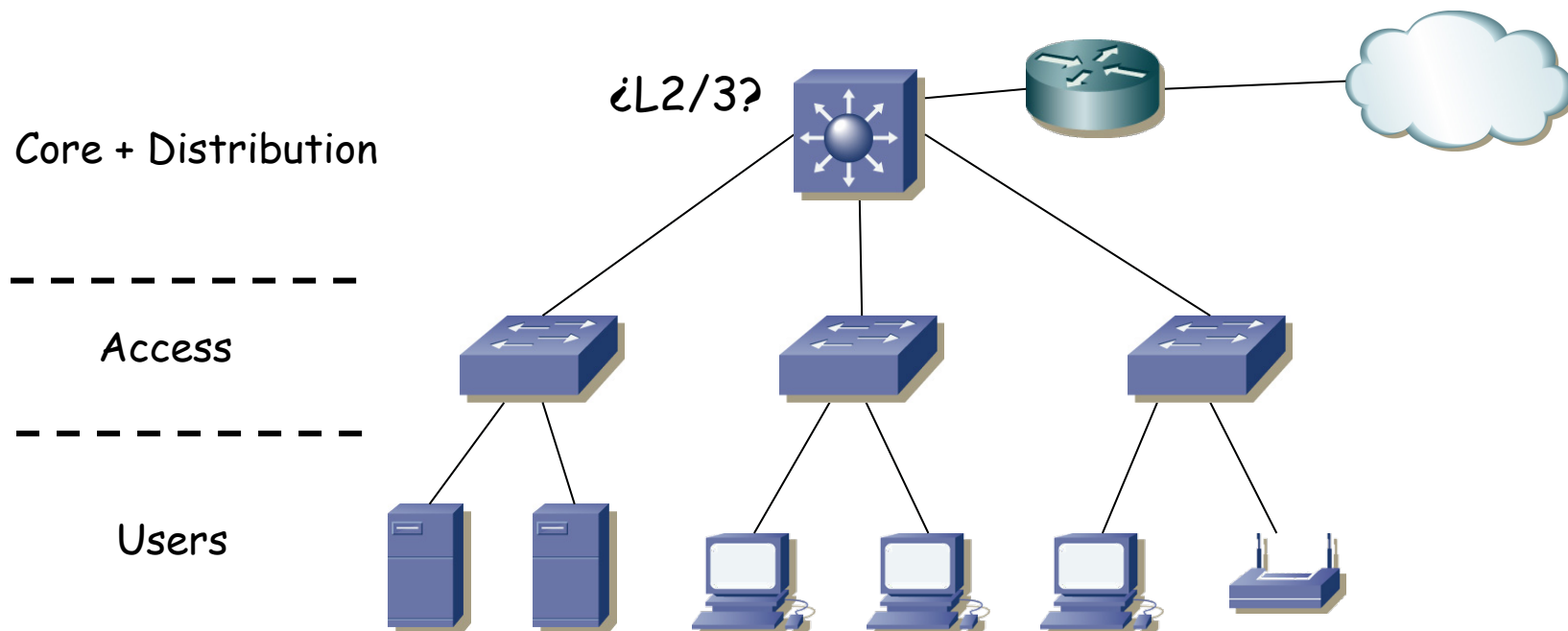
- No hay redundancia en la conmutación interna
- Aunque serviría de poco si los usuarios solo tienen un interfaz
- Tampoco hay redundancia en el acceso
- Pero para una red tan pequeña no suele ser crítico



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 (...)



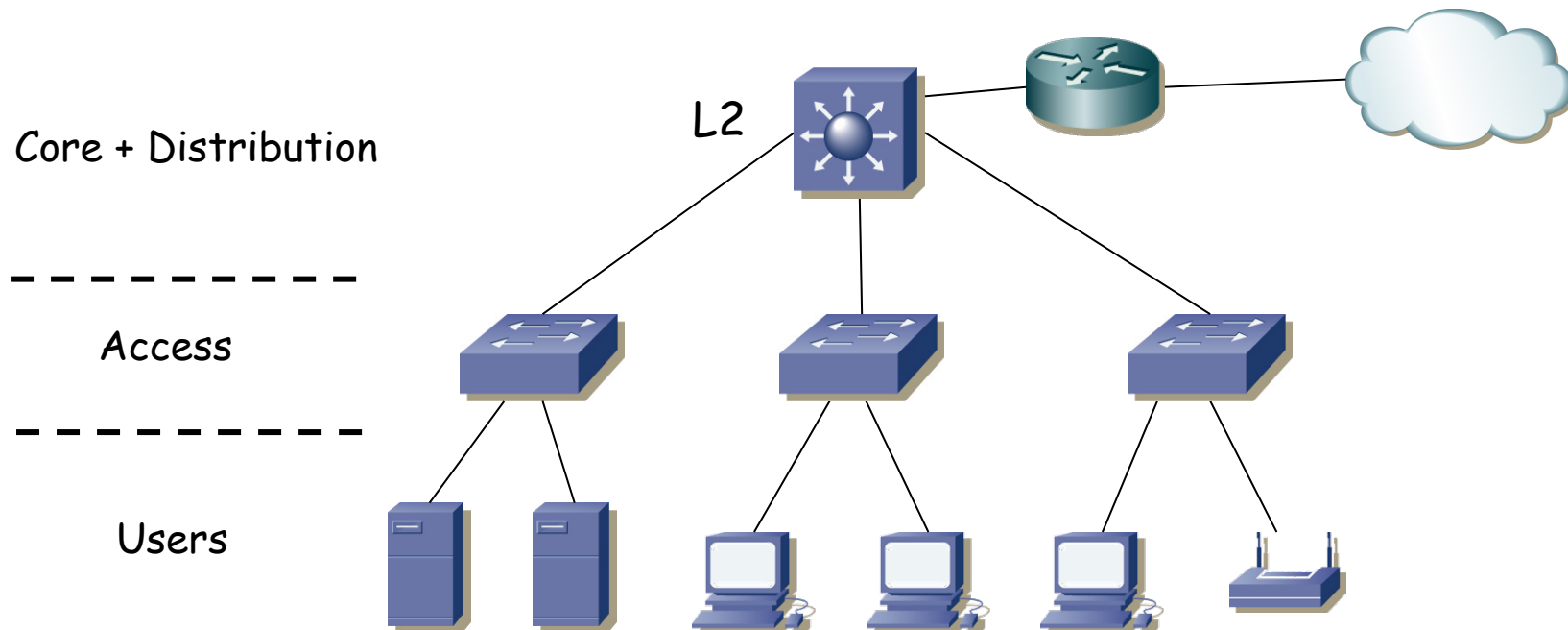
Collapsed core (2-tiers)

- 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 o no (entonces varios enlaces al router de acceso o un trunk)
- (...)



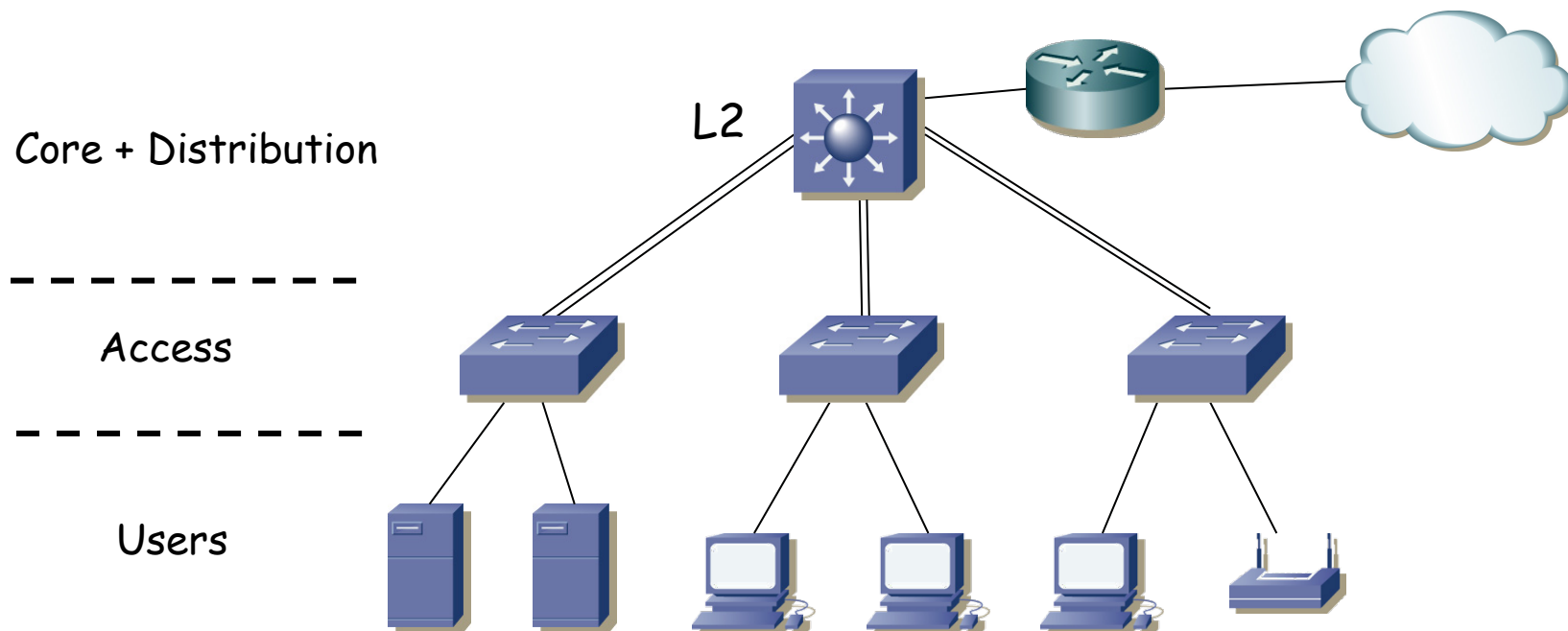
Collapsed core (2-tiers)

- Si la red es crítica, necesitará cierta protección (...)



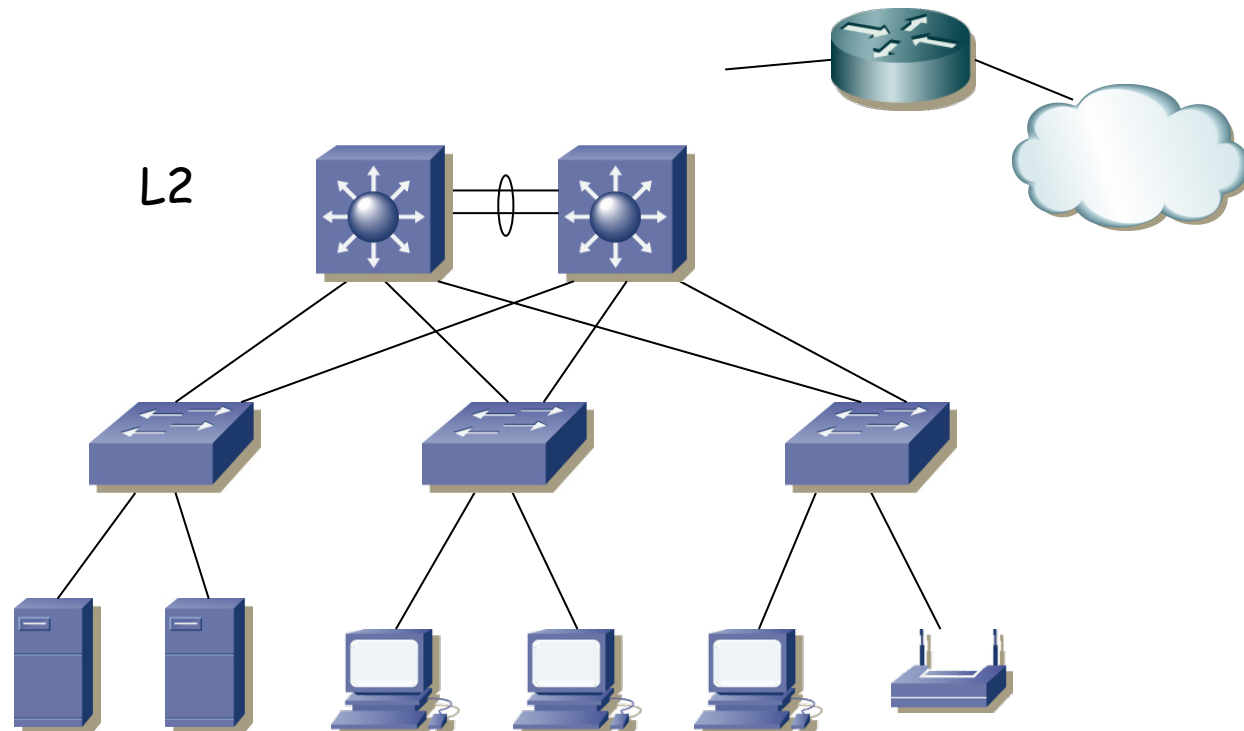
Collapsed core (2-tiers)

- 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



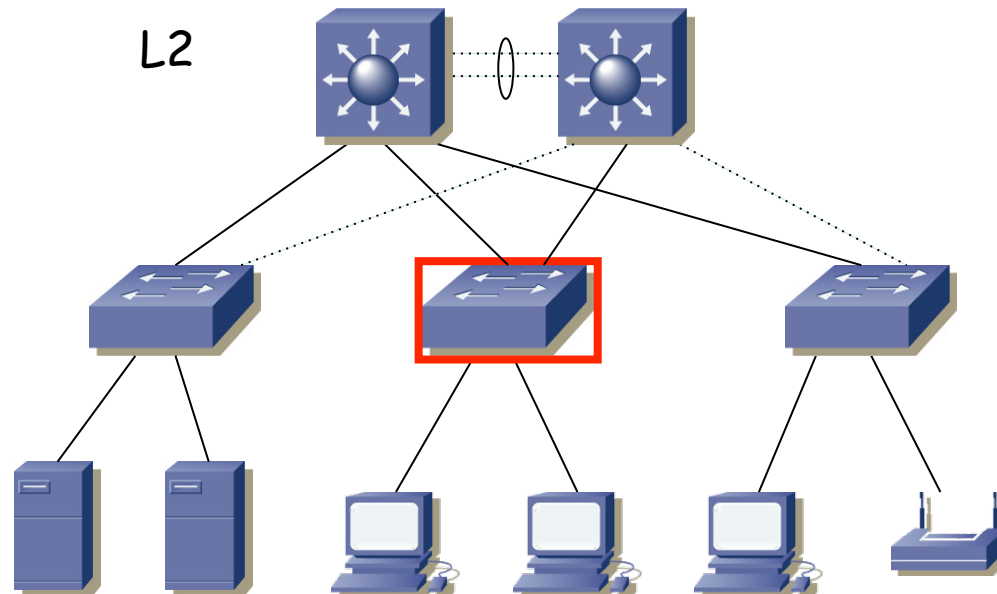
Redundant collapsed core

- 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 ? (...)



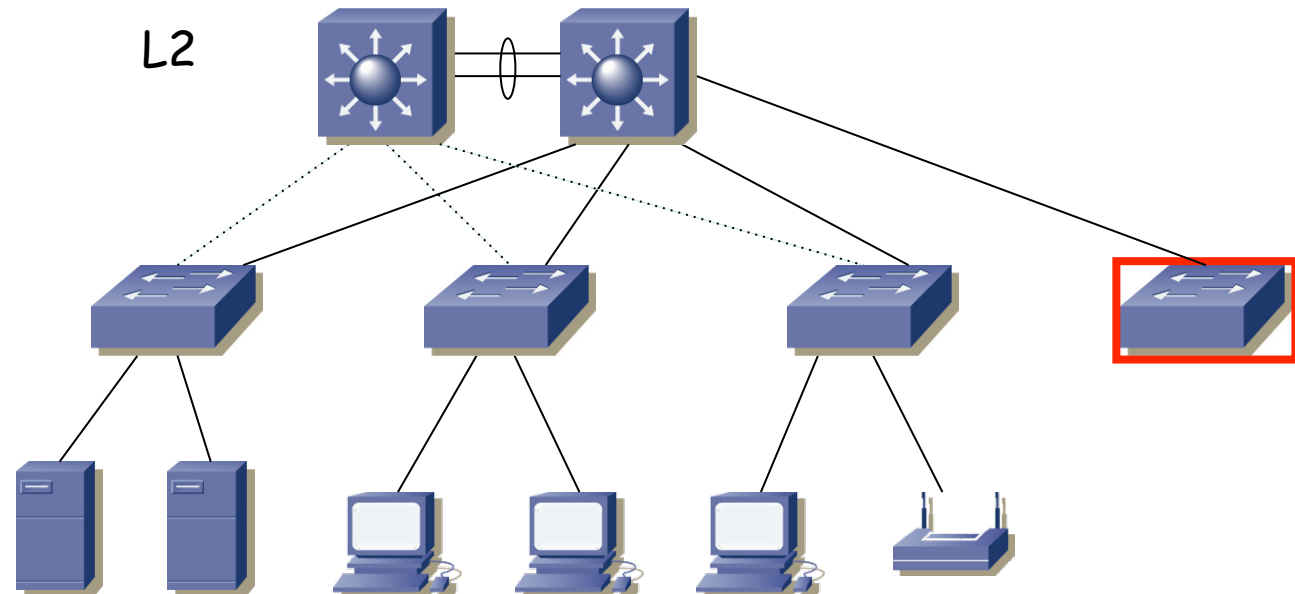
Redundant collapsed core

- 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 (...)



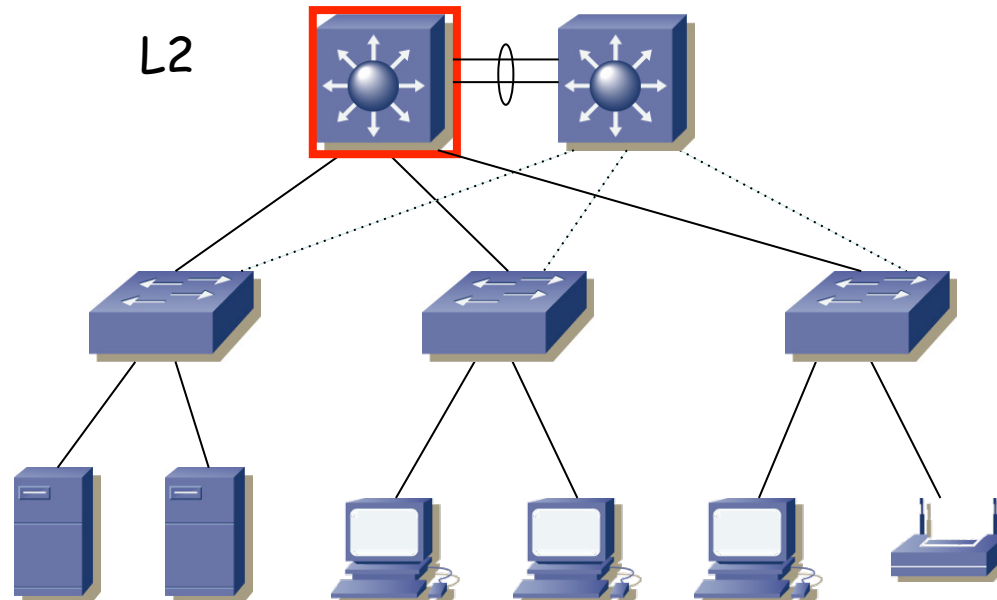
Redundant collapsed core

- 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



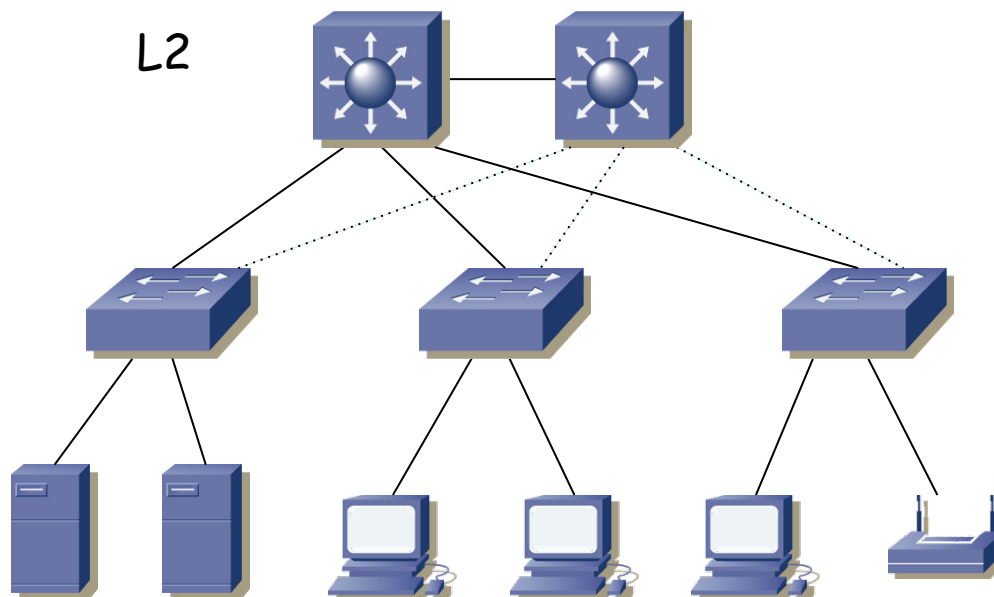
Redundant collapsed core

- 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



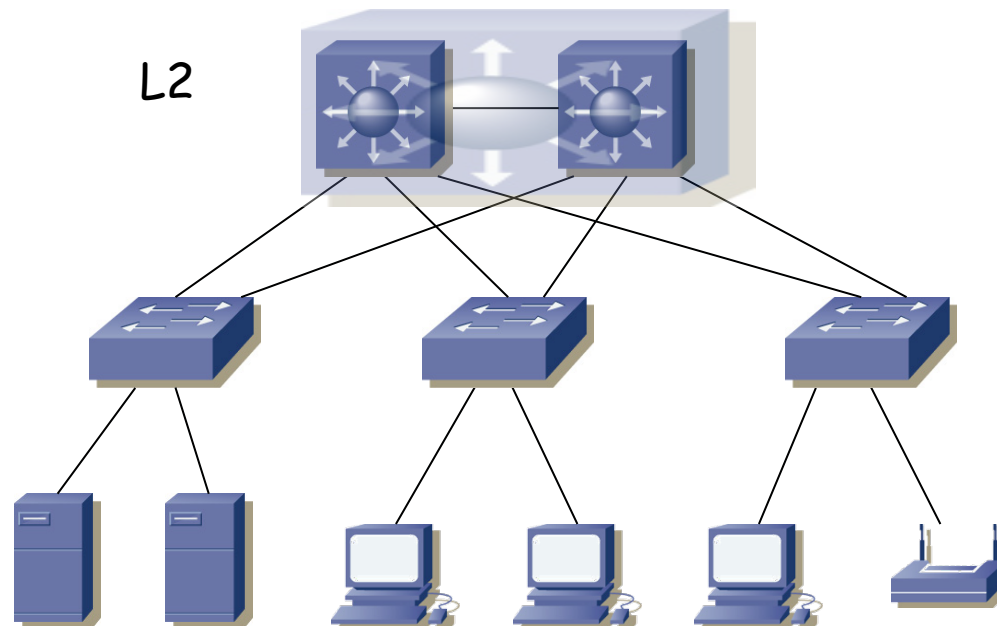
Redundant collapsed core

- Hemos acabado con varios enlaces bloqueados por STP
- Algunos fabricantes ofrecen otras posibilidades para sacar provecho a esos enlaces
- Por ejemplo (...)



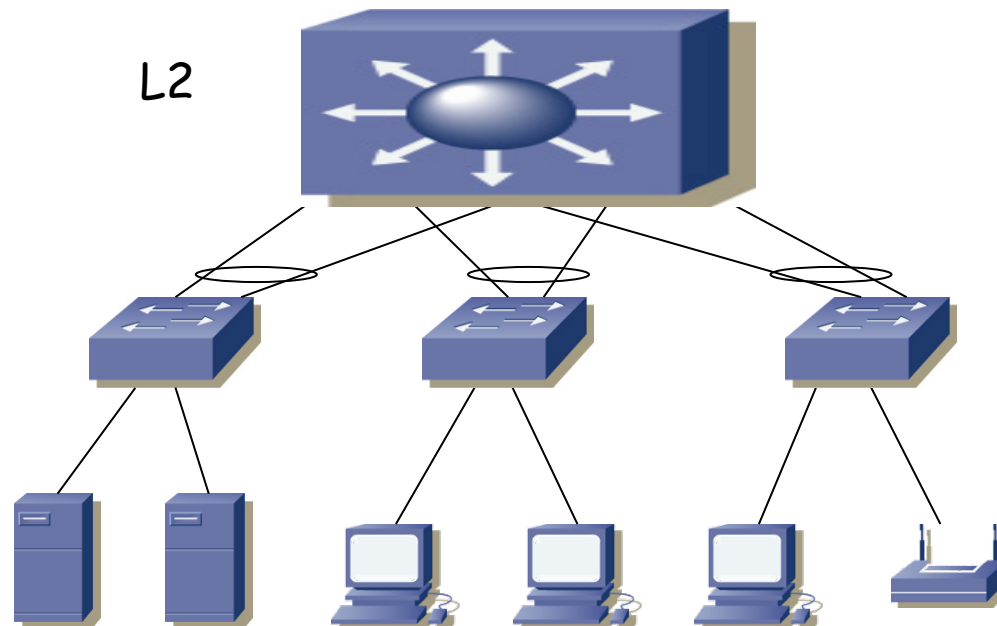
Redundant collapsed core

- 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” (...)



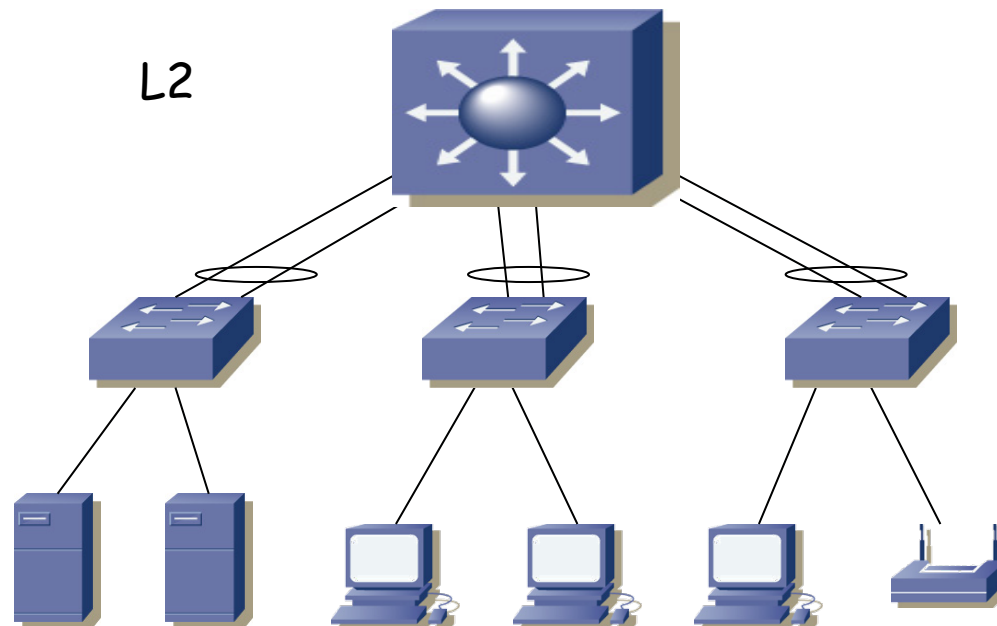
Redundant collapsed core

- 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 (...)



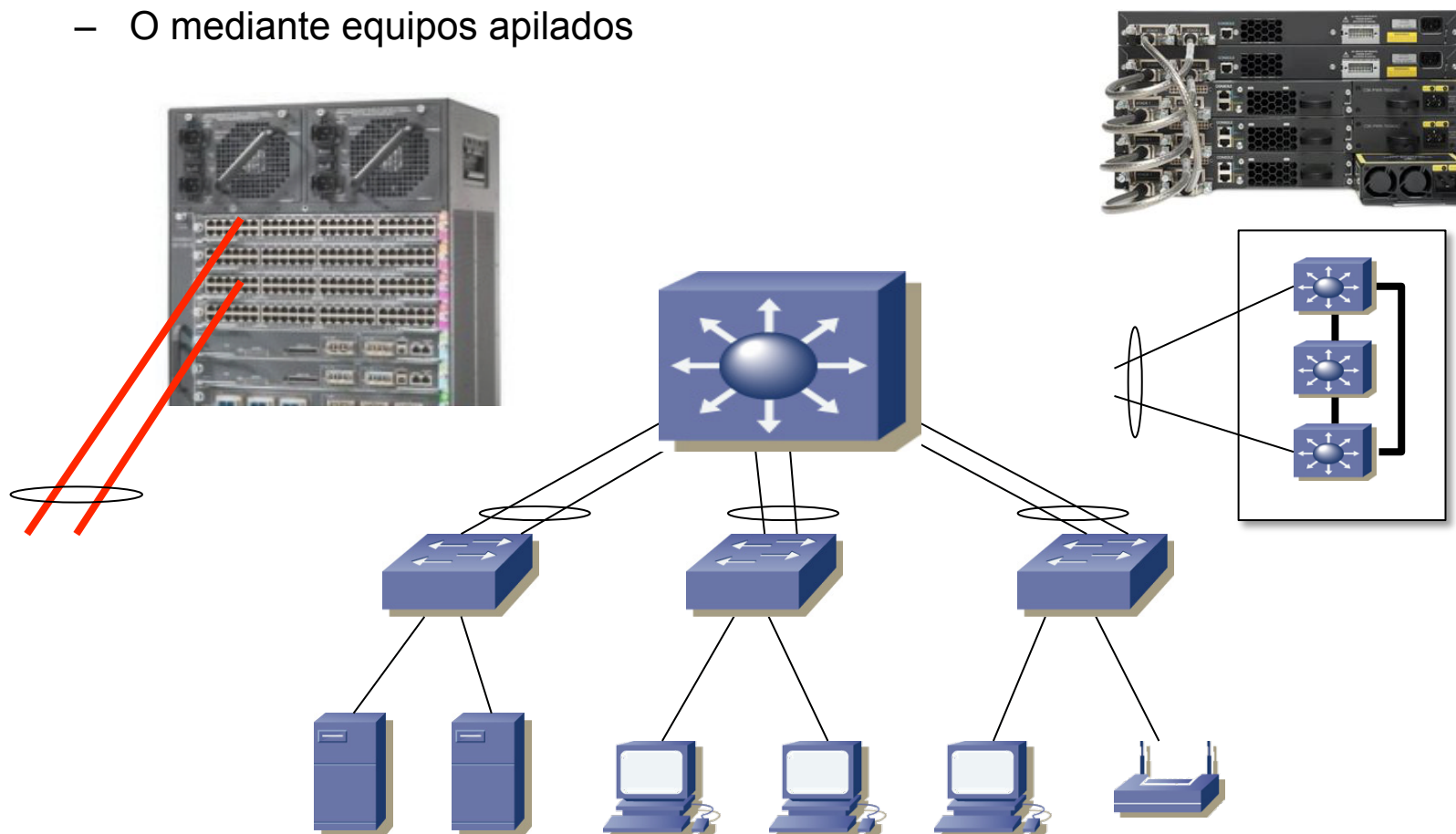
Redundant collapsed core

- 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



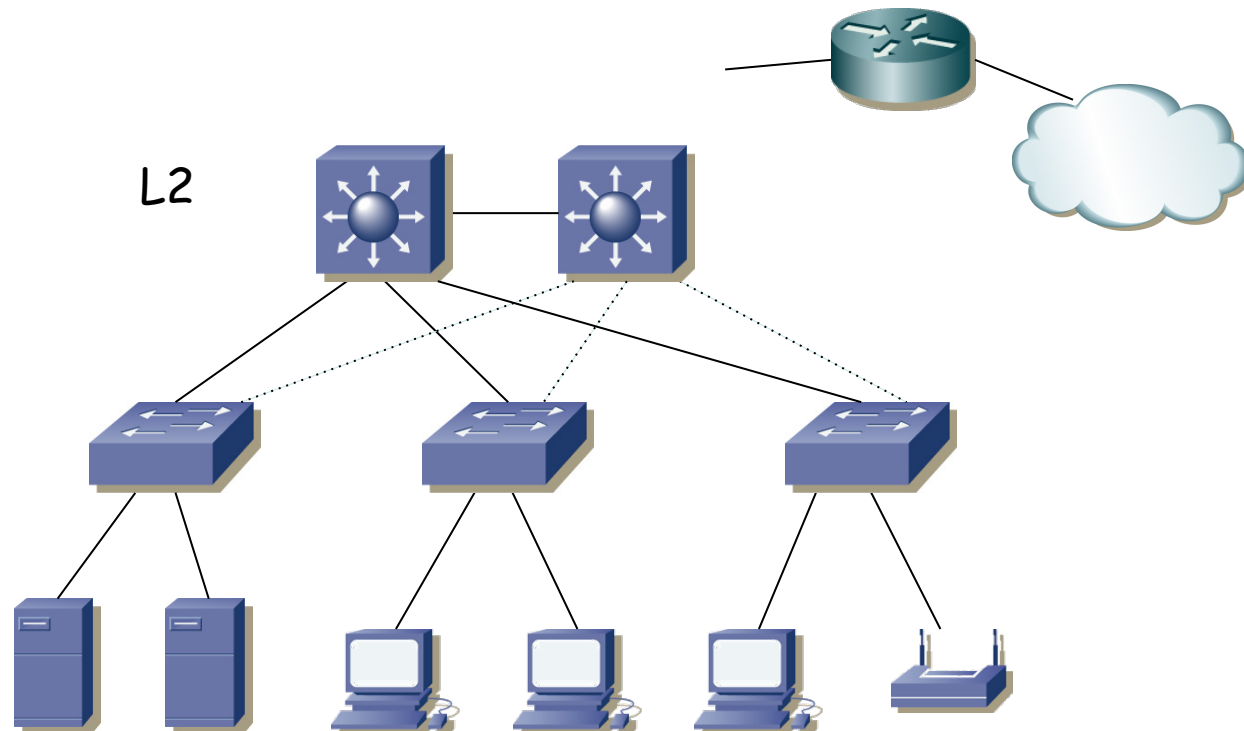
Redundant collapsed core

- 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



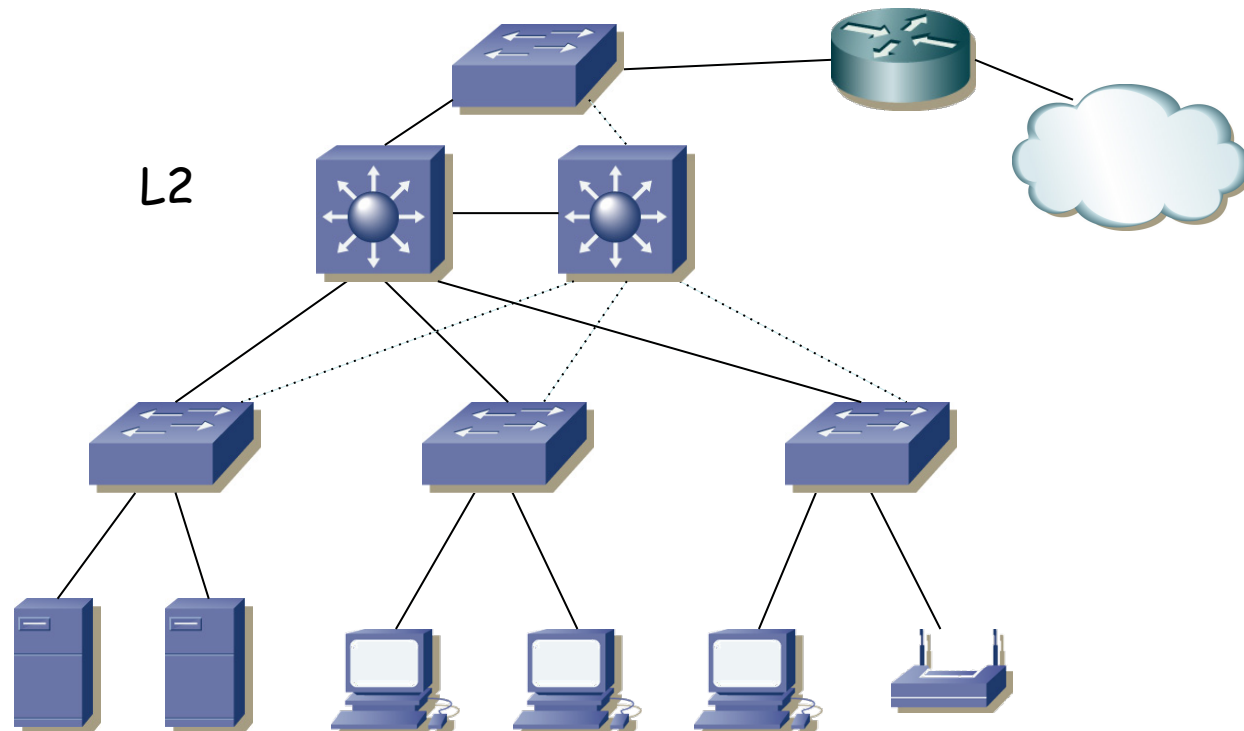
Enrutamiento

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



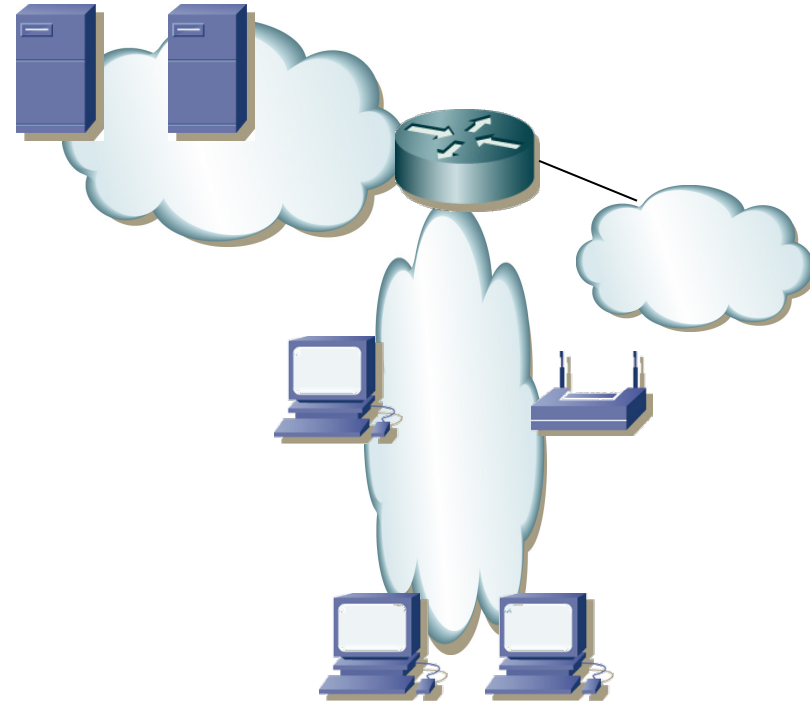
Enrutamiento

- 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
- (...)



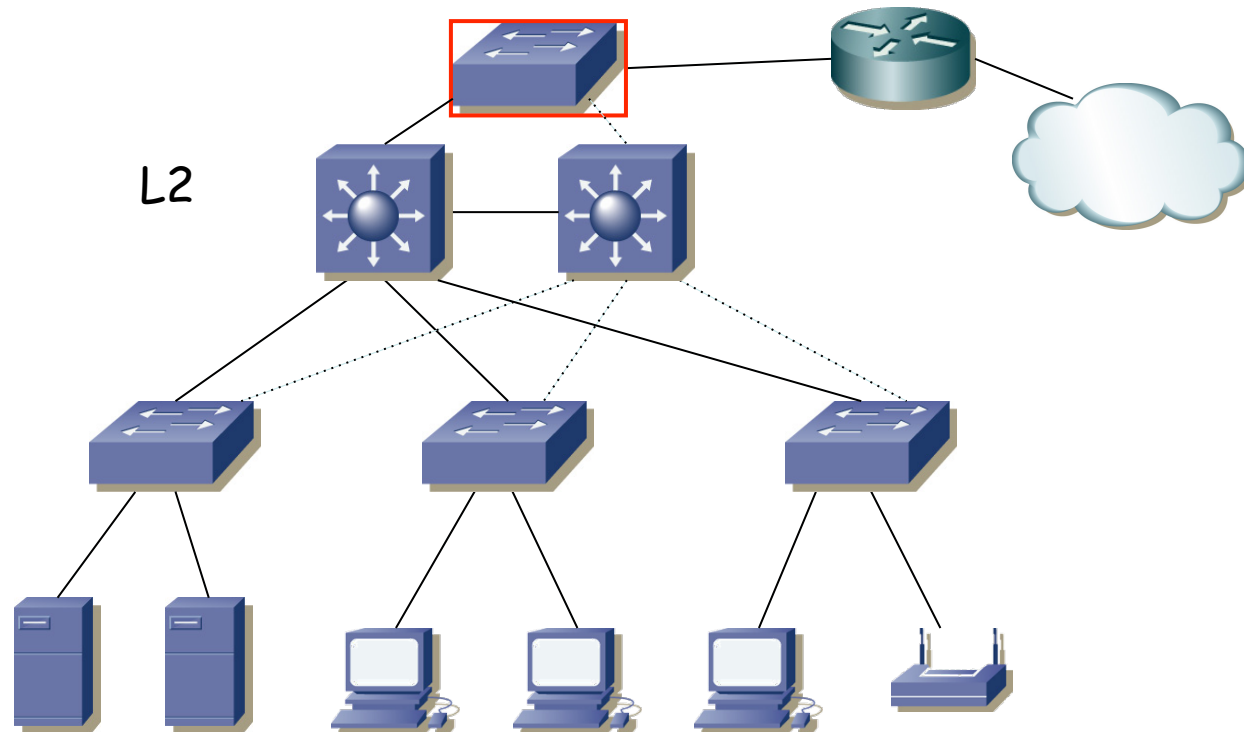
Enrutamiento

- 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)
- (...)



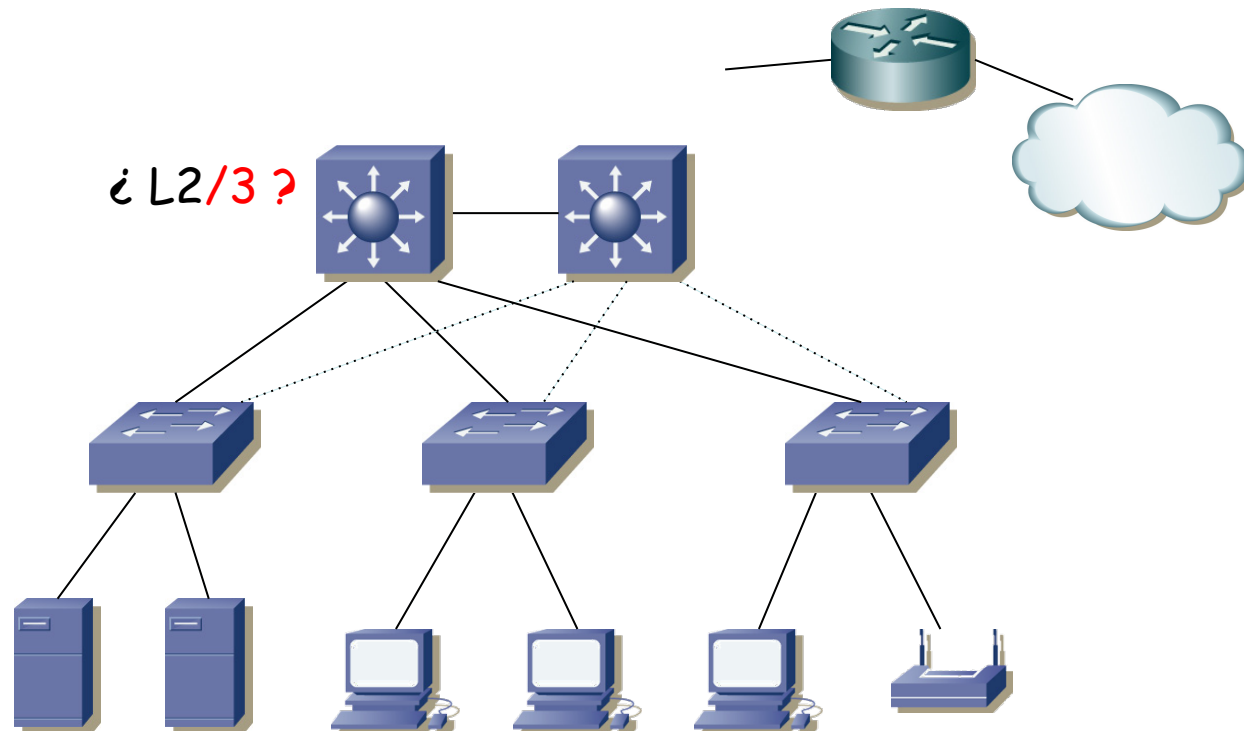
Enrutamiento

- 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



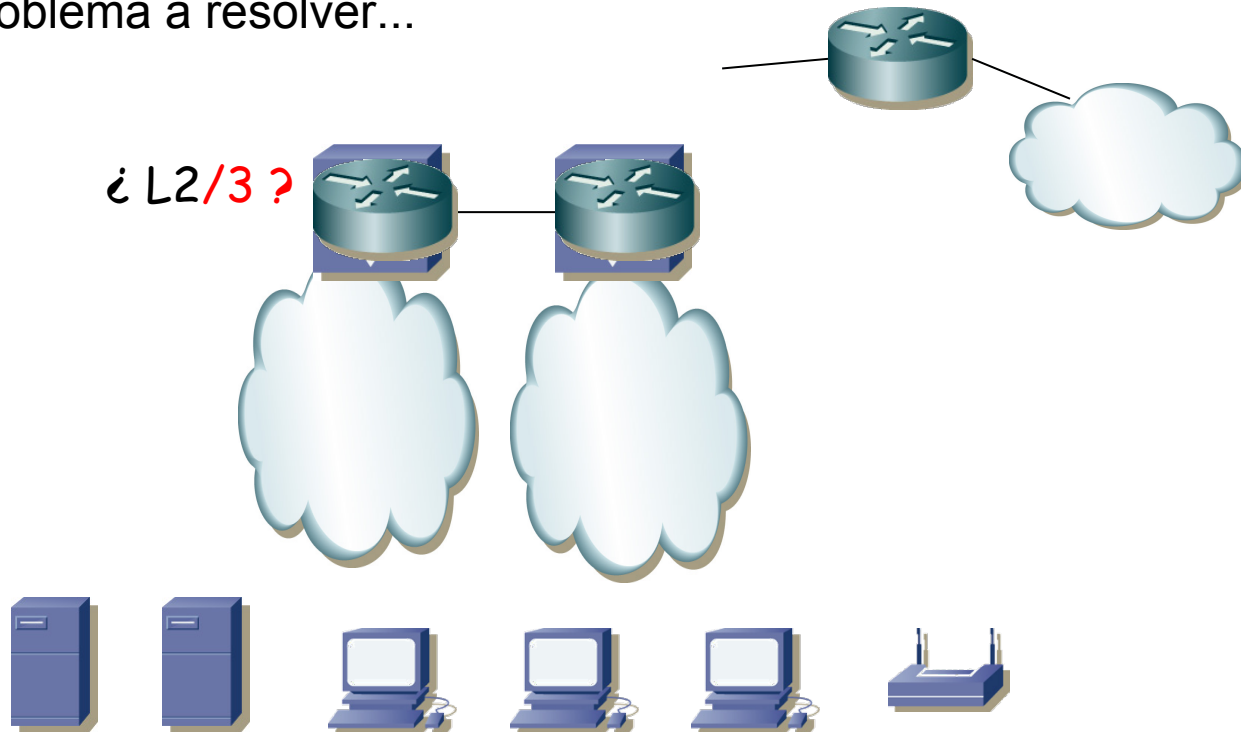
Enrutamiento

- 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

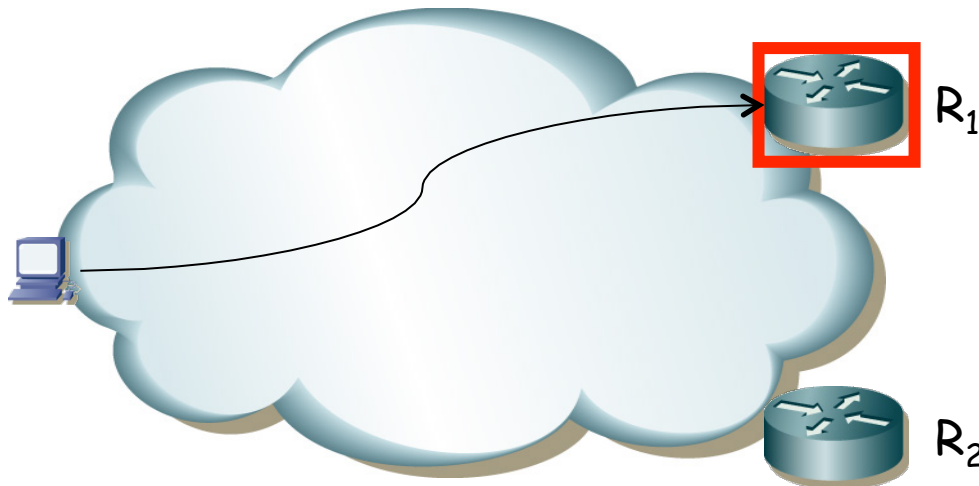
- Volviendo al caso con conmutadores de gama media (no se “agregan”)
- ¿Cómo hacemos en encaminamiento capa 3?
- ¿Podríamos enrutar en los conmutadores de distribución?
- ¿Y cómo sería eso en capa 3?
- ¿Repartimos los routers como router por defecto para las VLANs?
- El router por defecto sigue siendo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



FHRPs

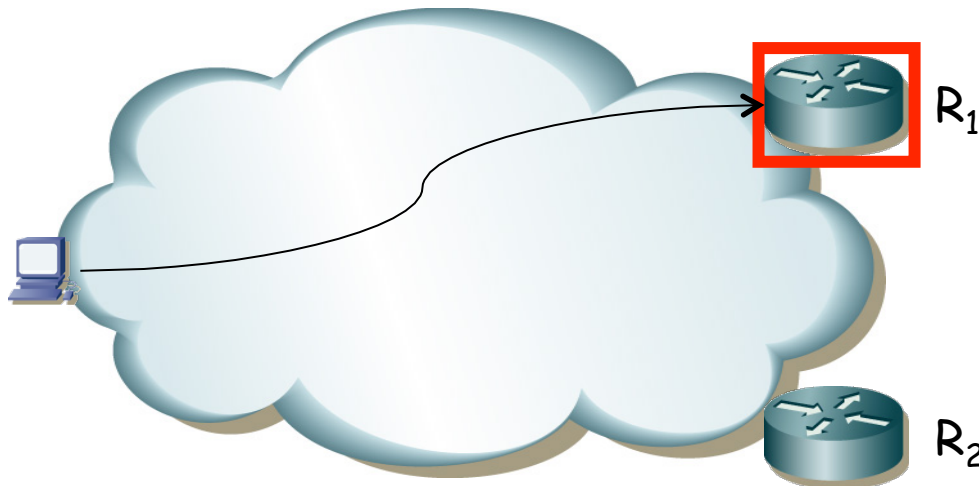
FHRP

- *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



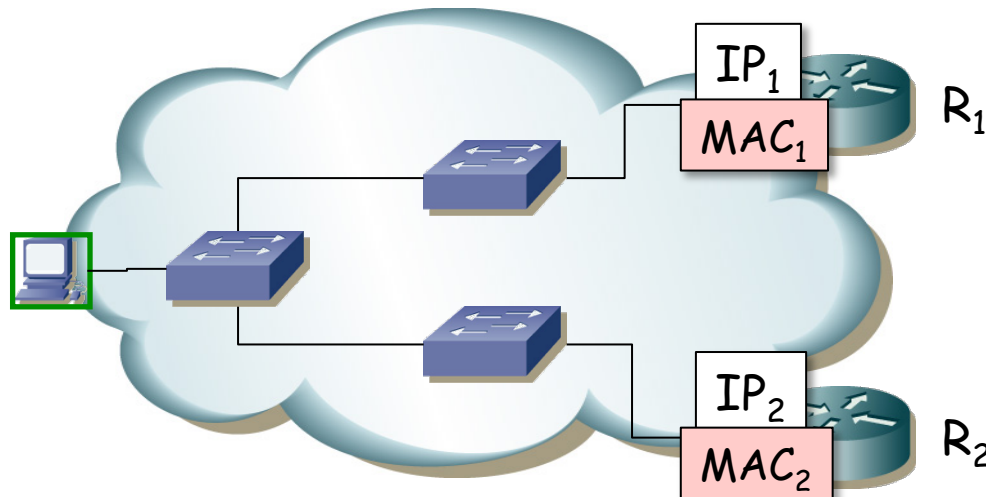
FHRP

- Hot Standby Router Protocol (HSRP): Propietario de Cisco
- Virtual Router Redundancy Protocol (VRRP): Similar pero IETF
- 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.



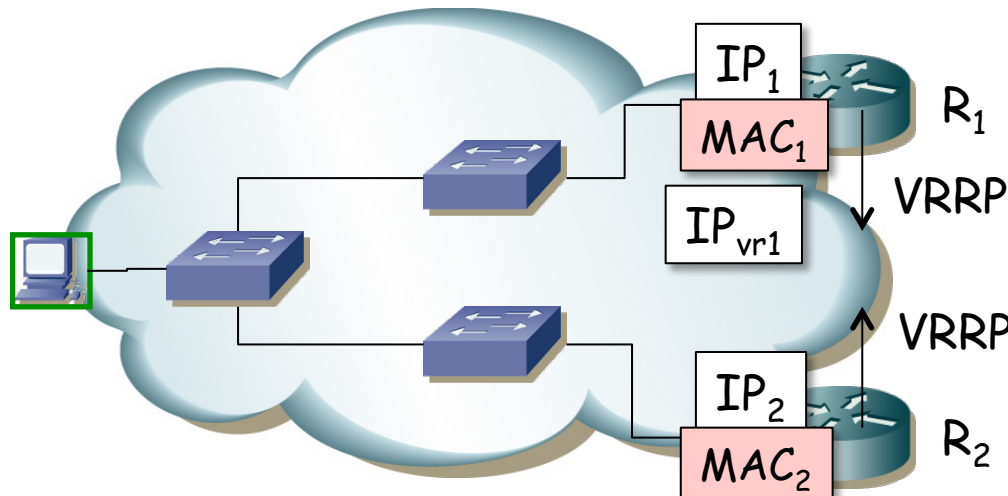
VRRP: Cómo funciona

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



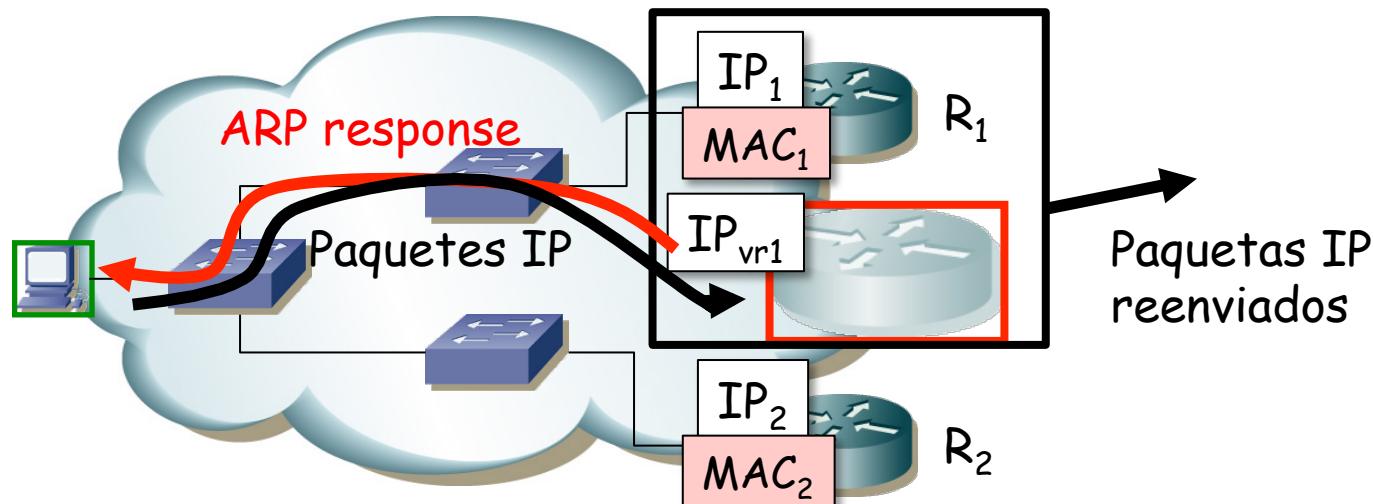
VRRP: Selección de maestro

- 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 el elegido
- Si uno tiene configurada la IP del router virtual en un interfaz físico será el maestro (anuncia máxima prioridad)
- Estos mensajes son paquetes IP dirigidos a 224.0.0.18 (mcast) por esa subred IP
- El protocolo es 112 (no es UDP ni TCP ni ICMP, es VRRP)



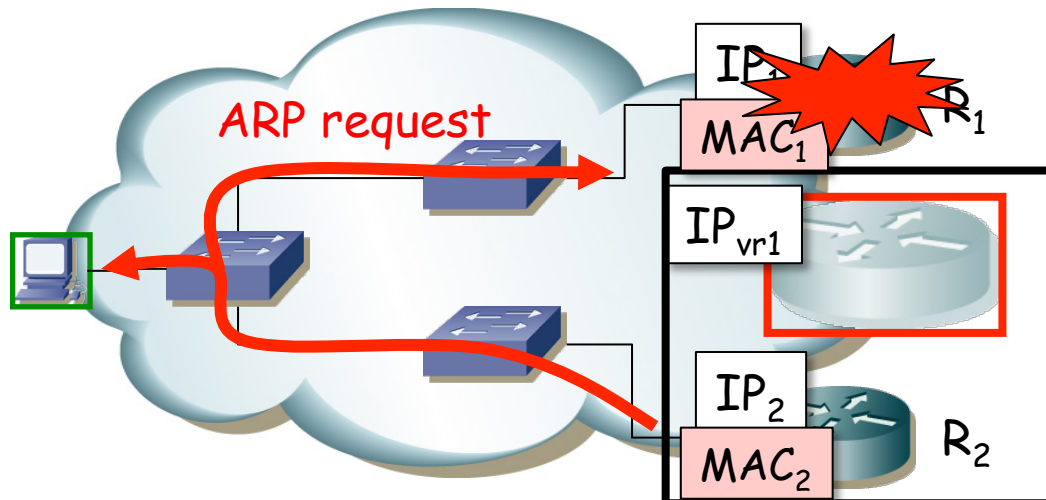
VRRP: Selección de maestro

- Se selecciona uno de los routers como maestro mediante el protocolo
- Seguirá mandando mensajes VRRP periódicos para que el otro sepa que sigue vivo (el otro se autodesigna de backup y no los envía más)
- Ese maestro responderá a los ARP request para la IP_{vr1}
- El ARP reply viene de la MAC física del interfaz del router pero
- **La dirección MAC en los datos del mensaje de ARP Reply será 00:00:5E:00:01:{VRID} (para IPv4) y es la que aprende el host**
- Está dentro del rango de direcciones MAC reservadas para IANA
- Además los mensajes VRRP vienen de la MAC virtual, con lo que los conmutadores aprenden el camino al maestro



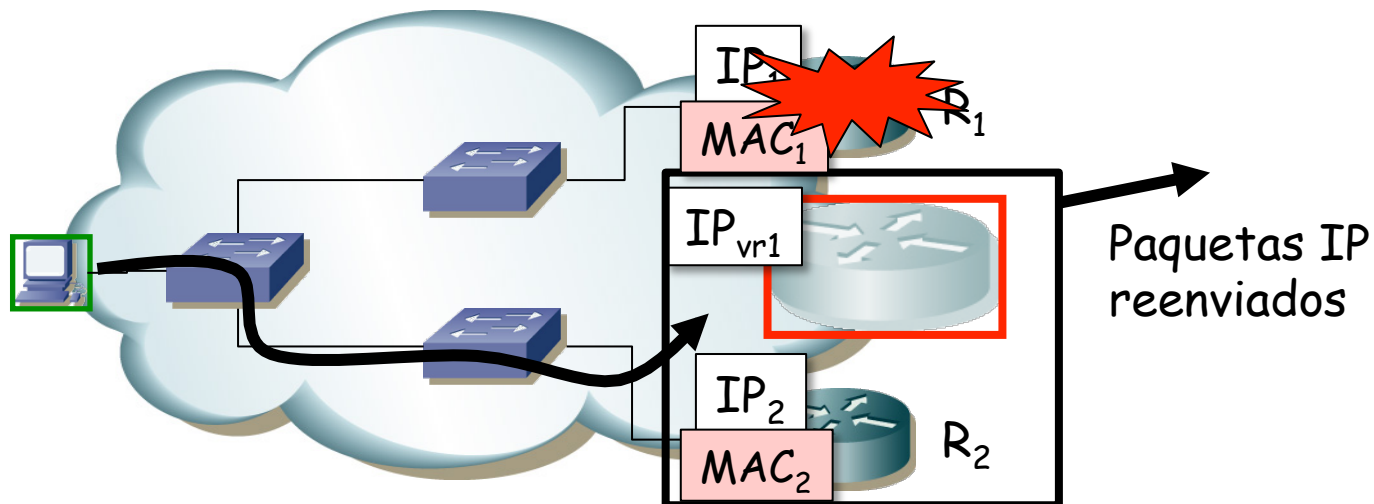
VRRP: Cómo funciona

- 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 (...)



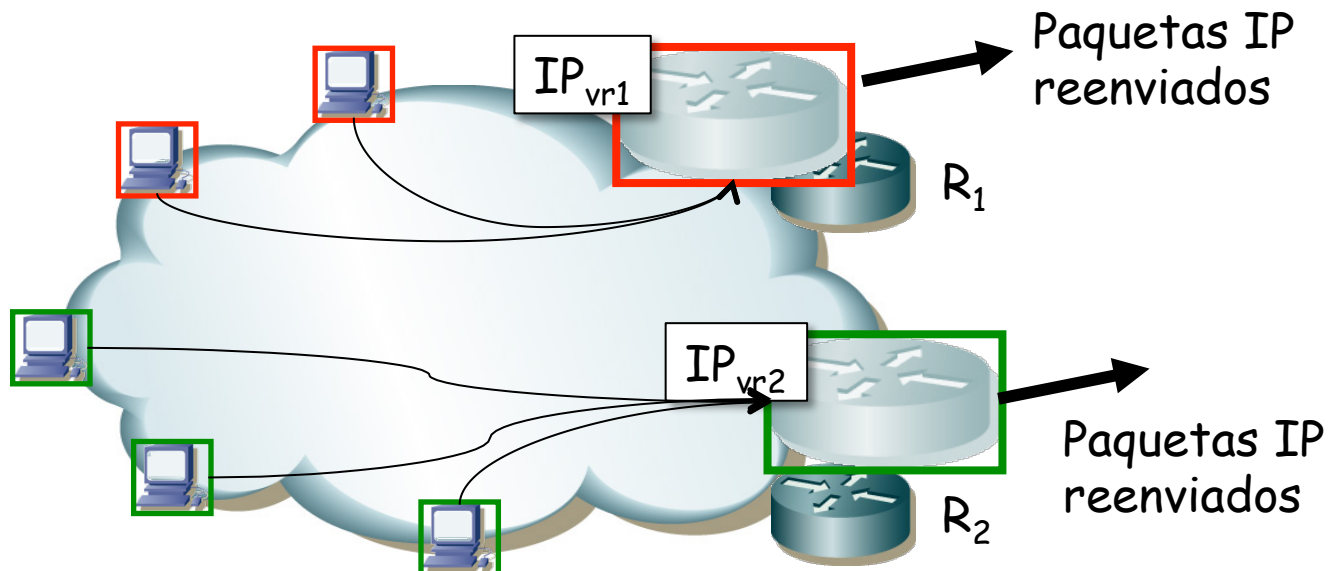
VRRP: Cómo funciona

- 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
- Pasa a enviar periódicamente mensajes VRRP
- 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
- Esto con HSRP se suele llamar MHSRP (Multiple HSRP)

