



REDES

Tecnología de Centro de Cómputos y Oficinas

Cableado Estructurado

- Tendido de cables que provee voz, datos, video, audio, seguridad, control y monitoreo, en cualquier puesto de trabajo.

Diferentes escenarios

- Oficina única
- Varias oficinas en un piso
- Edificio completo
- Varios edificios en un terreno
- Centro de Cómputos

Cableado Estructurado

- Estandarización EIA/TIA 568
- Debido a que el cableado es independiente de la aplicación y del proveedor, los cambios pueden realizarse por los cables existentes.
- Debido a que las tomas están cableadas de igual forma, los movimientos de personal pueden hacerse sin modificar la base de cableado.
- La ubicación centralizada de los equipos de red permite que las fallas sean localizadas más fácilmente.

Historia

- Instalaciones

- Heterogéneas

- Cableado telefónico tradicional (par CAT 2)
 - Cableado de datos estructurado (UTP)

- Homogéneas

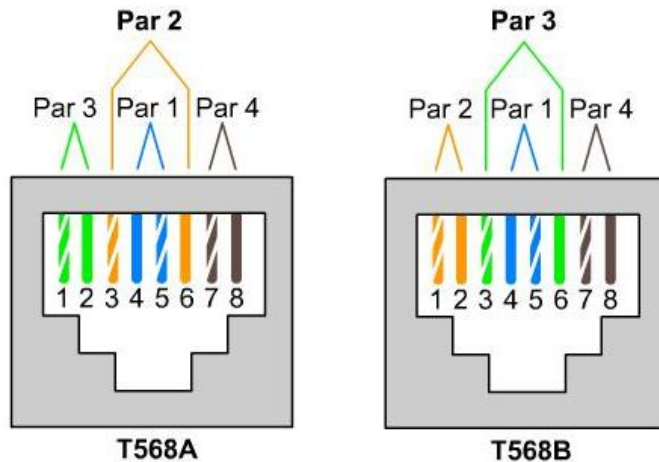
- Sólo cableado estructurado (UTP)

Cable UTP

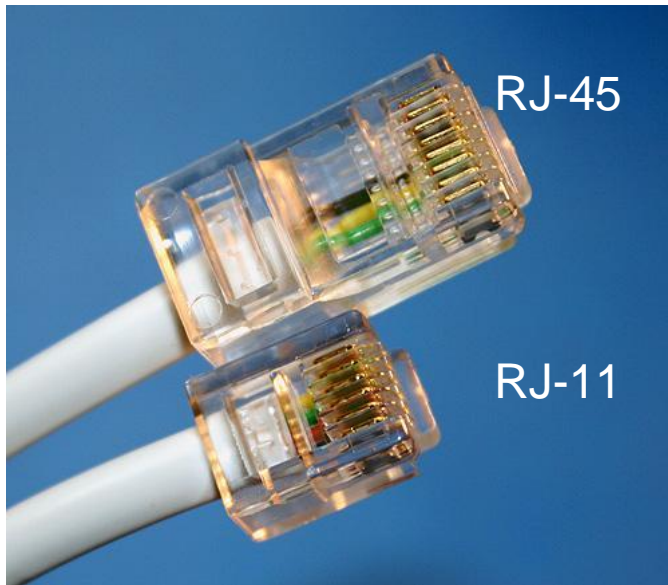
Variantes de armar los cables.

Difieren en donde estan los cables 2 o 3 (transmision y recepcion).

Antes habia que cambiar el tipo de cable segun el uso que se le queria dar, ahora ya las placas lo solucionan automaticamente



Conectores



RJ-45

RJ-11

RJ11: telefonia
RJ45: internet



ST (Straight Tip)



LC (Local Connector)



MT-RJ



SC (Subscriber Connector)

Cableado Estructurado - Rack

- 40 unidades
- 12 unidades
- 1 U de rack = 1,75" = 4.445 cm

Este es un tamaño estándar (altura) que usan los servidores, switches, etc. Siempre se usan unidades enteras de U.



Para el ancho de los mismos hay un par de estándares pero a veces cambian de tamaño. Si se quiere poner un equipo más angosto, se colocan unas vías en los costados.

El rack es un lugar en donde los equipos de red están protegidos, tienen fácil acceso a los cables de red y tienen buena disipación del calor. Son la estandarización física de donde instalar dichos equipos.





Imagen de rack "lleno".
Atras se puede acceder al cableado

La patchera puede ir en el frente o atras. Su objetivo es no estar tocando los puertos de los equipos cada vez que quiero cambiar algo. Solo toco los puertos de los equipos en la instalacion del sistema. Si se llega a romper algo arreglo la patchera y listo, es mas barato.

Cableado Estructurado – Patchera de Cobre

Las patcheras son una serie de conectores que me permiten insertar de a 8 cables.

En la patchera se ponen los cables con una impactadora (parecido a soldar pero con un golpe), esto nos permite ahorrar fichas.



Vista frontal



Antes se hacia mas cableado del lado de adelante, ahora se tiende a que no

Vista posterior

Rack prolijo



Ordenador
de cables

Es muy importante planificar los cables para que queden prolijos.
De esta manera le damos mejor mantenibilidad al sistema.



Vista frontal

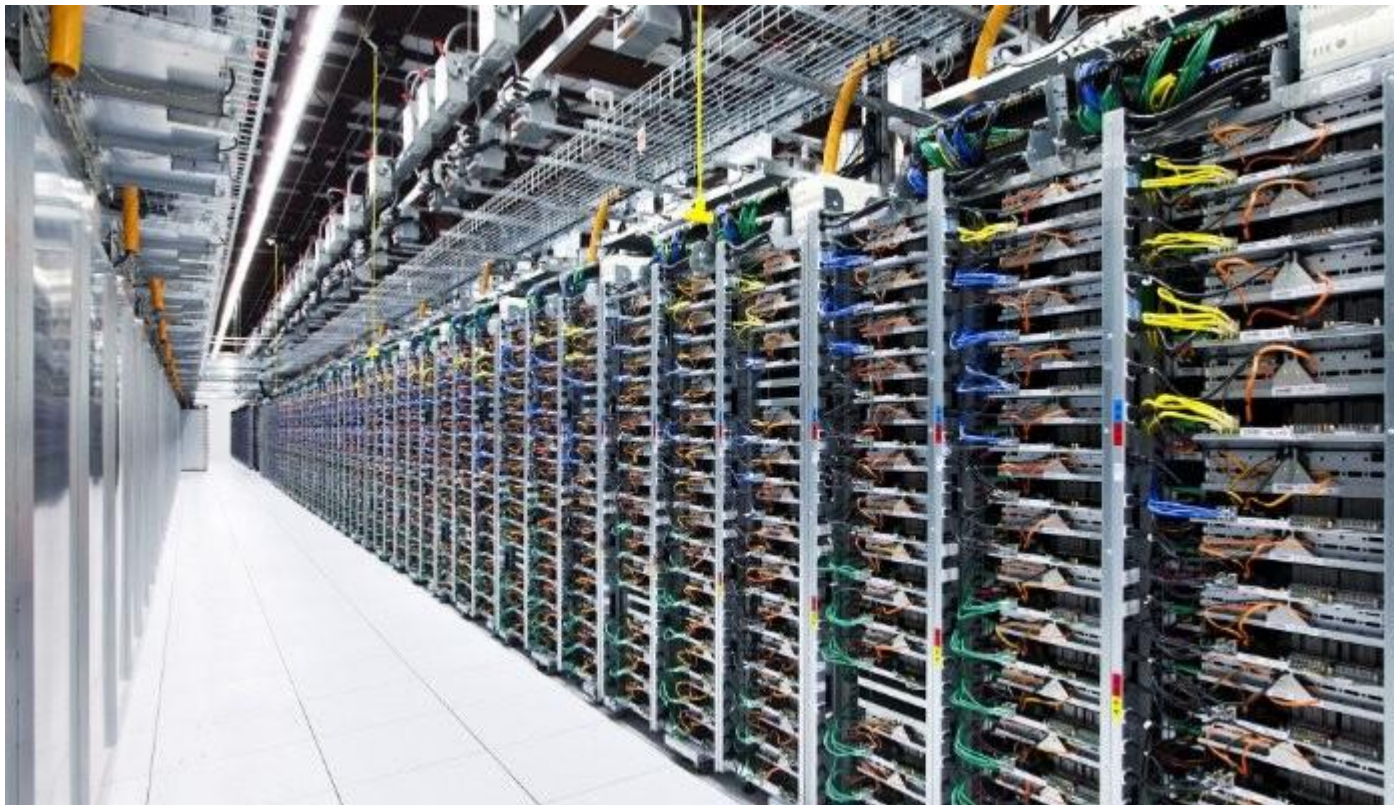
Esta es una patchera frontal

Racks no prolijos

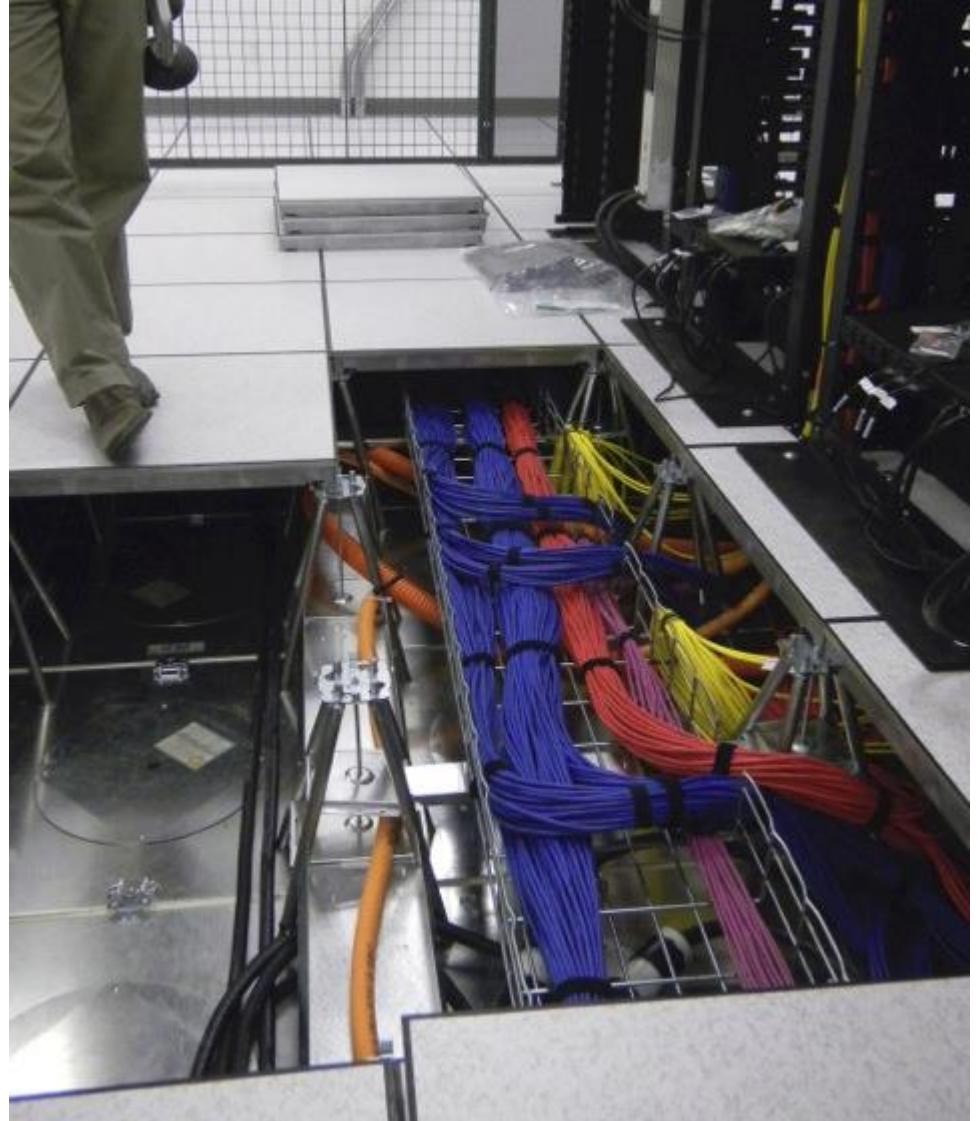


Data Centers

Todas las empresas grandes tienen data centers como estos. (no solo google y amazon)



Piso Técnico / Raised Floor



El piso esta levantado como un metro, hay bandejas por donde viajan los cables que van a cada una de las filas de racks.

Tambien hay piso tecnico para las oficinas. Tiene mucha menos cantidad de cables que en el caso anterior, pero nos ahorra pasar cables por la pared

Overhead Cabling Trays



Cables que viajan por el techo. Muchas veces se combinan con los cables que van por el piso. Para evitar que hacer un cooling de todo el lugar, a veces hay refrigeración directa arriba de cada rack.

Los cables no se suelen sobrecalentar pero los racks si.

Cableado Estructurado

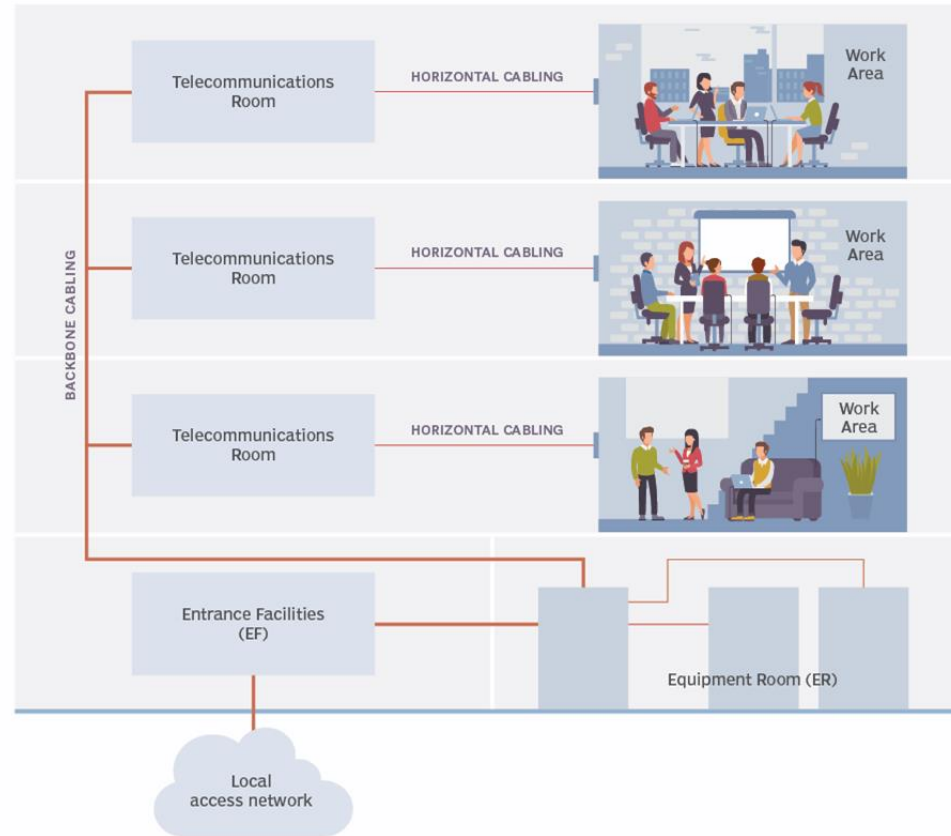
- Se puede dividir en:
 - Cableado de campus (entre edificios)
 - Cableado vertical
 - Cableado horizontal
 - Cableado de Usuario

Cableado Estructurado - Organización

Backbone cabling: cableado vertical.

Hay un cableado horizontal para llegar a cada una de las estaciones de trabajo en el piso. Se extiende desde el area de trabajo hasta el area de telecomunicaciones, y tiene topologia estrella (porque hay un switch de piso que le da servicio a cada PC por separado). Estos cables no pueden tener mas de 90 metros (si se pasa hay que poner otro switch, esta restriccion viene del tipo de cable ethernet).

Cuando tenemos varios edificios, generalmente solo uno tiene entrance facilities (por donde llega el ISP) y equipment room



El patch core es el cableado de usuario. Este se conecta desde la roseta hasta la PC de cada computadora.

Cableado Estructurado Horizontal

- Se extiende desde el área de trabajo (WA) hasta el armario de telecomunicaciones del piso.
- Debe tener una topología de estrella.
- Los cables no pueden extenderse por más de noventa metros.
- La máxima longitud de los patch cords y de los cables en el WA no debe superar los cinco metros.

Cableado Estructurado

Rack

Switch

Roseta

**Patchera de
datos**

**Patchera de
telefonía**

**Patchera reflejo de
PABX**

Multipar

Regleta

PABX

Tener en cuenta que la patchera es pasiva. No hace absolutamente nada, mientras que el switch es activo (entre otras cosas también regenera la señal)

No mas de 5m

No mas de 90m

No mas de 5m

**Puesto de
trabajo**

Cableado Estructurado

- Longitud de los cables para Ethernet
 - El cableado horizontal no puede tener más de 90 metros
 - El cable de usuario se calcula de 3 metros
 - El cable en el patch panel se calcula de 7 metros.

La estimacion es de 100 metros maximo en total.

Cableado Estructurado – Puesto



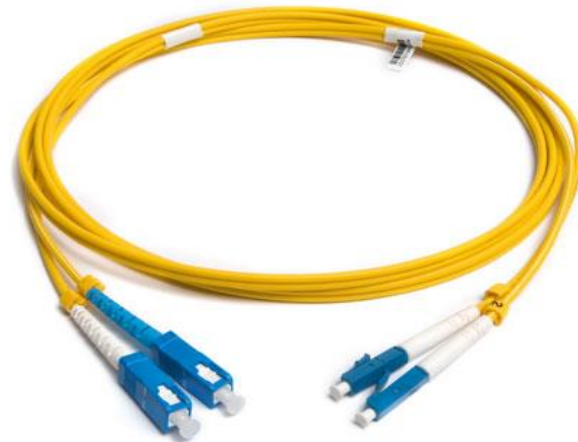
Roseta



**RJ-45 hembra
(jack)**



**Patch Cord
De UTP**



**Patch Cord
De Fibra Optica**

Tester de cable UTP



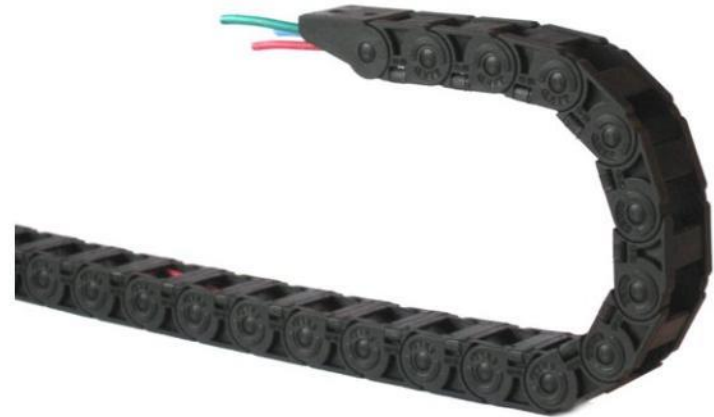
- Conectividad de pares
- Tipos de norma

Es para ver si estan bien armadas las cosas. Se emite una potencia de un lado y se mide la potencia de salida.

Cable Canal



Plástico para
pared



Tipo cadena

Cableado Estructurado Vertical

- Conecta los pisos de un edificio
- Suele tener redundancia Minimo se pasan dos cables de 10GB/s entre pisos
- Para redundancia se cablea en anillo y sin redundancia en cascada En cascada es cuando conectas cada piso con el de arriba y el de abajo. El tema es que si se rompe un piso se puede afectar el comportamiento de varios pisos.
- Recibe el nombre de “backbone”
- Suele ser el enlace de mayor velocidad en la red

Cableado Estructurado – Montante

La montante es por donde pasan los cables entre pisos.



Cableado Estructurado – Patchera de Fibra



Cableado Estructurado – Patchera de Fibra



Switch de Fibra (1)

Los switches pueden ser de fibra o ethernet

- Switch de fibra
- Switch de fibra + UTP













REDES

Switches

Dispositivos de Red

Dispositivos de red	
Repetidor 	Puente 
Hub 10BASE-T 	Switch de grupo de trabajo 
Hub 100BASE-T 	Router 
Hub 	Nube de red 

Ethernet

Capa 1 (física): tiene que ver con como se transmiten los bytes.
El interpacket gap existe para no pisarse con otros paquetes.

Antes ethernet estaba pensado para medio compartido, pero ahora con los switches esto es bastante raro.
La capa 2 (ejemplo: IP) es la que me resuelve poder mandar un paquete a otra maquina en la red local (usando las MAC addresses).
El CRC es un redundancy check.

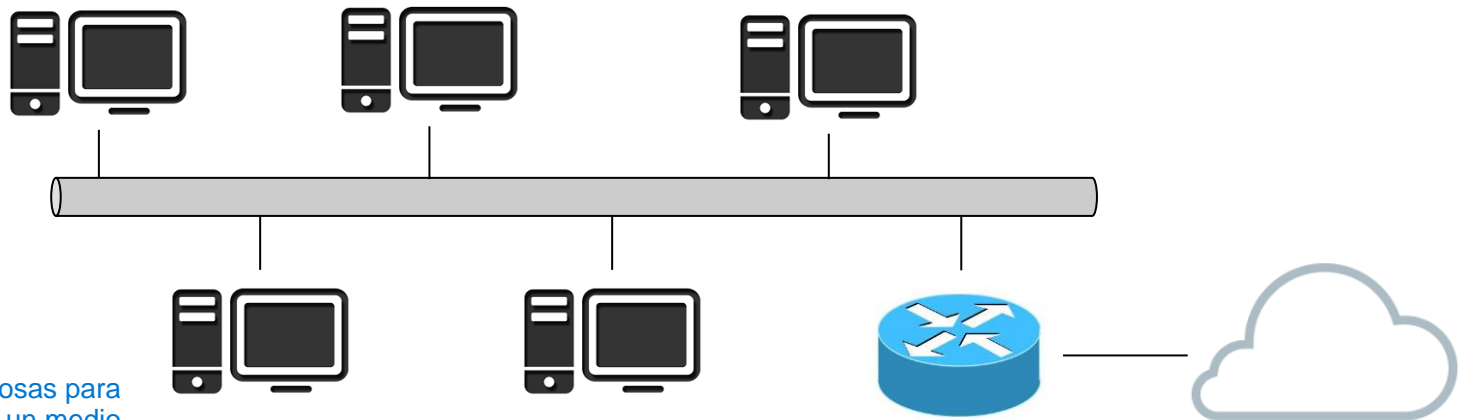
Capa OSI	Preám bulo	Inicio de Frame	MAC Destino	MAC Origen	VLAN tag opcional	Type of Frame o longitud	Payload	CRC	Inter packet gap
	7 Bytes	1 Byte	6 Bytes	6 Bytes	4 Bytes	2 Bytes	46-1500 Bytes	4 Bytes	12 Bytes
Capa 1									
Capa 2									

La tabla entera es un paquete ethernet completo.

En el payload van las capas de abajo

Evolución - Medio Compartido

❑ Carrier Sense Multiple Access with Collision Detection (CSMA-CD)



Primero se pensaron las cosas para que sean compatibles con un medio compartido. Esto significa que las PC estaban conectadas en cascada (el mismo cable iba de computadora en computadora).

Todas escribían en el mismo bus, y la manera de entenderse es con carrier sense (solo escribo si veo que nadie está escribiendo) y collision detection (si veo que alguien me piso tengo que volver a mandar el paquete).

La idea es que si yo quiero mandar algo y detecto que ya hay alguien mandando algo, espero un tiempo random y vuelvo a intentar.



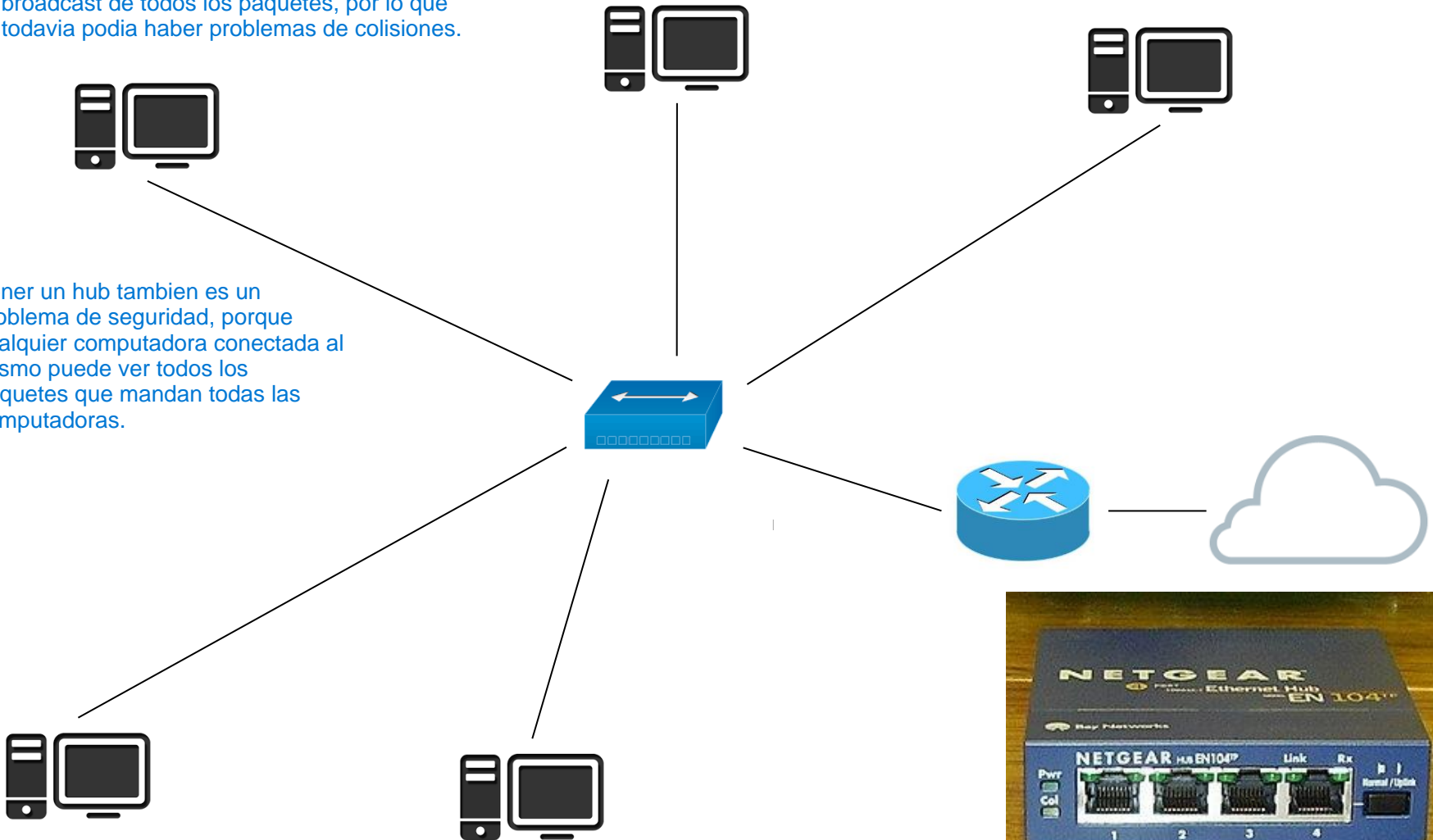
Al estar en cascada, si una compu se quedaba sin conexión, el resto también



El HUB llego para solucionar el problema de topología en cascada.
Lo que hacia es que si una computadora perdía la conexión, el resto no.
Sin embargo, el hub se encarga de hacer broadcast de todos los paquetes, por lo que todavía podía haber problemas de colisiones.

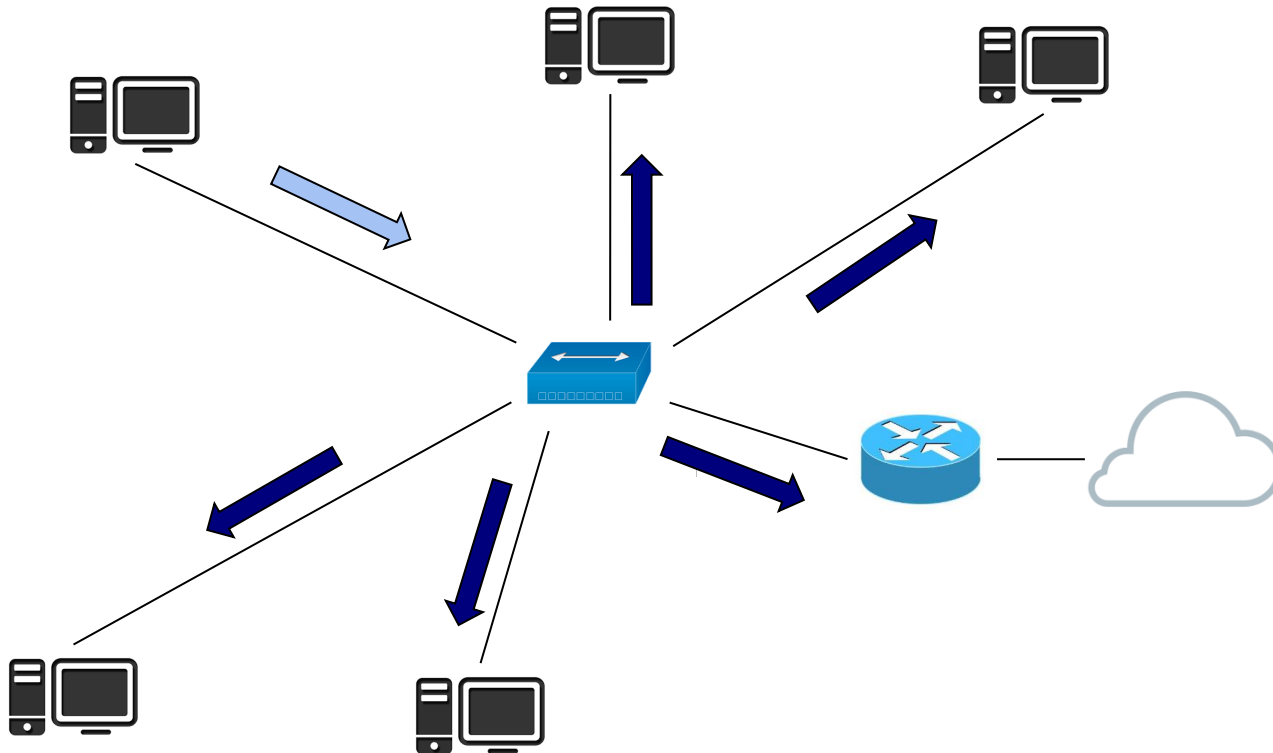
Evolución - Hub

Tener un hub también es un problema de seguridad, porque cualquier computadora conectada al mismo puede ver todos los paquetes que mandan todas las computadoras.



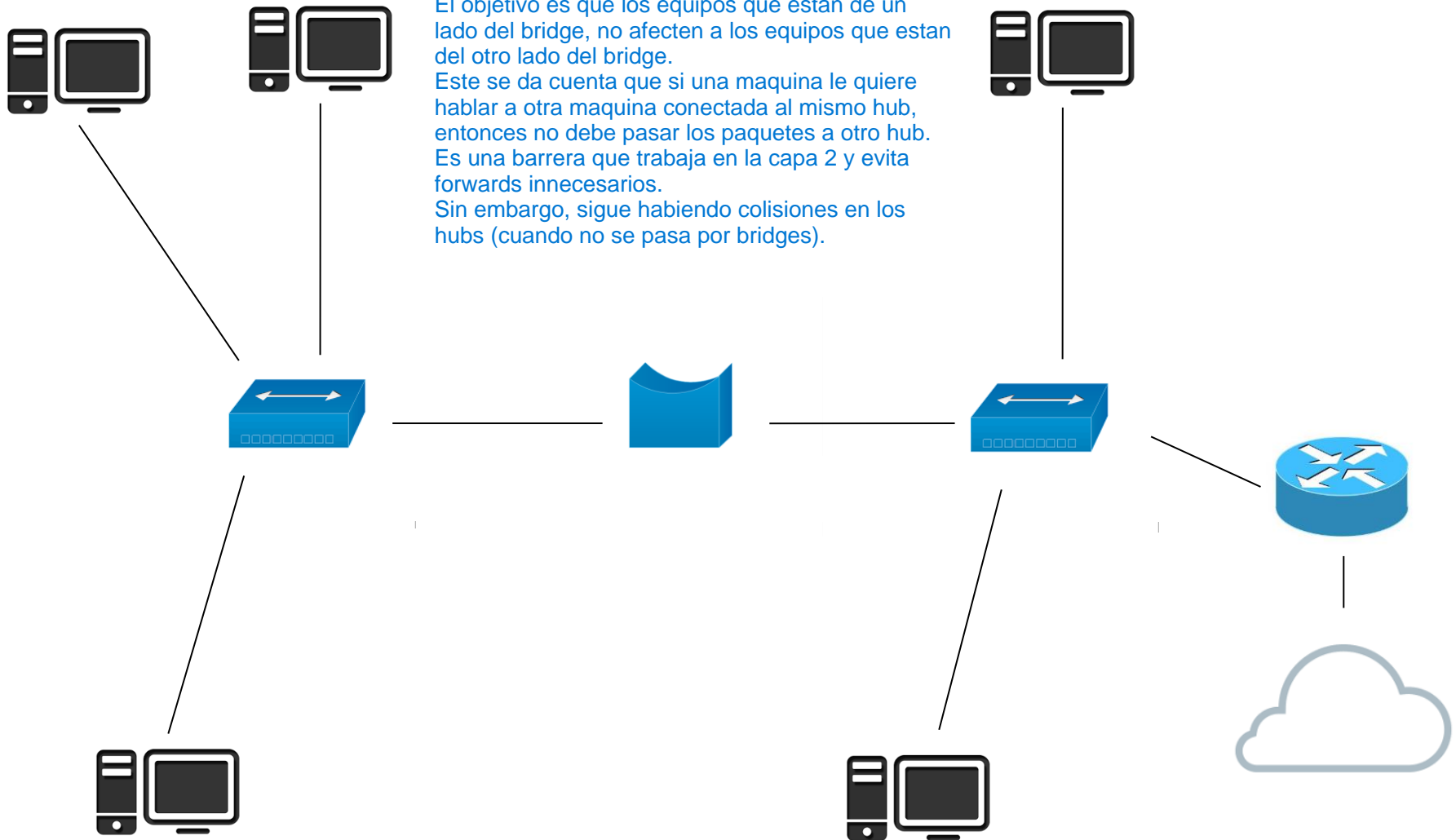
Hub - Funcionamiento

- Broadcast Siempre



Evolución - Bridge

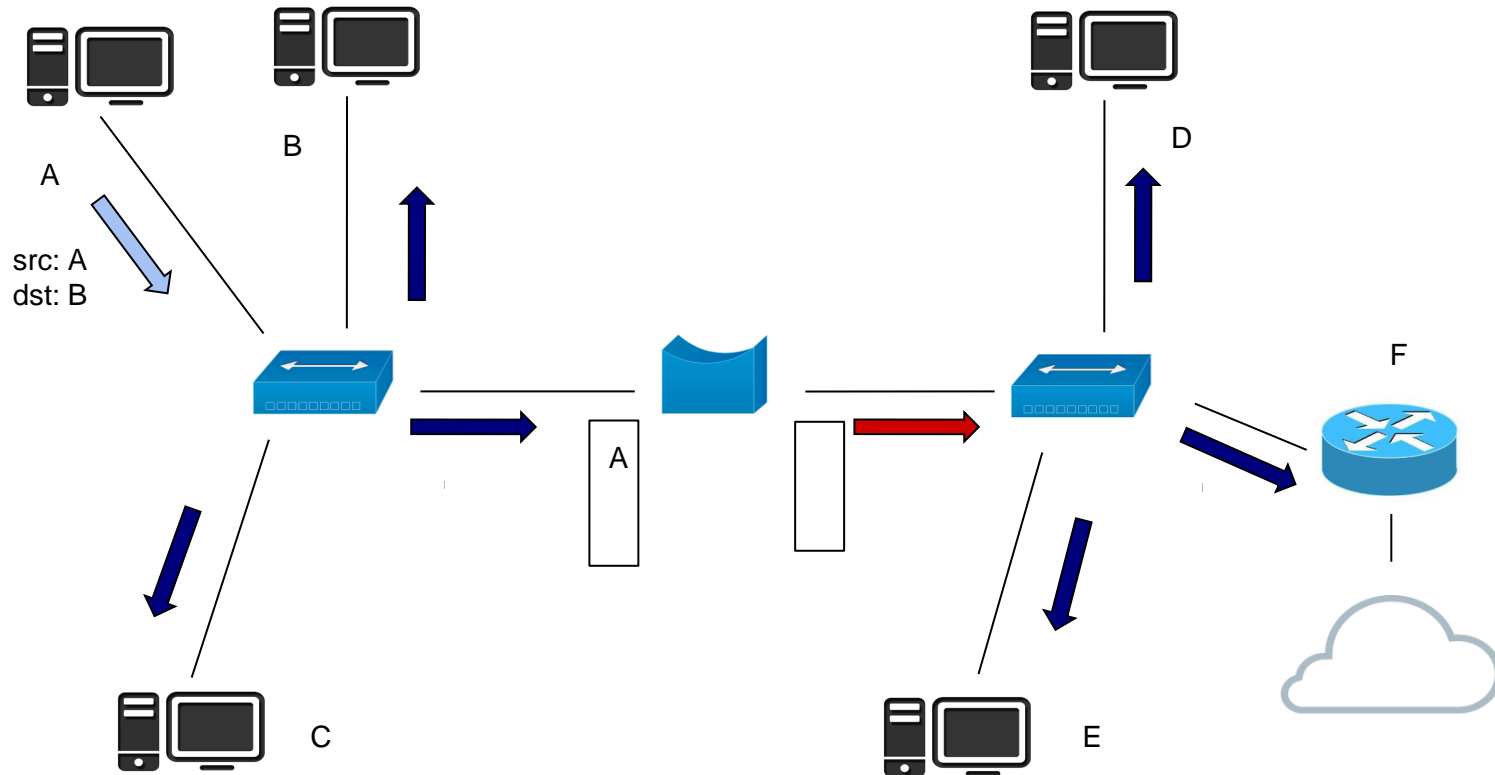
El bridge apaciguo un poco los problemas del hub. El objetivo es que los equipos que estan de un lado del bridge, no afecten a los equipos que estan del otro lado del bridge. Este se da cuenta que si una maquina le quiere hablar a otra maquina conectada al mismo hub, entonces no debe pasar los paquetes a otro hub. Es una barrera que trabaja en la capa 2 y evita forwards innecesarios. Sin embargo, sigue habiendo colisiones en los hubs (cuando no se pasa por bridges).



Puente ó Bridge

- Conecta dos LAN
- Opera en la Capa 2 del modelo OSI
- Decide que frames pasan o no entre interfaces
- Sirve para dividir dominios de colisión
- Se usan en forma virtual en la actualidad
- Como equipo se pueden usar como “stealth firewall”
- No cambian la topología de la red, no cambian los gateways ni se ven en un traceroute

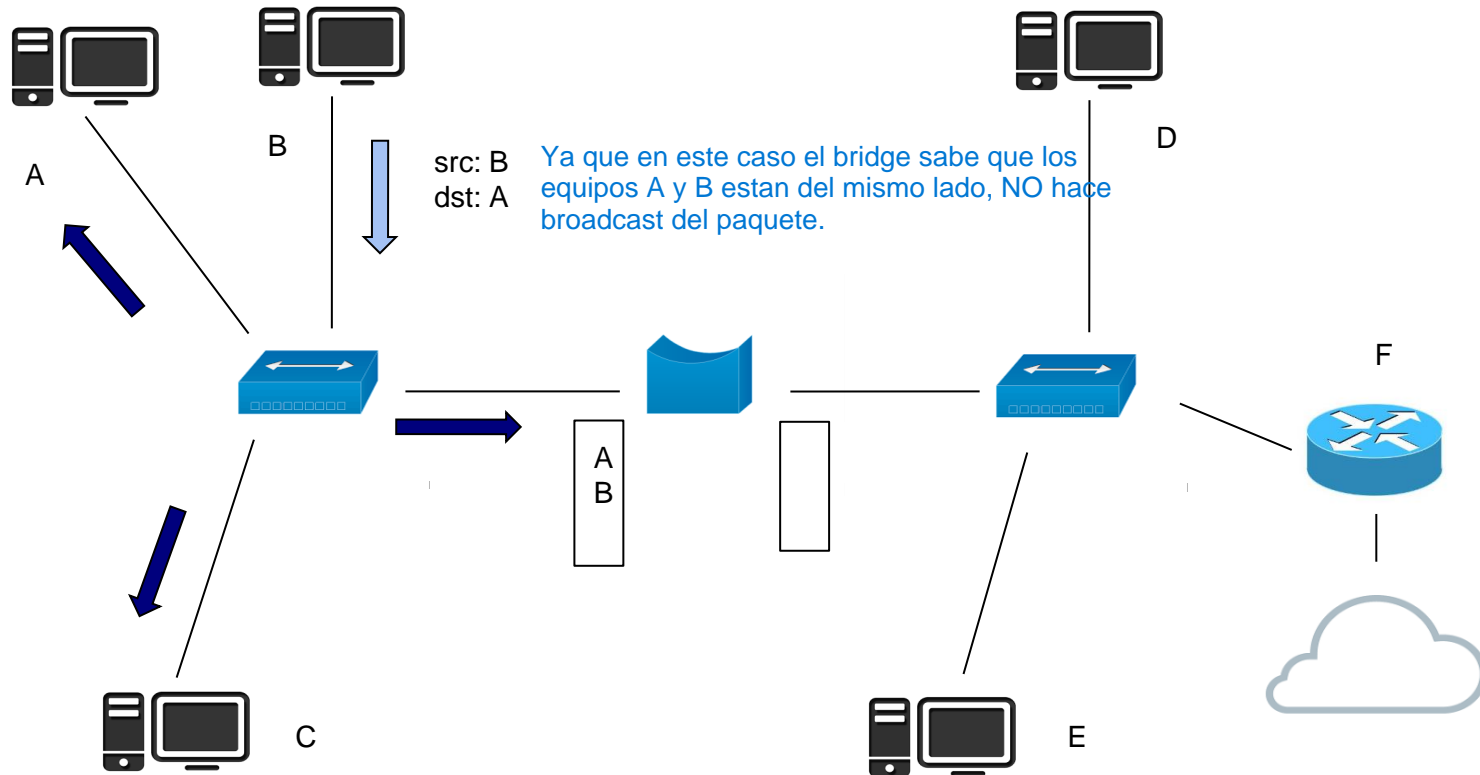
Bridge - Inicial



■ Bridge inicialmente broadcast

Quando el bridge no sabe de que lado esta cada MAC, hace broadcast. A medida que los equipos se comunican entre si, va completando la tabla de donde esta cada equipo.

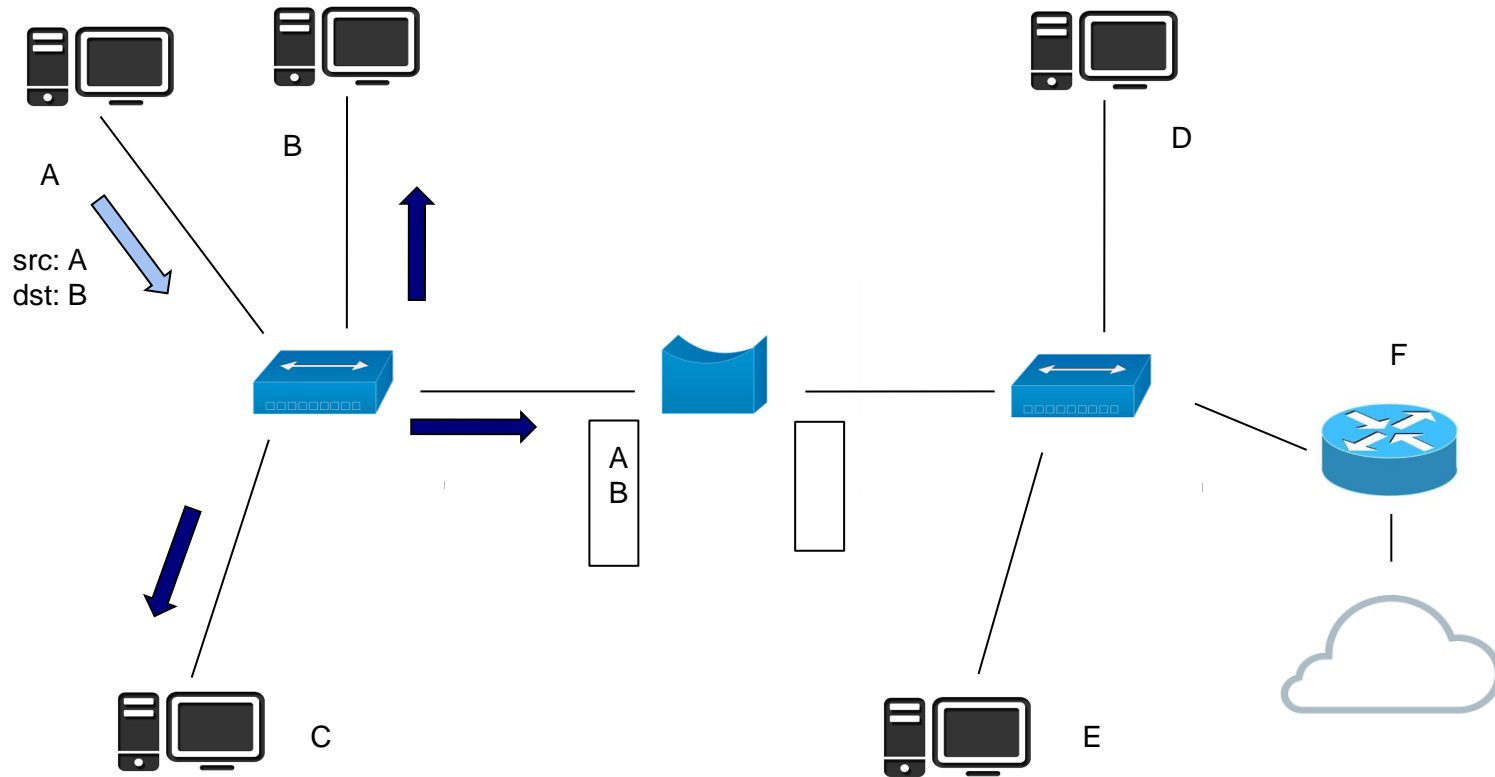
Bridge - Inicial II



- Bridge no hace el Broadcast
- Bridge continua armando tabla

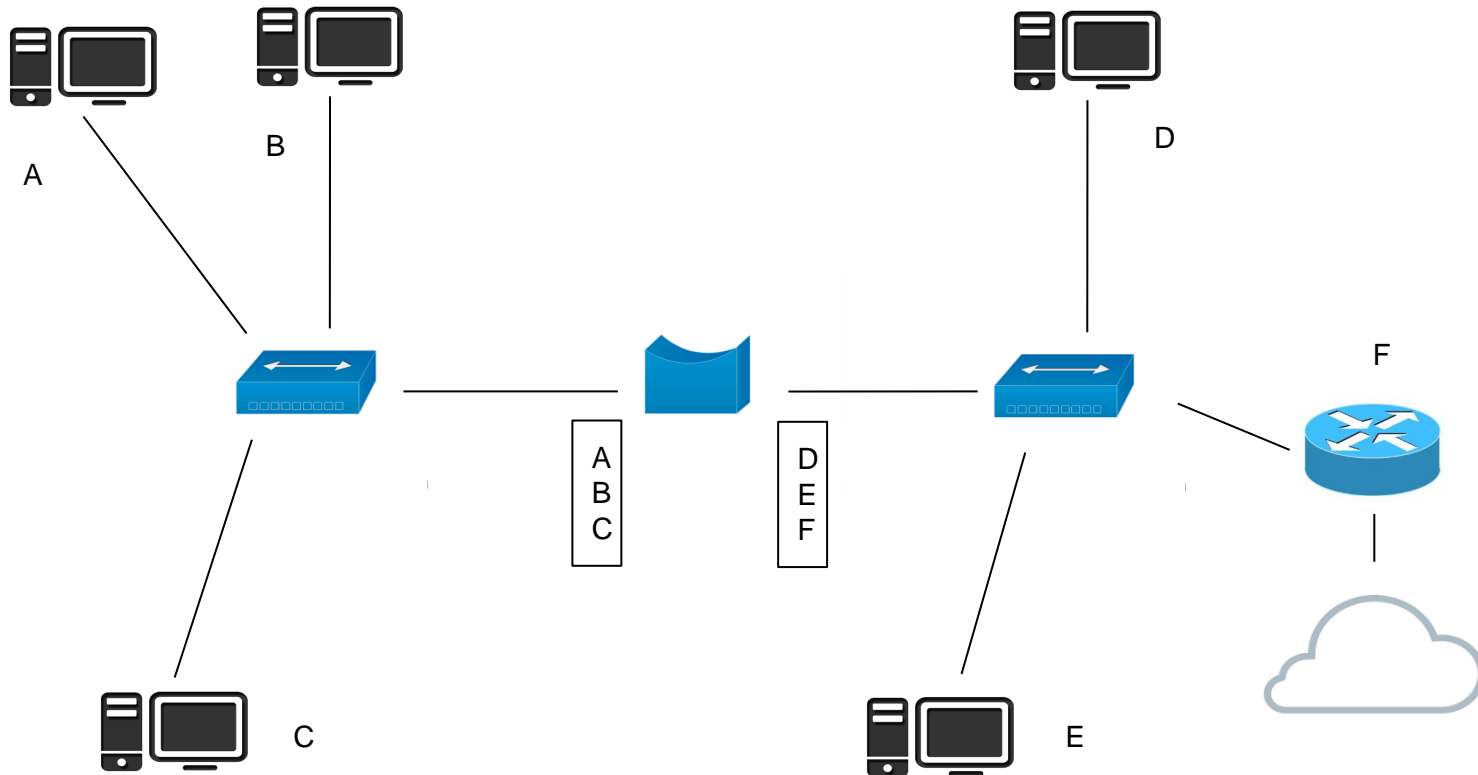
Los items de la tabla tienen un TTL, se van refrescando.
Si esto no fuera así, tendría problemas si cambio de lado un equipo.

Bridge - Estable



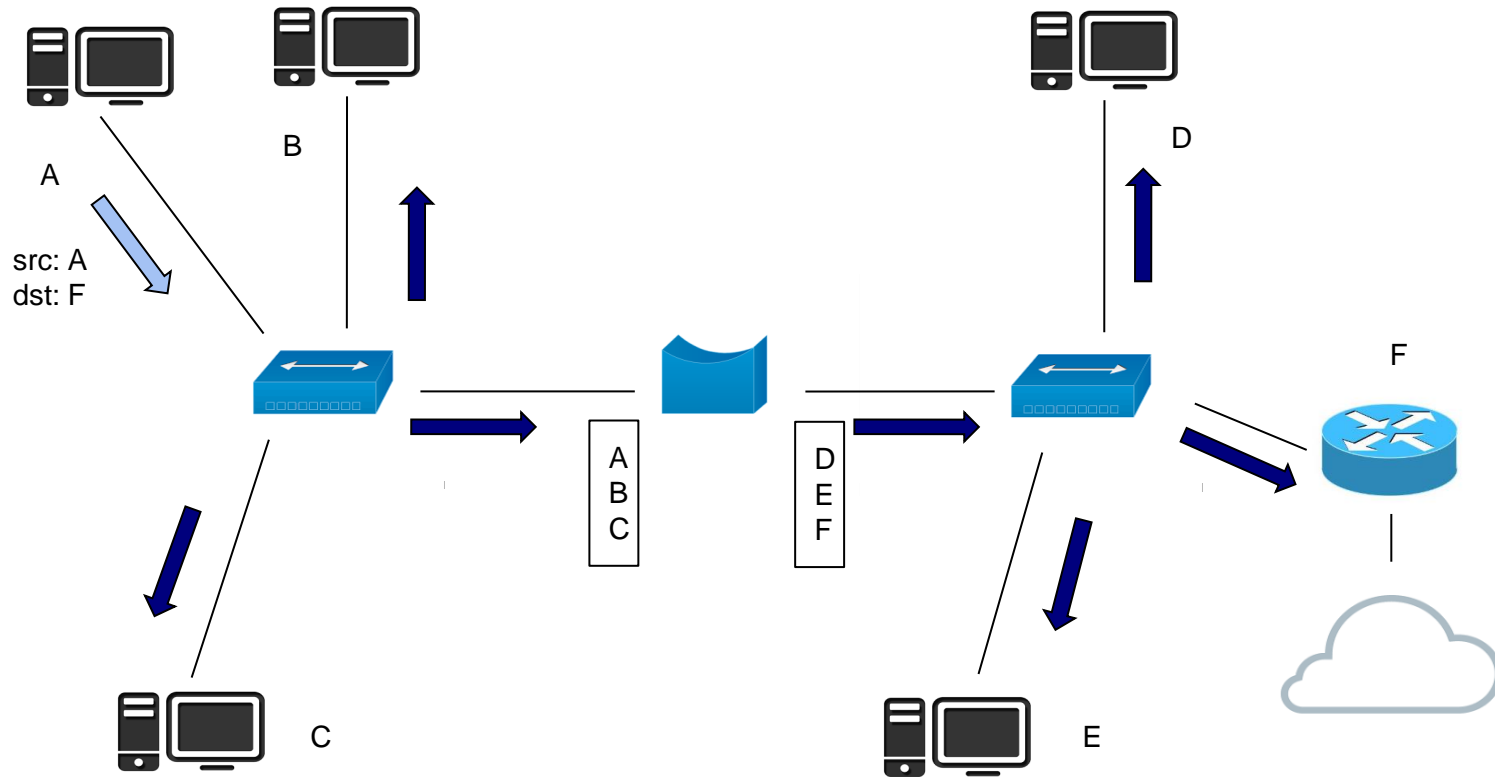
- Bridge no hace broadcast

Bridge - Estado Final



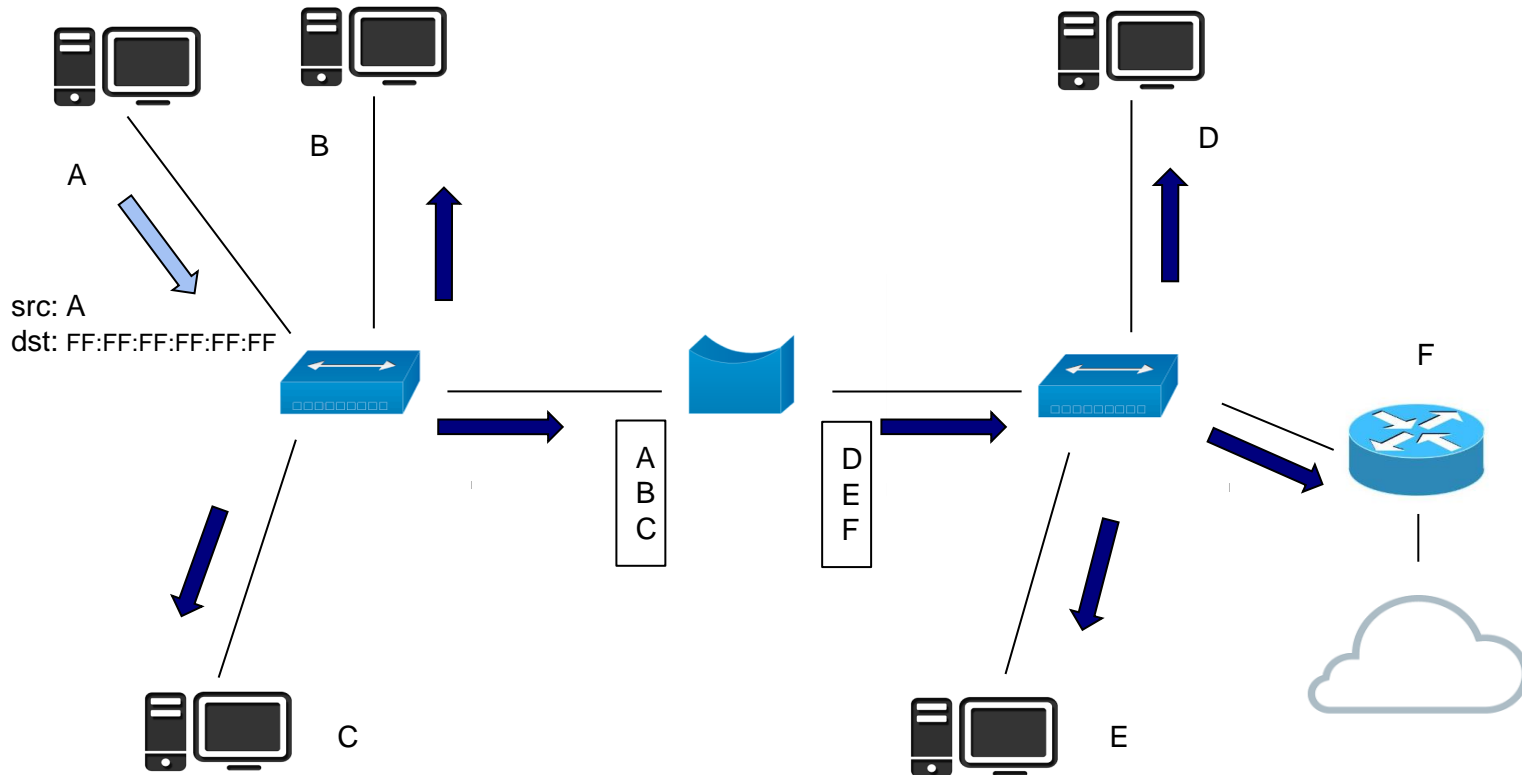
- Bridge tablas completas

Bridge



- Bridge pasa para el otro lado porque sabe que F está ahí

Bridge - Broadcast

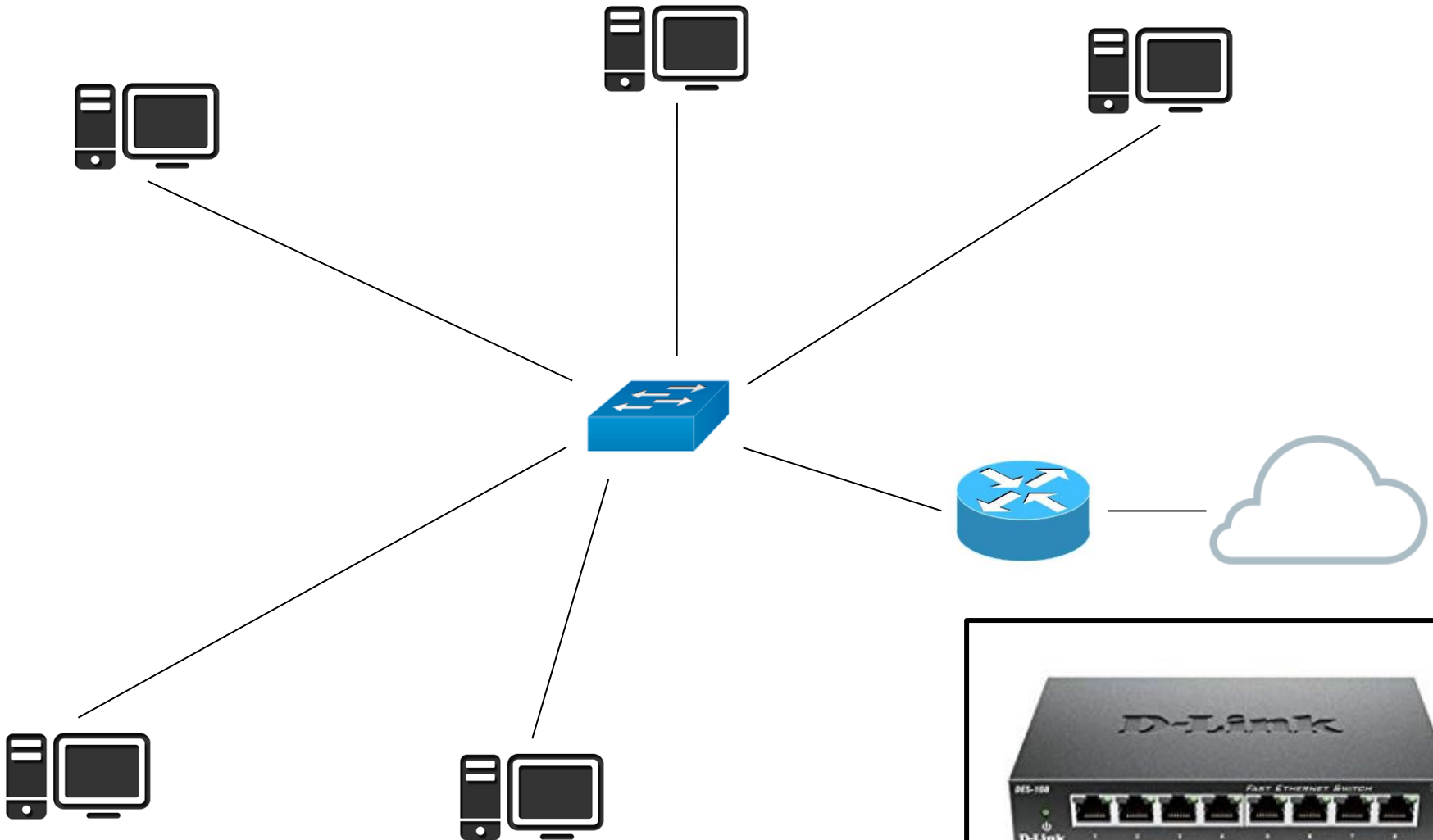


- Bridge pasa para el otro lado porque reconoce MAC de Broadcast (FF:FF:FF:FF:FF:FF)

En la actualidad, se usan "bridge virtuales" para conectarse con una VM en nuestra PC

Evolución - Switch

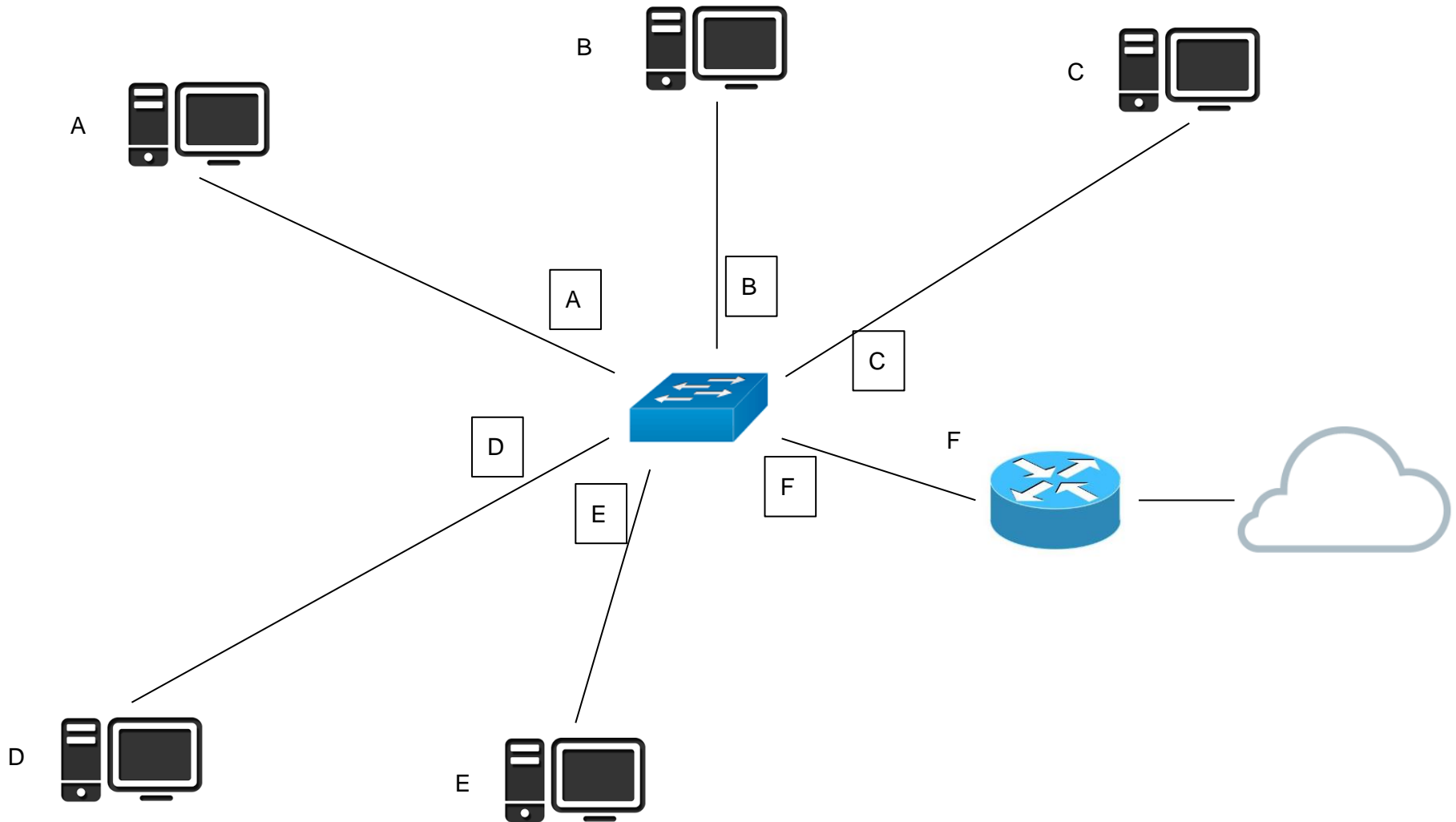
El switch basico, es un bridge con mas de dos puertos.



Switch

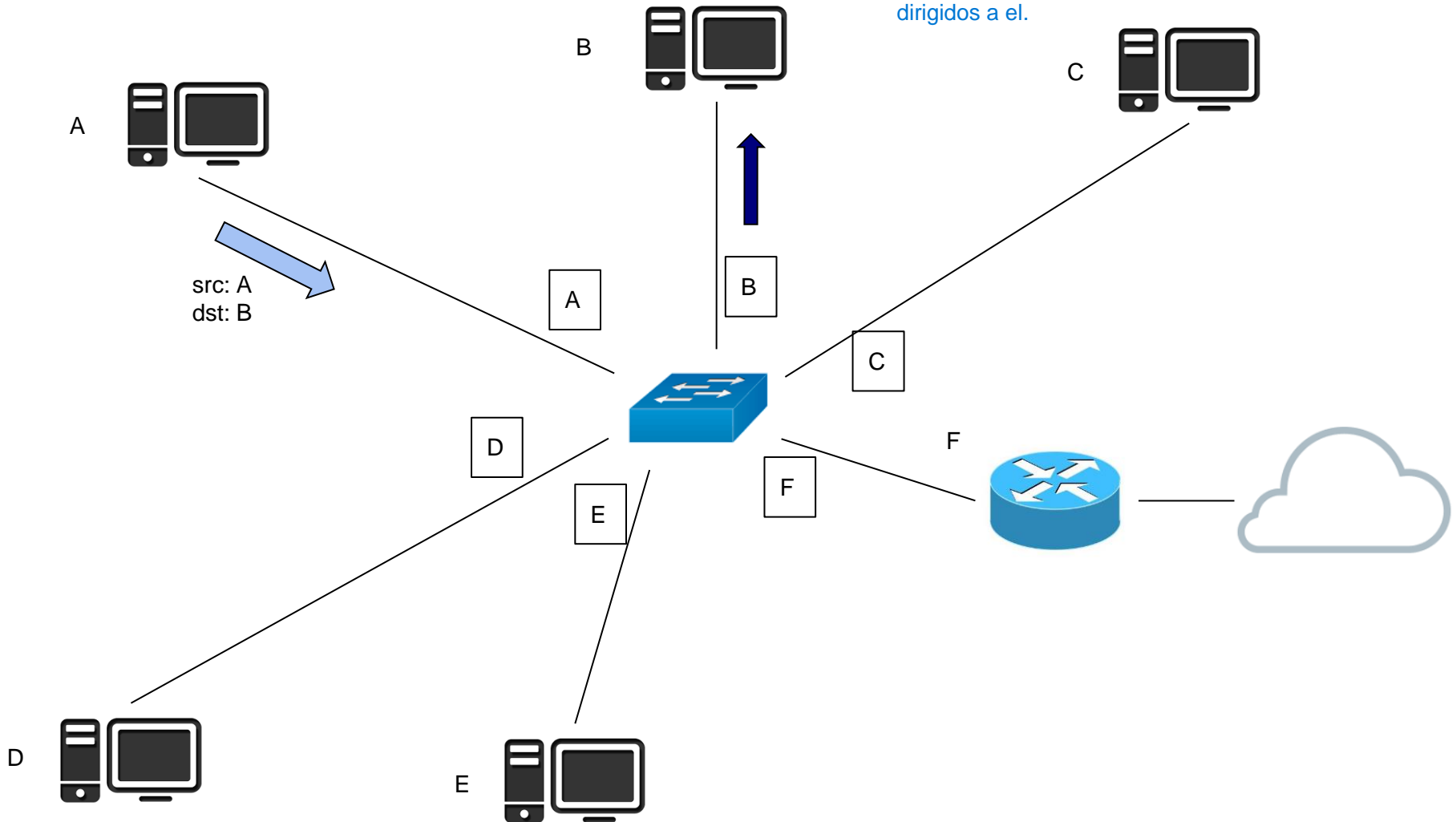
- “Bridge” de más de 2 puertos
- Muy difundidos
- Conmutan paquetes entre los puertos correspondientes
- Generan automáticamente la tabla de Switching
- Manejan Unicast, Broadcast y Multicast
- Existen los siguientes tipos:
 - Switch Layer 2 - Unmanaged
 - Switch Layer 2 - Managed
 - Switch Layer 3

Switch Tablas

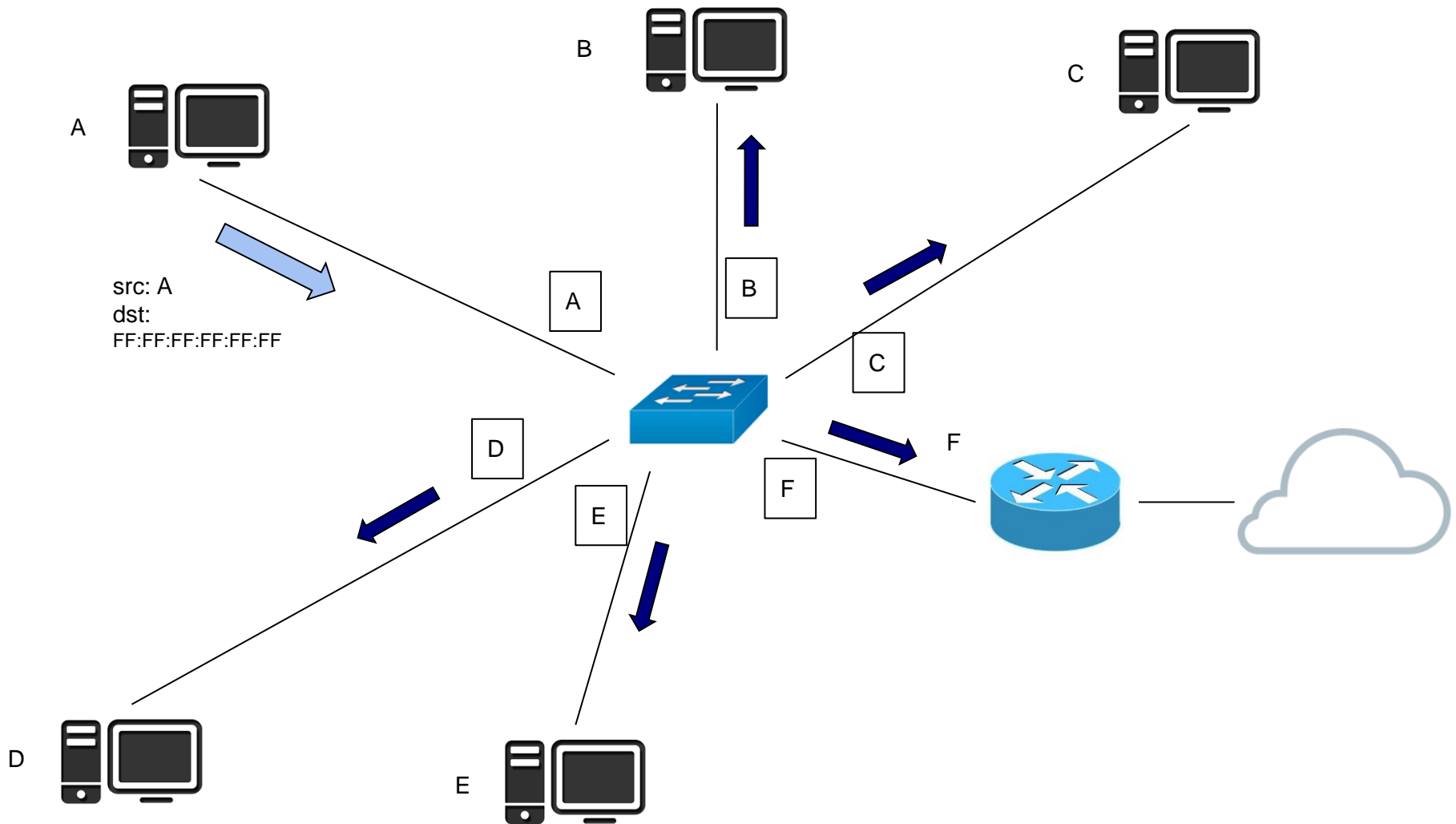


Switch - Estado Estable

Cuando el switch ya tiene la tabla armada, no hay colisiones en la red. Cada equipo solo recibe los paquetes que están dirigidos a él.

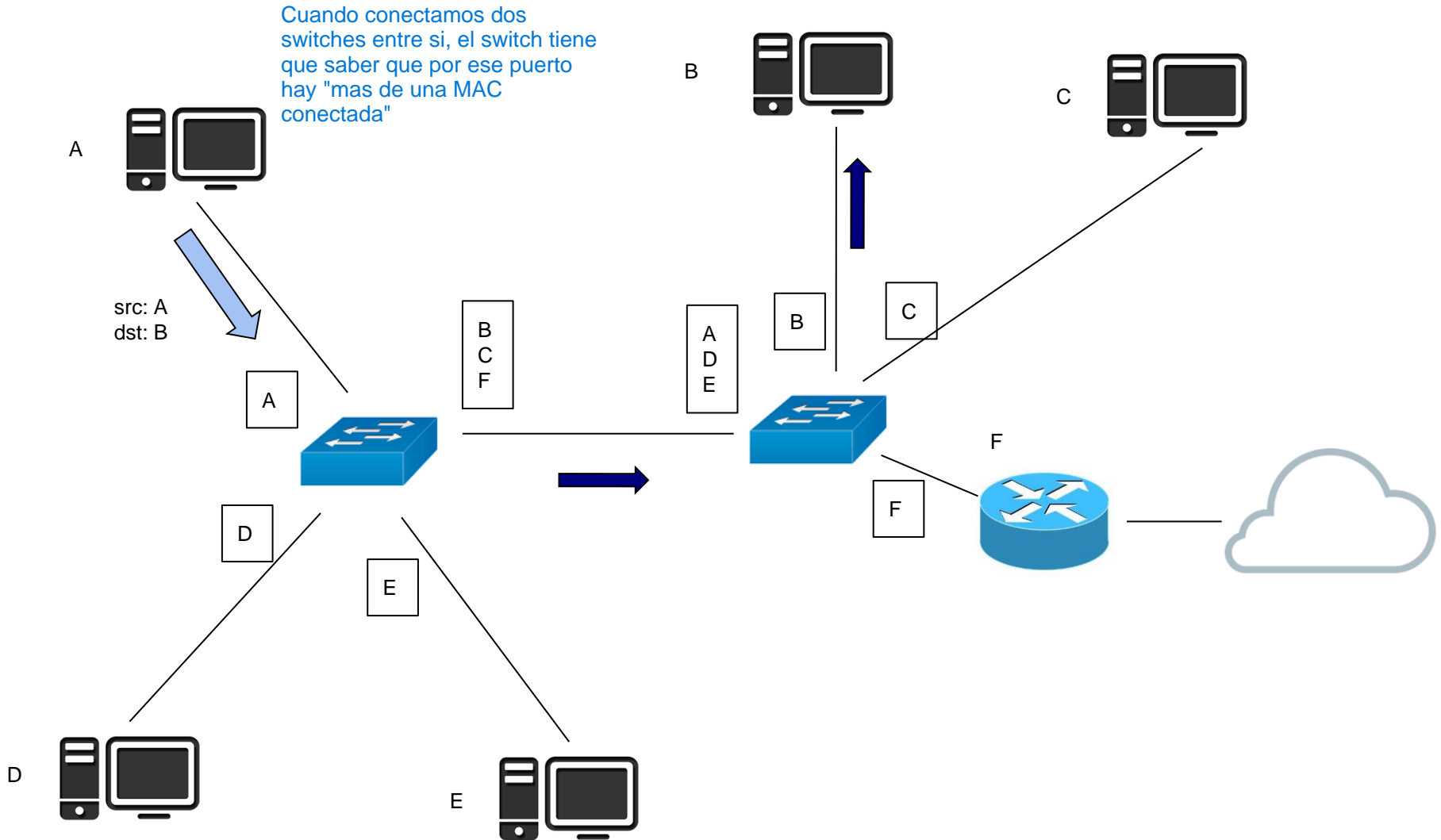


Switch - Broadcast

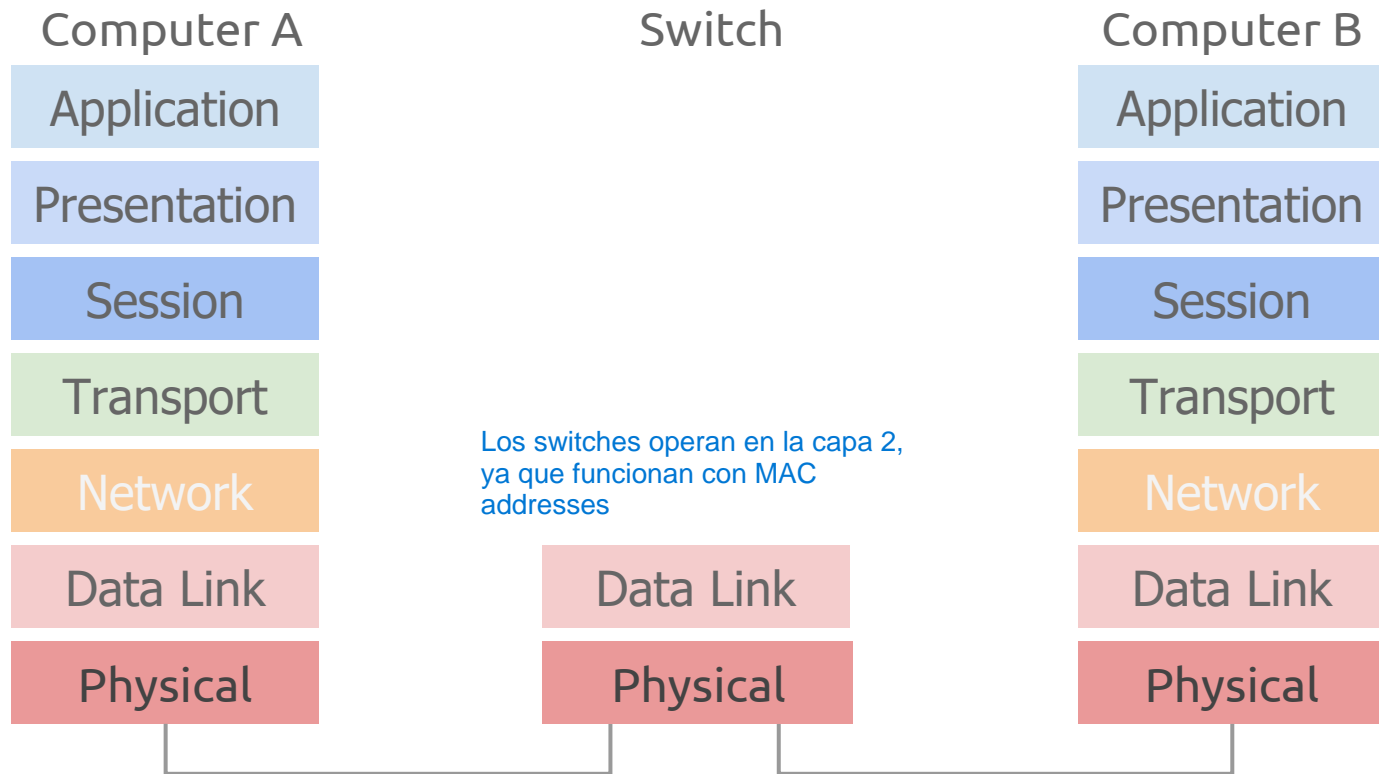


Switches en Cascada - Estado Estable

Cuando conectamos dos switches entre si, el switch tiene que saber que por ese puerto hay "mas de una MAC conectada"



OSI - Switch/Bridge





Switches Comerciales

Unmanaged Switches

PnP: no me tengo que conectar para configurarlo

- Plug and Play
- No tienen IP
- 10M/100M/1G/10G
- 4 a 24 puertos



Managed Switches L2 - Funcionalidades

L2: layer 2 managed

- VLANs
- Stacking de Switches Usar varios switches como si fueran uno solo
- Link Aggregation Usar varios puertos como si fueran uno solo (para mejorar el ancho de banda).
Uso dos puertos fisicos como un puerto logico.
- Multicast Se usa poco. Esta en capa 2 pero usa algo de capa 3.
- Spanning Tree Protocol/Rapid Spanning Tree Protocol
- Priorización de Tráfico (CoS)
- Limitación de Velocidad
- Flow control
- SNMP/RMON Monitorizacion

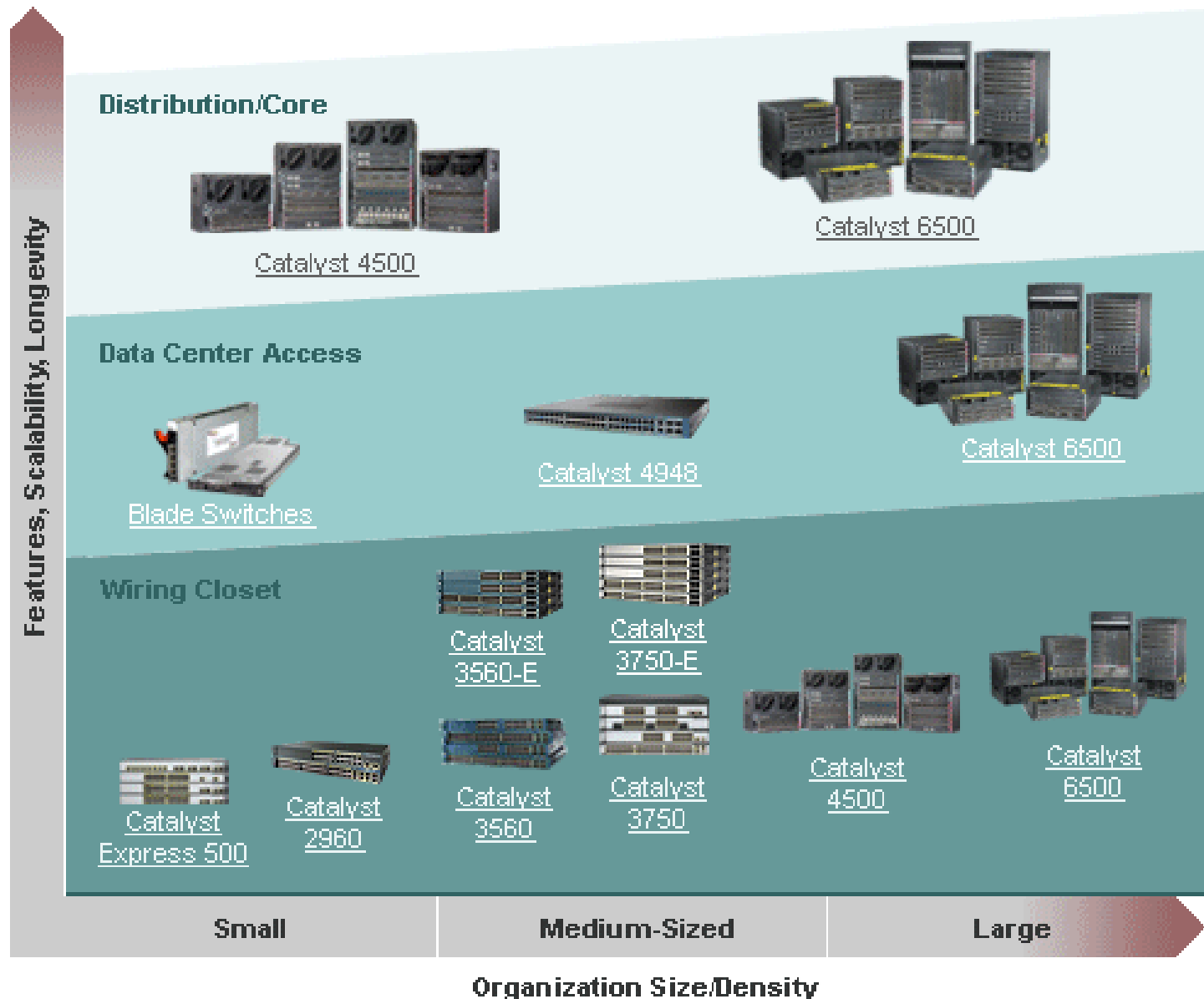
Managed Switches L3 - Funcionalidades

L3: layer 3 managed. Basicamente son routers (porque rutean y ven la capa 3)

- Toda la funcionalidad de L2
- Principalmente agregan IP Routing
- Ruteo estático y RIP
- Ruteo avanzado: OSPF, IGRP, BGP
- Permiten ruteo entre VLANs
- No poseen puertos WAN

No se conectan directamente a internet

Managed Switches – Familia CISCO

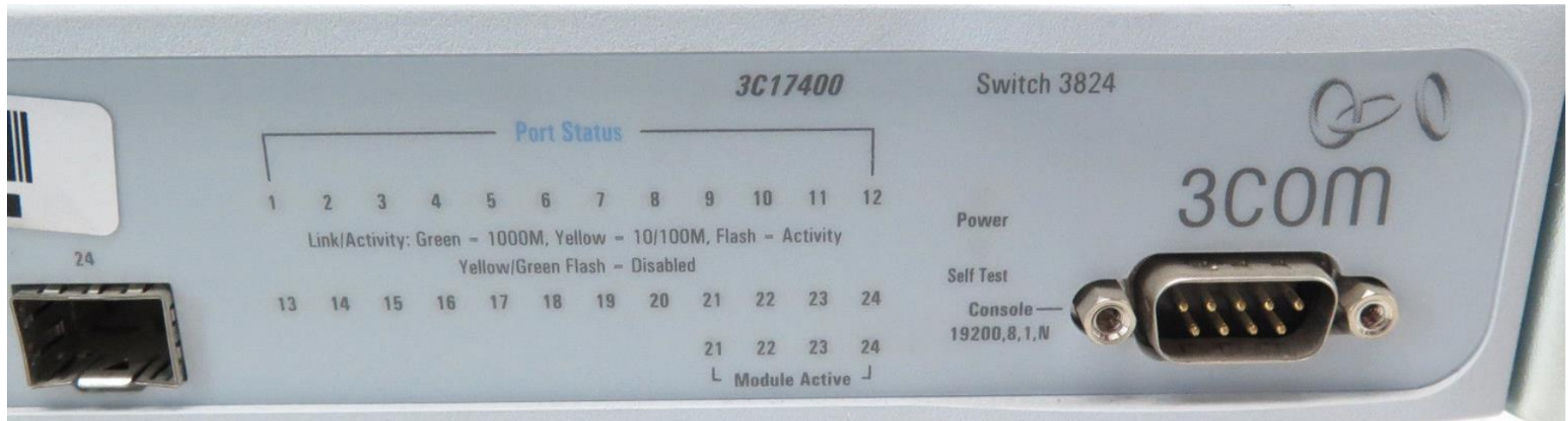


Switch de capa 2

- 3Com SuperStack 3 Switch 3824
- Managed 10/100/1000 switch.
- 24 Gigabit ports, 4 SFP ports. Los SFP son para poner conectores de fibra.
- Link aggregation (LACP) hasta 8-Gbps.
- Switch fabric capacity: 48 Gbps.
- MAC Address: 16.000.
- Hasta 254 VLANs.
- Rapid Spanning Tree Protocol.
- Management: SNMP, RMON, Web
- Protocolos: ARP, IGMP, IP, DHCP, TFTP.
- Expansiones: 1000Base-T (RJ-45), 1000Base-SX, 1000Base-LX, 10Base-T/100Base-TX (RJ-45) Cada puerto puede manejar distintas bases



Switch de capa 2 frente



Algunos todavía tienen el puerto serie. Esto sirve para configurarlos, porque si está muy mal configurado tal vez ni siquiera puedes conectarte a configurarlo de vuelta.

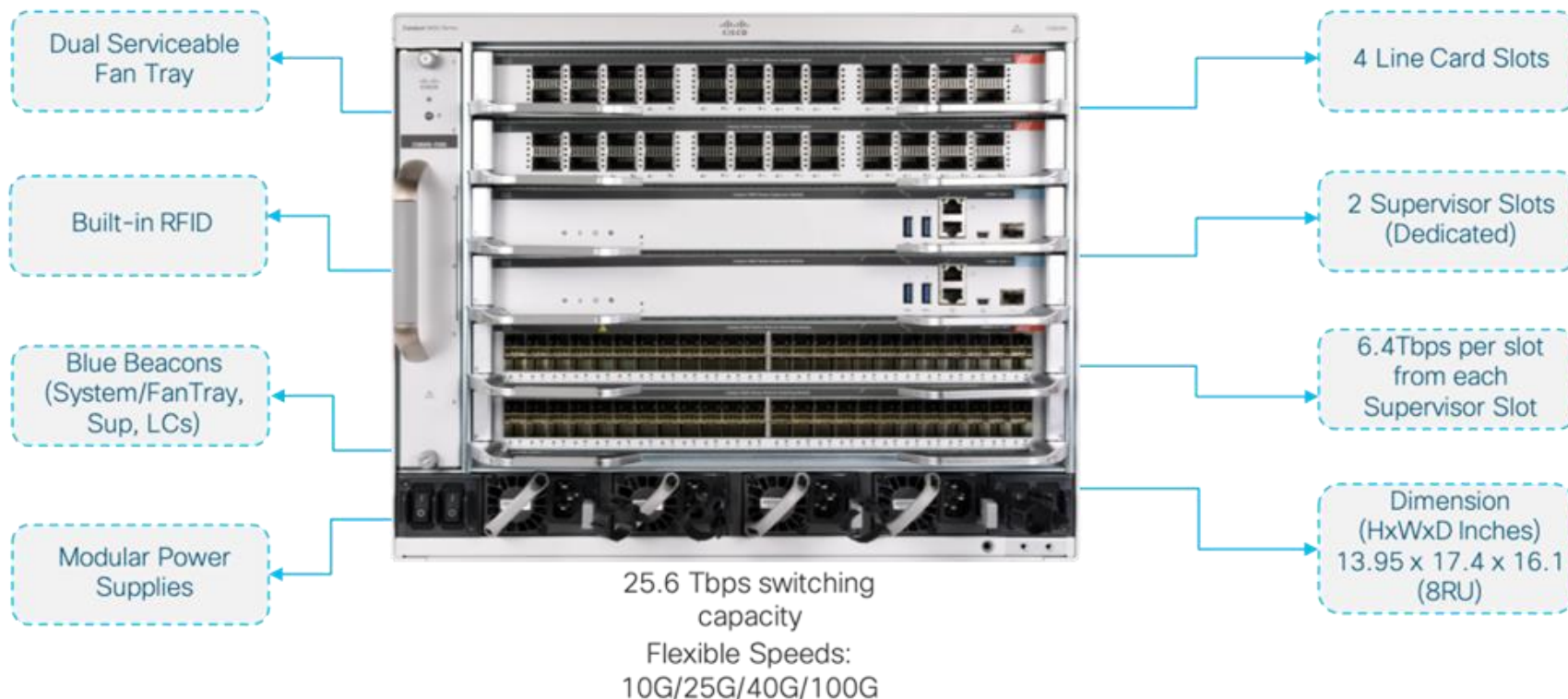
Switch de capa 3

- Cisco Catalyst 3560 Switch
- Managed 10/100/1000 Layer 3 switch.
- 24 Gigabit ports, 4 SFP ports.
- Basic IP unicast routing: static, RIPv1, RIPv2 and RIPv6
- Advanced IP unicast routing: OSPF, IGRP, EIGRP, BGPv4
- IPv6 routing capability: OSPFv3, EIGRPv6
- Inter-VLAN IP routing
- 32 Gbps forwarding bandwidth
- 38.7 Mpps

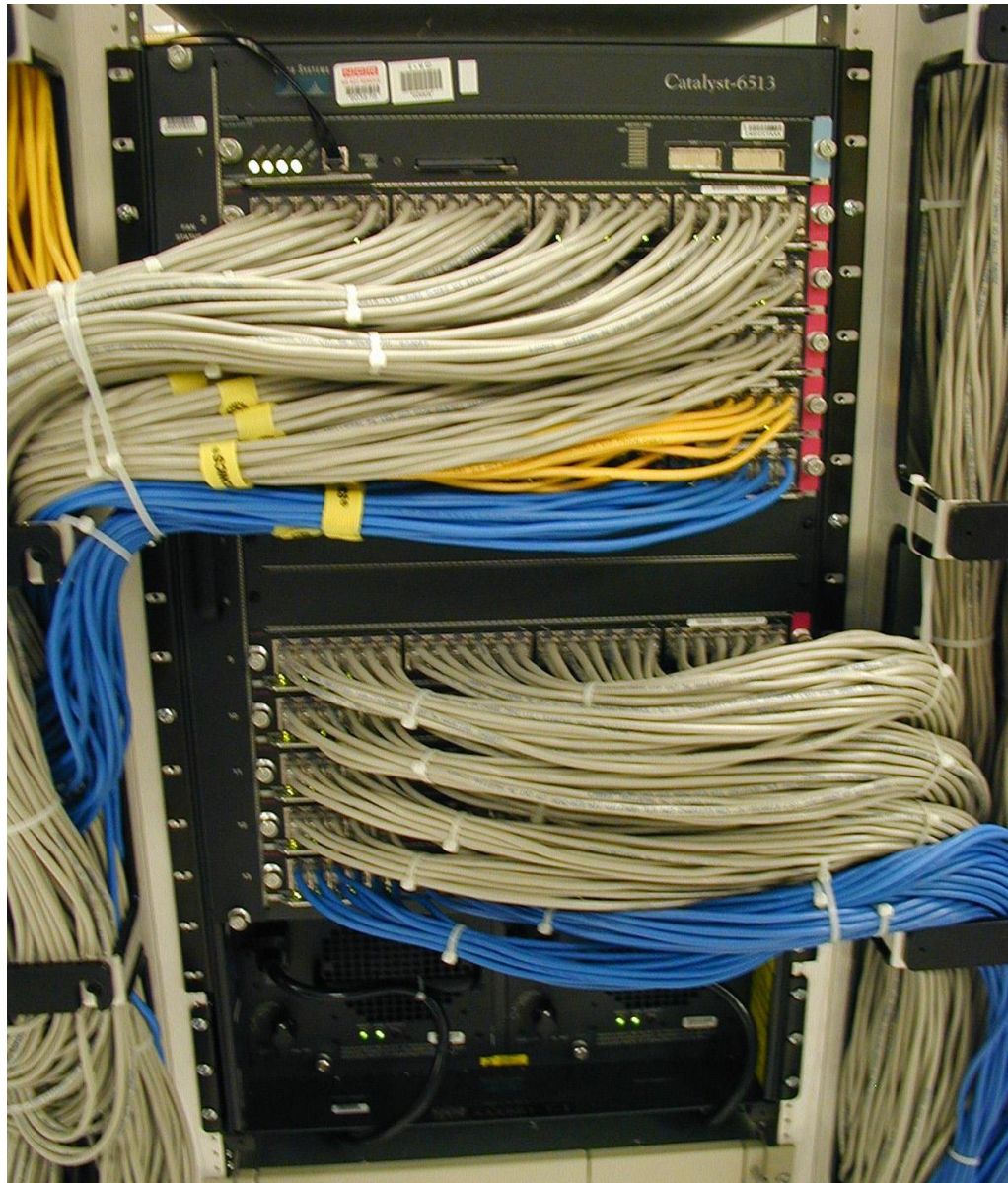


Switch Cisco Catalyst 9600

- Cisco Catalyst 9600 Switch
- 25.6 Tbps forwarding bandwidth
- 3 Bpps 3 billones de paquetes por segundo
- Hasta 48 100 Gigabit Ethernet ports
- Hasta 256 50G/25G/10G Gigabit Ethernet ports
- 8 Rack Units



Switch Cableado



Nos permite ver varios switches como un solo switch.
Esta tecnología es propietaria de cada marca.

Stacking de Switch

A veces estos switches se configuran en anillo para tener redundancia

- Interconexión de Switches por puertos especiales
- Única dirección IP de administración
- Mayor Gbps en puertos especiales.
- Mejor distribución de frames
- Tienen que ser de la misma marca (propietario)



Allied
Telesis

Stacking de Switch

- Se suele utilizar topología anillo
- A uno de los switch se lo configura como MASTER
- A otro como SLAVE
- El resto como miembros del stack
- Todos tienen un ID único
- El sistema descubre el camino optimo para el frame





Break!

Ethernet

Si no hay VLAN, estos 4 bytes ni se mandan

Capa OSI	Preám bulo	Inicio de Frame	MAC Destino	MAC Origen	VLAN tag opcional	Type of Frame o longitud	Payload	CRC	Inter packet gap
	7 Bytes	1 Byte	6 Bytes	6 Bytes	4 Bytes	2 Bytes	46-1500 Bytes	4 Bytes	12 Bytes
Capa 1									
Capa 2									

El prio nos permite definir la prioridad de nuestros paquetes

TPID	Prio	DEI	VLANID
16 bits	3 bits	1 bit	12 bits

El VLANID es el identificador de cada VLAN

0x8100

Si el type of frame vale esto, entonces quiere decir que van a venir unos bytes adicionales que son de VLAN

VLAN

La VLAN nos permite dentro del mismo switch, generar el equivalente a tener varios switches distintos (generando distintas LANs).

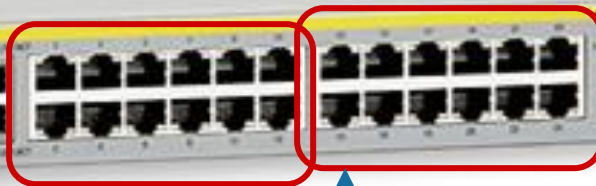
Esto permite administrar mejor la red, generando redes locales separadas aunque estemos compartiendo el switch

- Define dominio de Broadcast (para ARP por ejemplo)
- Separación de tráfico
- Permite tener IP overlapping
- Debe estar configurado en los Switches o en los hosts
- Requiere de un Switch Managed L2 o L3

VLAN es de layer 2

VLAN

VLAN 2



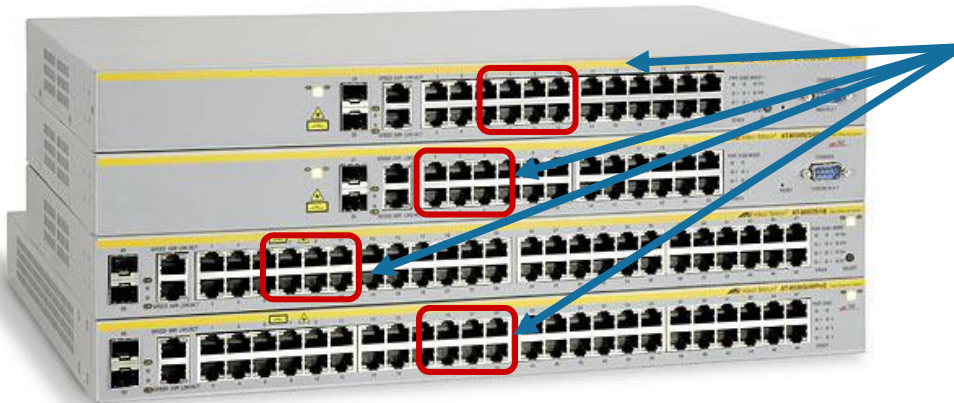
Puedo tener mas VLAN que puertos

VLAN 1



VLANs

- Las VLANs se pueden crear en stacking
 - Por ejemplo la VLAN 2 puede existir en varios switch del stack

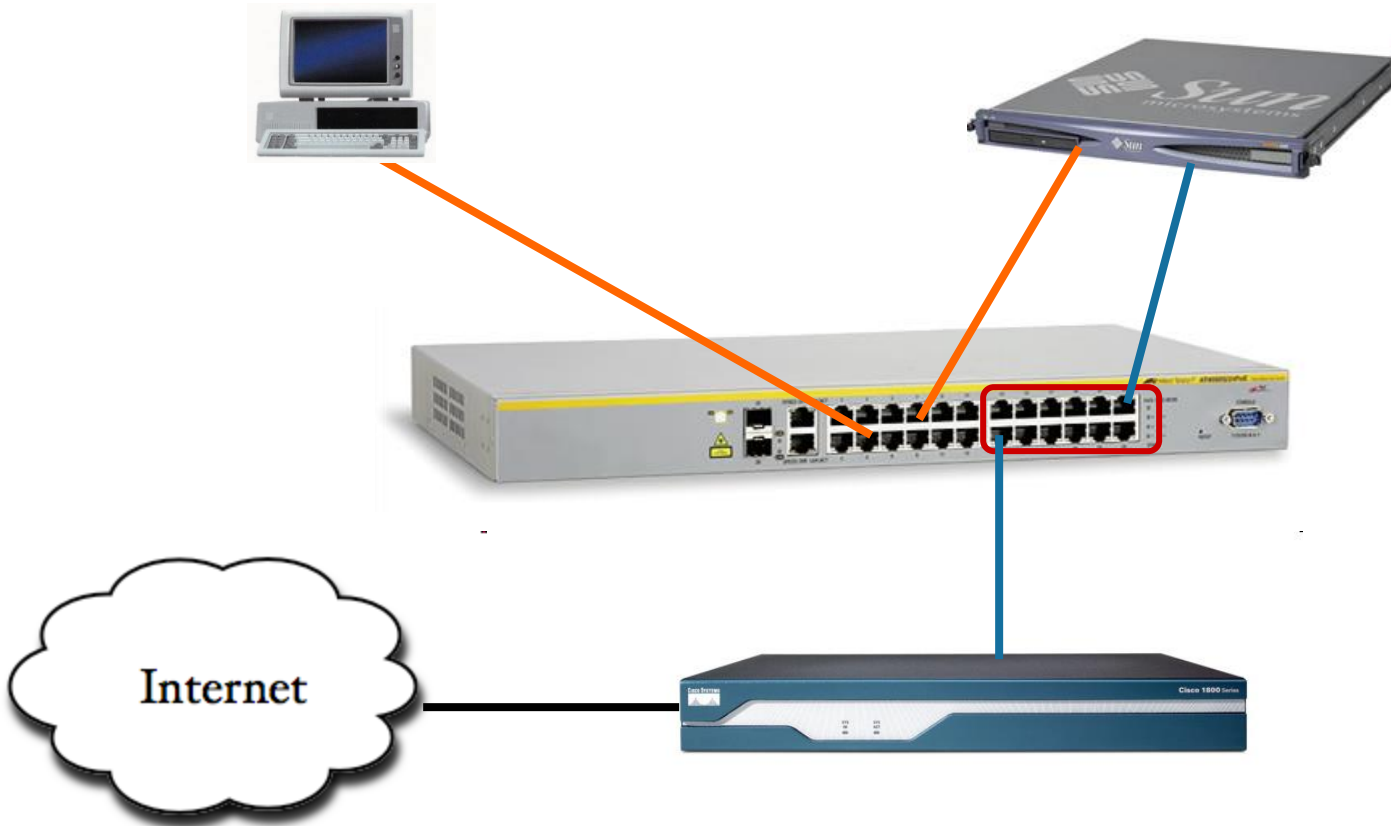


VLAN 2

Ejemplo de VLAN

■ VLAN para INTERNET

Hay 2 VLAN una local y una que se conecta a internet. La única que esta en las dos VLAN esta en el firewall.



VLAN - Untagged

Hay dos tipos de VLAN. Tagged y Untagged.

En untagged, cuando un emisor manda un paquete viene sin VLAN, se le agrega el tag de la VLAN. Cuando va a un paquete a ese emisor, se saca la tag de VLAN.

Este caso se debería a que mi computadora puede no saber que esta en una VLAN. Hacer que sea untagged hace que el proceso sea transparente para la computadora.

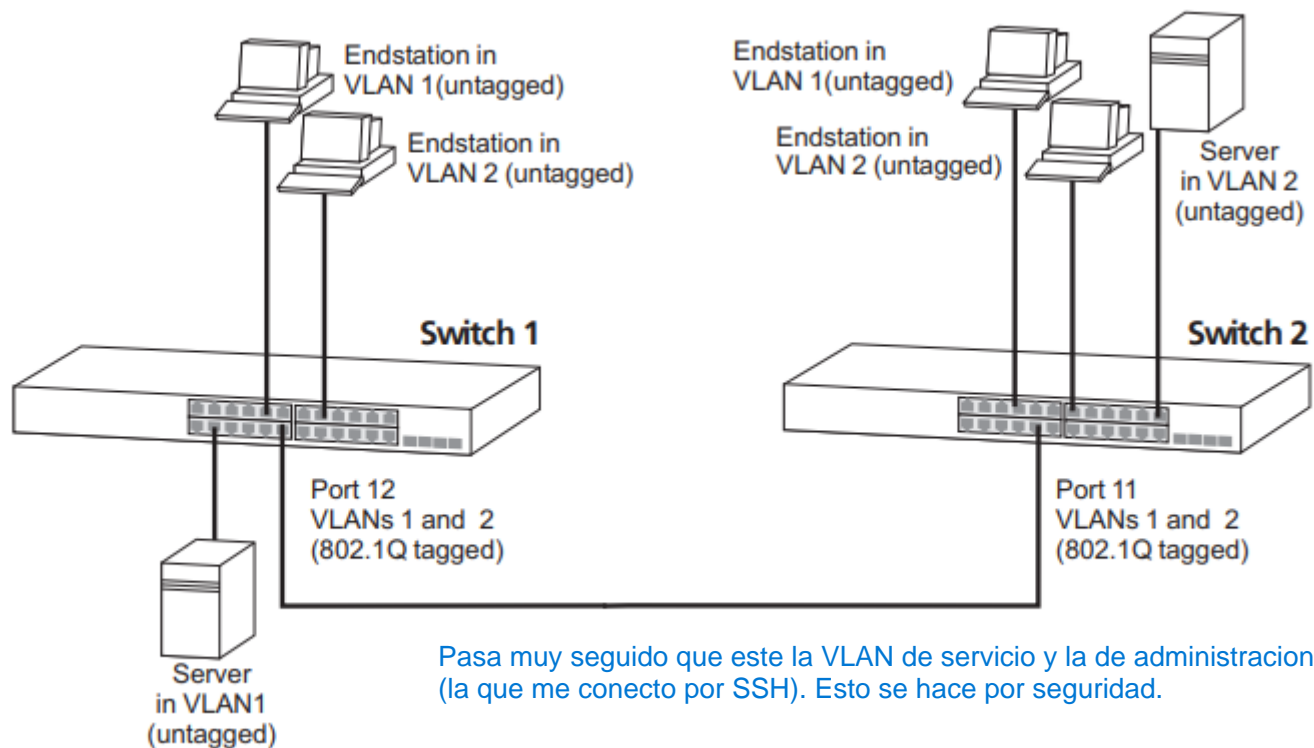
- Hosts no tienen configurado el VLAN
- El Switch agrega el VLAN Tag al recibir un paquete en un puerto Untagged
- El Switch quita el VLAN Tag al enviar un paquete por un puerto Untagged

VLAN - Tagged

- Hosts deben tener configurado el VLAN
- El Switch espera el VLAN Tag al recibir un paquete en un puerto Tagged
- El Switch mantiene el VLAN Tag al enviar un paquete por un puerto Tagged
- Los puertos Tagged pueden incluir un 'Native VLAN' que define el tag para el tráfico Untagged que llega al puerto.

Si viene sin tag, se asume que es tagged y le agrega el tag default de una VLAN en específico

Ejemplo de VLAN tagged

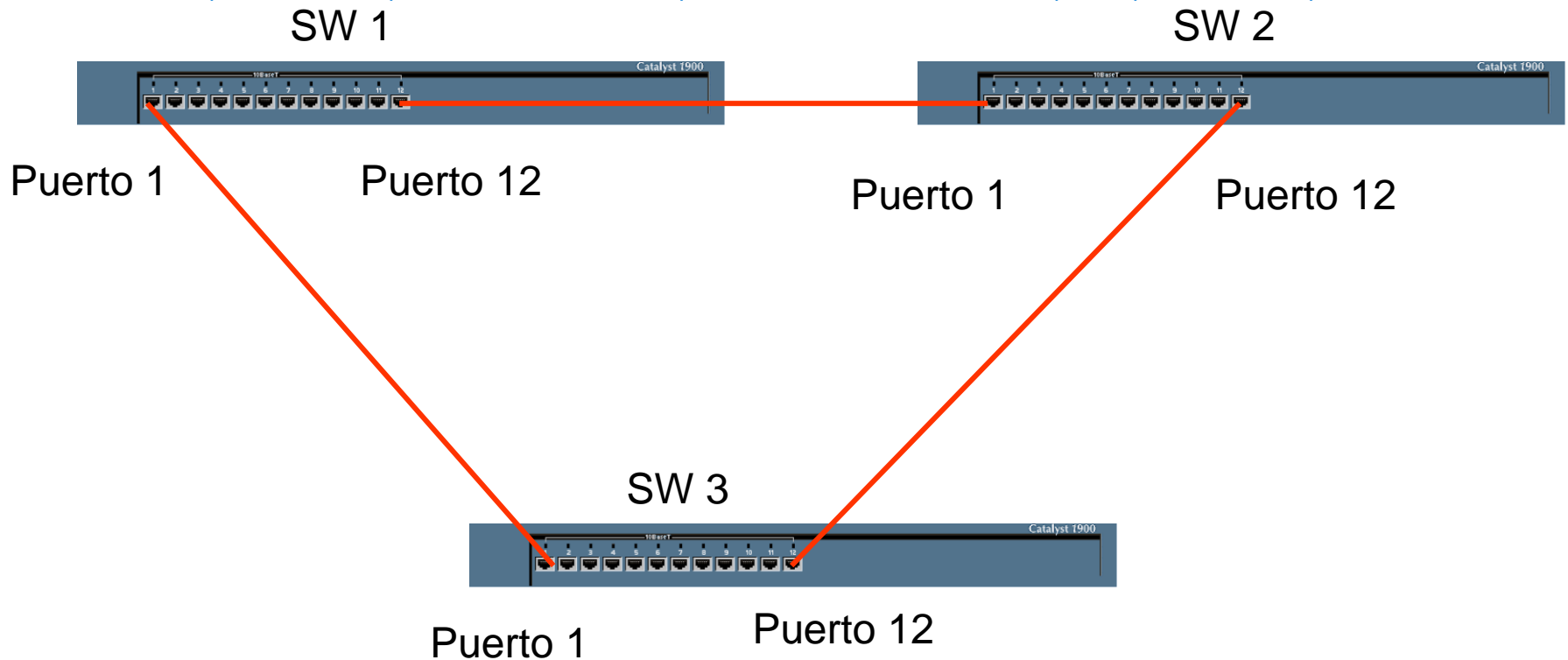


Spanning Tree Protocol

■ Problema de loop o enlaces redundantes

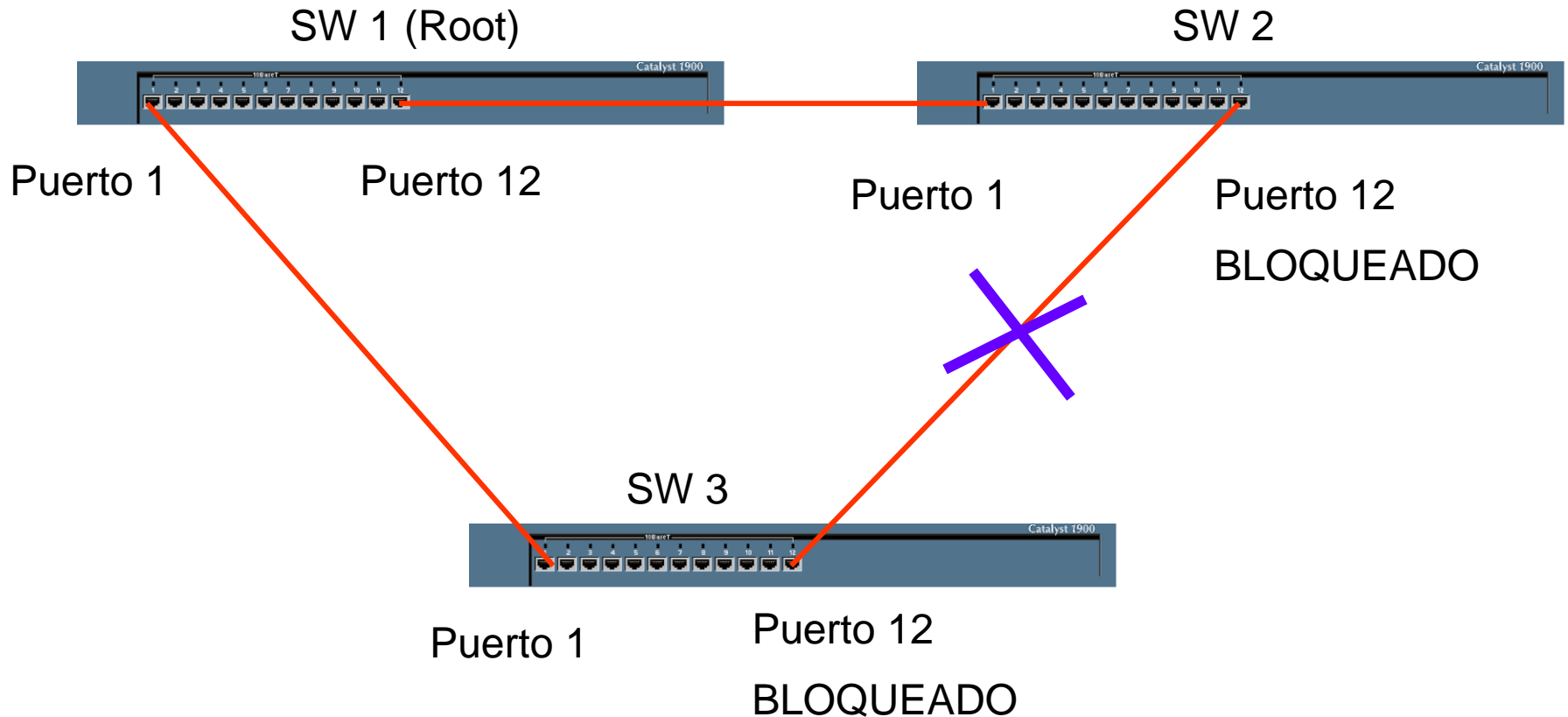
Cuando alguien manda broadcast, el paquete puede reenviarse para siempre.

El spanning tree es un algoritmo para bloquear puertos en el switch, para que haya un unico camino hacia cualquier lado, y que los otros caminos queden de backup. Ante la deteccion de un problema en el camino, se desbloquea el puerto de backup.



Spanning Tree Protocol

- Priorización de puertos



Spanning Tree Protocol – STP

- IEEE 802.1 D
- Permite enlaces redundantes
- Aumenta la disponibilidad
- Se puede calificar a los enlaces paralelos
- Prioriza enlaces más eficientes
- Ante caída de enlace habilita al siguiente en orden de prioridad
- Por default envío de paquete BPDU cada 2 segundos

Originalmente, el STP tardaba de 30 segundos a 1 minuto en encontrar una respuesta.
Despues surgio el Rapid Tree Protocol, que tarda pocos segundos pero es mas complejo

STP – Procedimiento

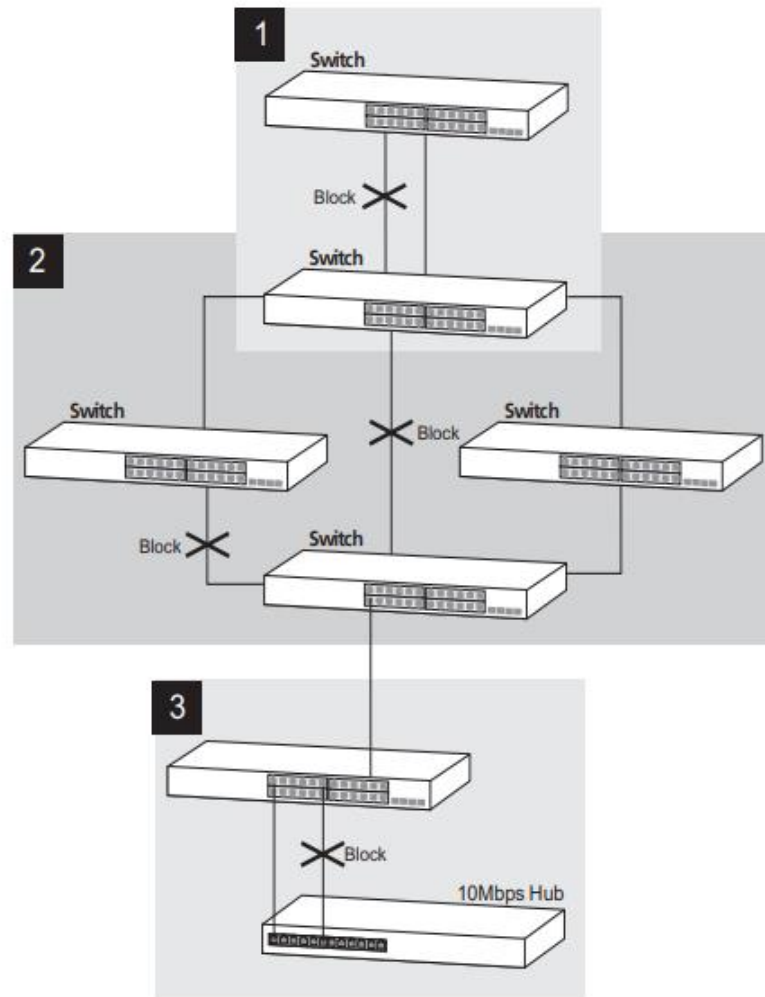
- La idea es armar un árbol deshabilitando enlaces extra
- Entre los nodos se elige un node “root”
 - Se utiliza la MAC de cada Switch (MAC propio del switch para Management o STP) + Priority configurable
- Cada switch elige un root port que es el puerto de menor costo con el que llegar al root
- Bloquea los links que pueden causar loops dejandolos como backup

STP – Costos de los puertos

Rapid Spanning Tree Protocol

Puerto	Costo Original (STP)	Costo Actualizado (RSTP)
10 Mbit/s	100	2.000.000
100 Mbit/s	19	200.000
1 Gbit/s	4	20.000
10 Gbit/s	2	2.000
100 Gbit/s	N/A	200
1 Tbit/s	N/A	20

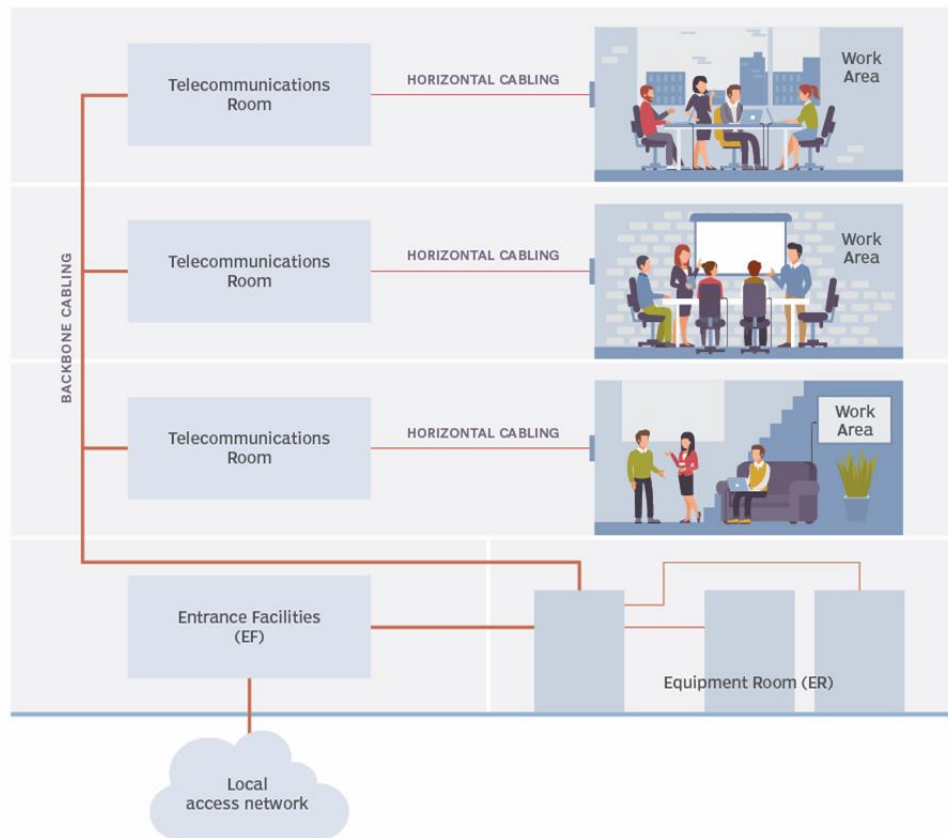
STP – Ejemplos



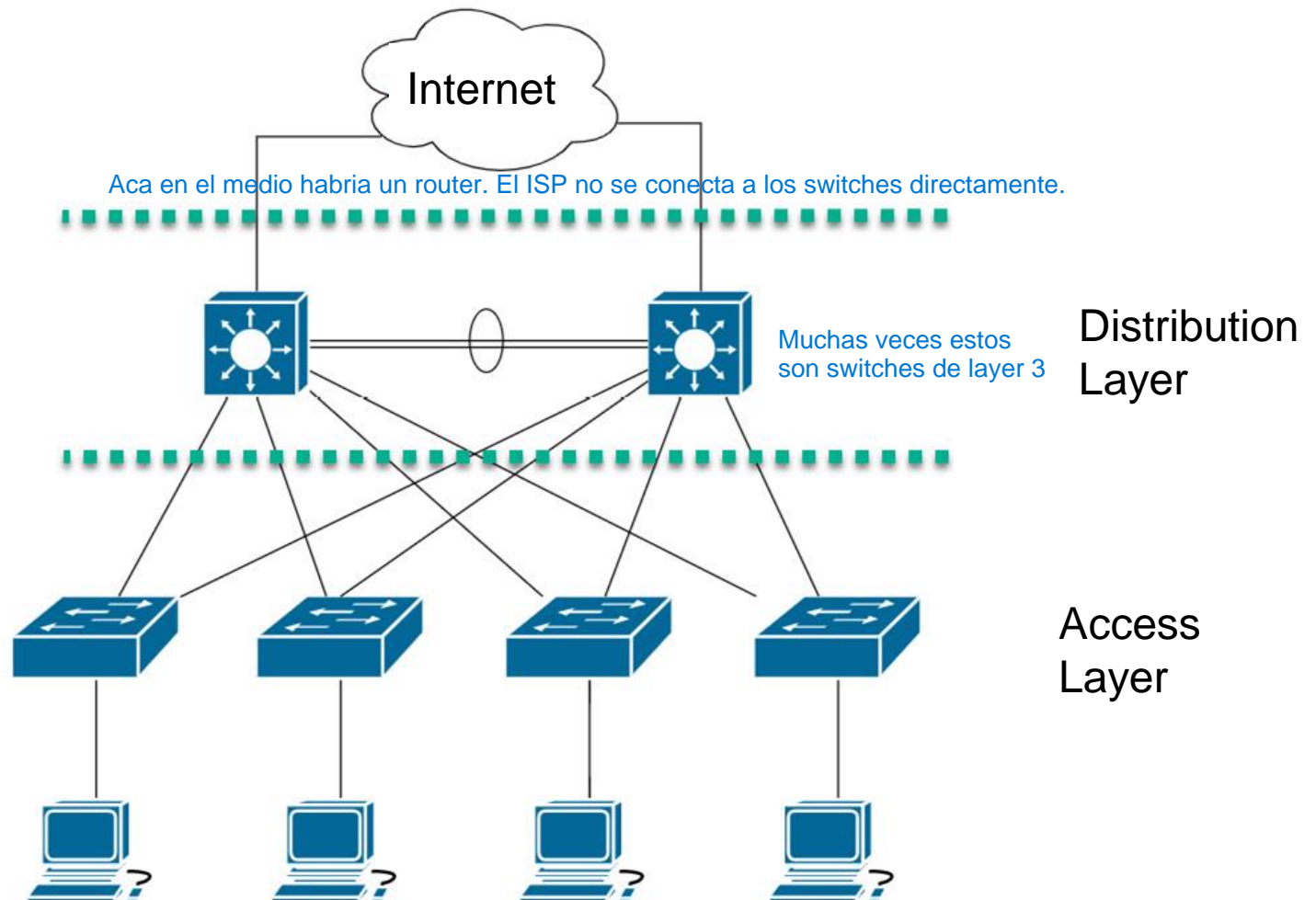


Diseño de Redes

Por cada Telecommunications Room, ponemos un switch.
Cada uno de estos switches de piso va al Equipment Room.

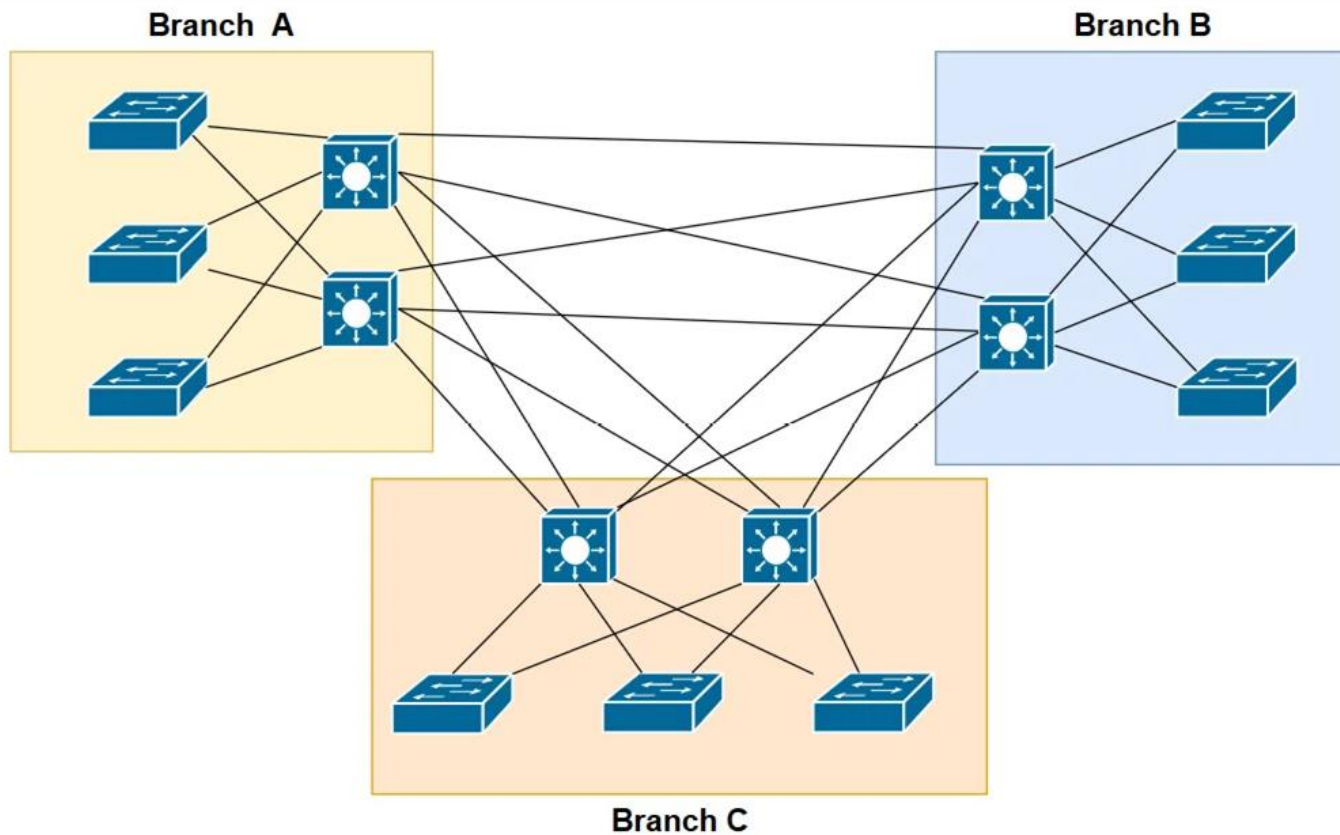


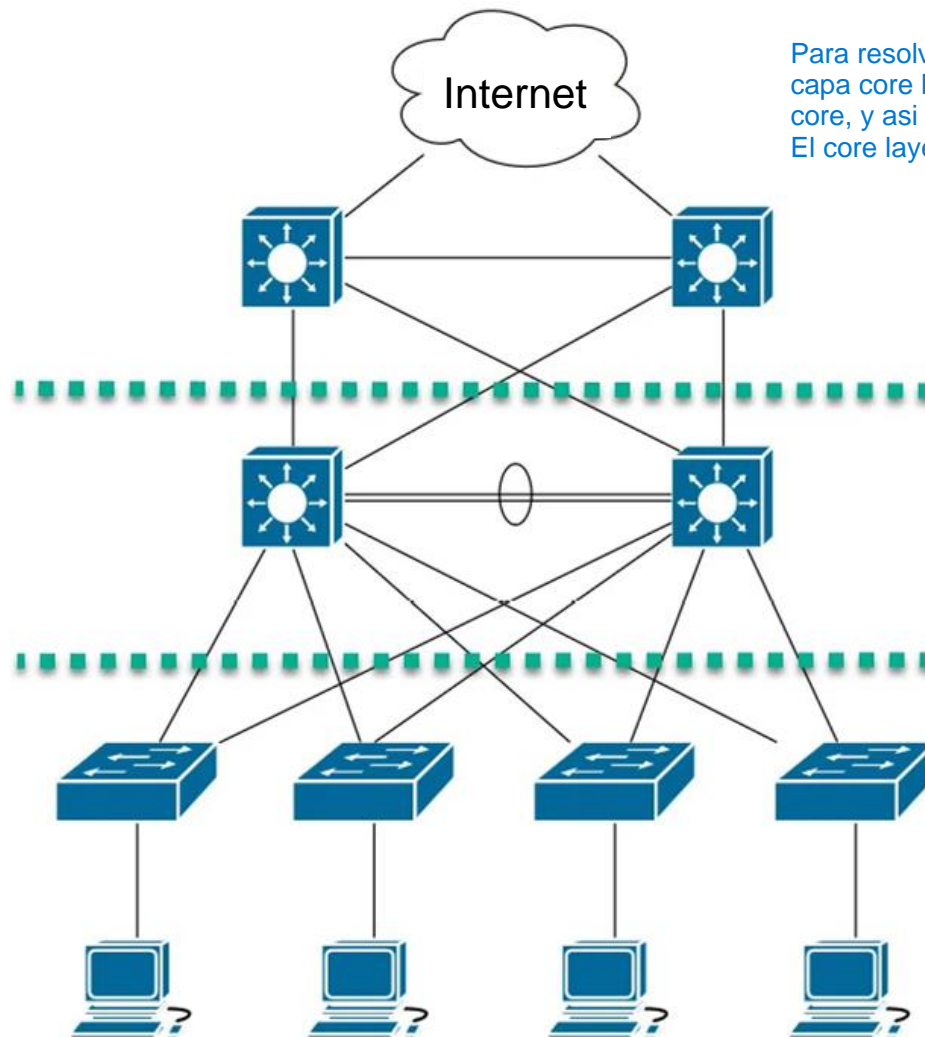
Diseño de Redes



Diseño de Redes

Cuando tenemos muchas distribution layers y tenemos que empezar a conectar todas con todas, empiezan los problemas. Tal vez se puede armar algo en forma de anillo pero cuando hay mas de 3 ya es un problema.





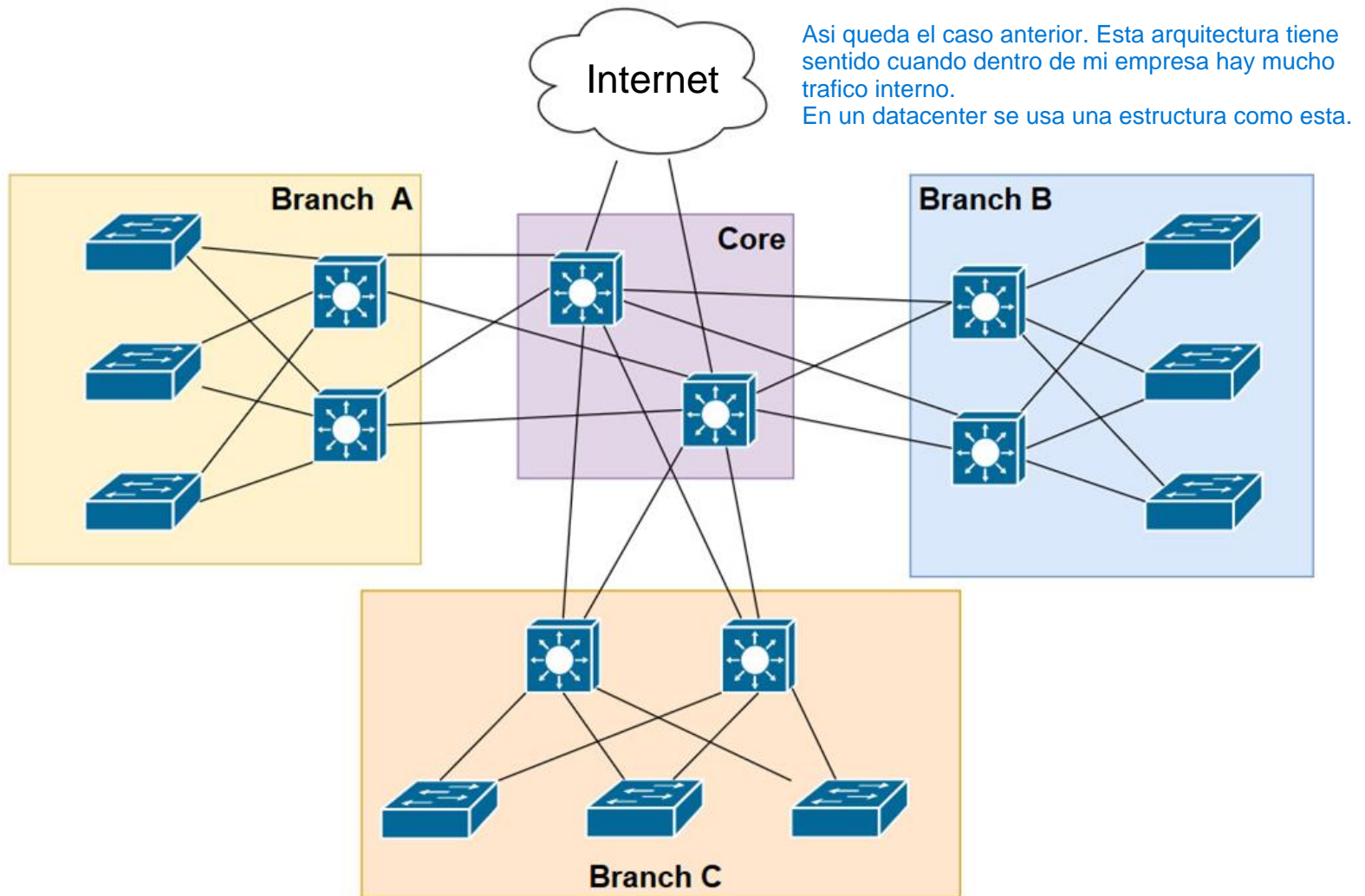
Para resolver lo de la diapositiva anterior, se agrega la capa core layer. Todos los switches se conectan con el core, y así centralizamos todo el ruteo en ese lugar. El core layer está en uno de los switches.

Core
Layer

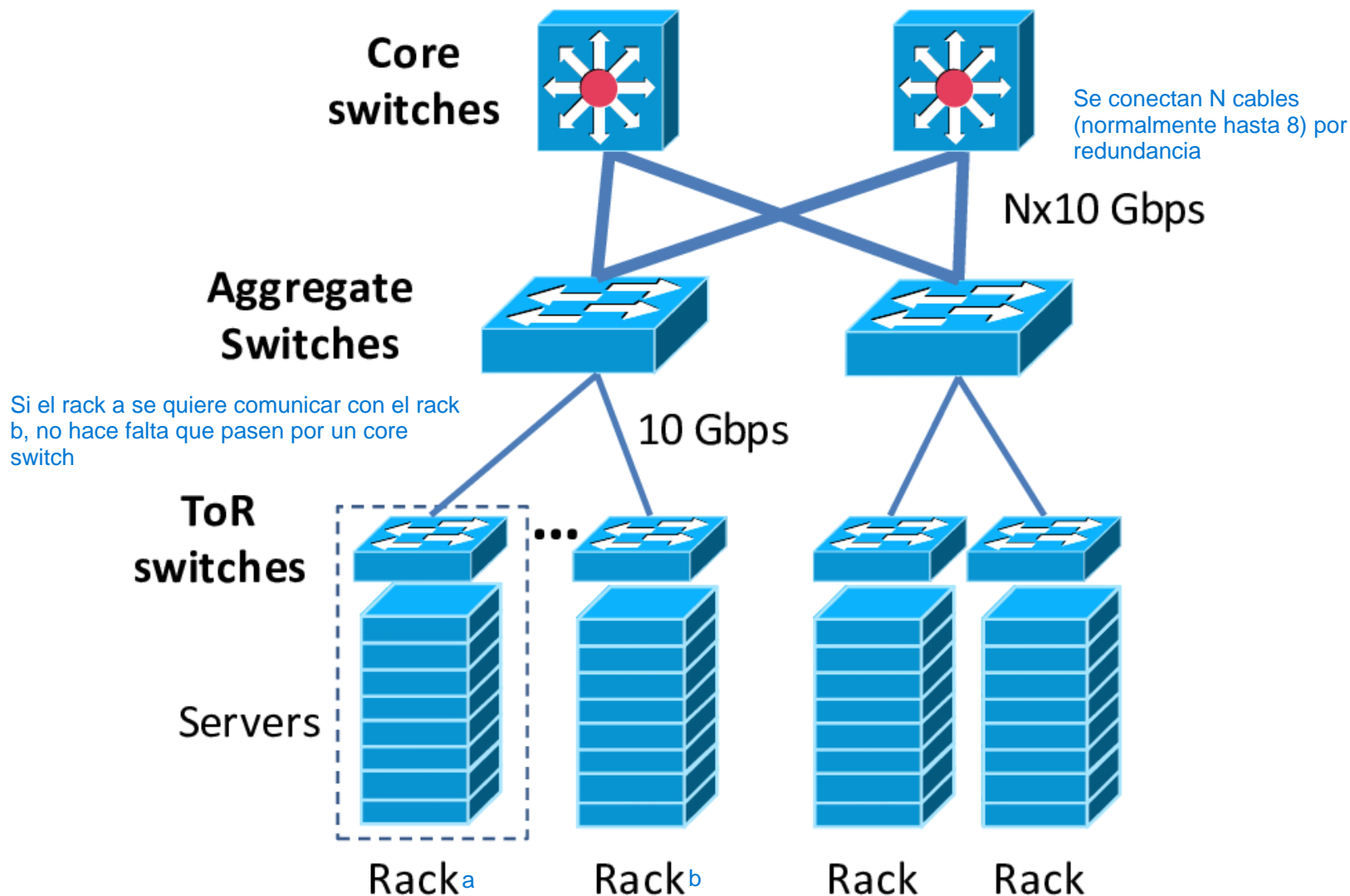
Distribution
Layer

Access
Layer

Diseño de Redes



Diseño de Redes - Data Center



POE – Power Over Ethernet

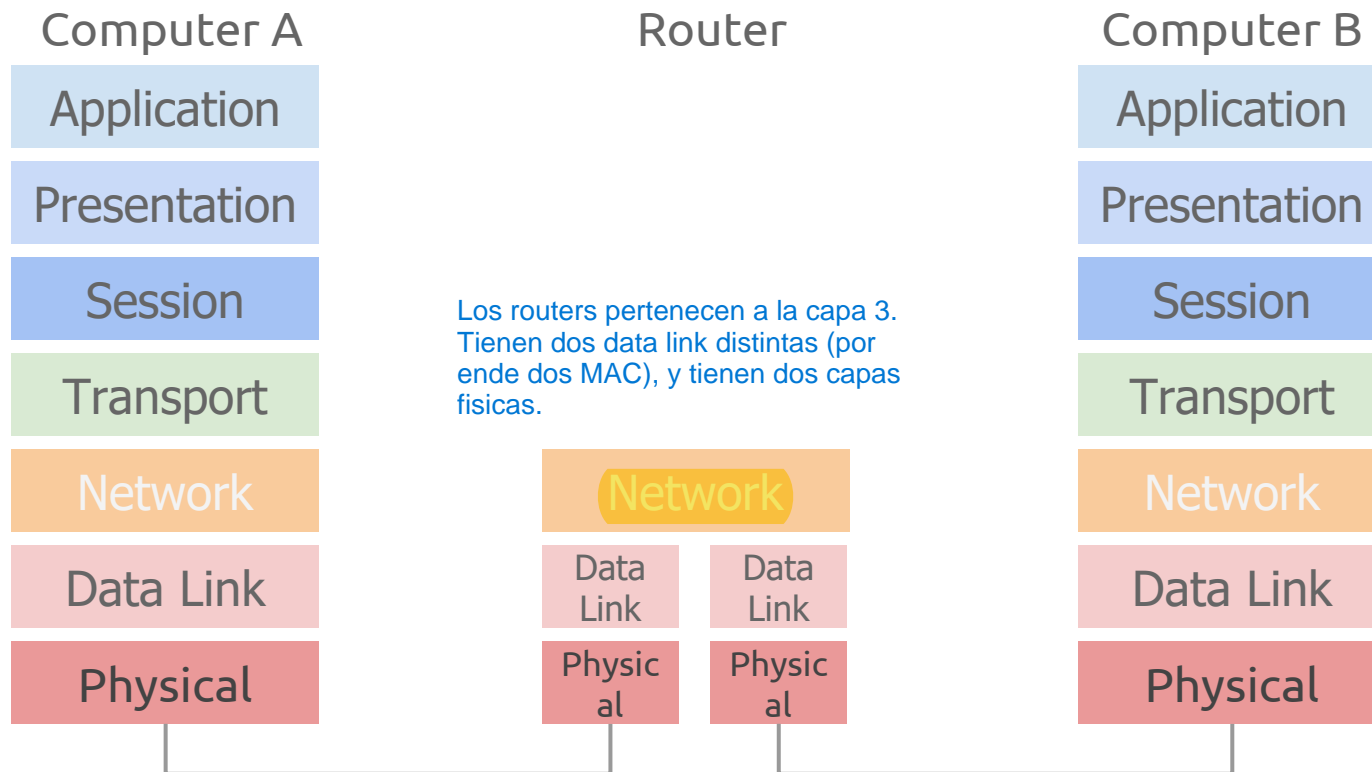
Algunos switches pueden dar tensión para alimentar algunos dispositivos a través de ethernet. Se usa uno de los 4 pares del ethernet para este fin.

- Provee alimentación a dispositivos
 - Teléfonos IP
 - Access Points
 - Cámaras IP
 - Control de acceso
 - IEEE 802.3af standard que utiliza los pares de datos para dar energía.



Routers

OSI - Router



Routers

- Conectar dos redes distintas haciendo FWD de los paquetes entre ambas
- NAT? (lo veremos más adelante)
- Usualmente se refiere a la conexión de LAN a WAN

Por ende las capas físicas

Routers

■ Familia 2600 de CISCO

Resumen de las características de toda la serie Cisco 2600

Procesador	CPU Power PC RISC	Ranuras de la tarjeta de interfaz WAN (WICS)	2 WICS
Memoria Flash,	8 MB, ampliables a SIMM de 16 MB	Ranura para módulo de red	1
Memoria DRAM del sistema	24 MB de DRAM, ampliables a DIMM de 64 MB de DRAM	Ranura del módulo de integración avanzada (AIM)	1
Puertos LAN	Cisco 2621: 2 Ethernet 10/100 Cisco 2620: 1 Ethernet 10/100 Cisco 2613: 1 Token Ring Cisco 2612: 1 Ethernet + 1 Token Ring Cisco 2611: 2 Ethernet Cisco 2610: 1 Ethernet	Sistema de alimentación interno	Corriente alterna (CA), de corriente continua (CC) o adaptador RPS
		Dimensiones (Al x An x Pr)	1,69 x 17,5 x 11,8 pulgadas
		Rendimiento	Entre 15 y 25 Kpps
		Puertos auxiliares y de consola	115,2 Kbps con acceso telefónico activado Enrutamiento bajo demanda (aux)

Routers – Tipos de líneas WAN

- Línea dedicada: La mejor opción. La mas cara. Se utilizan líneas que alcanzan 1Gbps. Se suelen utilizar HDLC y PPP como protocolos de encapsulamiento.
- MPLS: permite conexiones con calidad de servicio garantizada por el proveedor.
- DSL/Cable/Fibra: distintas opciones de conexión hacia otras redes remotas
- Wireless: utilizando 4G o 5G pública o privada.

Routers – Vínculos WAN Comerciales

- Punto a Punto: Se coloca un router en cada sitio y se acuerda la velocidad total (subida + bajada)
- LAN to LAN: Se interconectan dos LAN en sitios remotos con velocidades de 10, 100 Mbps o 1 Gbps, se utiliza el backbone de la empresa.
- Fibra oscura: Pares de fibra tendidos que no utiliza la empresa y los comercializa a los clientes.

Routers – Back Panel

- Router CISCO 2901

WIC Ports

Aux

GbEth

Console

WIC
4G

WIC SFP



Router vs Switch Layer 3

■ Router:

- WAN
- Soportan protocolos PPP, Frame Relay, OSPF, RIP, etc
- Enrute por Software muy flexible con tablas muy grandes
- Limitado ancho de banda y cantidad de paquetes
- Algunos permiten redundancia de WAN o Load Balancing

■ Switch Layer 3:

- LAN
- Principalmente enruta entre VLANs
- No soportan protocolos específicos de enrute
- Enrute por hardware
- Gran capacidad de manejo de paquetes

En conclusion, el router funciona por software (mas flexible pero mas lento), y el switch funciona por hardware (menos flexible pero mas rapido)



REDES

Wifi

Wifi

- ☐ WiFi: Wireless Fidelity
- ☐ Normas IEEE 802.11x
- ☐ Define Layers 1 y 2
- ☐ Es similar a Ethernet pero difiere en muchos detalles específicos de Wireless

Wifi - Características

- ☐ Medio Compartido - Canal Dos problemas:
- Seguridad
- Colision
- ☐ Solo uno incluido el AP transmite con destino a otro y ese toma el canal y nadie puede transmitir mientras ese transmite AP es el access point (el router)
- ☐ Cuando un transmisor falla muchas veces va bajando la velocidad para tratar de transmitir

Medio Compartido - Problemas

PROBLEMA 1;

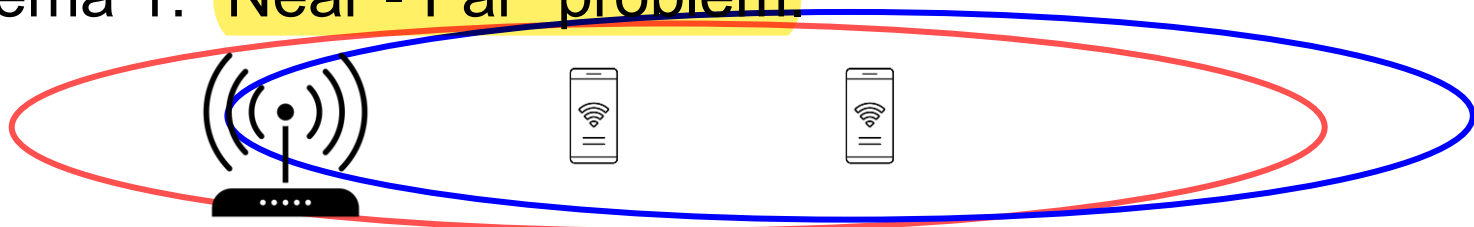
El dispositivo que esta mas cerca tiene mas potencia (y puede tapar) que el que esta mas lejos. El que esta mas lejos puede tener que bajar mucho su velocidad para llegar mas lejos (bajando la velocidad del resto)

PROBLEMA 2:

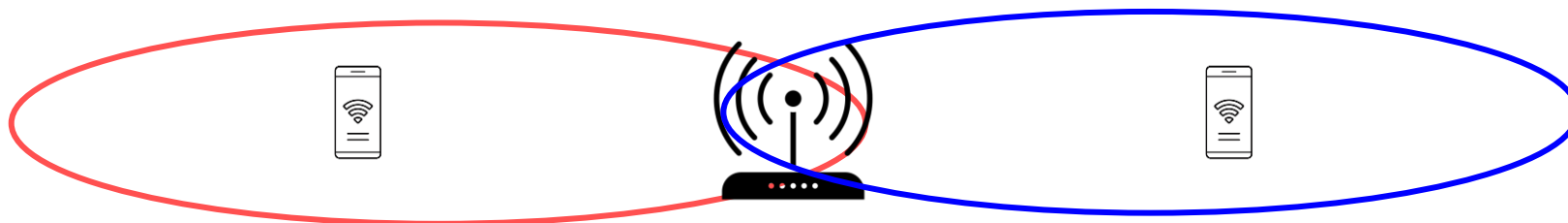
Parecido a ethernet, se usa carrier sense (me fijo si ya hay otro transmitiendo). El problema que surge es que en el grafico 2 el dispositivo de la izquierda no puede ver si el dispositivo de la derecha ya esta transmitiendo, por lo que no puede evitar colisiones.

☐ El emisor chequea y si está libre el medio transmite

☐ Problema 1: “Near - Far” problem



☐ Problema 2: “Hidden Node” problem.



Medio Compartido - Soluciones

- ❑ Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)
- ❑ Después de chequear espera un valor random de tiempo antes de volver a chequear y transmitir
- ❑ Después de transmitir espera un ACK sino retransmite y baja la velocidad
- ❑ Request to Send/ Clear to Send (RTS/CTS)
- ❑ Se usa solo para paquetes grandes para evitar retransmisiones

Los dispositivos mandan un request to send. Cuando el AP ve que nadie esta mandando nada, le da permiso (clear to send) a un dispositivo para que mande. Esto es una solucion al problema 2 de la slide anterior.

Medio Compartido - Elementos Típicos

- ❑ **Cliente:** dispositivo terminal que Envía o Transmite paquetes

- ❑ **AP:** Access Point punto de acceso hacia el que se envía o del que se reciben paquetes
 - ❑ Puede estar co-localizado con el router pero no necesariamente lo es.
 - ❑ Puede brindar interconexión con la red Ethernet

Wifi - Tipos de Paquete

☐ Management:

- ☐ Beacon
- ☐ Authentication
- ☐ Association

☐ Control

- ☐ RTS/CTS
- ☐ ACK

☐ Data

Wifi - MAC

Capa OSI	PLCP Preámbulo	PLCP Header	Frame Control	Duration	Addr 1	Addr 2	Addr 3	Seq	Addr 4	Payload	Trailer
	16 Bytes	2 Bytes	2 Bytes	2 Bytes	6 Bytes	6 Bytes	6 Bytes	2 Bytes	0/6 Bytes	0/2304 Bytes	4 Bytes
Capa 1											
Capa 2											

Version	Type	Subtype	To DS	From DS	Frag	Retry	Pwr	Data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Control
Mgmt
Data

Beacon
RTS/CTS
Data

ITBA - RED - 2024

Addresses:

- Source Address
- Destination Address
- Transmitter Address (la del AP)
- Receiver Address normalmente no se usa

Wifi - MAC Addresses

- ❑ Típicamente se usan 3:
 - ❑ Source Address
 - ❑ Destination Address
 - ❑ BSSID: MAC Address del AP
- ❑ El 4to es opcional y se usa en casos especiales como Mesh
- ❑ Depende de los bits To DS, From DS como se interpretan

Wifi - Beacon

❑ El Beacon incluye:

El beacon se envia todo el tiempo para que todos los dispositivos sepan que dicha red existe o que sigue activa.

- ❑ SSID: nombre de la red WiFi

- ❑ Supported Rates

- ❑ Información del canal

En las nuevas wifi, se apagan las antenas periodicamente para ahorrar bateria en los dispositivos

- ❑ Intervalo del Beacon (para Sync y Power Mgmt)

- ❑ Opciones de Seguridad soportadas

De que manera se va a autenticar

- ❑ Otros (QoS, Traffic Indication Map)

El traffic indication map detecta donde esta cada dispositivo y envia la señal mas dirigida en esa direccion, para evitar interferencias

Wifi - Conexión

- ❑ El cliente se conecta a la red WiFi mediante:
 - ❑ Autenticación: se autentica utilizando alguno de los métodos disponibles.
 - ❑ Asociación:
 - Association Request (capabilities)
 - Association Response
 - ❑ Key Exchange:
 - Claves de encriptación

Wifi - Seguridad

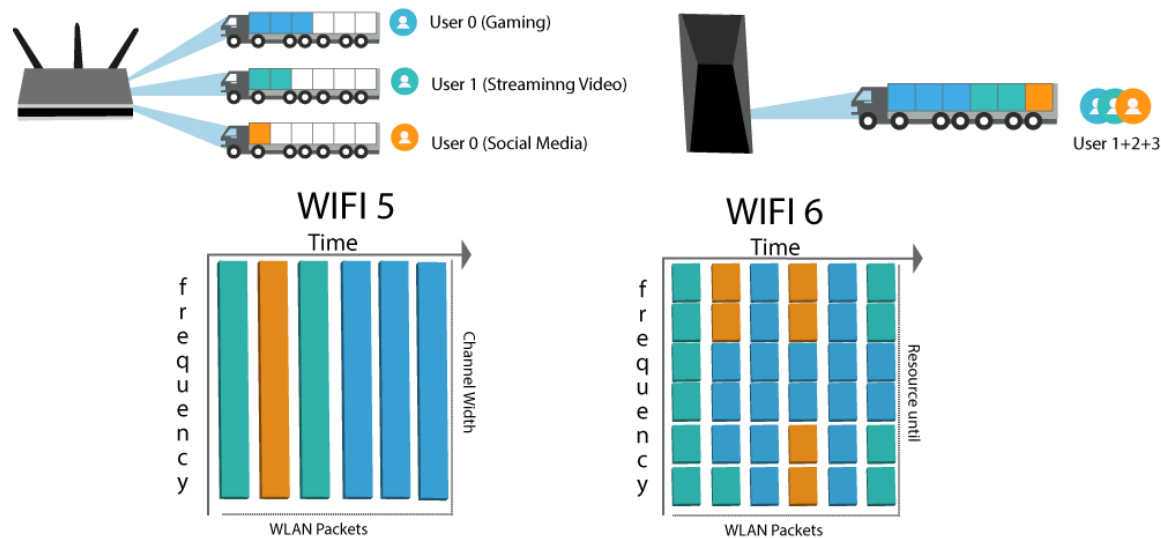
- ❑ **WEP:** muy inseguro. Encriptación insegura. No soporta servidor de autenticación.
- ❑ **WPA:** soporta servidor de autenticación pero la encriptación (TKIP) es insegura y susceptible de ataques para passwords simples.
- ❑ **WPA2:** encriptación AES. Ataques para passwords simples.
- ❑ **WPA3:** encriptación SAE. El más seguro actualmente.

Wifi - Variantes

- ❑ 802.11**g**: 2.4 GHz 54Mbps
- ❑ 802.11**n**: 2.4 & 5 GHz 600Mbps
- ❑ 802.11**ac**: 2.4 & 5 GHz 1-3.5 Gbps WiFi-5
- ❑ 802.11**ax**: 2.4 & 5 GHz 1.2-9.6 Gbps WiFi-6

Wifi6 - Mejoras sobre WiFi 5

- ❑ Wifi 5 - Max 3.5 Gbps vs Wifi 6 - Max 9.6 Gbps
- ❑ Wifi 6 OFDMA -> Envío de múltiples datos a distintos destinos en el mismo paquete



MIMO (Multi Input Multi Output)

- ❑ Pre WiFi 5 -> SU-MIMO (Single User)
- ❑ WiFi 5 -> MU-MIMO (Multi User) Solo Download, hasta 4 dispositivos
- ❑ WiFi 6 -> MU-MIMO (Multi User) Download y Upload, hasta 12 dispositivos

Se usan distintos subcanales para mas de un dispositivo

