



DISEÑO DE REDES

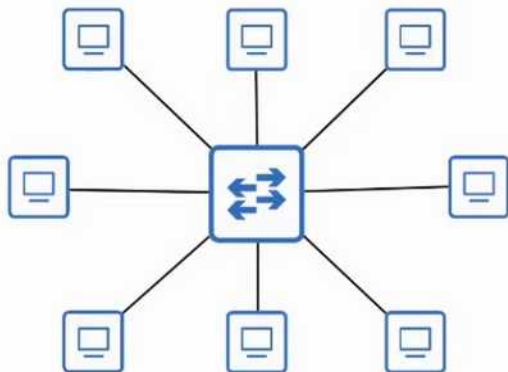


Campus LAN

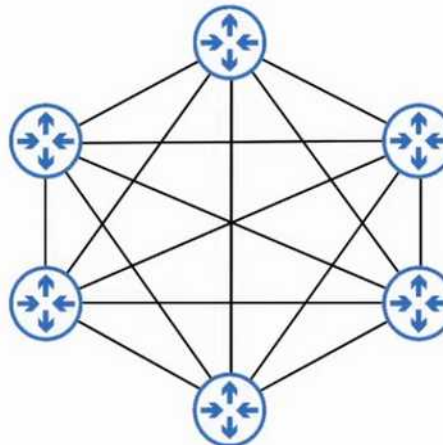
- Un conjunto de edificios próximos entre sí (distancias de LAN)
- Por ejemplo una empresa con varios edificios en un parque empresarial
- O el campus de una universidad centralizada
- Puede tener conexión a sedes remotas a través de una WAN (no es parte del campus)
- Alta disponibilidad es crucial
-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



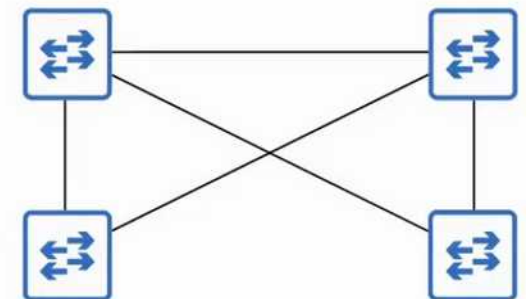
Star



Full Mesh



Partial Mesh





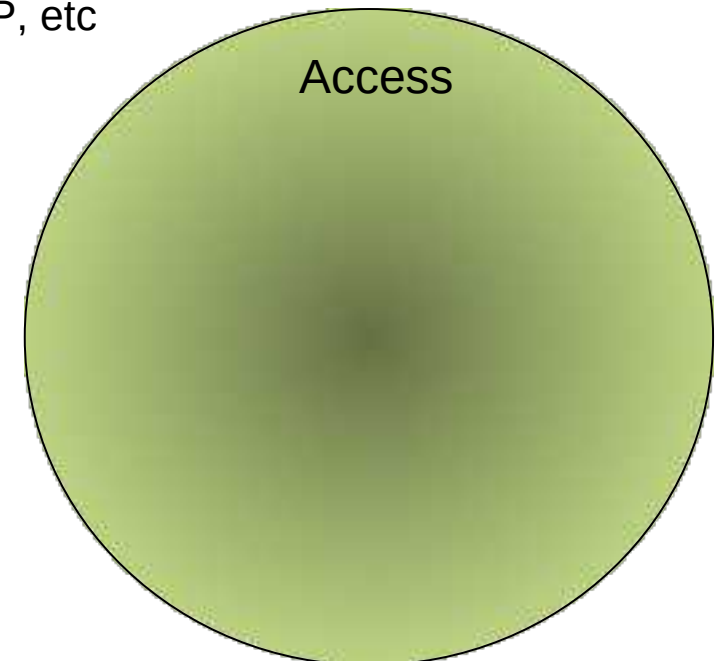
Terminología de 3 capas



Terminología para 3 capas

- **Access**

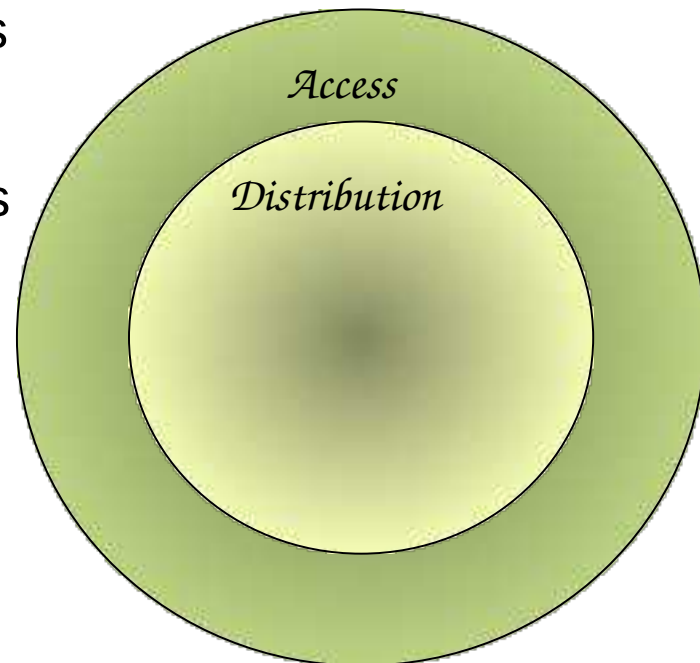
- Acceso de los usuarios a la red
- Usuarios locales o remotos
- Debe dar acceso solo a usuarios autorizados
- IDF (Intermediate Distribution Frame) Armario de cableado
- Hay que tener en cuenta:
 - Número de usuarios. Son switches con gran número de puertos
 - Deben tener PoE+ para WAP, telefonos IP, etc
 - Uso de VLANs
 - Redundancia
 - QoS marcado para voz por ejemplo
 - Seguridad :
Port Security, DAI, etc. Se hacen aquí



Terminología para 3 capas

- **Distribution/Agregación**

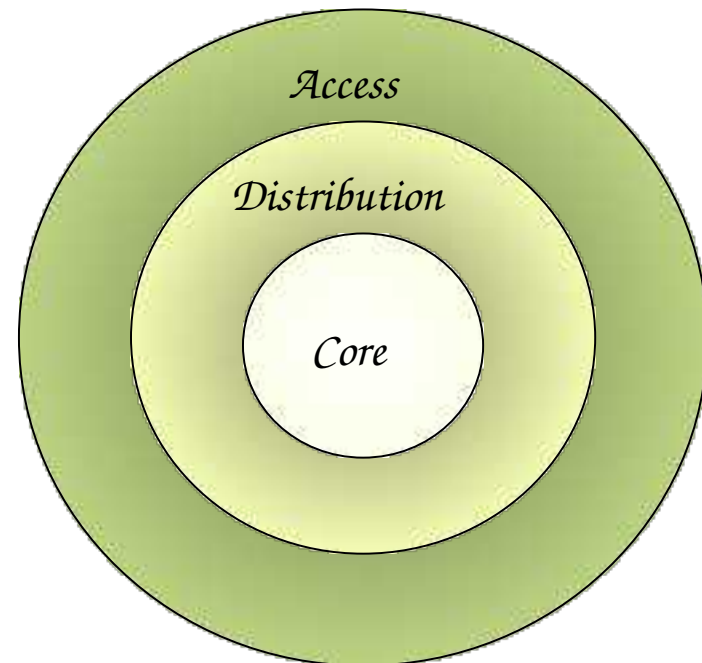
- Conexión entre grupos de trabajo y de ellos al núcleo
- Agrega accesos de baja velocidad en enlaces de alta velocidad
- Es el borde entre capa 2 y capa 3. Pueden correr STP y OSPF a la vez
- Suelen ser switches multicapa
- Ofrecer conexiones redundantes
- MDF (Main Distribution Frame)
- Los default-gateway de los hosts suelen ser los SVI de las VLAN de estos switches



Terminología para 3 capas

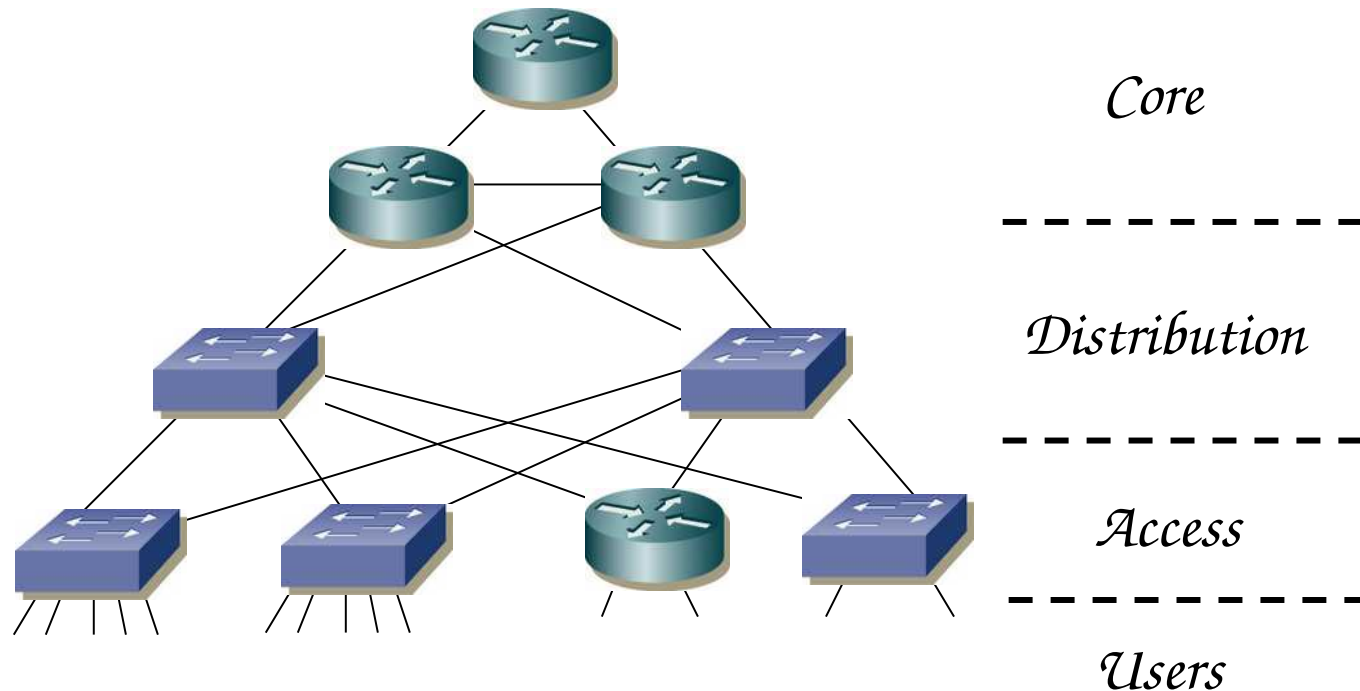
- **Core**


- 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. SOHO



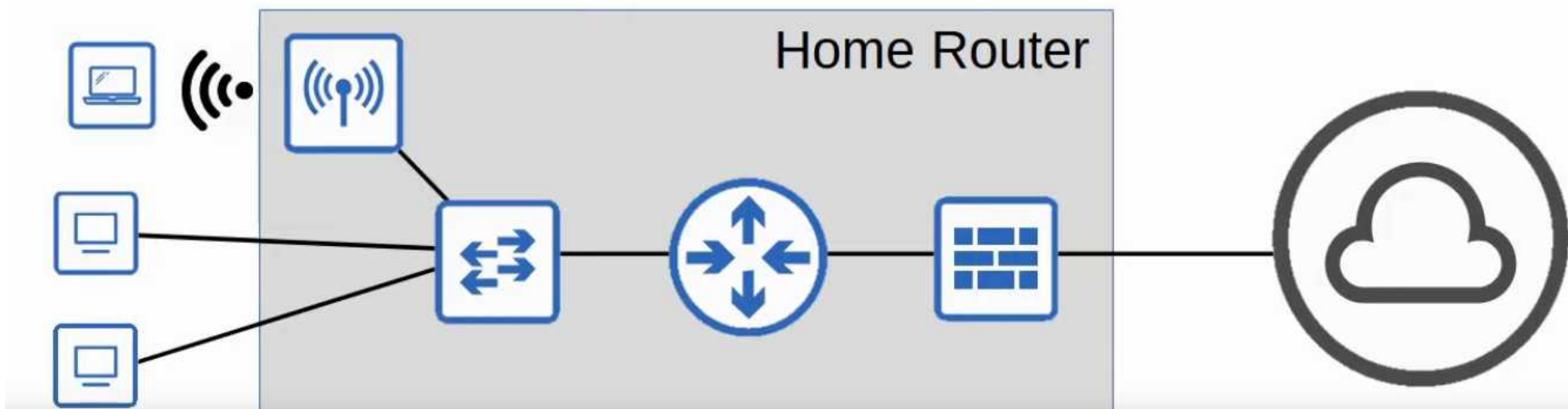
Pocos usuarios

- Unas pocas decenas de usuarios
- Cuidado con las diferentes “calidades” en los equipos (particulares, empresa, operadora...)
- Hoy en día al escritorio al menos 1000Mbps
- 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 (...)



SOHO y no tanto...

- 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
- En una red pequeña el router, switch y punto de acceso puede ser el mismo
- Hay empresas grandes con toda su infraestructura en la nube que tienen
Toda su infraestructura local del lado de un router doméstico, se conectan a su nube donde tienen todo lo necesario para su trabajo.



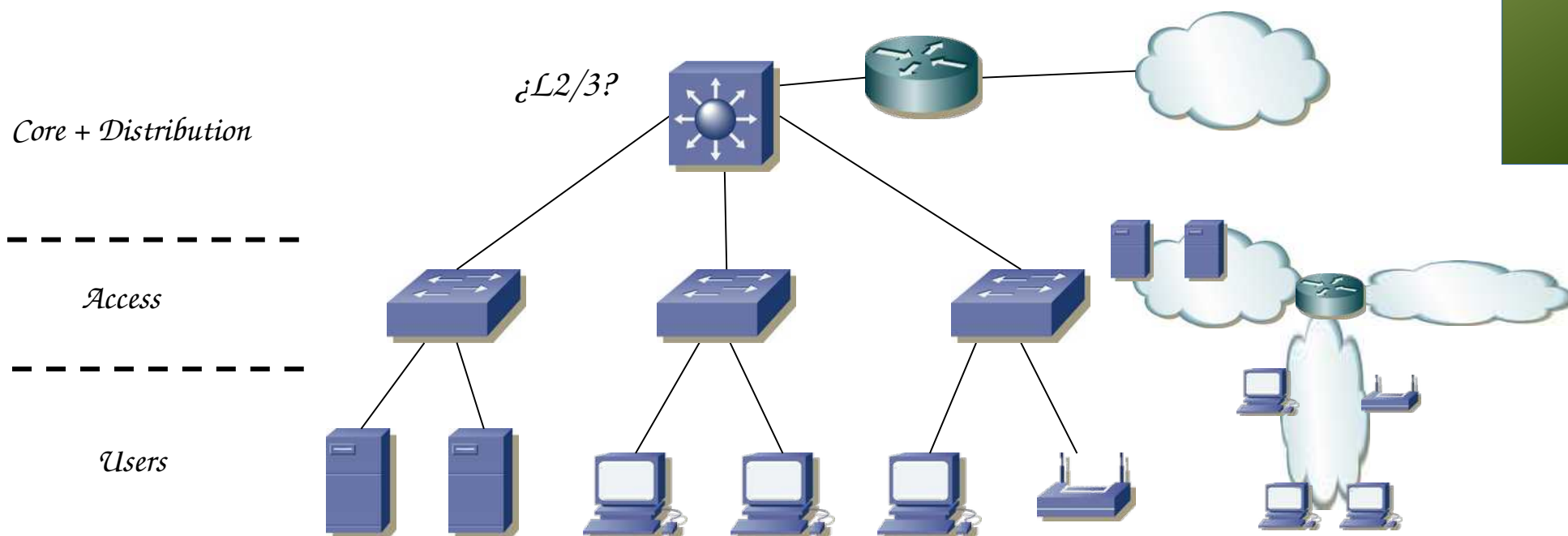


2 tier. Collapsed core



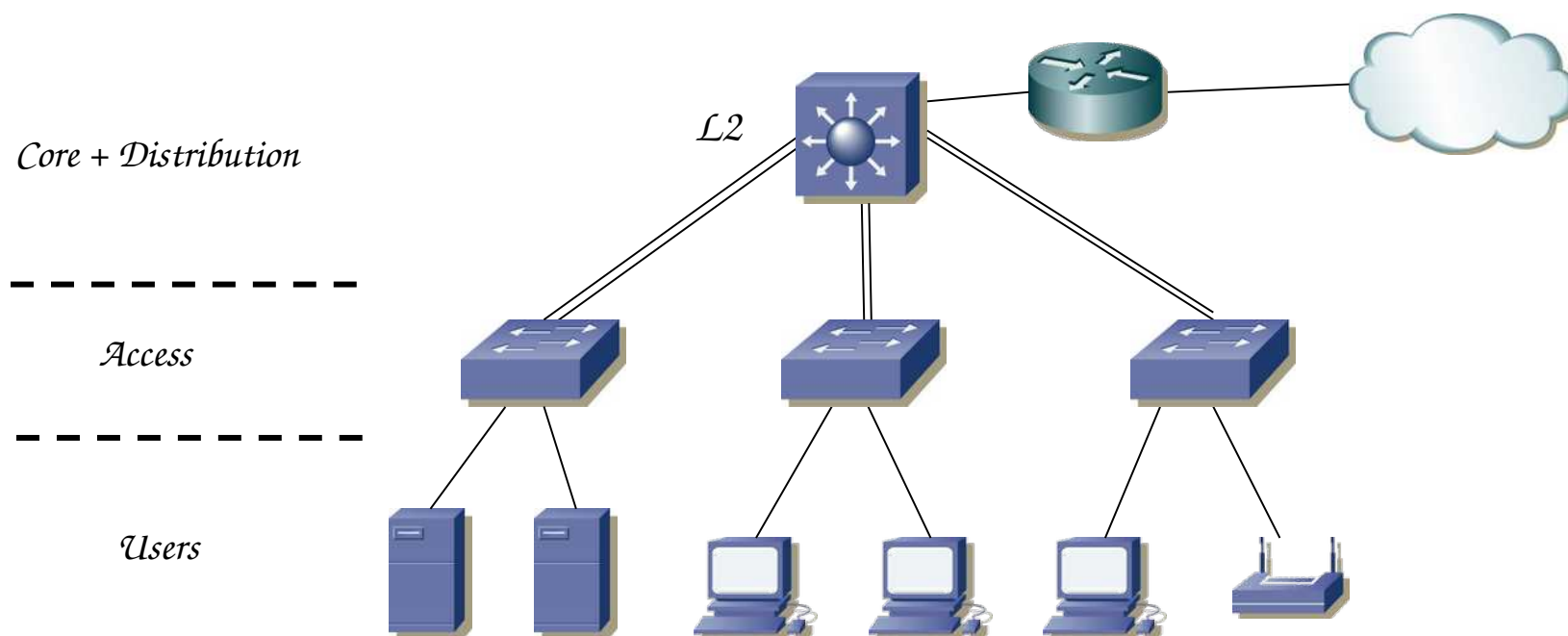
Collapsed core (2-tiers)

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



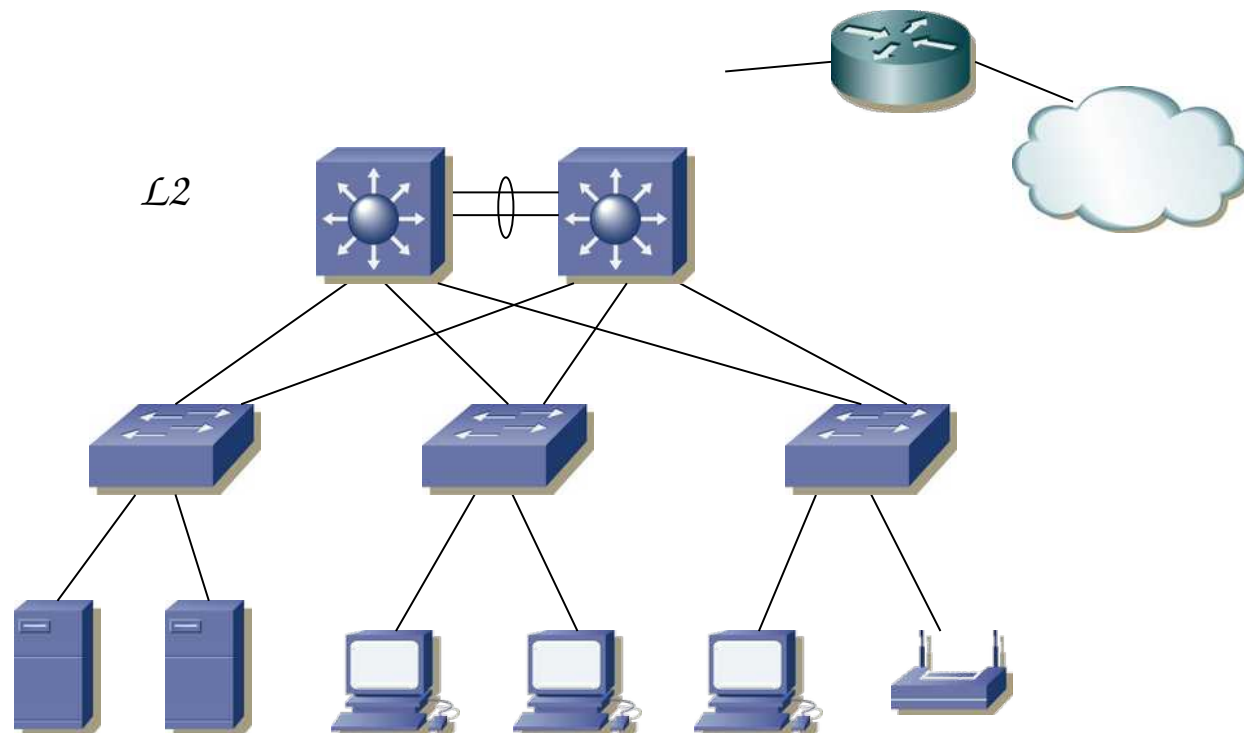
Collapsed core (2-tiers)

- 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



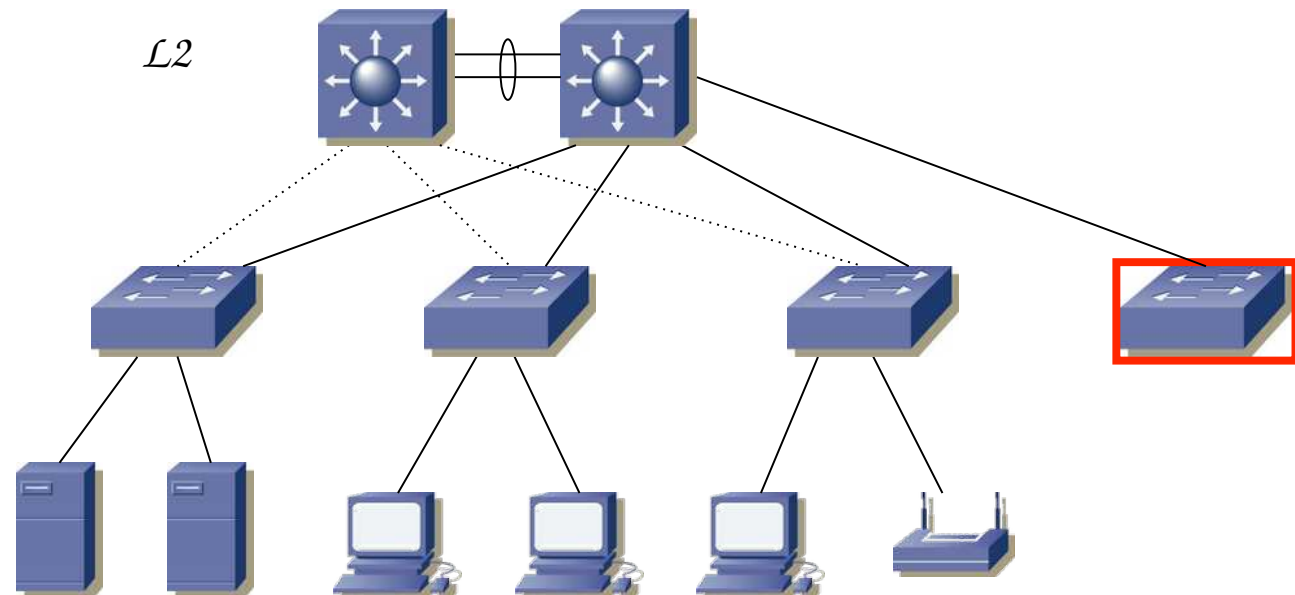
Redundant collapsed core

- 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 ? (...)



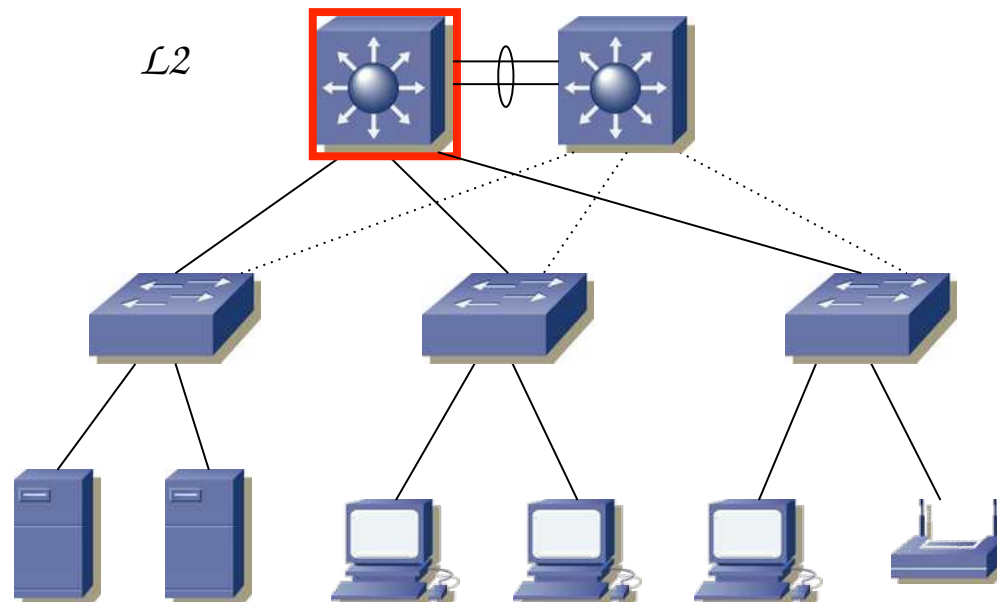
Redundant collapsed core

- 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 cambia todo el árbol, con la interrupción correspondiente



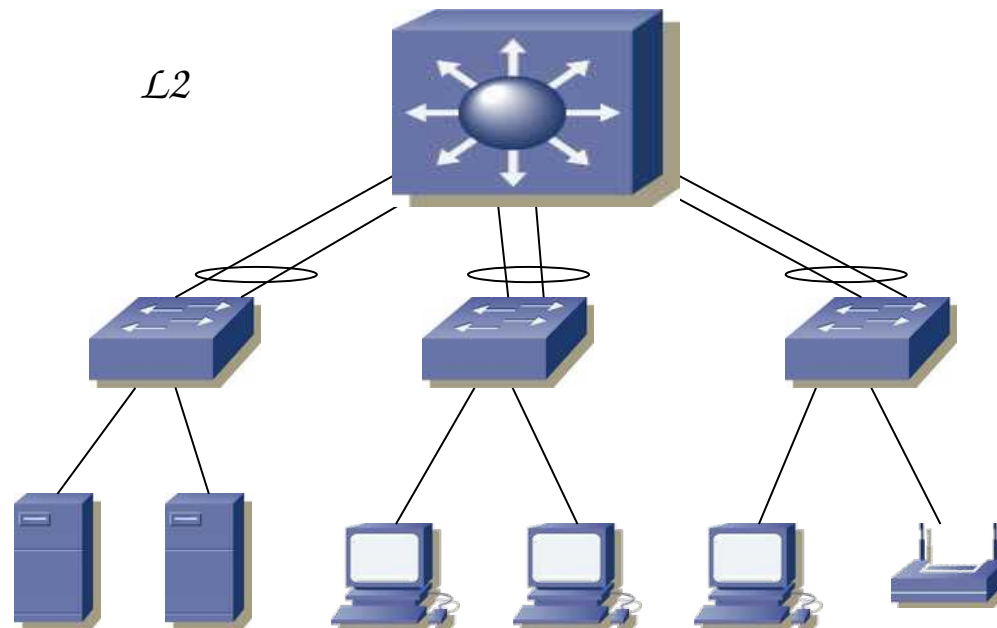
Redundant collapsed core

- 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 tocando las prioridades de los capa3
 - En este caso el LAG en la distribución no es muy útil si no hay nada más en el conmutador derecho



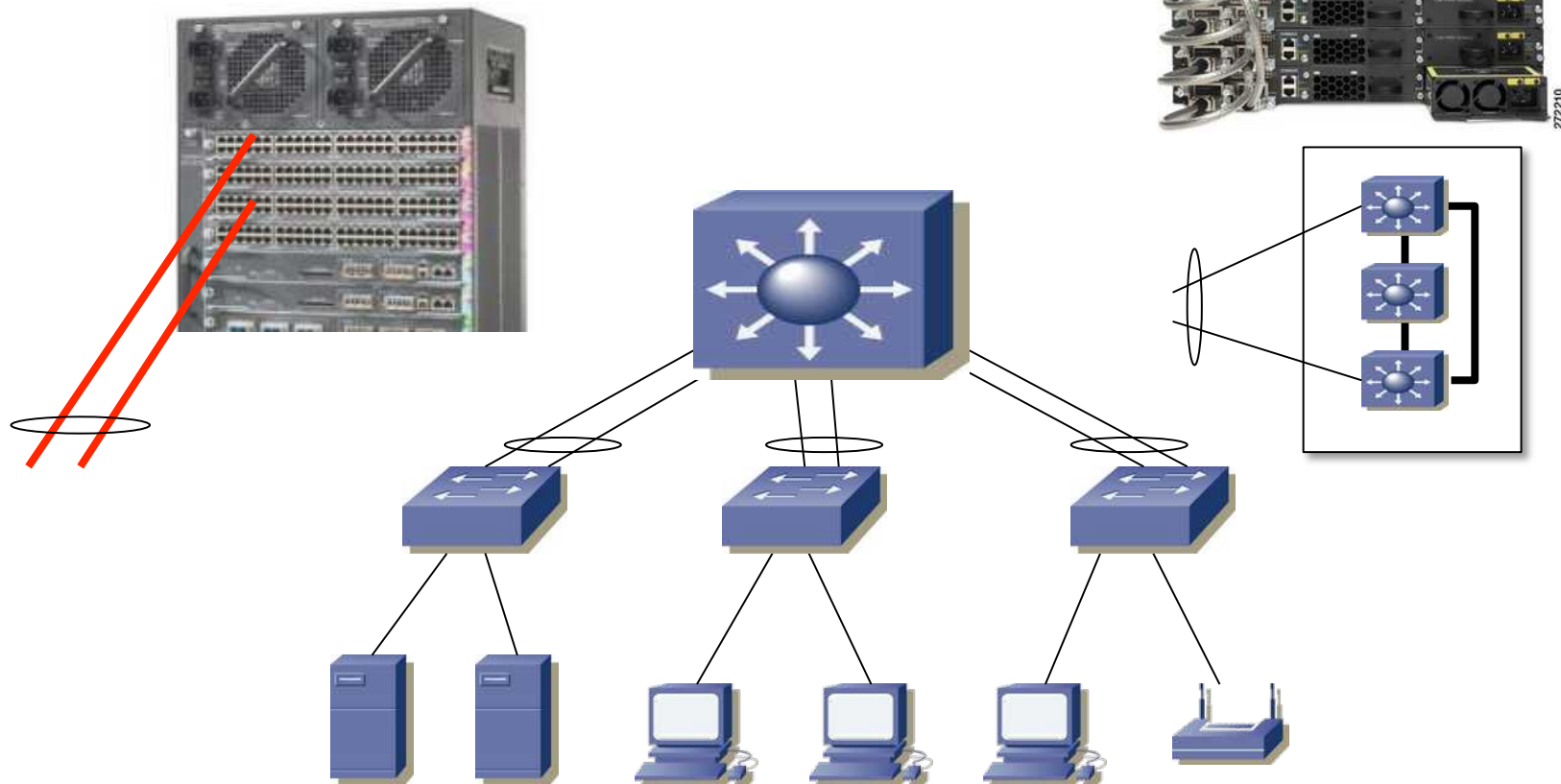
Redundant collapsed core

- 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”
- Se comportan como un solo conmutador de cara a STP ya no hay bucles
- Los enlaces al acceso se convierten en agregados
- Conmutadores de gama alta



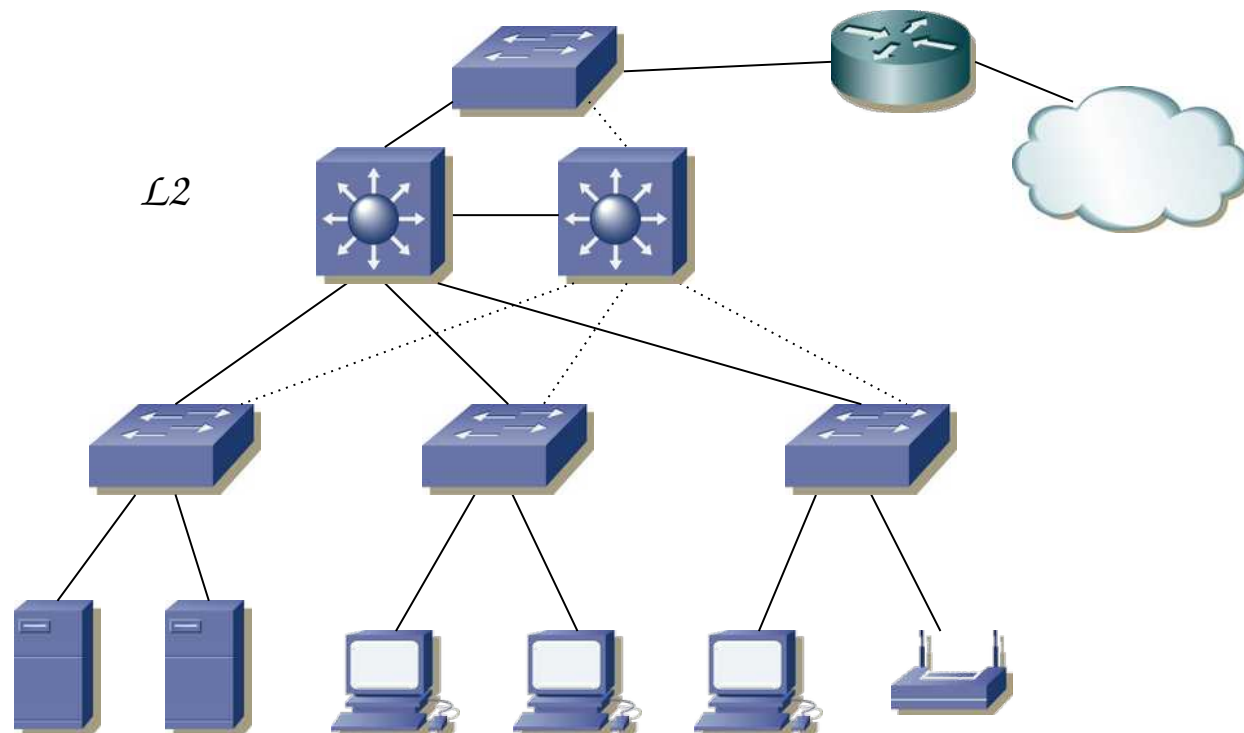
Redundant collapsed core

- 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 (stack) redunda datos Y alimentación



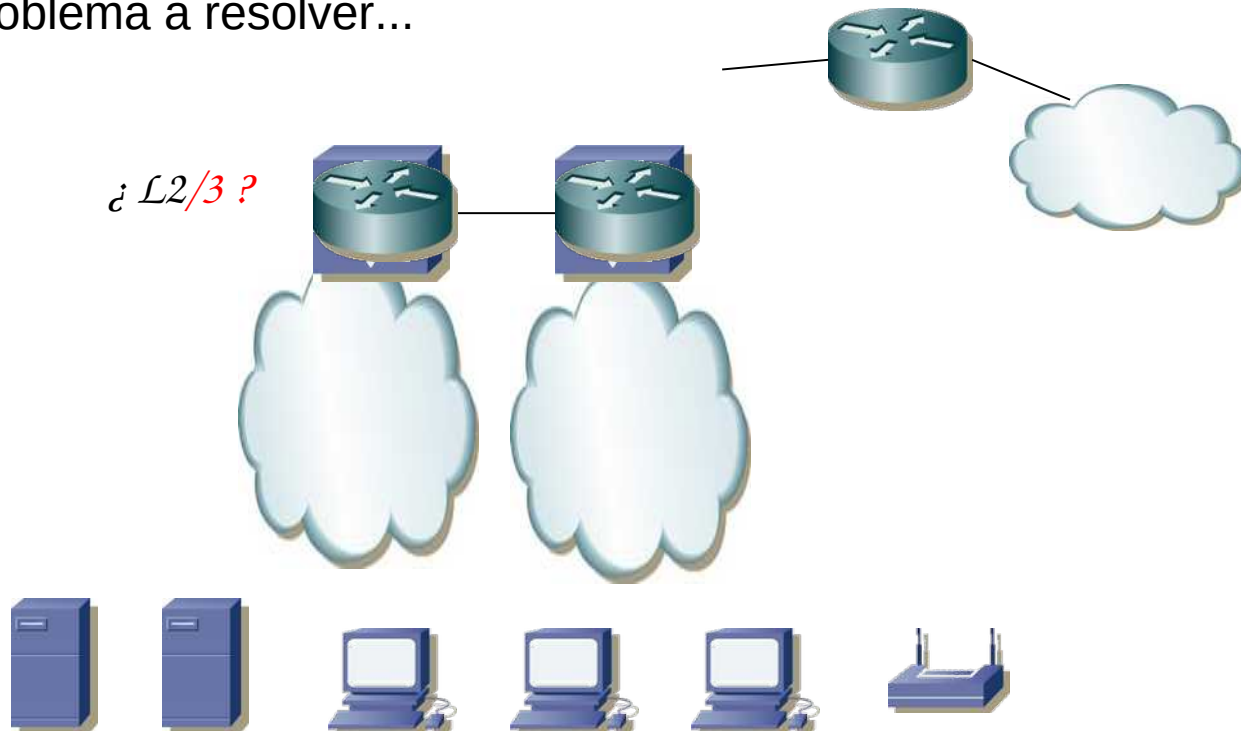
Enrutamiento

- 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?
- ¿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...



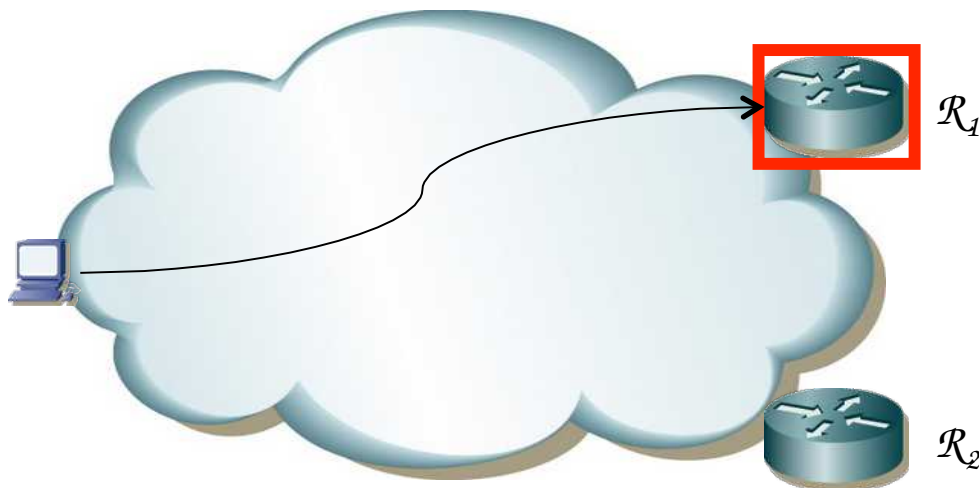


FHRP



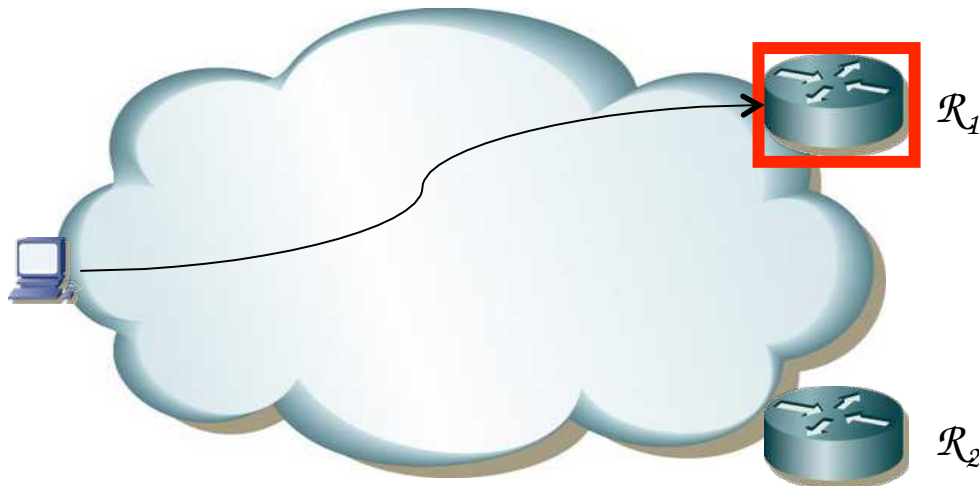
FHRP

- *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



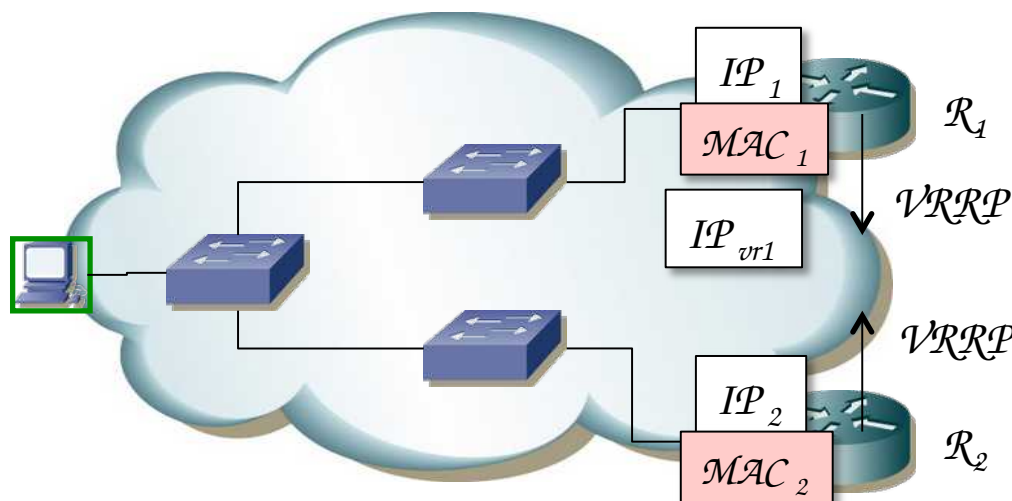
FHRP

- 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.



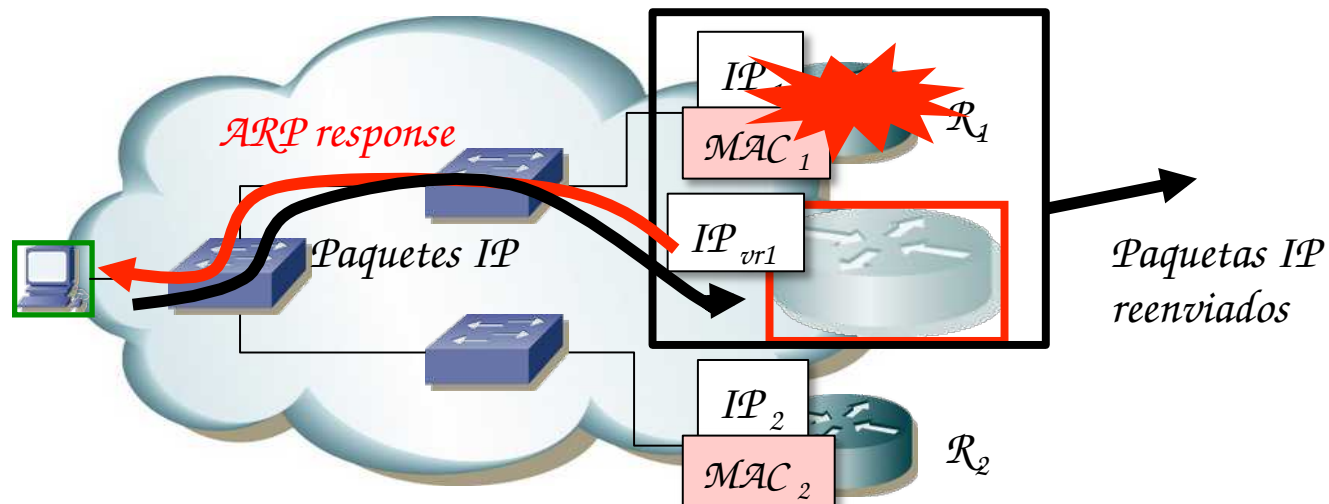
VRRP: Selección de maestro

- 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)



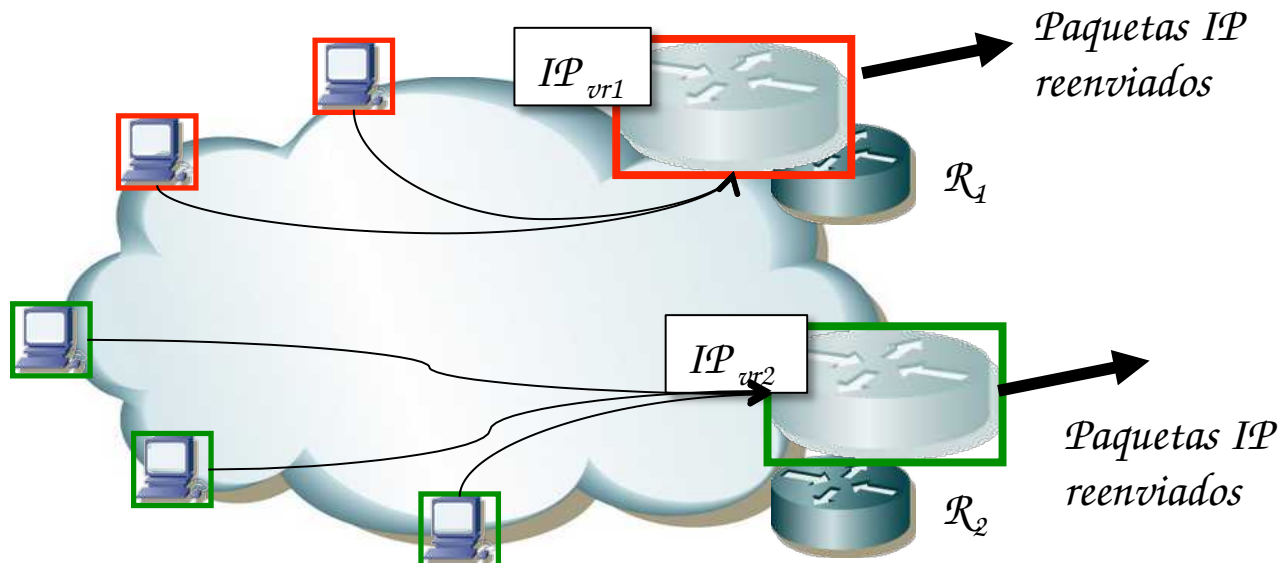
VRRP: Selección de maestro

- 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
- 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 (...)



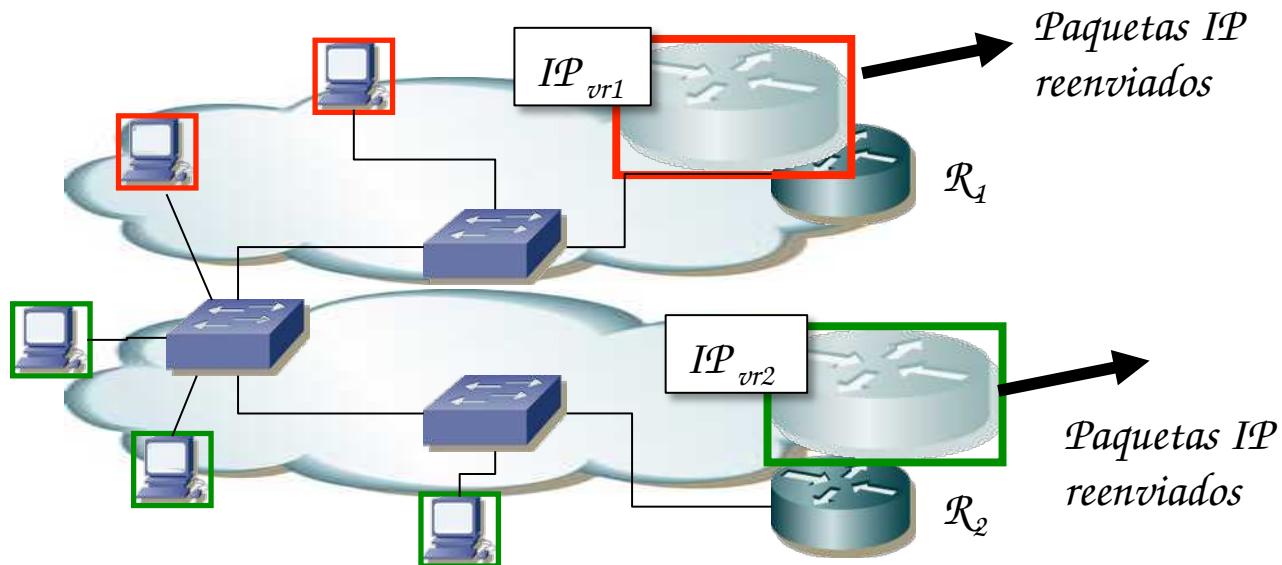
VRRP y reparto de carga

- 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



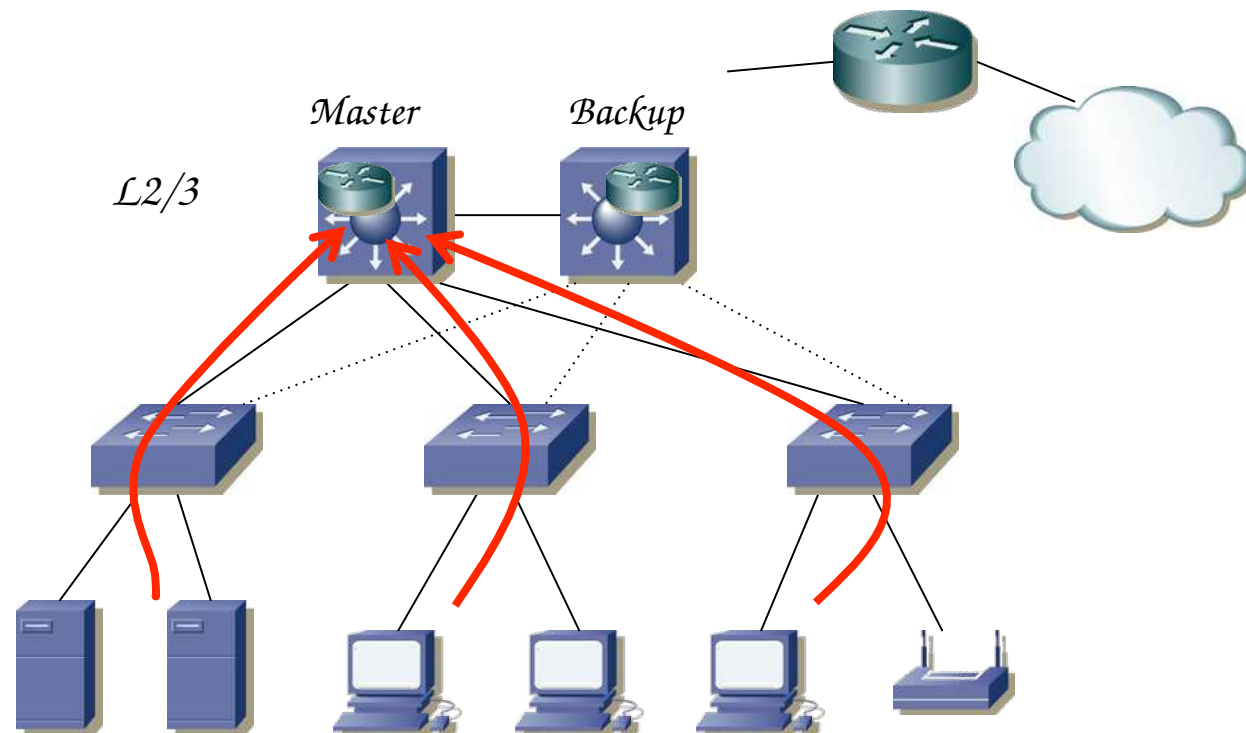


Collapsed core y FHR



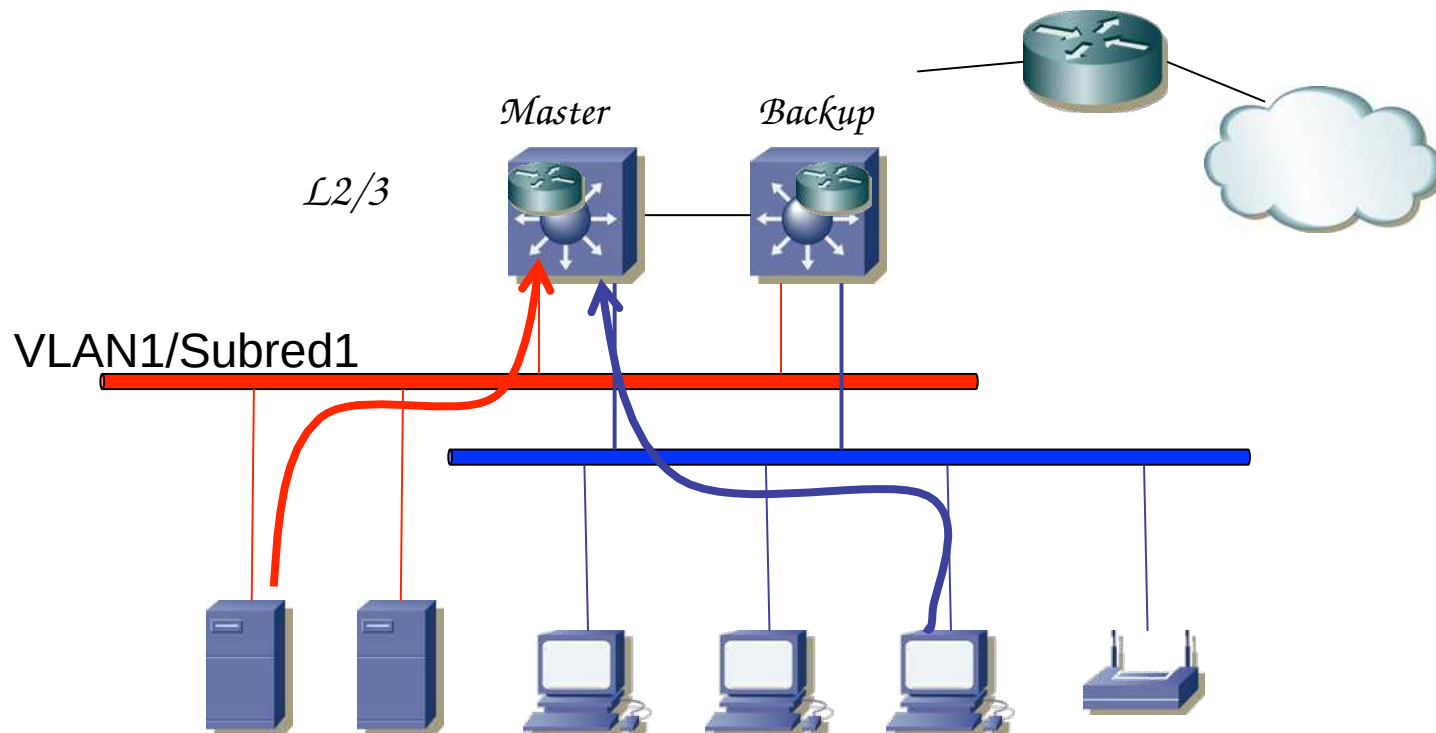
Collapsed core y FHR

- 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



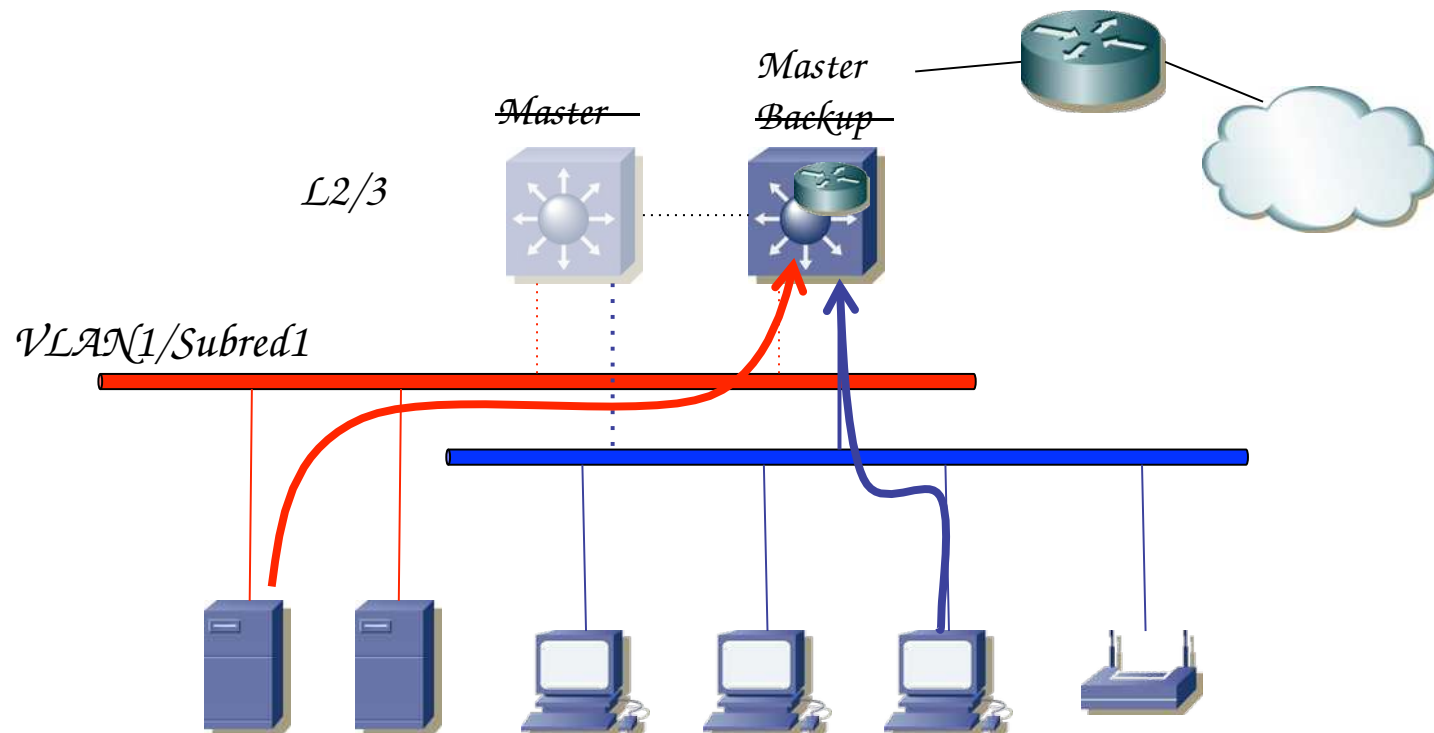
Collapsed core y FHR

- 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

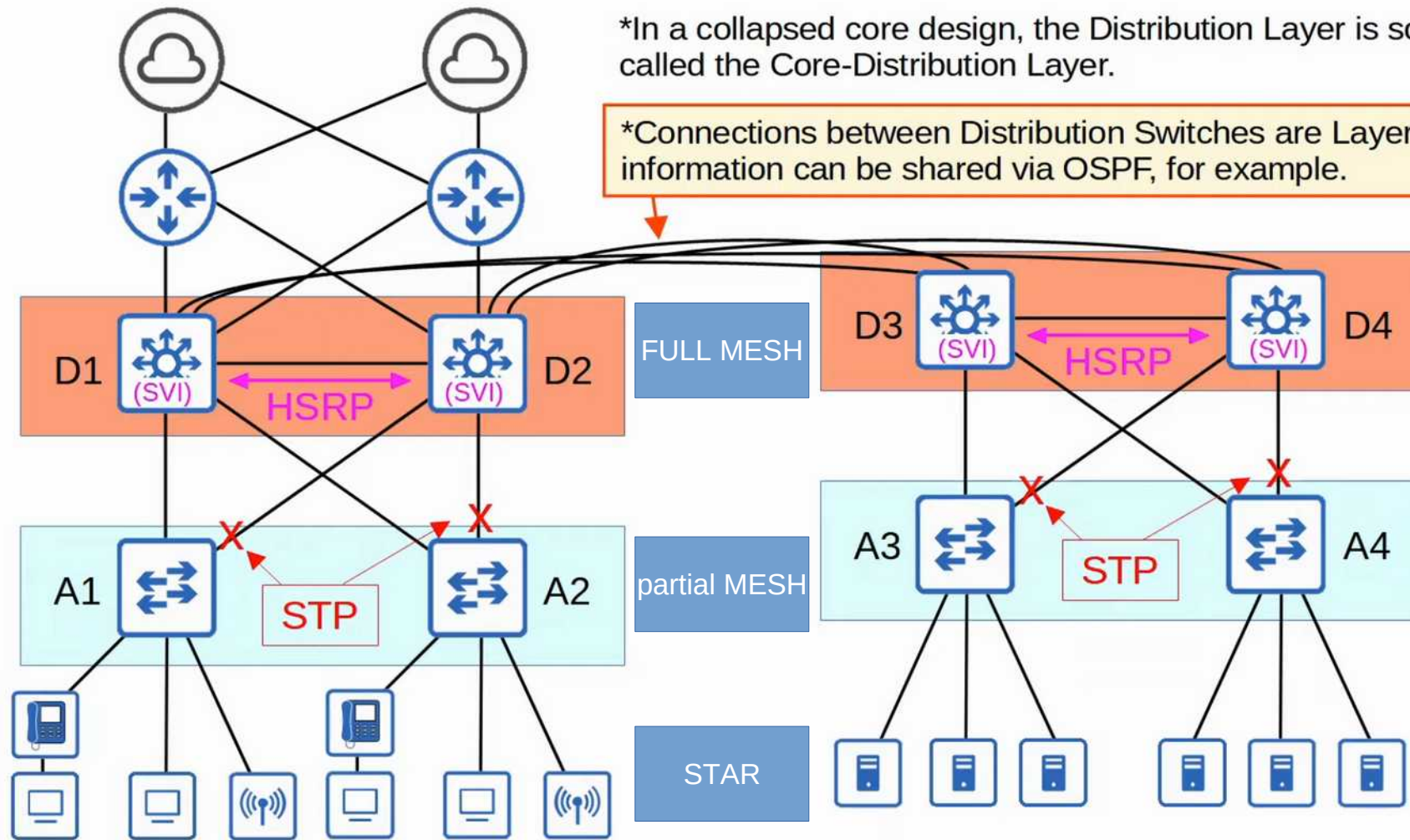


Collapsed core y FHR

- ¿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...

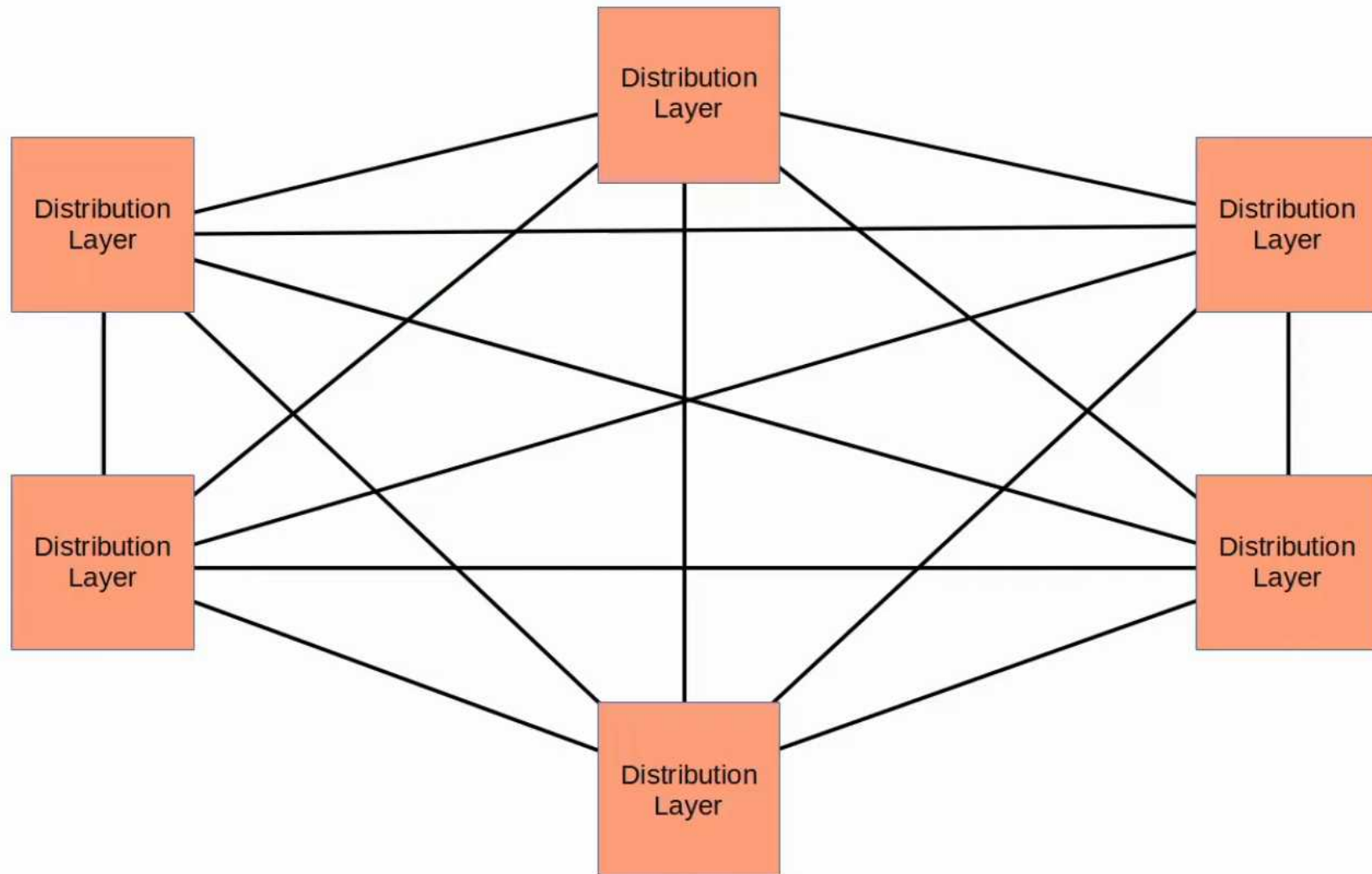


Ampliación de la red



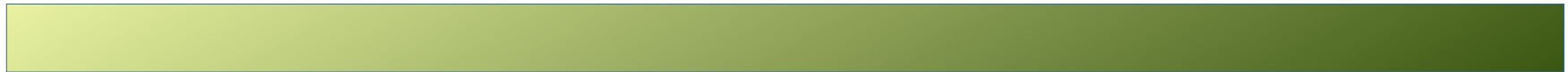
Ampliación de la red

Si el número de capas de distribución aumenta la red se hace inmanejable. Si hay por ejemplo Varios edificios, Cisco recomienda introducir una capa Core cuando hay 3 o más centros De distribución





3 tier



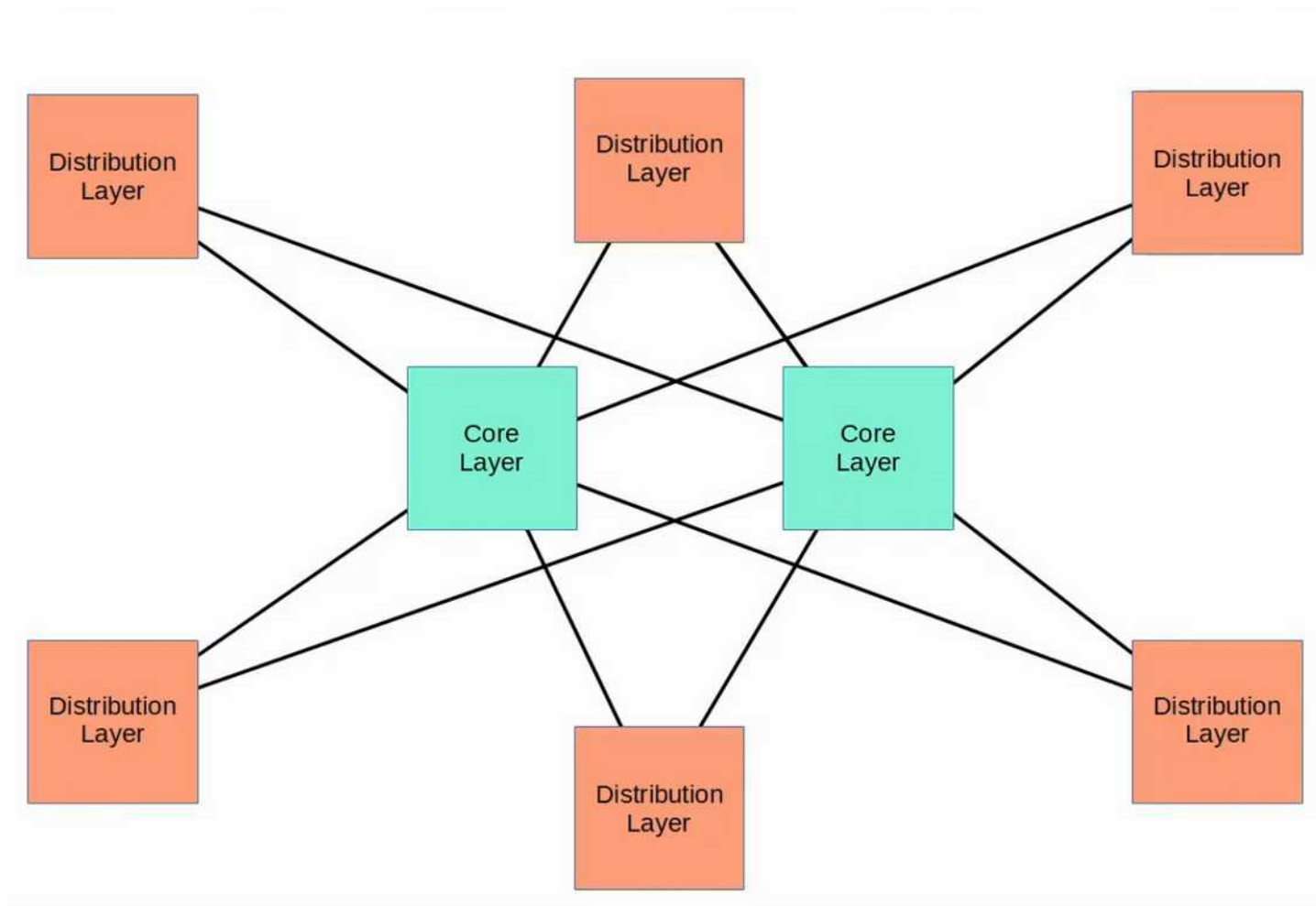
Se añade un Core que hace que elimine el full mesh entre todos los switches de las capas de distribución pero con gran redundancia.

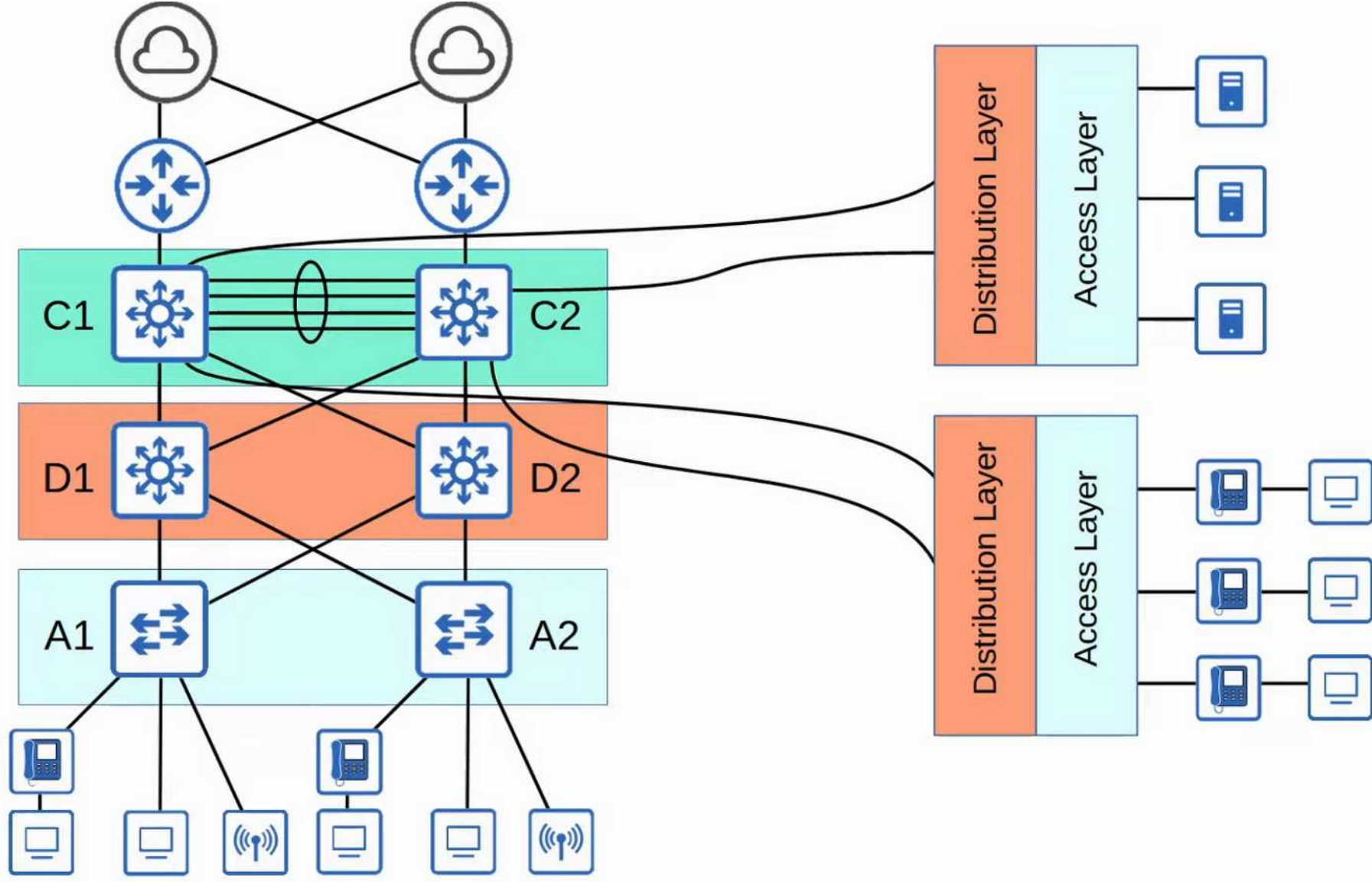
El core tendrá los switches más rápidos, de más capacidad y más modernos.

Está focalizado en la velocidad

Se deben evitar operaciones CPU intensivas como las de seguridad, QoS etc.

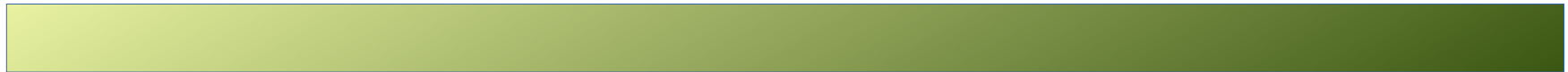
Todo es capa3 nunca STP







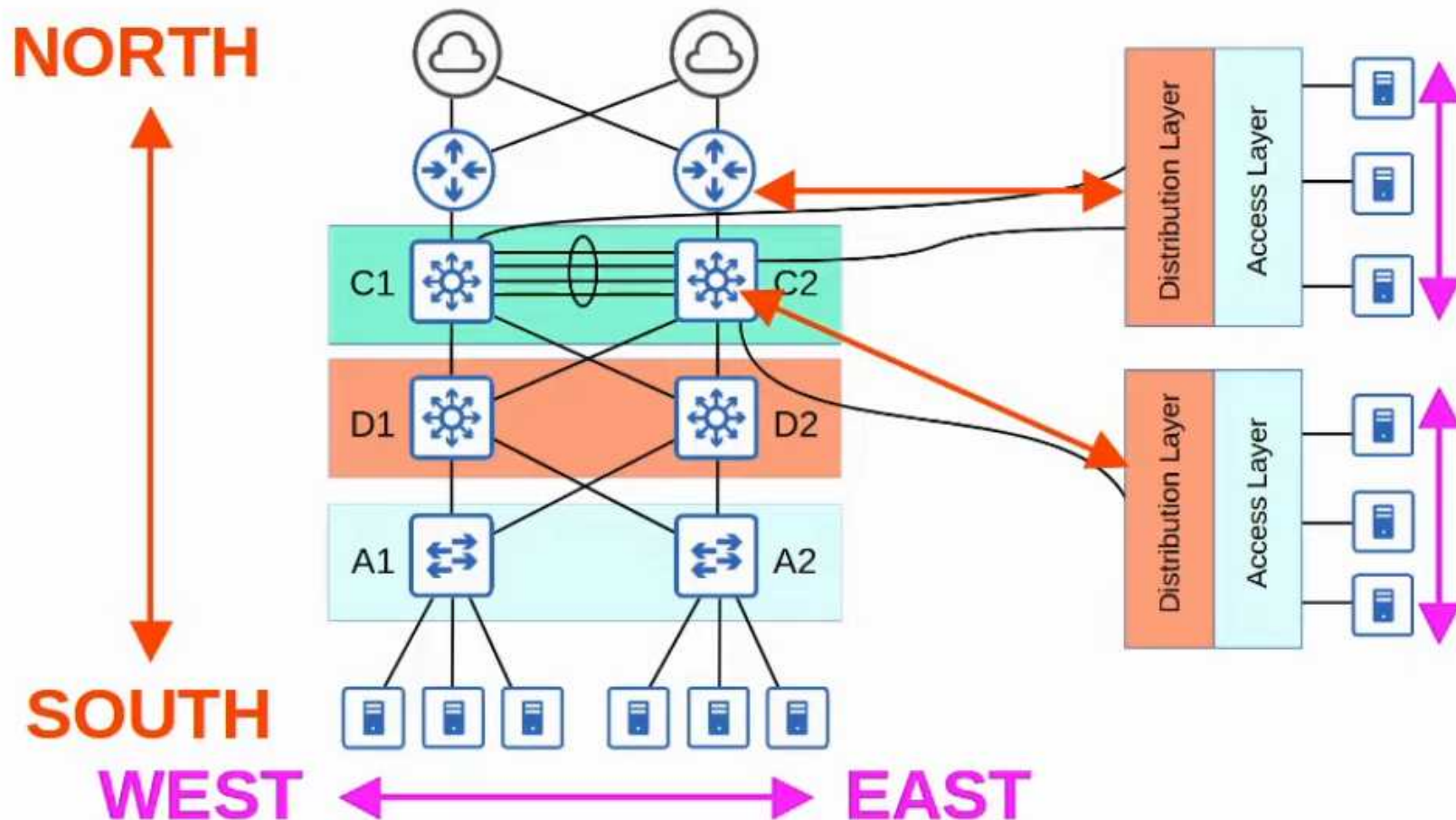
Spine Leaf



Tráfico Norte/Sur Este/Oeste

La arquitectura en 3 niveles funciona bien si el tráfico es Norte/Sur, o sea, de los usuarios hacia Internet o un servidor colocado en la capa de distribución. La arquitectura tradicional está destinada a que el tráfico vaya de A->D->C->Internet

Con el aumento de la computación distribuida, esto ya no es cierto, las aplicaciones se instalan en multiples servidores de virtualización o en contenedores lo que hace que la mayor parte de los datos se mueva de este a oeste, es decir, de manera horizontal entre servidores



Spine Leaf

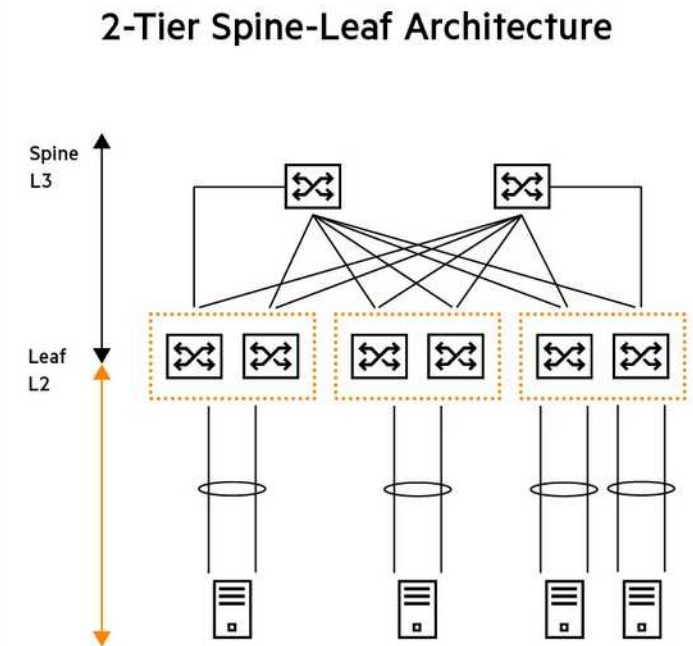
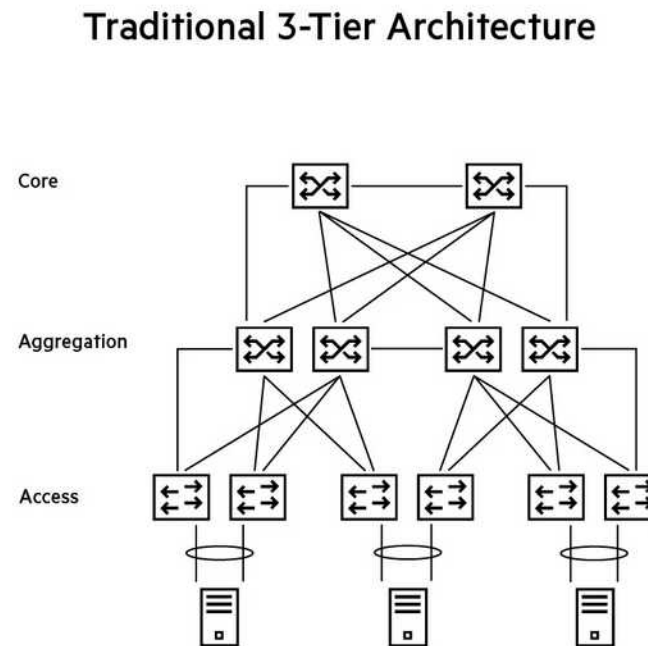
Una arquitectura spine-leaf es una topología de red de centro de datos que consta de dos capas de conmutación: una «spine» o columna vertebral y una «leaf» u hoja. La capa leaf consta de conmutadores de acceso que agregan tráfico de los servidores y se conectan directamente a la spine o al núcleo de la red. Los conmutadores de spine interconectan todos los conmutadores de leaf en una topología de malla completa.

Tradicionalmente, las redes de los centros de datos se basaban en un modelo de tres niveles:

- Los conmutadores de acceso se conectan a los servidores
- Los conmutadores de agregación o distribución proporcionan conexiones redundantes a los de acceso
- Los conmutadores centrales o core proporcionan un transporte rápido entre los conmutadores de agregación

En el nivel más básico, una arquitectura spine-leaf concentra uno de estos niveles. Otras diferencias comunes en las topologías spine-leaf incluyen:

- La eliminación del protocolo de árbol de extensión (STP)
- Se necesita comprar y administrar más cableado, dada la mayor cantidad de interconexiones
- Una infraestructura de escalabilidad horizontal en lugar de vertical



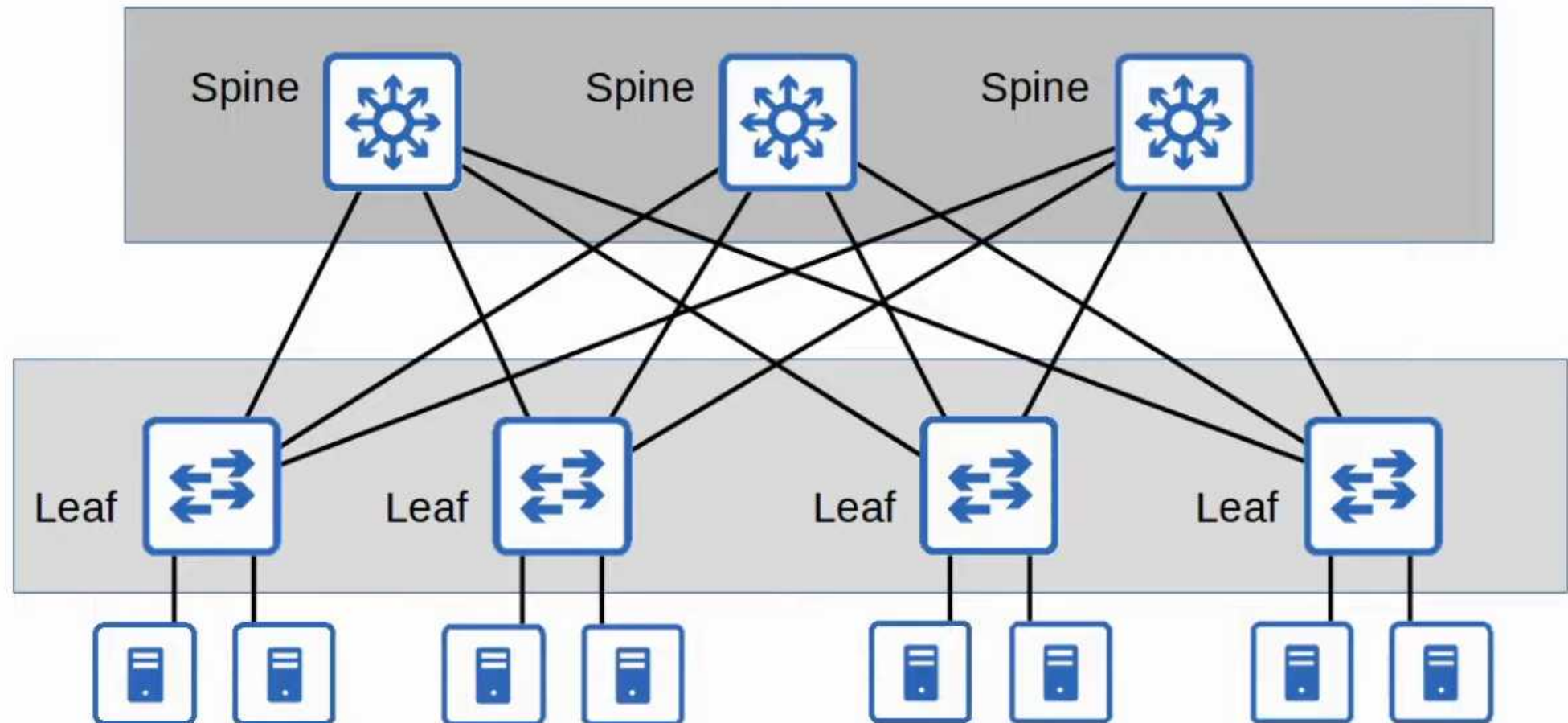
Se parece a la arquitectura en dos niveles que hemos visto antes, pero cumple estas reglas.

1. Todos los switches Spine se conectan con todos los switches hoja en una malla completa
2. Todos los switches Leaf se conectan con todos los switches Spine
3. Ni los Spine ni los Leaf se comunican entre si
4. Los Servidores sólo se pueden conectar a los Leaf

El camino que siguen los paquetes se distribuye aleatoriamente entre los Spine de forma que el tráfico se distribuye.

Todos los Servidores están separados por un salto. Si queremos más servidores añadimos Leafs y si queremos más ancho de banda añadimos Spines.

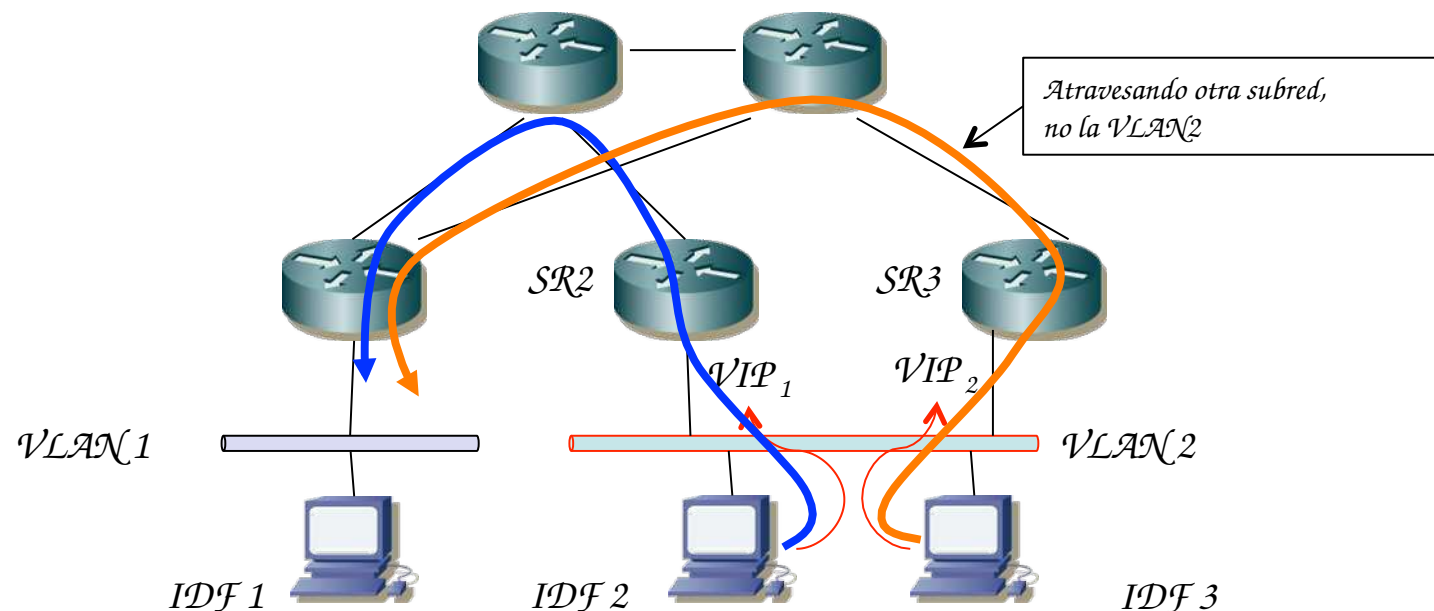
Se usan arquitecturas nuevas como VXLAN, y soluciones como ACI de Cisco y su controlador APIC



Layer 3 Collapsed Core

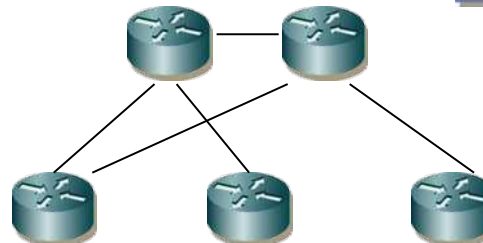
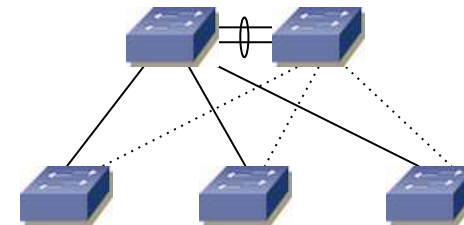
Ejemplo:

- 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



Resumen sobre protección

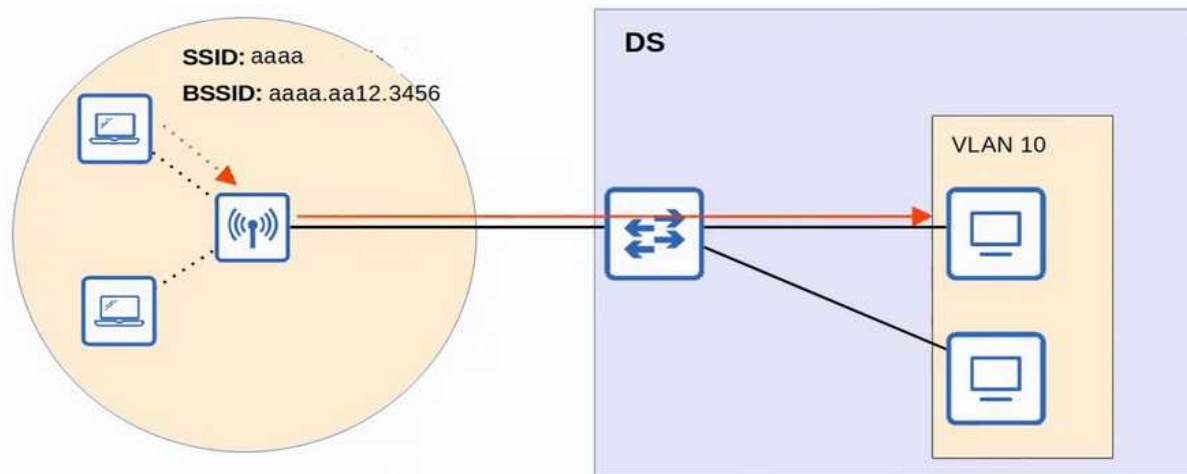
- En el hardware del host
 - NICs dobles
- En el hardware interno del conmutador
 - Controladora (supervisor module)
 - Fuentes de alimentación
 - Sistemas de refrigeración
- En el hardware de conmutación
 - Equipos replicados y agregados en un conmutador virtual
 - Equipos apilados
 - Redundancia de 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



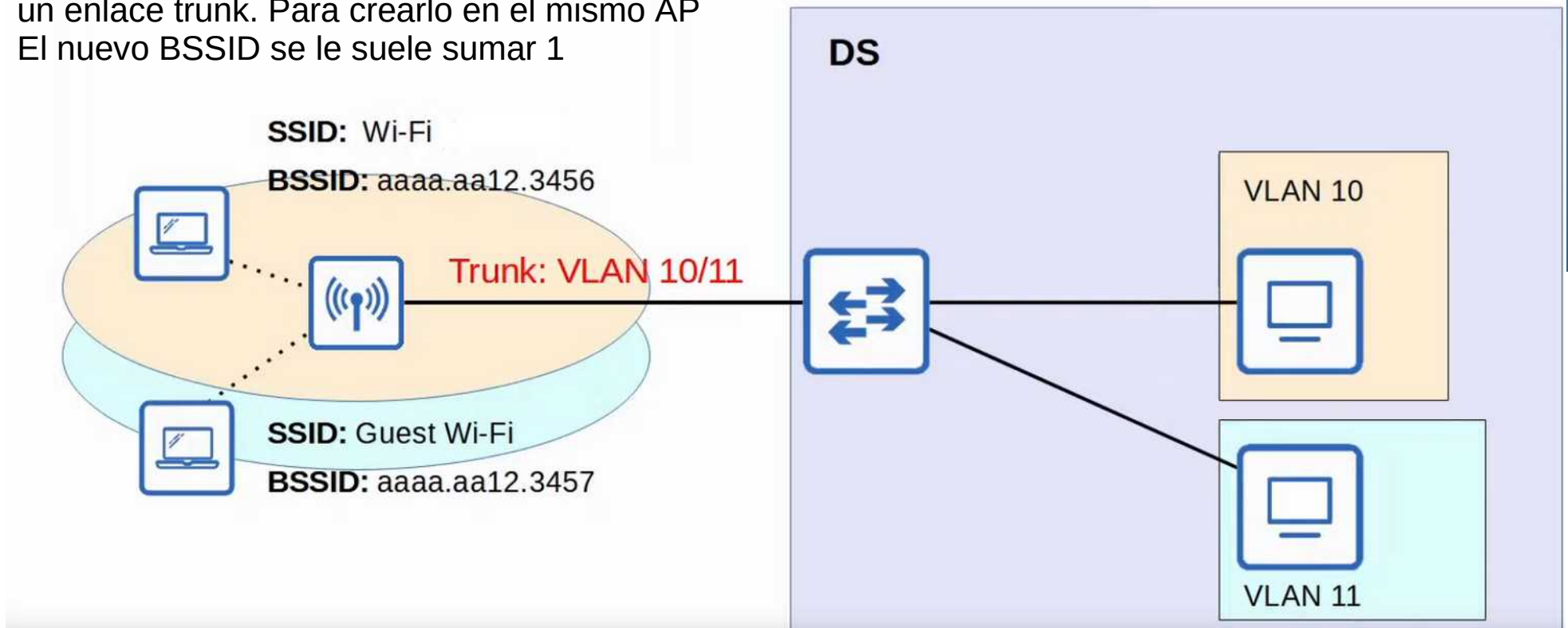


Arquitecturas Wireless





Cada SSID tiene un BSSID distinto, se mapea en una VLAN distinta y se une al punto de acceso por un enlace trunk. Para crearlo en el mismo AP
El nuevo BSSID se le suele sumar 1



Asociación

Los Access Points (APs) sirven como puente entre dispositivos inalámbricos y la red cableada. Pero para que un cliente (station) envíe tráfico a través del AP, primero debe asociarse con él. Tres estados de conexión:

No autenticado ni asociado (sin conexión).

Autenticado pero no asociado (el cliente está autenticado pero aún no puede enviar tráfico).

Autenticado y asociado (el cliente puede enviar tráfico).

Pasos del proceso de asociación:

Probe Request & Probe Response (Sondeo)

El cliente envía un Probe Request para descubrir APs disponibles.

El AP responde con un Probe Response indicando que está disponible.

O el cliente puede usar escaneo pasivo, escuchando Beacon Frames enviados periódicamente por el AP.

Autenticación

El cliente envía credenciales (ej. contraseña) y el AP lo autentica.

Ahora está en el Estado 2 (Autenticado pero no asociado).

Asociación

El cliente envía un Association Request.

El AP responde con un Association Response.

Si es exitoso, el cliente pasa al Estado 3 (Autenticado y asociado) y puede enviar tráfico.



There are two ways a station can scan for a BSS:

→ **Active scanning**: The station sends probe requests and listens for a probe response from an AP.

→ **Passive scanning**: The station listens for **beacon** messages from an AP. Beacon messages are sent periodically by APs to advertise the BSS.

Tipos de mensajes

Hay tres tipos principales de mensajes 802.11:

Management Frames (Tramas de Gestión). Se usan para administrar la BSS (Basic Service Set).

Ejemplos:

Beacon: Anuncia la presencia del AP.

Probe Request/Response: Descubrimiento de redes.

Authentication

Association request y association response.

Control Frames (Tramas de Control). Gestionan el acceso al medio inalámbrico (RF).

Ejemplos:

RTS/CTS (Request to Send / Clear to Send): Control de colisiones.

ACK (Acknowledgement): Confirma recepción de tramas.

Data Frames (Tramas de Datos) Transportan datos reales (ej. tráfico de usuario).

Tipos de AP's

Existen tres modelos principales de despliegue de Aps:

Autonomous APs (APs Autónomos)

Son independientes, no requieren un Wireless LAN Controller (WLC).

Lightweight APs (APs Ligero + WLC)

Usan arquitectura split-MAC:

El AP maneja operaciones en tiempo real (RF, encriptación).

El WLC gestiona configuración, autenticación, roaming, etc.

Cloud-based APs (APs en la Nube, ej. Cisco Meraki)

Autonomous APs con gestión centralizada en la nube.

El tráfico de datos NO pasa por la nube, solo la gestión.

AP's autónomos

Autonomous APs (APs Autónomos)

Son independientes, no requieren un Wireless LAN Controller (WLC).
Se configuran individualmente (vía consola, SSH, HTTP/HTTPS).

Problemas:

No escalables en redes grandes (configuración manual de cada AP).

Necesitan una IP para ser configurados remotamente

Se configura todo en ellos por separado:
seguridad, QoS, canal, frecuencia, etc

Requieren enlaces trunk en switches para múltiples VLANs.
Realmente aunque sólo tengamos una SSID también debemos usar enlaces Trunk porque si separamos el tráfico de configuración de switches, etc en la VLAN de administración vamos a necesitar que ese tráfico llegue a los AP's

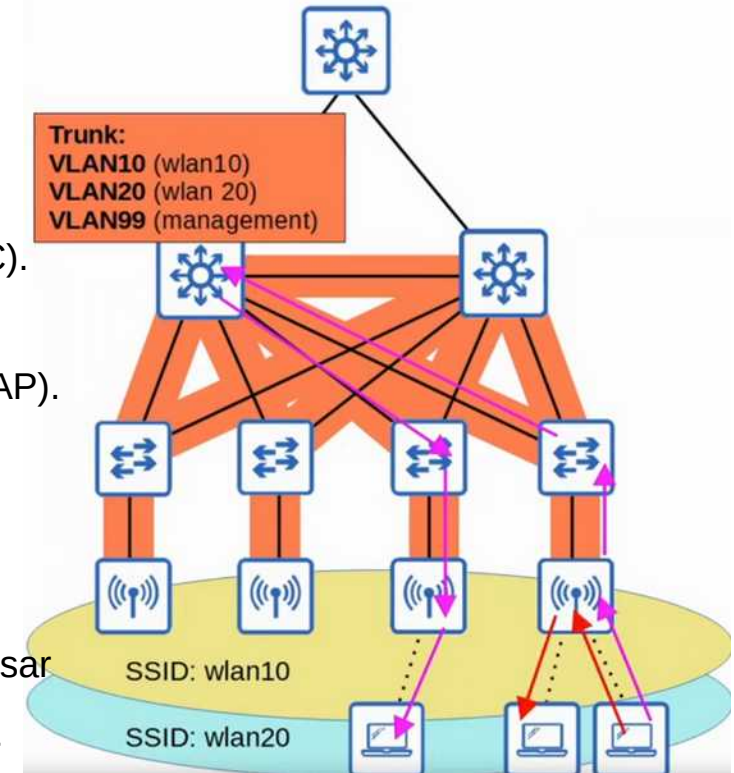
Además los tráficos de datos de los clientes tienen un acceso demasiado directo a la red cableada o a otros clientes asociados al mismo AP.

Cada una de las VLAN se expande por toda la red, como en el caso de la imagen

Esto está considerada una mala práctica ya que:

- > el dominio de broadcast se hace grande
- > STP bloquea enlaces y ya hemos visto que esto desperdicia ancho de banda
- > Añadir o quitar SSID's / VLAN es una tarea costosa pues tenemos que hacerlo en un montón de switches

Es por ello que los AP Autónomos se usan en redes pequeñas pero no en redes medianas / grandes



AP's ligeros

Arquitectura Split-MAC

Las funciones de un AP se dividen entre el AP y un WLC (Wireless LAN Controller).

Los APs ligeros manejan operaciones en tiempo real, como:

- Transmitir y recibir tráfico de RF.

- Cifrado/descifrado de tráfico.

- Envío de mensajes Beacon y Probe.

Otras funciones las realiza el WLC, como:

- Gestión de RF (canales, potencia).

- Gestión de seguridad y QoS.

- Autenticación de clientes.

- Asociación y roaming de clientes.

Esto se llama arquitectura split-MAC (división de control de acceso al medio), porque las funciones se dividen entre los APs ligeros y el WLC.

Configuración Centralizada

El WLC se utiliza para configurar centralmente todos los APs ligeros.

Ya no es necesario iniciar sesión en la CLI de cada AP para configurarlos manualmente.

Autenticación Mutua

El WLC y los APs ligeros se autentican entre sí mediante certificados digitales X.509 el mismo estándar que usan los sitios web para autenticarse en Internet. Esto evita que AP no autorizados se unan a la red.

Protocolo CAPWAP

El WLC y los APs ligeros usan el protocolo CAPWAP (Control And Provisioning of Wireless Access Points) para comunicarse. CAPWAP se basa en un protocolo anterior llamado LWAPP (Lightweight Access Point Protocol).

Se crean dos túneles entre cada AP y el WLC:

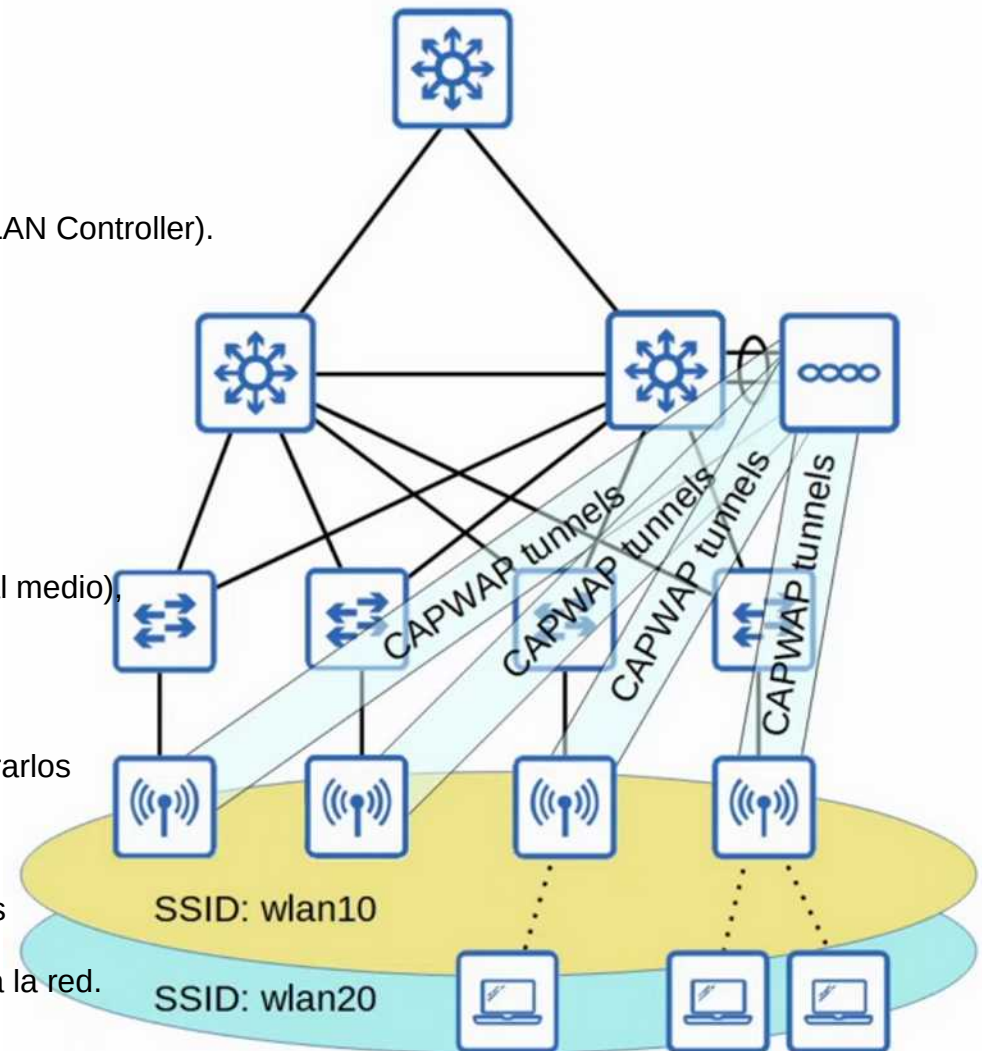
- Túnel de control (Control Tunnel - UDP 5246): Se utiliza para configurar y gestionar los Aps. Todo el tráfico en este túnel está cifrado.

- Túnel de datos (Data Tunnel - UDP 5247): Todo el tráfico de los clientes inalámbricos se envía a través de este túnel al WLC.

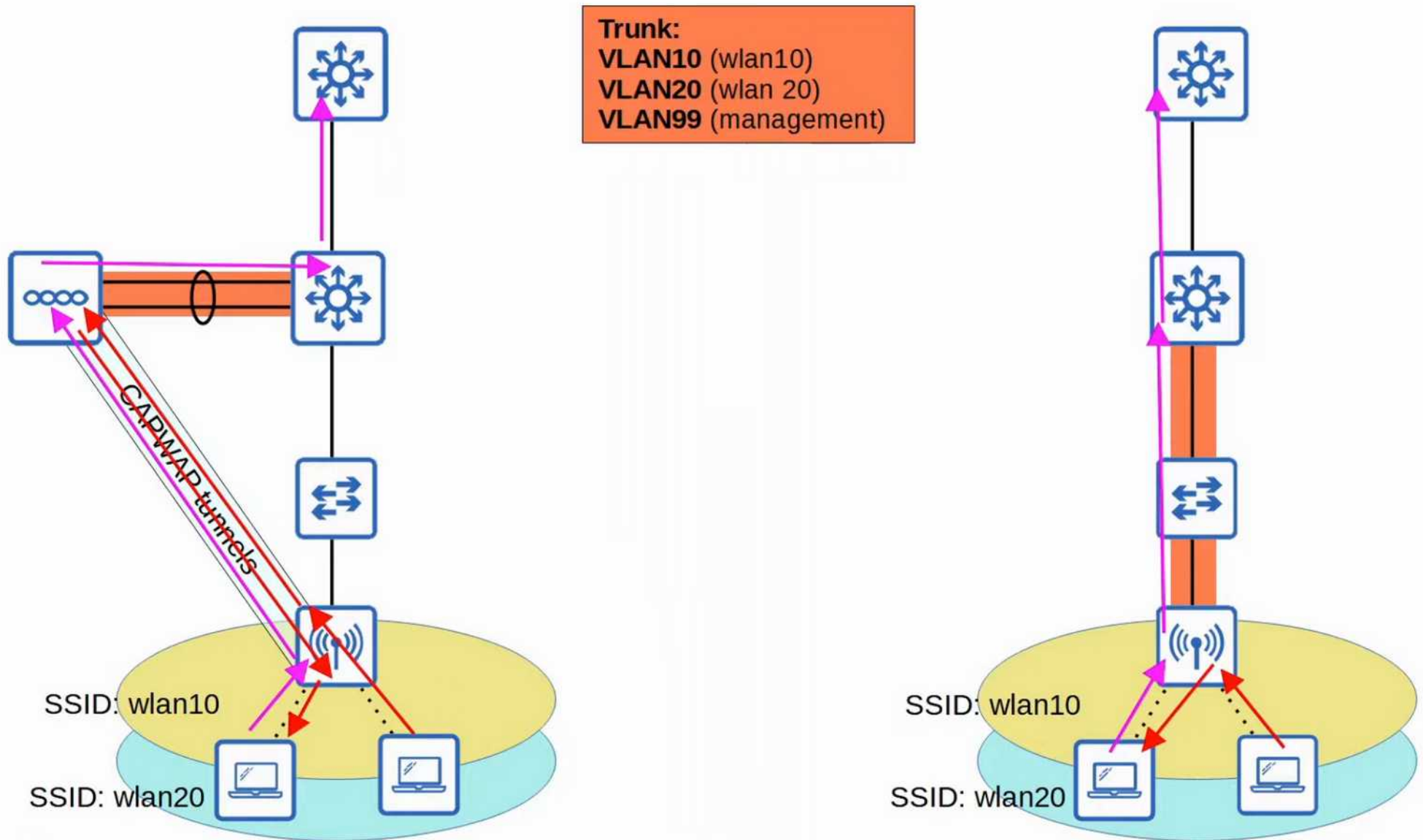
No pasa directamente a la red cableada, ni siquiera entre clientes del mismo AP. El tráfico no está cifrado por defecto, pero puede configurarse con DTLS (Datagram Transport Layer Security) que es como TLS pero por UDP en lugar de TCP.

Conexión a Puertos de Acceso (No Trunk)

A diferencia de los APs autónomos, los APs ligeros se conectan a puertos de acceso en los switches (no trunk). No es necesario que múltiples VLANs crucen ese enlace, ya que todo el tráfico se encapsula en los túneles CAPWAP.



AP's ligeros vs Autónomos



AP's ligeros vs Autónomos

Arquitectura Split-MAC (AP Ligero + WLC)

El AP se conecta al switch con un puerto de acceso.

El WLC se conecta con un enlace trunk (porque maneja múltiples VLANs).

Flujo de tráfico:

El tráfico del cliente inalámbrico se envía al AP → se tuneliza al WLC → el WLC lo envía a la red cableada.

Incluso si el destino está en el mismo AP, el tráfico primero va al WLC y luego vuelve.

Arquitectura Autónoma (Local-MAC)

Cada AP se conecta con un enlace trunk.

Flujo de tráfico:

El tráfico puede ir directamente del AP al gateway o a otro cliente en el mismo AP.

Beneficios de la Arquitectura Split-MAC

Escalabilidad: Con uno o varios WLCs, es fácil manejar miles de APs.

Asignación dinámica de canales: El WLC elige automáticamente el mejor canal para cada AP.

Autoajuste de potencia: El WLC configura la potencia de transmisión para evitar interferencias.

Autoreparación: Si un AP falla, el WLC aumenta la potencia de los APs cercanos para evitar huecos de cobertura.

Roaming sin interrupciones: Los clientes pueden moverse entre APs sin perder conexión.

Balanceo de carga: El WLC asocia los clientes al AP menos congestionado.

Gestión centralizada de seguridad y QoS.

Modos de Operación de APs Ligeros

Al igual que los APs autónomos, los APs ligeros tienen diferentes modos:

Modo **Local** (Local Mode):

Modo predeterminado. Ofrece uno o más BSSs para clientes.

Modo **FlexConnect**:

Permite que el AP reenvíe tráfico localmente si se pierde conexión con el WLC.

Modo **Sniffer**:

No ofrece BSS. Solo captura tramas 802.11 para análisis (ej. Wireshark).

Modo **Monitor**:

Detecta dispositivos no autorizados (rogue devices) y envía mensajes de desautenticación.

Modo **Rogue Detector**:

Escucha tráfico en la red cableada para detectar dispositivos no autorizados.

Modo **SE-Connect** (Spectrum Expert):

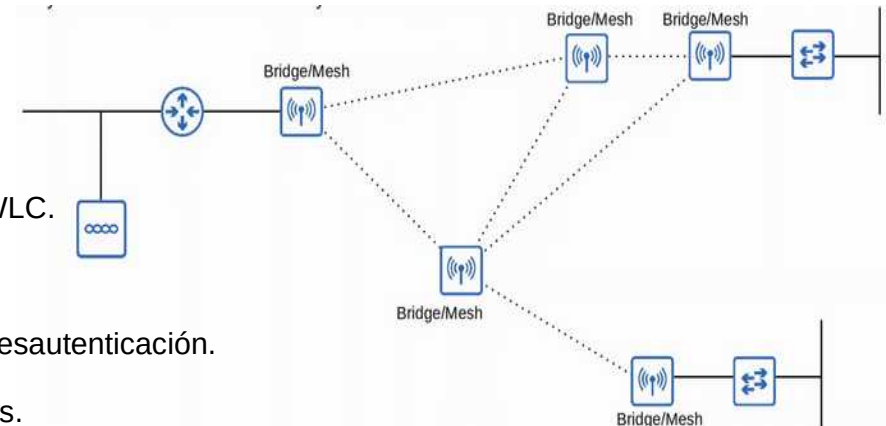
Analiza el espectro RF en todos los canales.

Modo **Bridge/Mesh**:

Conecta sitios remotos (similar a los puentes exteriores en APs autónomos).

Modo **Flex+Bridge**:

Combina FlexConnect con funcionalidad de puente.



Modelos despliegue WLC

Dado que estamos hablando de WLCs, esto aplica solo a la arquitectura split-MAC, no a las arquitecturas de APs autónomos o APs basados en la nube.

Existen cuatro modelos principales de implementación de WLC, es decir, cuatro formas de desplegar un WLC en una red. Mostraré cada uno con un diagrama, pero primero hagamos un resumen:

WLC Unico (Unified WLC)

El WLC es un dispositivo físico independiente, ubicado en una ubicación central de la red

WLC Basado en la Nube (Cloud-based WLC)

El WLC es una máquina virtual (VM) ejecutándose en un servidor, generalmente en una nube privada en un centro de datos.

Importante: Esto no es lo mismo que la arquitectura de APs basados en la nube que veremos luego. Aquí los APs siguen siendo ligeros (lightweight), y "basado en la nube" solo se refiere a dónde está ubicado el WLC.

WLC Integrado (Embedded WLC):

El WLC está integrado dentro de un switch en la red.

Cisco Mobility Express:

La funcionalidad del WLC está integrada dentro de uno o más APs de la red.

WLC Unico

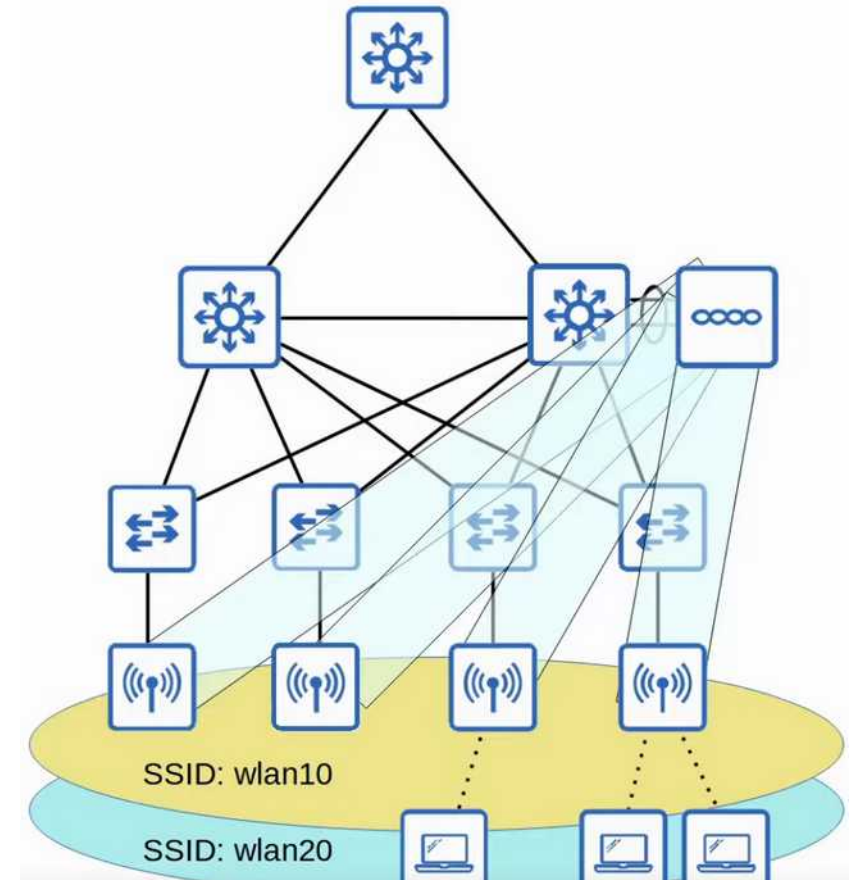
Aquí tenemos un ejemplo de un WLC unificado: un dispositivo hardware independiente, desplegado en una ubicación central de la red.

Capacidad: Puede soportar hasta ~6000 APs. Si se necesitan más, se pueden agregar WLCs adicionales.

Uso típico: Adecuado para grandes campus empresariales.

Imagen de diferentes modelos de WLC de Cisco:

Los modelos más grandes son más potentes y soportan más APs que los más pequeños.



WLC basado en la nube

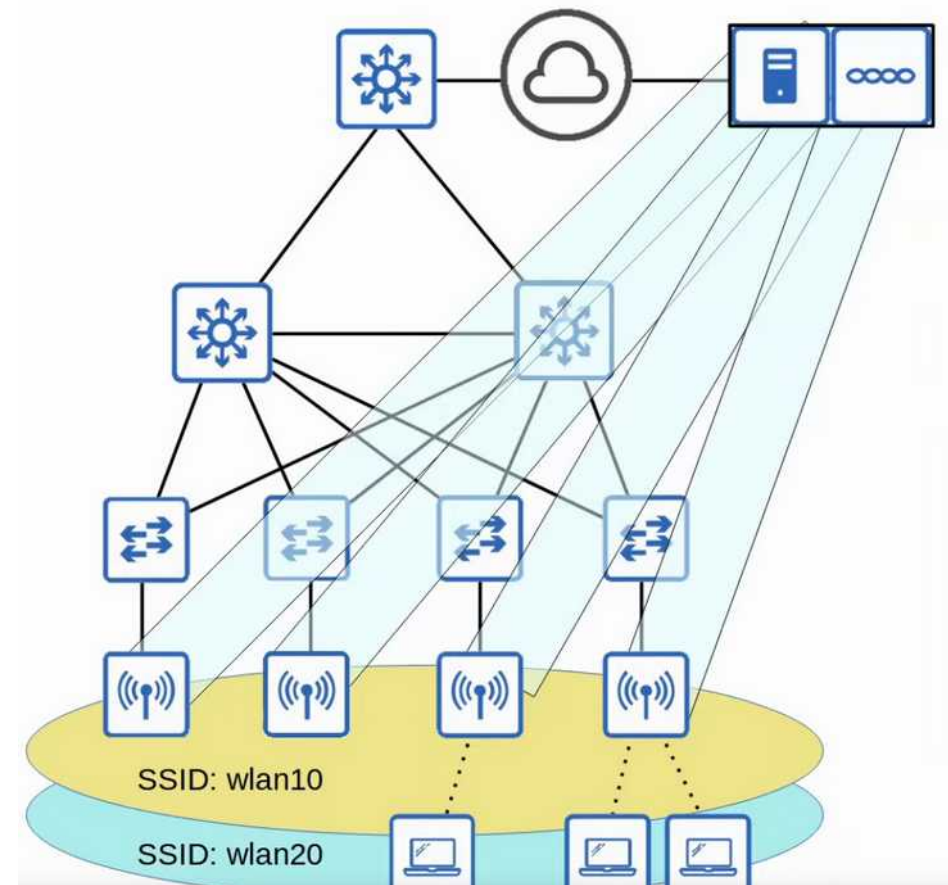
En este caso, el WLC es una máquina virtual (VM) ejecutándose en un servidor, normalmente en una nube privada en un centro de datos.

Capacidad: Soporta hasta ~3000 APs. Si se necesitan más, se pueden agregar más VMs de WLC.

Aclaración importante:

Esto no es lo mismo que los APs basados en la nube (como Meraki).

Aquí los APs siguen siendo ligeros (lightweight), y "basado en la nube" solo indica que el WLC está alojado en la nube, no los APs.

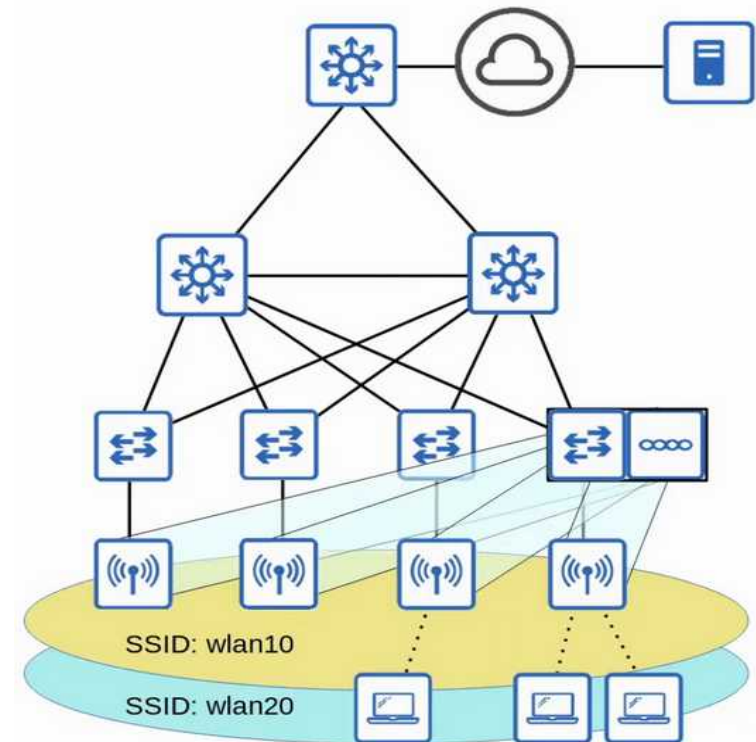


WLC integrado

En este modelo, el WLC está integrado dentro de un switch en la red.

Capacidad: Soporta hasta ~200 APs. Si se necesitan más, se deben agregar más switches con WLCs integrados.

Uso típico: Adecuado para redes de campus pequeños o medianos.



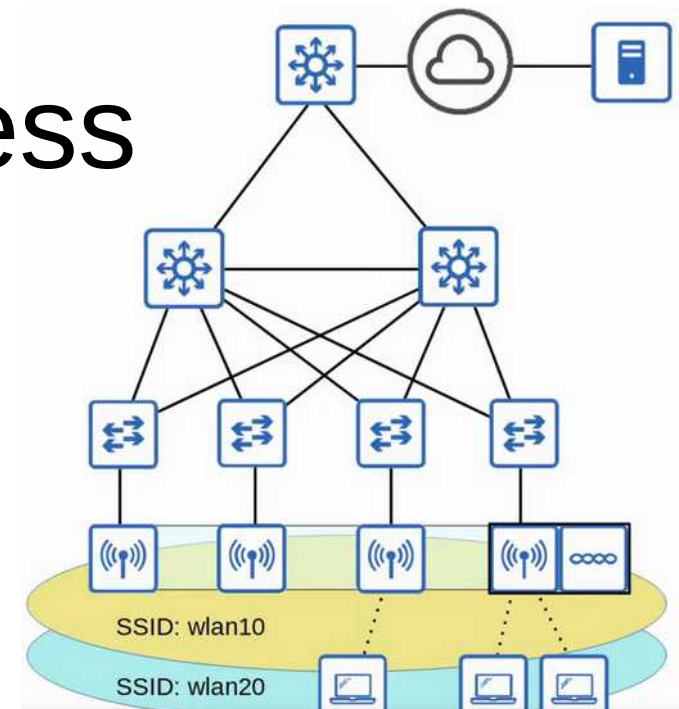
CISCO Mobility Express

En este modelo, la funcionalidad del WLC está integrada dentro de uno o más APs de la red.

El AP que contiene el WLC establece túneles CAPWAP internos, y los demás APs también se conectan a él.

Capacidad: Soporta hasta ~100 APs. Si se necesitan más, se deben agregar más APs con WLCs Mobility Express.

Uso típico: Adecuado para pequeñas oficinas o sucursales.



AP's ligeros vs Autónomos

Arquitectura Split-MAC (AP Ligero + WLC)

El AP se conecta al switch con un puerto de acceso.

El WLC se conecta con un enlace trunk (porque maneja múltiples VLANs).

Flujo de tráfico:

El tráfico del cliente inalámbrico se envía al AP → se tuneliza al WLC → el WLC lo envía a la red cableada.

Incluso si el destino está en el mismo AP, el tráfico primero va al WLC y luego vuelve.

Arquitectura Autónoma (Local-MAC)

Cada AP se conecta con un enlace trunk.

Flujo de tráfico:

El tráfico puede ir directamente del AP al gateway o a otro cliente en el mismo AP.

Beneficios de la Arquitectura Split-MAC

Escalabilidad: Con uno o varios WLCs, es fácil manejar miles de APs.

Asignación dinámica de canales: El WLC elige automáticamente el mejor canal para cada AP.

Autoajuste de potencia: El WLC configura la potencia de transmisión para evitar interferencias.

Autoreparación: Si un AP falla, el WLC aumenta la potencia de los APs cercanos para evitar huecos de cobertura.

Roaming sin interrupciones: Los clientes pueden moverse entre APs sin perder conexión.

Balanceo de carga: El WLC asocia los clientes al AP menos congestionado.

Gestión centralizada de seguridad y QoS.

Modos de Operación de APs Ligeros

Al igual que los APs autónomos, los APs ligeros tienen diferentes modos:

Modo **Local** (Local Mode):

Modo predeterminado. Ofrece uno o más BSSs para clientes.

Modo **FlexConnect**:

Permite que el AP reenvíe tráfico localmente si se pierde conexión con el WLC.

Modo **Sniffer**:

No ofrece BSS. Solo captura tramas 802.11 para análisis (ej. Wireshark).

Modo **Monitor**:

Detecta dispositivos no autorizados (rogue devices) y envía mensajes de desautenticación.

Modo **Rogue Detector**:

Escucha tráfico en la red cableada para detectar dispositivos no autorizados.

Modo **SE-Connect** (Spectrum Expert):

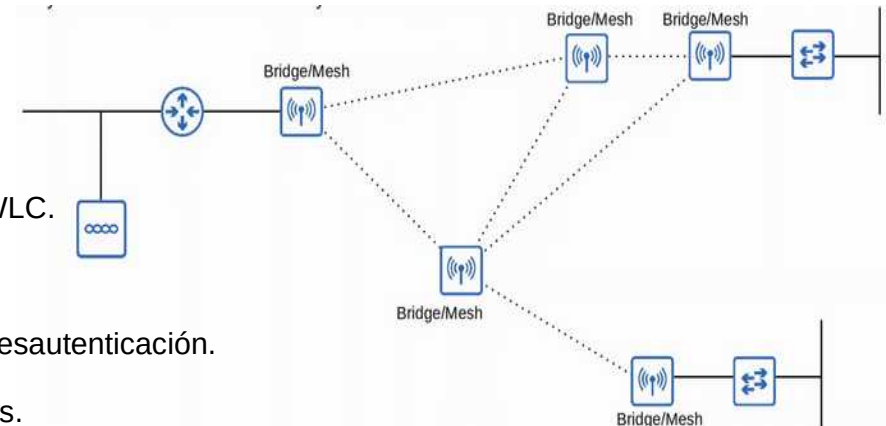
Analiza el espectro RF en todos los canales.

Modo **Bridge/Mesh**:

Conecta sitios remotos (similar a los puentes exteriores en APs autónomos).

Modo **Flex+Bridge**:

Combina FlexConnect con funcionalidad de puente.



AP's en Cloud

Este modelo es un híbrido entre APs autónomos y ligeros:

APs autónomos gestionados desde la nube (ej. Cisco Meraki).

El tráfico de datos NO pasa por la nube, solo el tráfico de gestión.

Ejemplo: Meraki Dashboard (interfaz web para configuración y monitoreo).

Modelos de Implementación de WLC

Solo aplica para APs ligeros (split-MAC). Hay cuatro modelos:

WLC Unificado (Unified):

Dispositivo físico centralizado. Soporta hasta 6000 APs.

WLC en la Nube (Cloud-based):

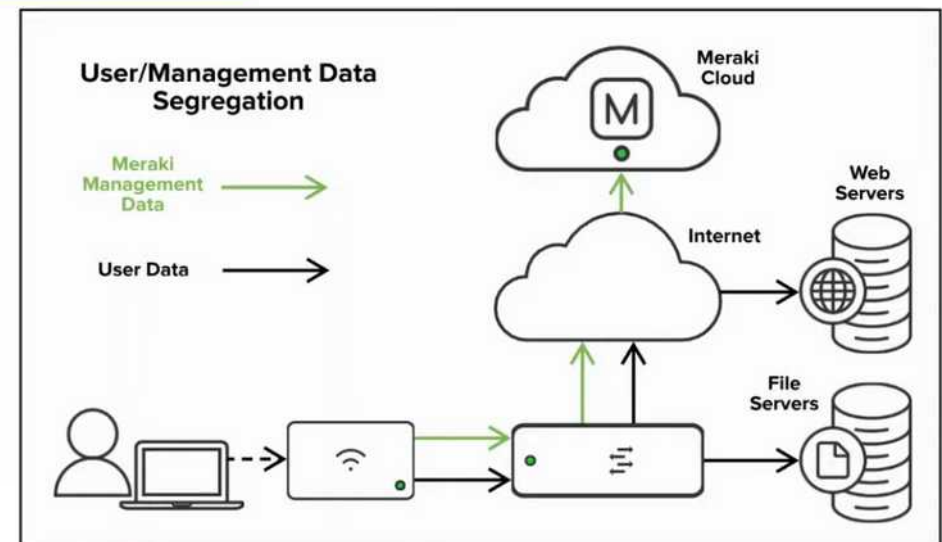
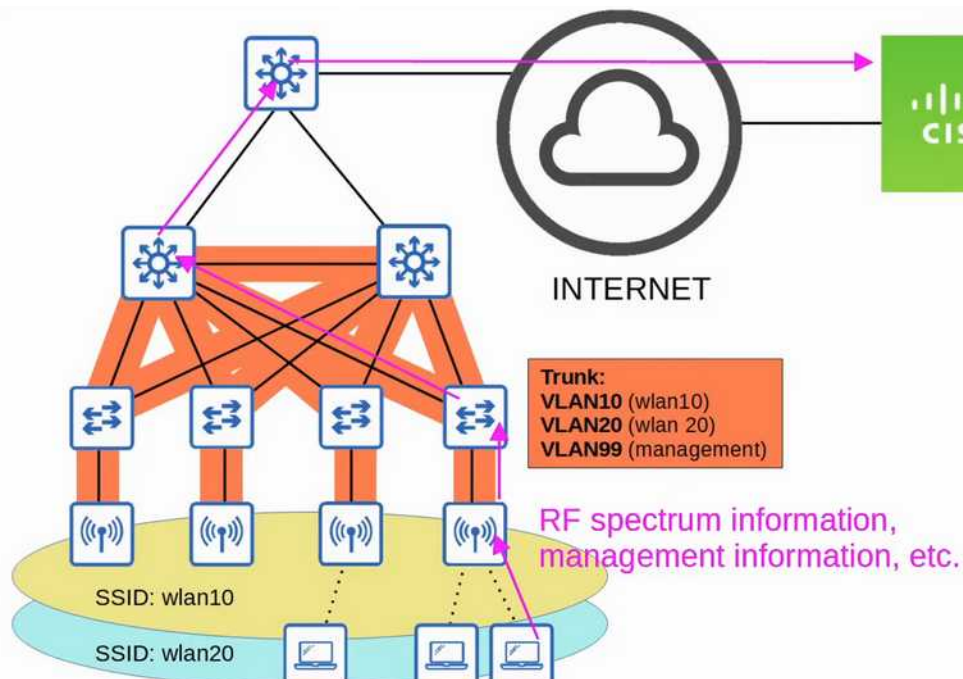
VM en un centro de datos. Soporta hasta 3000 APs.

WLC Integrado (Embedded):

Funcionalidad de WLC dentro de un switch. Soporta hasta 200 APs.

Cisco Mobility Express:

WLC integrado en un AP. Soporta hasta 100 APs.



AP's ligeros vs Autónomos

Arquitectura Split-MAC (AP Ligero + WLC)

El AP se conecta al switch con un puerto de acceso.

El WLC se conecta con un enlace trunk (porque maneja múltiples VLANs).

Flujo de tráfico:

El tráfico del cliente inalámbrico se envía al AP → se tuneliza al WLC → el WLC lo envía a la red cableada.

Incluso si el destino está en el mismo AP, el tráfico primero va al WLC y luego vuelve.

Arquitectura Autónoma (Local-MAC)

Cada AP se conecta con un enlace trunk.

Flujo de tráfico:

El tráfico puede ir directamente del AP al gateway o a otro cliente en el mismo AP.

Beneficios de la Arquitectura Split-MAC

Escalabilidad: Con uno o varios WLCs, es fácil manejar miles de APs.

Asignación dinámica de canales: El WLC elige automáticamente el mejor canal para cada AP.

Autoajuste de potencia: El WLC configura la potencia de transmisión para evitar interferencias.

Autoreparación: Si un AP falla, el WLC aumenta la potencia de los APs cercanos para evitar huecos de cobertura.

Roaming sin interrupciones: Los clientes pueden moverse entre APs sin perder conexión.

Balanceo de carga: El WLC asocia los clientes al AP menos congestionado.

Gestión centralizada de seguridad y QoS.

Modos de Operación de APs Ligeros

Al igual que los APs autónomos, los APs ligeros tienen diferentes modos:

Modo **Local** (Local Mode):

Modo predeterminado. Ofrece uno o más BSSs para clientes.

Modo **FlexConnect**:

Permite que el AP reenvíe tráfico localmente si se pierde conexión con el WLC.

Modo **Sniffer**:

No ofrece BSS. Solo captura tramas 802.11 para análisis (ej. Wireshark).

Modo **Monitor**:

Detecta dispositivos no autorizados (rogue devices) y envía mensajes de desautenticación.

Modo **Rogue Detector**:

Escucha tráfico en la red cableada para detectar dispositivos no autorizados.

Modo **SE-Connect** (Spectrum Expert):

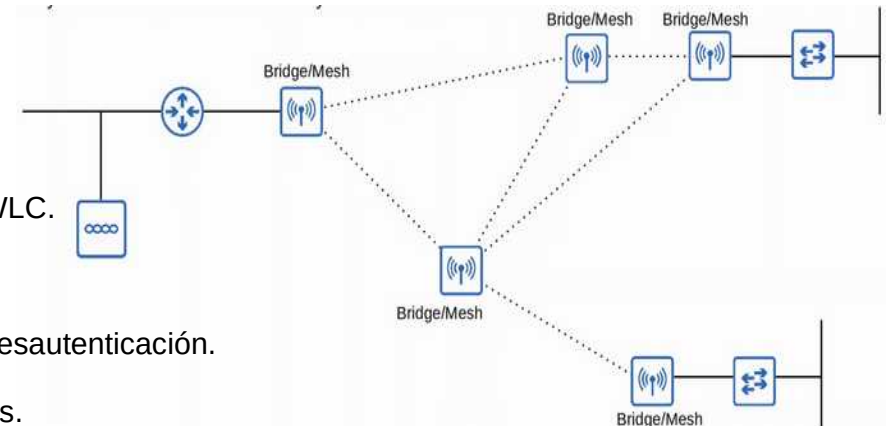
Analiza el espectro RF en todos los canales.

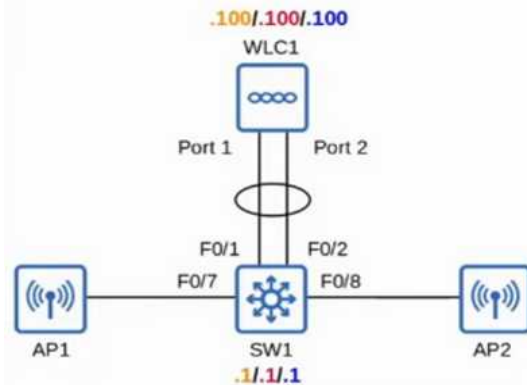
Modo **Bridge/Mesh**:

Conecta sitios remotos (similar a los puentes exteriores en APs autónomos).

Modo **Flex+Bridge**:

Combina FlexConnect con funcionalidad de puente.





WLANs/VLANs

VLAN 10: Management,

192.168.1.0/24

VLAN 100: Internal, SSID: Internal,

10.0.0.0/24

VLAN 200: Guest, SSID: Guest,

10.1.0.0/24

```

SW1(config)#vlan 10
SW1(config-vlan)#name Management
SW1(config-vlan)#vlan 100
SW1(config-vlan)#name Internal
SW1(config-vlan)#vlan 200
SW1(config-vlan)#name Guest

```

```

SW1(config)#int range f0/6 - 8
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 10
SW1(config-if-range)#spanning-tree portfast

```

```

SW1(config-if-range)#interface range f0/1 - 2
SW1(config-if-range)#channel-group 1 mode on

```

```

SW1(config-if-range)#interface port-channel 1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 10,100,200

```

Le dice a los AP donde está el WLC, sólo es útil si está en una red donde no recibe los broadcast de los clientes

```

SW1(config)#interface vlan 10
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#interface vlan 100
SW1(config-if)#ip address 10.0.0.1 255.255.255.0
SW1(config-if)#interface vlan 200
SW1(config-if)#ip address 10.1.0.1 255.255.255.0

```

```

SW1(config)#ip dhcp pool VLAN10
SW1(dhcp-config)#network 192.168.1.0 255.255.255.0
SW1(dhcp-config)#default-router 192.168.1.1
SW1(dhcp-config)#option 43 ip 192.168.1.100

```

```

SW1(config)#ip dhcp pool VLAN100
SW1(dhcp-config)#network 10.0.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.0.0.1

```

```

SW1(config)#ip dhcp pool VLAN200
SW1(dhcp-config)#network 10.1.0.0 255.255.255.0
SW1(dhcp-config)#default-router 10.1.0.1

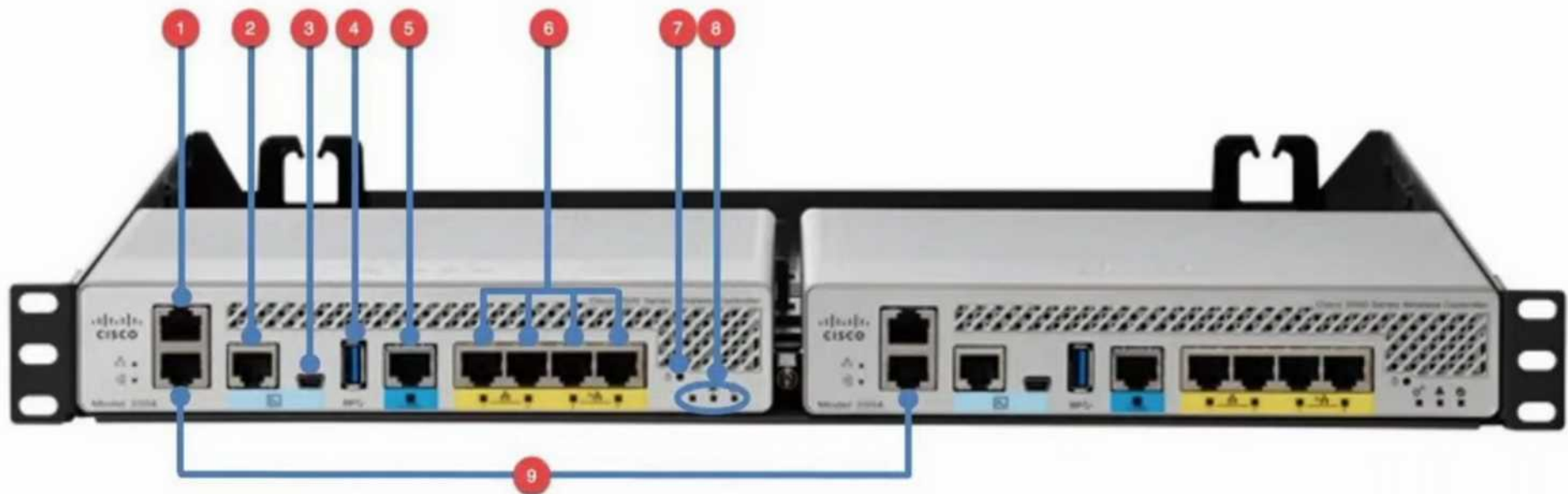
```

→ **Service port:** A dedicated management port. Used for out-of-band management. Must connect to a switch access port because it only supports one VLAN. This port can be used to connect to the device while it is booting, perform system recovery, etc.

→ **Distribution system port:** These are the standard network ports that connect to the 'distribution system' (wired network) and are used for data traffic. These ports usually connect to switch trunk ports, and if multiple distribution ports are used they can form a LAG.

→ **Console port:** This is a standard console port, either RJ45 or USB.

→ **Redundancy port:** This port is used to connect to another WLC to form a high availability (HA) pair.



- 1) Service port
- 2) Console port (RJ45)
- 3) Console port (USB)
- 4) USB (for software updates)
- 5) Distribution system port (multi-gigabit)
- 6) Distribution system ports (1-gig)
- 7) Reset button
- 8) Status LEDs

interfaces

→ **Management interface:** Used for management traffic such as Telnet, SSH, HTTP, HTTPS, RADIUS authentication, NTP, Syslog, etc. CAPWAP tunnels are also formed to/from the WLC's management interface.

→ **Redundancy management interface:** When two WLCs are connected by their redundancy ports, one WLC is 'active' and the other is 'standby'. This interface can be used to connect to and manage the 'standby' WLC.

→ **Virtual interface:** This interface is used when communicating with wireless clients to relay DHCP requests, perform client web authentication, etc.

→ **Service port interface:** If the service port is used, this interface is bound to it and used for out-of-band management.

→ **Dynamic interface:** These are the interfaces used to map a WLAN to a VLAN. For example, traffic from the 'Internal' WLAN will be sent to the wired network from the WLC's 'Internal' dynamic interface.

Configuración

Crear interfaces dinámicos

Controller -> Interfaces (menú izquierdo) -> New

Mapeamos con la VLAN correspondiente y pulsamos Apply

Luego aparecerá la pantalla de la derecha donde pondremos la IP

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
guest	200	10.1.0.100	Dynamic	Disabled
internal	100	10.0.0.100	Dynamic	Disabled
management	10	192.168.1.100	Static	Enabled
virtual	N/A	172.16.1.1	Static	Not Supported

Ahora debemos mapear con las WLAN, pulsamos en esa opción en el menú superior
Creamos tantas WLAN como tengamos con su seguridad, nombre de SSID etc.

Interfaces > Edit

General Information

Interface Name

Internal

MAC Address

00:08:2f:10:65:6f

Configuration

Quarantine

☐

Quarantine Vlan Id

0

NAS-ID

WLC1

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management

☐

Interface Address

VLAN Identifier

100

IP Address

10.0.0.100

Netmask

255.255.255.0

Gateway

10.0.0.1

DHCP Information

Primary DHCP Server

10.0.0.1

Secondary DHCP Server

DHCP Proxy Mode

Global

Enable DHCP Option 82

☐

CISCO

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

FEEDBACK

WLANs

WLANs

Advanced

WLANs

Current Filter: None

[\[Change Filter\]](#) [\[Clear Filter\]](#)

Create New

Go

<input type="checkbox"/>	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
<input type="checkbox"/>	1	WLAN	Internal	Internal	Enabled	[WPA2][Auth(PSK)]
<input type="checkbox"/>	2	WLAN	Guest	Guest	Enabled	[WPA2][Auth(PSK)]

Entries 1 - 2 of 2