
Interconexión de Redes

RESUMEN



- 1** Introducción
- 2** Métodos de Interconexión a Nivel Físico: **REPETIDOR y HUB**
- 3** Métodos de Interconexión a Nivel de Enlace: **BRIDGE y SWITCH**
- 4** Prevención de loops - Protocolo Spanning Tree (**STP**)
- 5** **VLANs**

Introducción

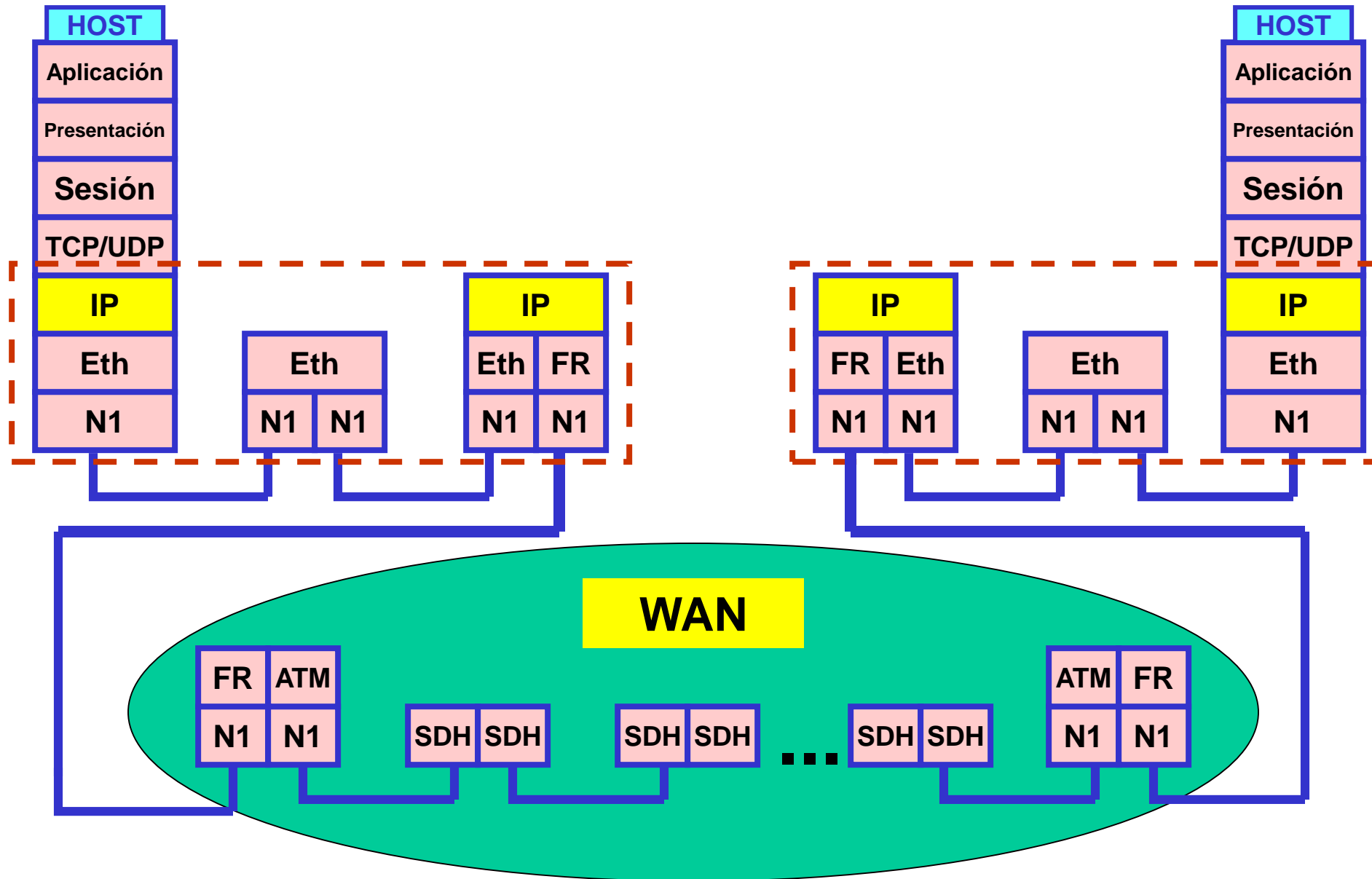
Métodos de Interconexión

+ A nivel Físico: Repetidores y Hubs

+ A nivel de Enlace: Bridges y Switches

+ A nivel de Red: Routers

Introducción



RESUMEN

1 Introducción



2 Métodos de Interconexión a Nivel Físico: **REPETIDOR y HUB**

3 Métodos de Interconexión a Nivel de Enlace: **BRIDGE y SWITCH**

4 Prevención de loops - Protocolo Spanning Tree (**STP**)

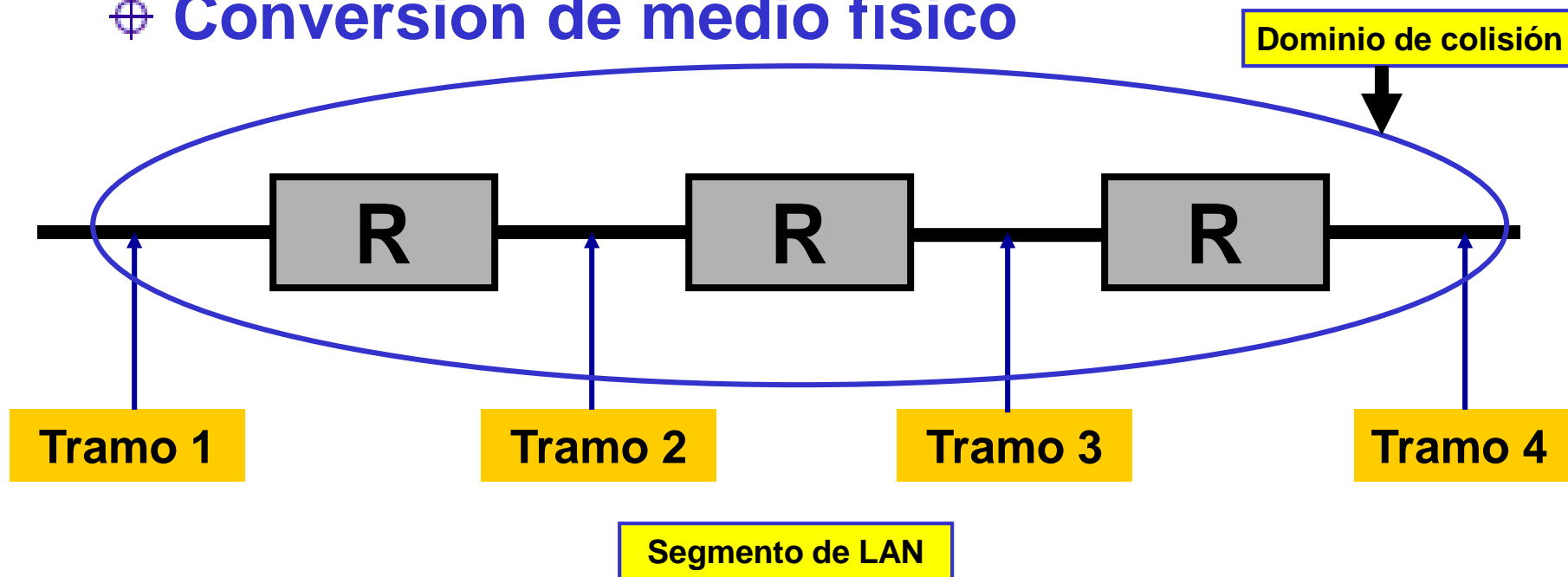
5 **VLANs**

⊕ **REPETIDOR**: dispositivo de interconexión de redes a nivel físico. Se empleaba con cable coaxil.

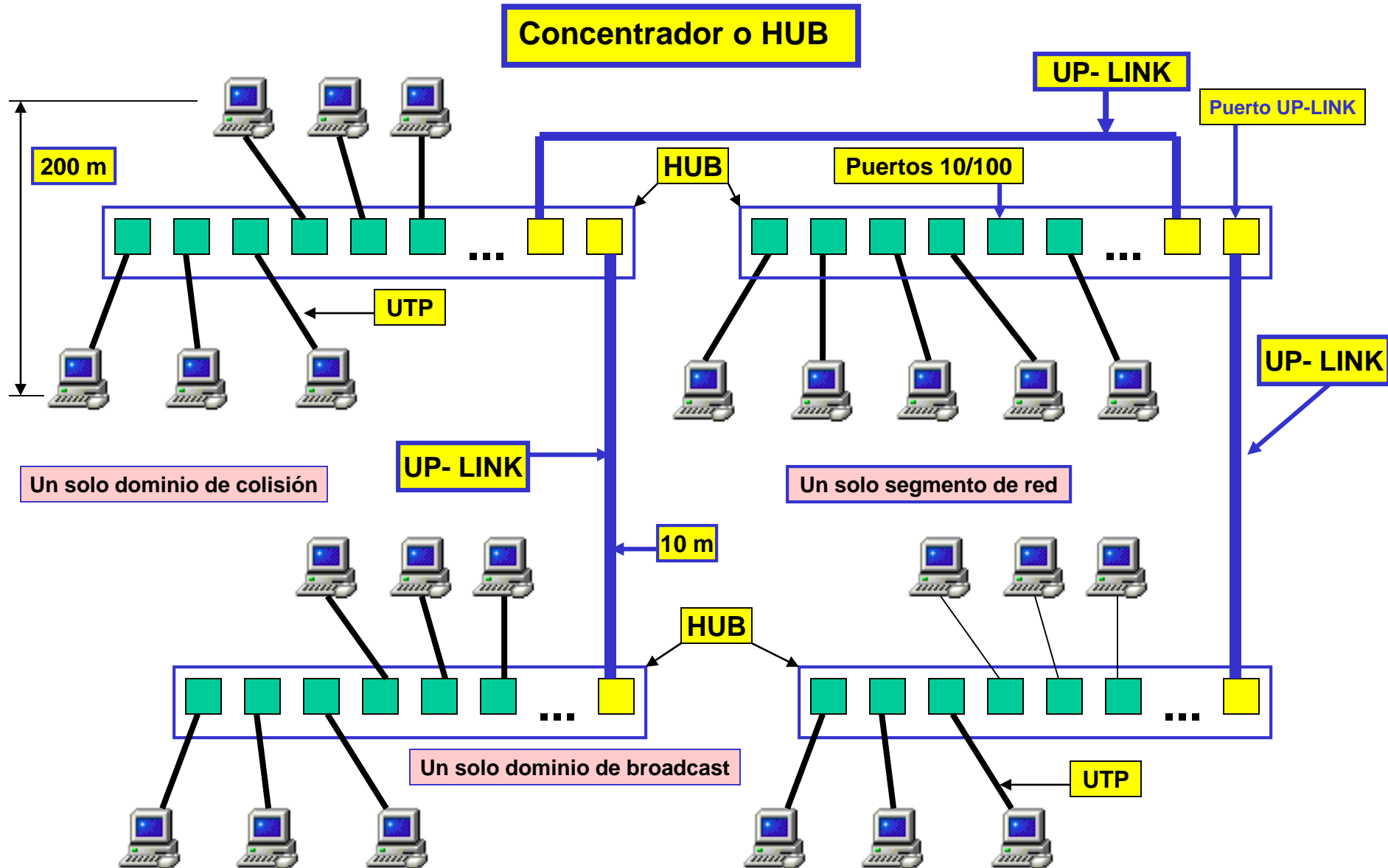
⊕ ¿ Por qué usar repetidores?

⊕ **Distancia**

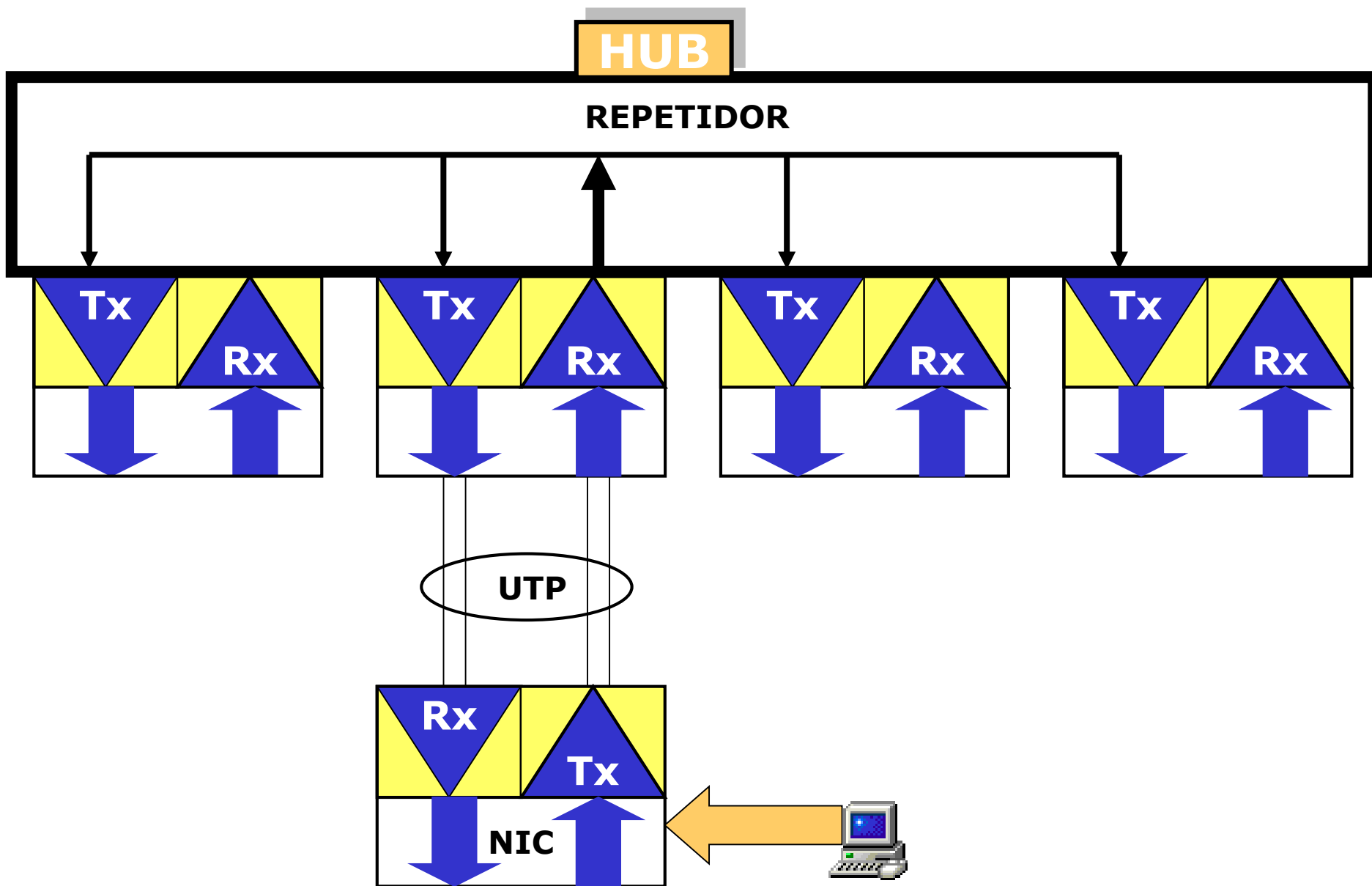
⊕ **Conversión de medio físico**



Métodos de Interconexión a Nivel Físico: REPETIDOR y HUB



Métodos de Interconexión a Nivel Físico: REPETIDOR y HUB



Problemática del HUB:

- ⊕ **Restricciones de configuración**
- ⊕ **Límites de distancia**
- ⊕ **No existe separación de tráfico (un solo dominio de colisión)**
- ⊕ **Seguridad**
- ⊕ **No permiten Gestión de Red**

RESUMEN

1 Introducción

2 Métodos de Interconexión a Nivel Físico: **REPETIDOR y HUB**

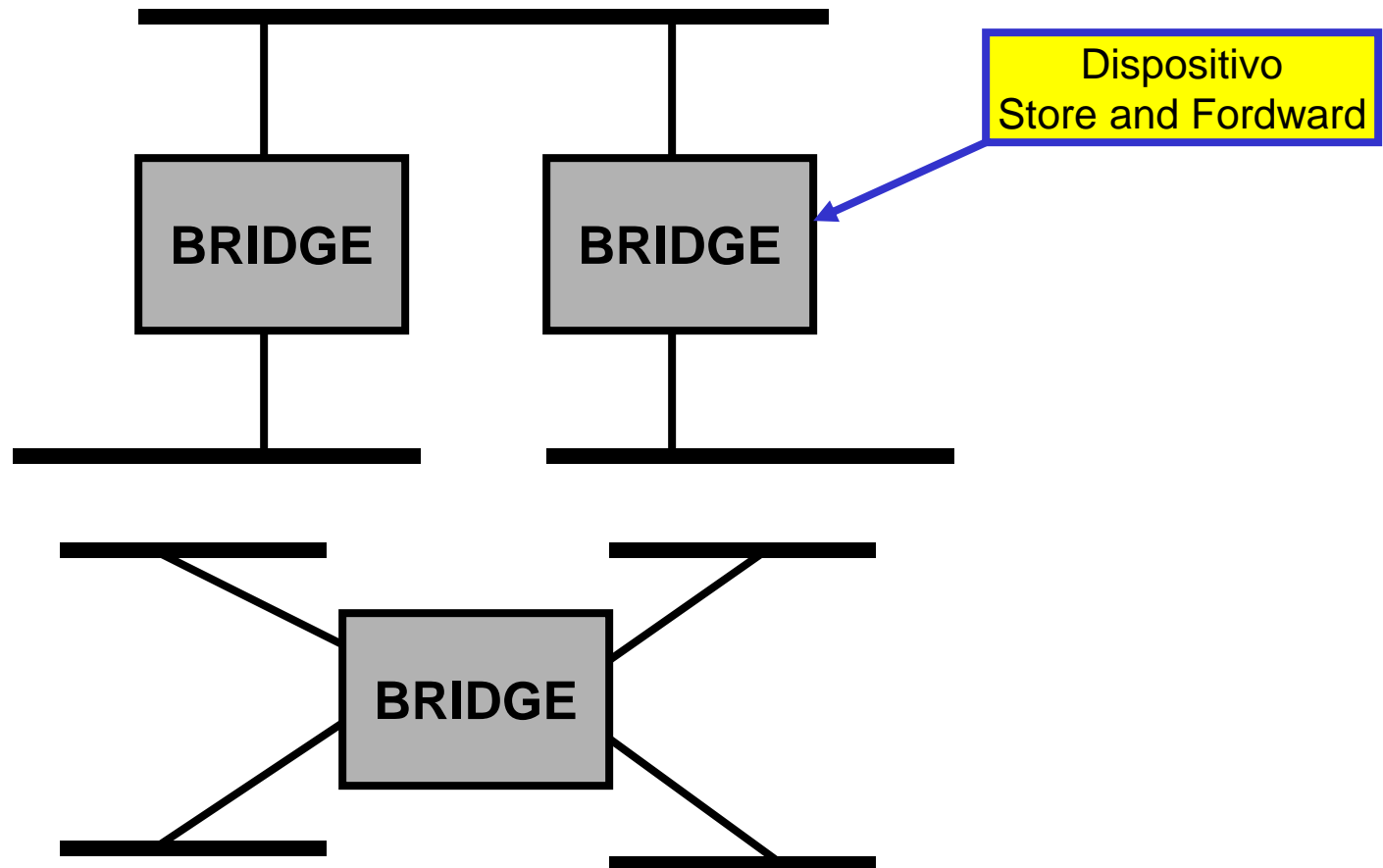
 **3** Métodos de Interconexión a Nivel de Enlace: **BRIDGE y SWITCH**

4 Prevención de loops - Protocolo Spanning Tree (STP)

5 **VLANs**

Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

⊕ **BRIDGE**: dispositivo de interconexión de redes que opera a nivel de **enlace**. Almacena y reenvía las tramas de unos segmentos de **LAN** a otros. **Aisla** segmentos dentro de una **LAN**, ya que separa los dominios de colisión. **Separa** el ancho de banda, por cada interfaz tenemos por ejemplo **10 Mbps**.

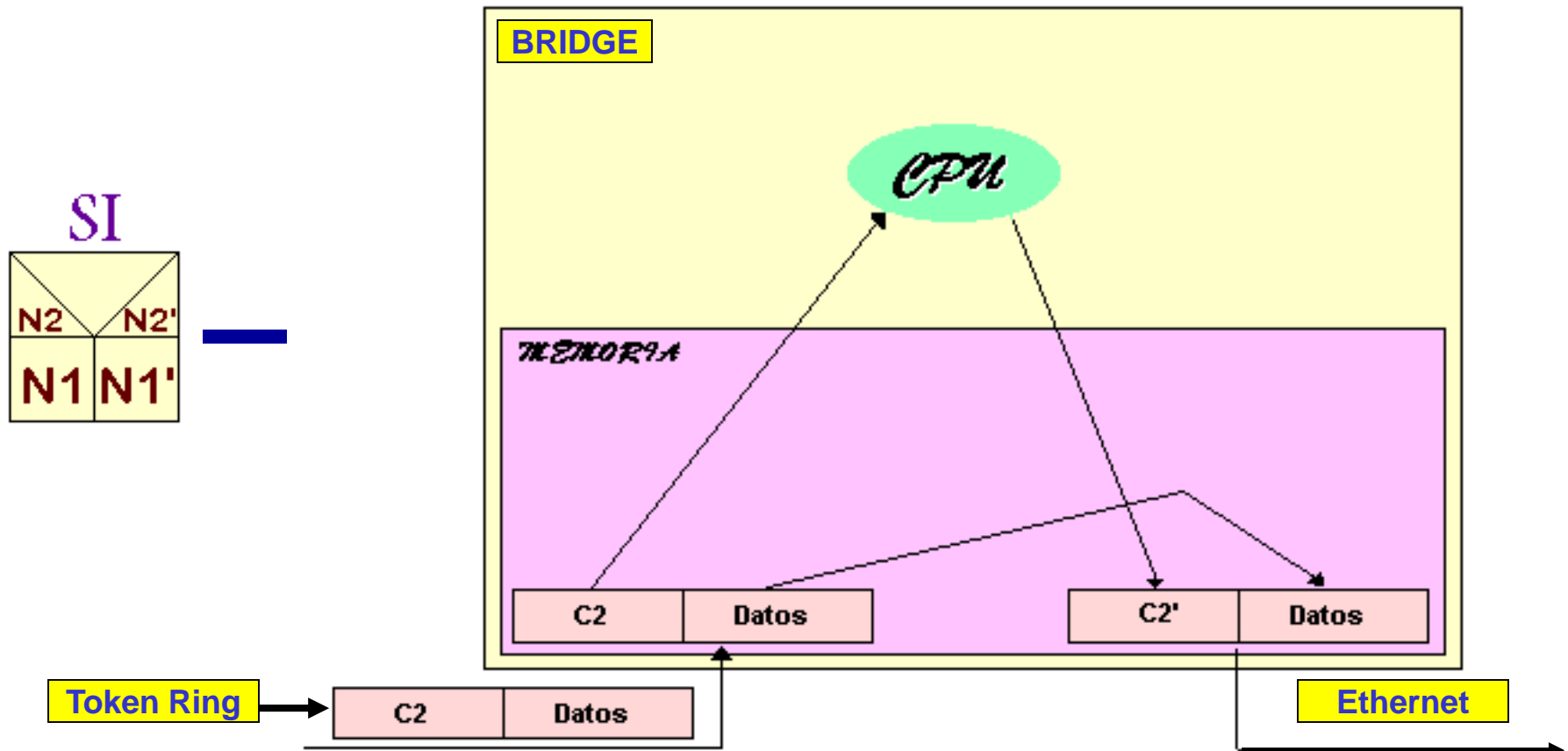


Características típicas:

- ⊕ **Soportan varios medios físicos**: thinnet, thicknet, **UTP**, etc.
- ⊕ Capacidad de **filtrado limitada**
- ⊕ Capacidad de conmutación **poco eficiente, ya que trabaja por software**
- ⊕ **Gestionables de forma local o remota**
- ⊕ **No propagan las colisiones**

Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

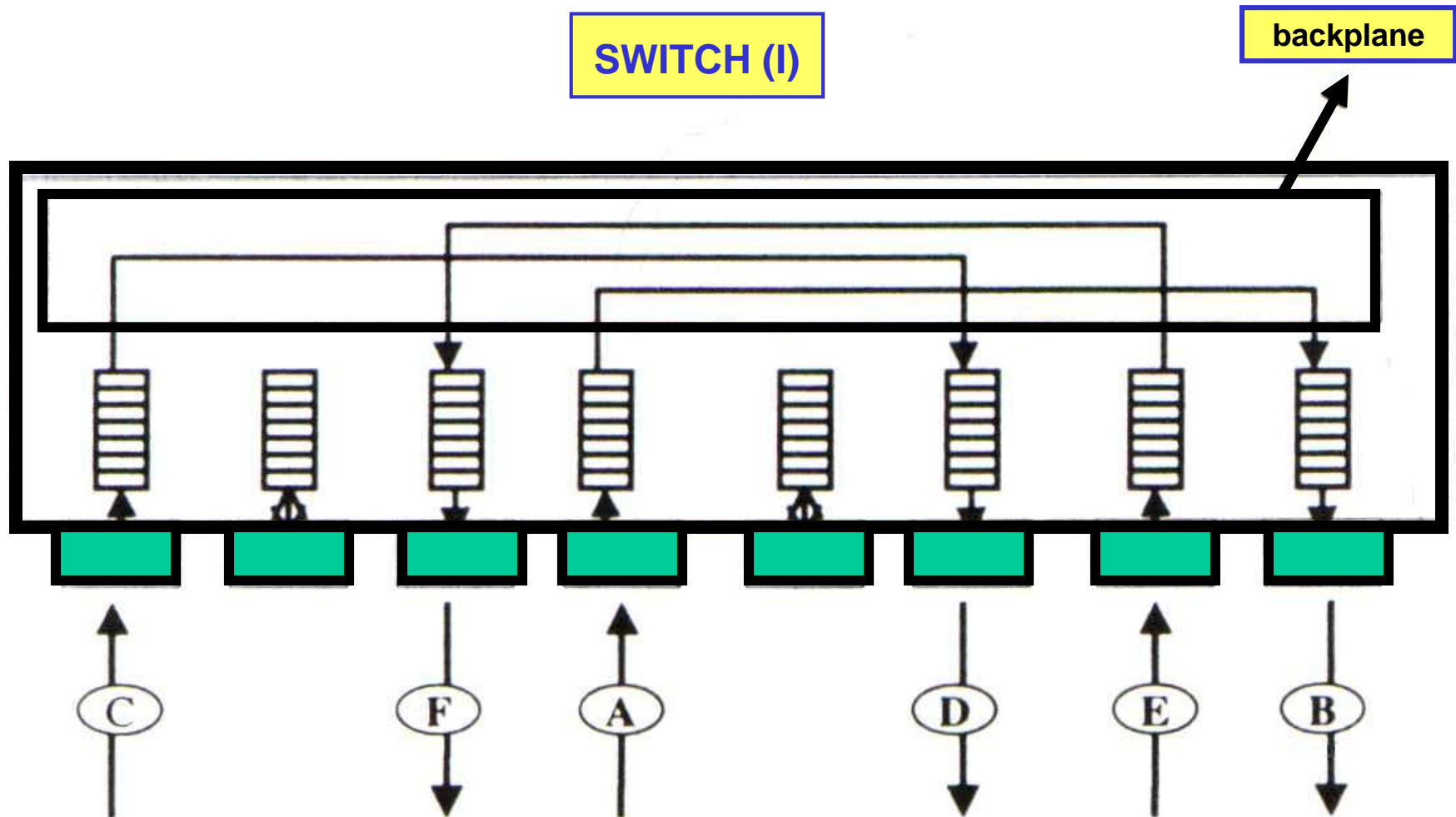
- ⊕ El bridge se dedica a escuchar las tramas del Token Ring (TR) y de **Ethernet**. Cada trama que llega se copia en su memoria interna.
- ⊕ La **CPU** analiza **C2** (cabecera de nivel 2 del TR en este caso). Si el destino está en el TR **descarta la trama**. Si el destino está en la **red Ethernet**, creará una cabecera **C2'** (cabecera **Ethernet** de nivel 2), convirtiendo **C2** y rellena el campo de datos con los datos originales (los que acompañaban a **C2**).



Problemas Principales:

- ⊕ El funcionamiento bajo **software** lo hace lento
- ⊕ En un **Bridge** hay sólo **una instancia de árbol de extensión (STP)**, en cambio en un **Switch** hay múltiples instancias de árboles de extensión (por lo general los switches soportan un **STP** por cada **VLAN**.)
- ⊕ Carecen de la **escalabilidad** necesaria para construir redes de **gran tamaño** (poca capacidad de puertos, **4** u **8** a lo sumo).
- ⊕ No permiten armar **VLANs**.
- ⊕ Los **Switches** conmutan por **hardware**, por lo tanto son **mucho más rápidos que los bridges**, emplean circuitos integrados de aplicación específica (**ASIC**) y permiten además la configuración de **VLANs**.

Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH



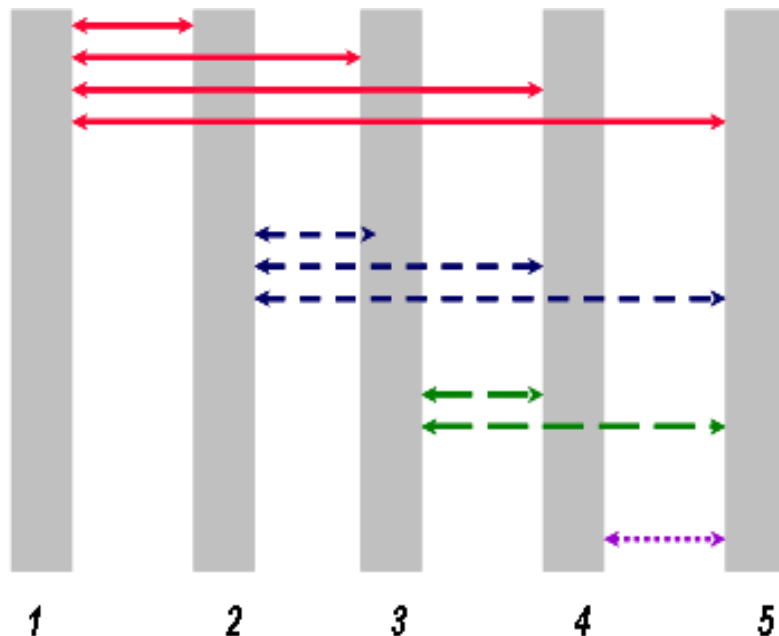
Una especificación muy importante para un switch es su capacidad de conmutación. La conmutación se lleva a cabo por un elemento denominado **backplane**. La finalidad del backplane es la de permitir la interconexión de cada puerto con el resto de los puertos del switch.

Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

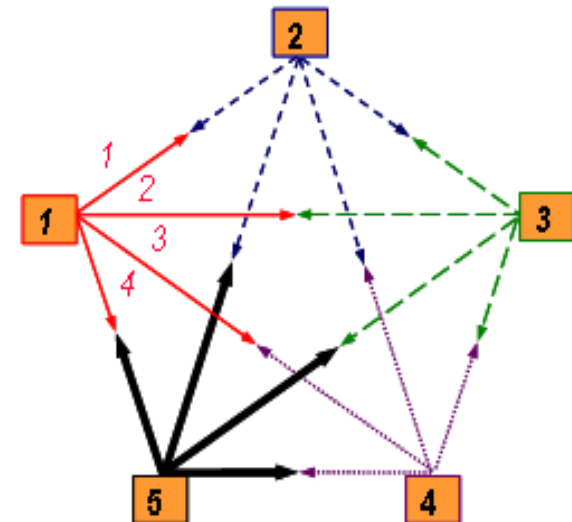
Ejemplo de switch de core marca ENTERASYS

SWITCH (II)

El backplane puede ser pasivo o activo. El backplane pasivo se suele dar por lo general en switches de gran porte, que se emplean en el core de la red. El core es el punto más álgido de la red y es donde se procesa todo el tráfico proveniente de las áreas de acceso y distribución de la red. En los switches de acceso o de borde (que son los que están más cerca del usuario), el backplane se lo suele denominar **switch fabric** y constituye toda la electrónica que hace el forwarding de los paquetes. A continuación vemos un ejemplo de un switch de core correspondiente a la marca **ENTERASYS**. Este switch tiene 5 tarjetas, donde cada tarjeta está interconectada con las cuatro restantes, formando un total de 10 links. El backplane mueve el tráfico entre las tarjetas vía un Frame Transfer Matrix (FTM). El FTM es una arquitectura de bus de 32 bits.



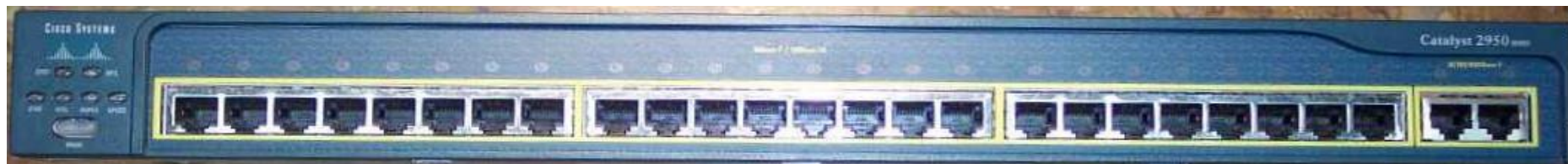
10 links



Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

SWITCH (III)

Cisco Catalyst modelo WS-C2950T-24



24 Puertos 10/100 BASE-T

2 Puertos
10/100/1000 BASE-T

- Matriz de conmutación de 8.8 Gb/s y 8,6 Mpps (millones de paquetes por segundo)
- Matriz 'non-blocking'

$$(2 \times 1000 \text{ Mb/s} + 24 \times 100 \text{ Mb/s}) \times 2 = 8.800 \text{ Mb/s} = 8.8 \text{ Gb/s}$$

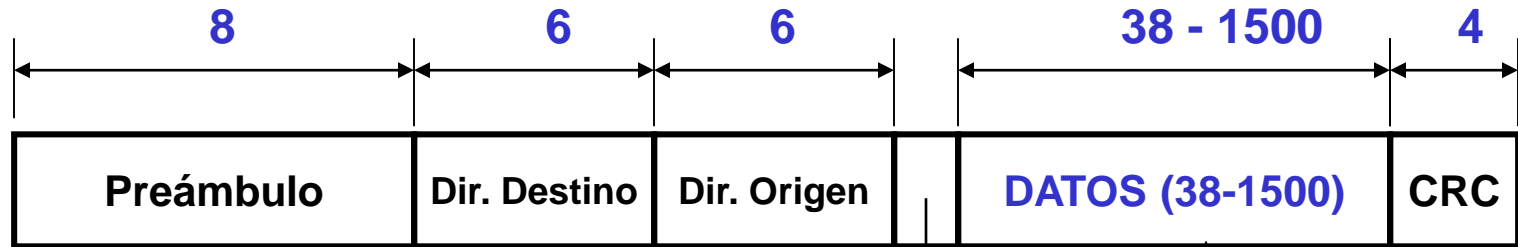
Con tramas de 64 bytes una Ethernet de 100 Mb/s equivale a 195,31 Kpps y un link de 1GB 1953,13 Kpps:

$$2 \times 1953,13 \text{ Kpps} + 24 \times 195,31 \text{ Kpps} = 8,6 \text{ Mpps}$$

La multiplicación por 2 corresponde al hecho que se especifica en **full duplex**, es decir por ejemplo el puerto 1 transmitiéndole al puerto 2 a 100 Mbps y el puerto 2 transmitiéndole al puerto 1 a la misma velocidad. La característica '**non-blocking**' significa que el switch conmutando simultáneamente tramas entre todos los puertos con las características especificadas no se bloquea.

Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

FORMATO DE LA TRAMA Ethernet II



Type

2 bytes

$$(38 + 26) * 8 = 512 \text{ bits}$$

Cabecera IP
20 bytes

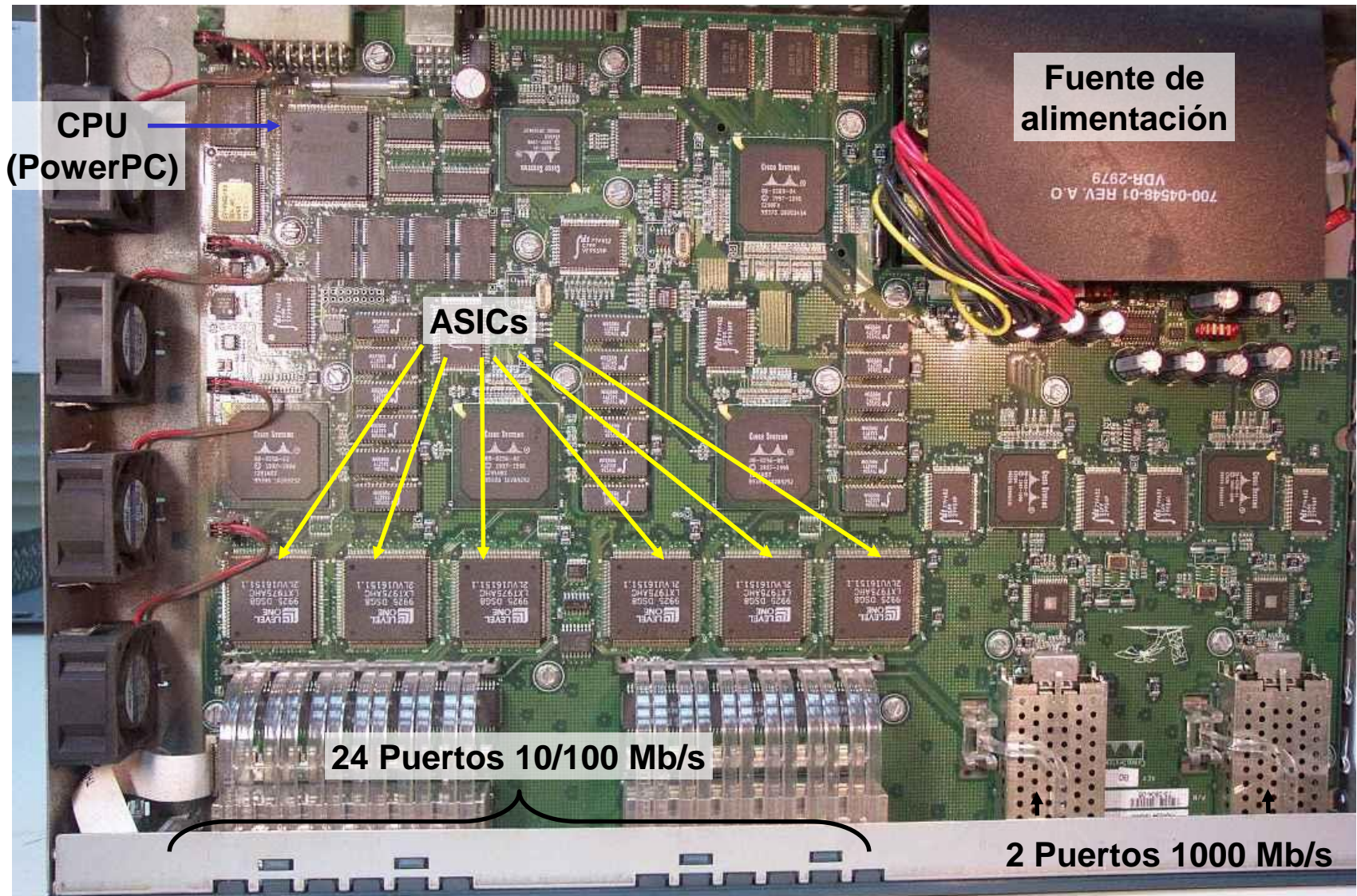
DATOS (18 bytes)

Paquete IP

Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

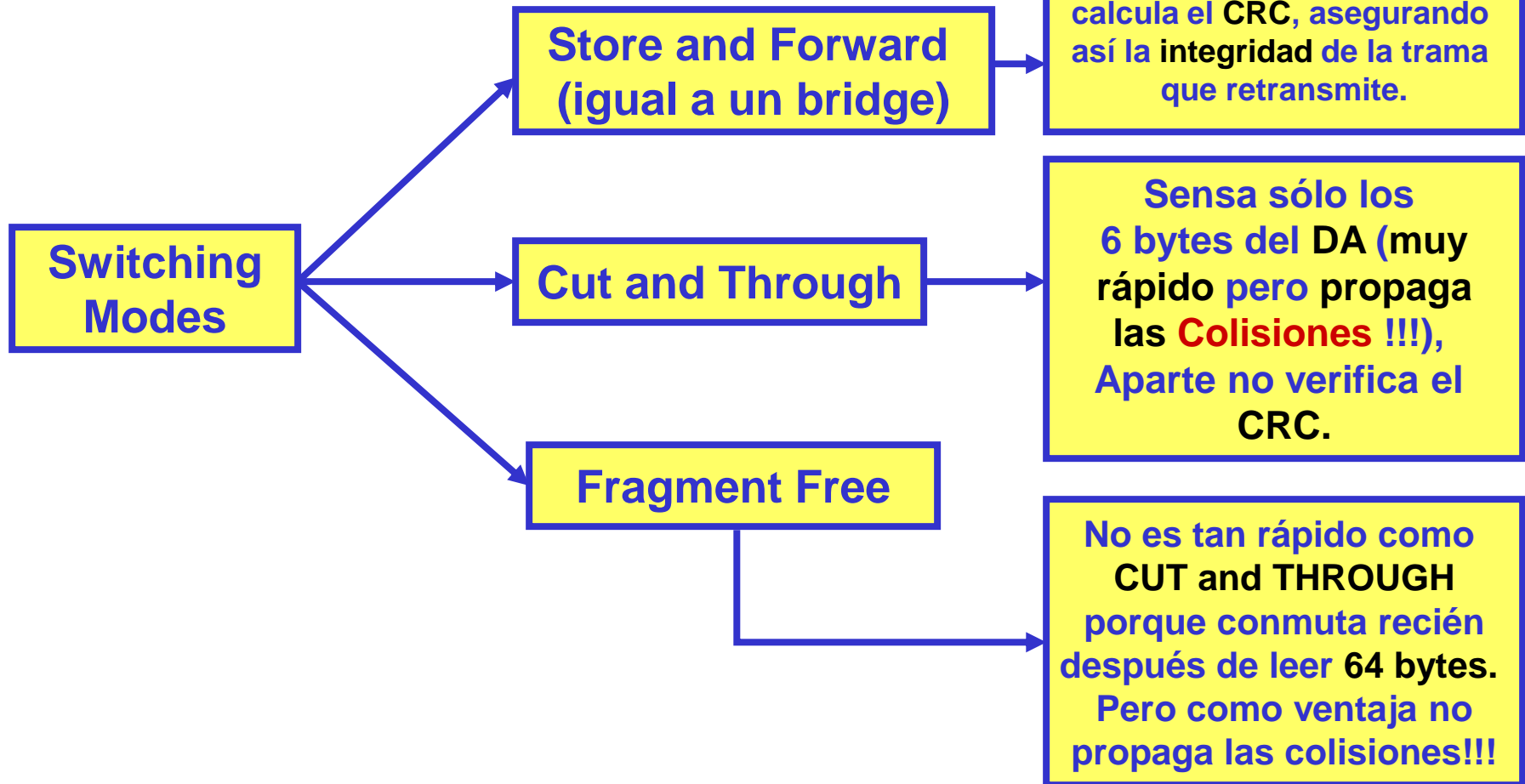
SWITCH (III)

Hardware del Switch CISCO CATALYST WS-C2950T-24



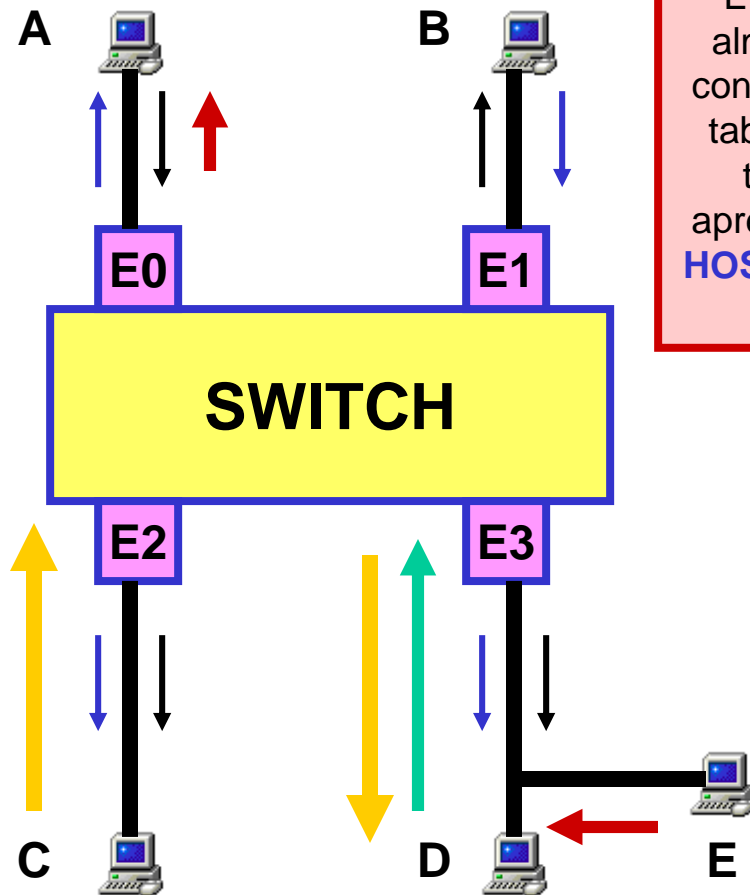
Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

Switch Ethernet – Posibles configuraciones



Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

Cómo aprenden los switches ? – Técnica de Transparent bridging



El switch va construyendo una tabla de **direccionamiento** que almacena en su memoria. Inicialmente cuando arranca la red no conoce nada, al recibir un **Frame** de un host, como inicialmente su tabla **MAC** está **vacía** hace un **flood** (esto es copiar la trama por todos los puertos del switch, **menos por el que la recibe**) y aprende de la trama recibida (del campo **SA**) la dirección **MAC del HOST** que envió dicho frame y la asocia con el puerto donde reside dicho host.

1º A → B
2º B → C
3º E → A
4º D → E
5º C → D

MAC ADDRESS	PORT
AAAAAA	E0
BBBBBB	E1
EEEEEE	E3
DDDDDD	E3
CCCCCC	E2

Importante: Cada Puerto del switch posee también una **mac address**

Cómo aprenden los switches ? – Técnica de Transparent bridging

Conclusiones:

- Inicialmente cuando el switch hace un **flooding** se está comportando como un **hub**.
- La tabla **MAC**, que es una tabla de encaminamiento a **nivel 2**, tiene una actualización **dinámica**. Además cada cierto tiempo (esto es **programable**), la tabla se borra.
- Si la tabla se borra **muy rápido**, por ejemplo cada **dos minutos**, se estarían mandando **floods** muy seguido, desaprovechando así la performance de la red, ya que se genera tráfico innecesario (**peligroso**).
- Si por el contrario, el tiempo de actualización de la tabla **MAC** es **muy elevado**, se corre el riesgo de estar enviando **frames** a segmentos donde por ejemplo ya no existan los **hosts** que poseían determinadas **mac address** (ya sea porque se cambiaron las **tarjetas de red** o simplemente se quitó el host del segmento).

Bucles múltiples en una red conmutada

Una red amplia con una estructura compleja de switches o bridges, podría dar lugar a la aparición de **múltiples lazos cerrados en la red conmutada**. El siguiente slide ilustra esta situación, se puede caer en uno de los siguientes escenarios de bucles múltiples:

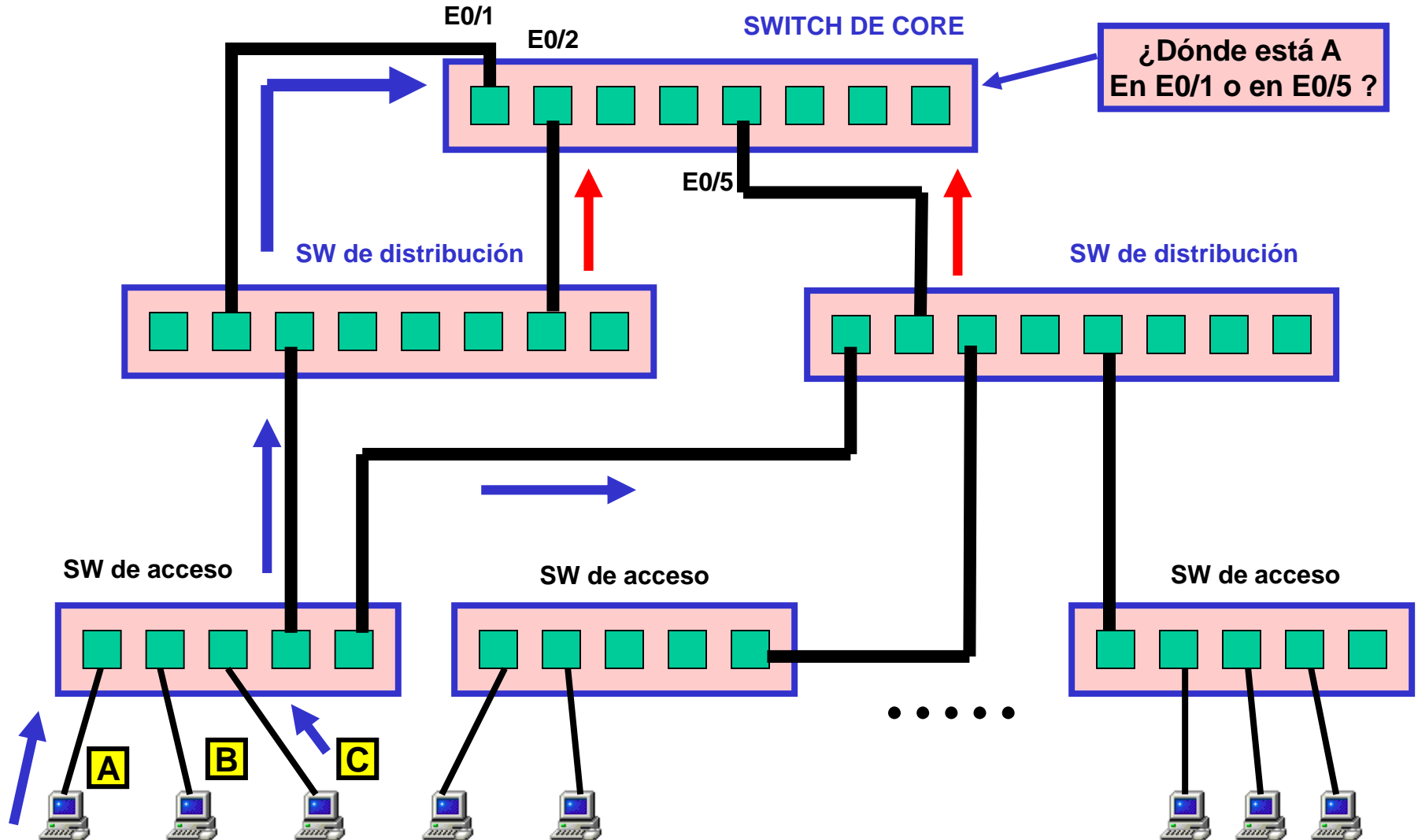
- ✚ Puede existir un **bucle** dentro de otro **bucle**

- ✚ Una **tormenta de broadcast** en bucle podría colapsar rápidamente la red con tráfico innecesario y evitar así la conmutación de paquetes dentro de la red.

Los protocolos de capa 2, como Ethernet o Token Ring, carecen de un mecanismo capaz de reconocer y eliminar los paquetes en bucle no deseados

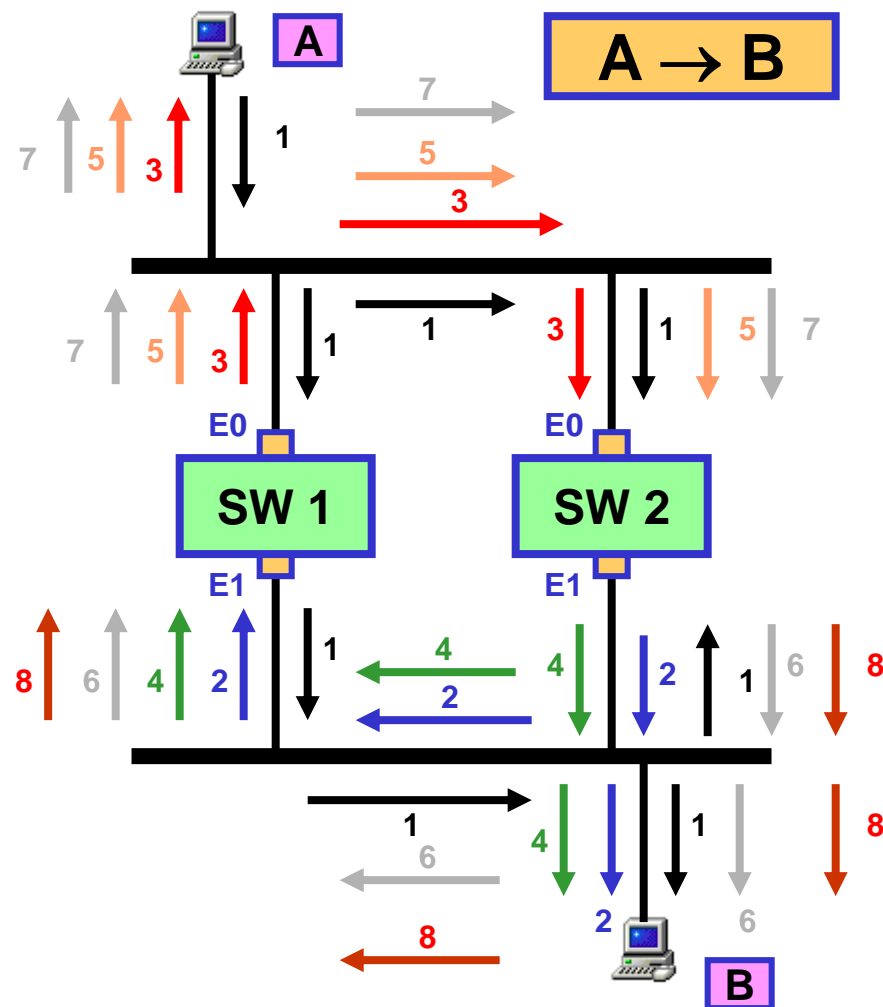
Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

Aparición de Loops en la interconexión con switches (II)



Métodos de Interconexión a Nivel de Enlace: BRIDGE y SWITCH

Aparición de Loops en la interconexión con switches (III)




SWITCH 1	
MAC	PORT
AAAAAA	E0
AAAAAA	E1

SWITCH 2	
MAC	PORT
AAAAAA	E0
AAAAAA	E1
AAAAAA	E0

Problemas:

- + Inestabilidades en tablas
- + Se inunda de tráfico la red (mal llamada Tormenta de Broadcast)

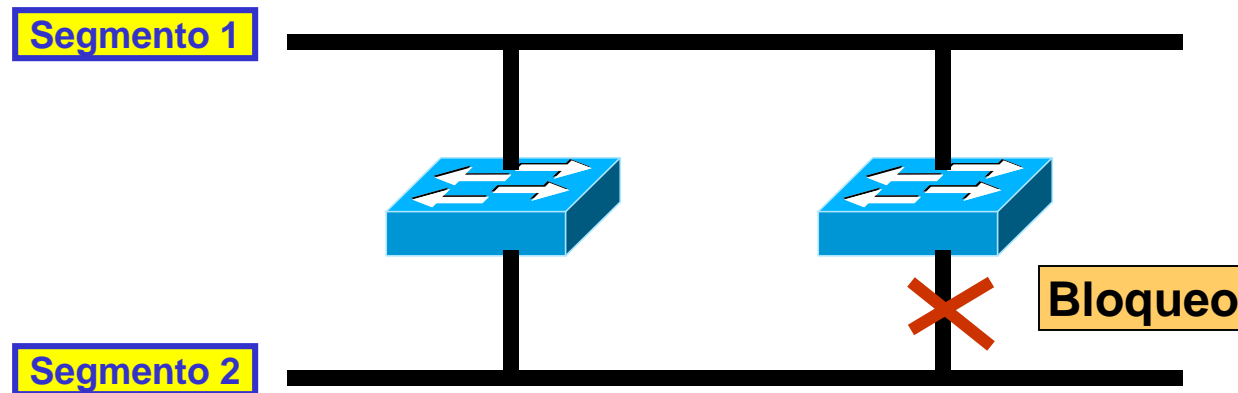
**Solución: PROTOCOLO
SPANNING TREE**

- 1** Introducción
- 2** Métodos de Interconexión a Nivel Físico: **REPETIDOR y HUB**
- 3** Métodos de Interconexión a Nivel de Enlace: **BRIDGE y SWITCH**
-  **4** Prevención de loops - Protocolo Spanning Tree (**STP**)
- 5** **VLANs**

PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE

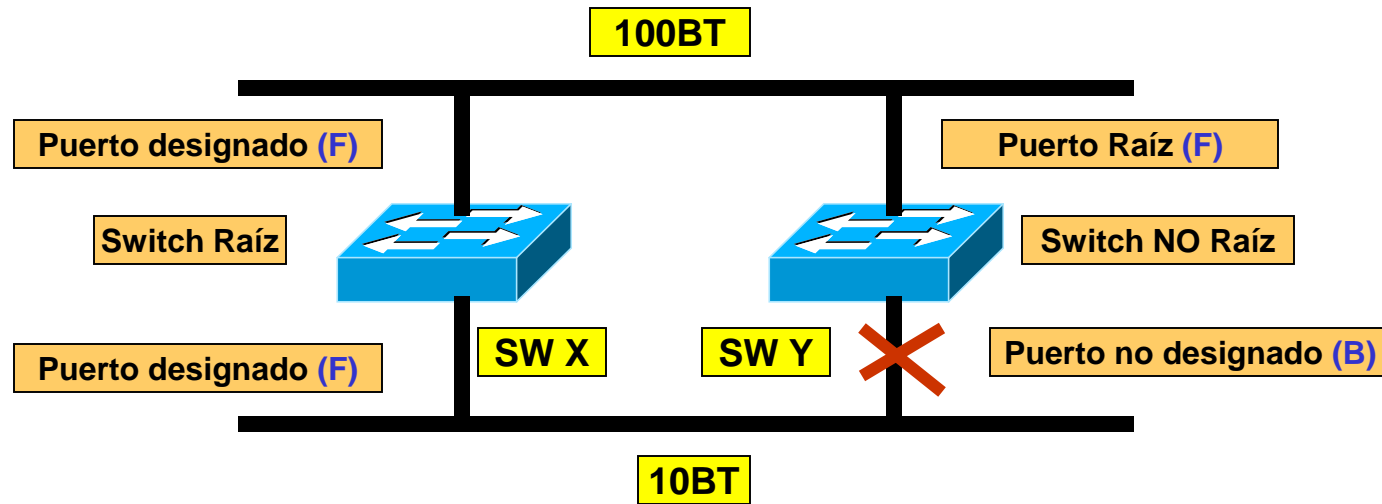
Introducción:

El protocolo **Spanning Tree** es un protocolo de tipo **bridge to bridge** o **Switch to Switch** desarrollado por **DEC**. El algoritmo Spanning Tree de DEC fue revisado posteriormente por el organismo **IEEE 802** y publicado en la especificación **IEEE 802.1d**. Los algoritmos de DEC y el de IEEE 802.1d no son los mismos, pero sí son **compatibles**. El objetivo del protocolo **STP** es mantener una red libre de bucles. Un camino libre de bucles se consigue cuando un dispositivo es capaz de **reconocer** un bucle en la topología y **bloquear** uno o más puertos redundantes. Como se ve en el siguiente ejemplo, tan sólo hay un trayecto activo desde el Segmento 1 al Segmento 2.



PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE

Definiciones básicas y Ejemplo de aplicación de STP



El **STP** proporciona una topología de red **libre de bucles** llevando a cabo las siguientes operaciones:

- ✦ **Se elige un Switch Raíz.** En un dominio de broadcast sólo puede existir un único **Switch Raíz**. Todos los puertos del Switch Raíz se encuentran en estado de **retransmisión (Fordwarding)** y se denominan **Puertos designados**. Cuando un puerto se halla en este estado puede enviar y recibir tráfico. En el ejemplo el **Switch X** ha sido elegido como **Switch Raíz**.

- ✦ **Para cada Switch NO RAÍZ, hay un Puerto Raíz.** El Puerto Raíz corresponde a la ruta de **menor métrica** desde el Switch **no** raíz hasta el Switch Raíz. Los Puertos Raíz se encuentran en estado de retransmisión y proporcionan **conectividad hacia el Switch Raíz**. El costo de la ruta para llegar al Switch Raíz es un costo **acumulativo tomándose como métrica el ancho de banda**. En el ejemplo, la ruta de menor métrica desde el Switch **Y** hasta el Switch **Raíz** (Switch X) tiene lugar a través del enlace **100BT (Fast Ethernet)**. En caso de igualdad de métricas, el factor decisivo sería la **MAC más baja del Puerto**.

PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE

Definiciones básicas y Ejemplo de aplicación de STP

✦ En cada segmento hay un solo Puerto designado. El Puerto designado se selecciona en el Switch que posee el trayecto de menor costo hasta el Switch Raíz. Los puertos designados se encuentran en estado de retransmisión y son responsables del reenvío de tráfico por el segmento. En el ejemplo, los puertos designados para ambos segmentos están en el Switch Raíz, debido a que dicho Switch está conectado directamente a ambos segmentos. El puerto 10BT del Switch Y no es un Puerto designado porque sólo puede haber un puerto designado por segmento. Los puertos no designados se encuentran normalmente en estado de bloqueo con el fin de “romper la topología de bucle”. Cuando un puerto está en estado de bloqueo, no retransmite tráfico. Esto no significa que el puerto está inhabilitado, significa que el STP está impidiendo que éste reenvíe tráfico.

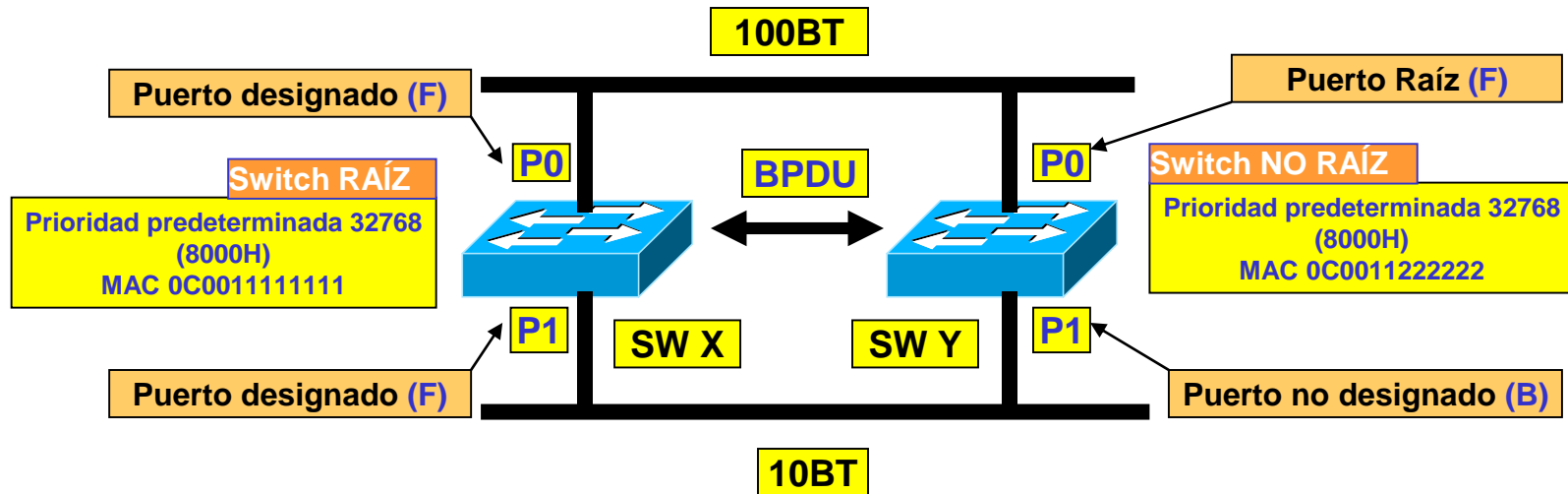
ID de bridge y estados de puerto

✦ Los switches que ejecutan STP intercambian mensajes de configuración con otros switches a intervalos regulares usando una trama de broadcast denominada Bridge Protocol Data Unit (BPDU). Por omisión, la BPDU se envía cada dos segundos. Uno de los elementos de información incluidos en la BPDU es el ID bridge. El STP llama a cada switch por un identificador denominado genéricamente “Bridge ID”. Normalmente el “Bridge ID” está compuesto por una prioridad (2 bytes) más la dirección MAC de base o canónica del switch (6 bytes). La prioridad predeterminada (IEEE 802.1d) es 32.768, es decir, el valor correspondiente a la mitad del rango (de los dos bytes). El switch raíz es el que tiene el “Bridge ID” más bajo.

Estados de STP

- **Bloqueo:** Ninguna trama puede ser enviada, sólo se escuchan **BPDUs**
- **Escucha:** No se envían tramas, sólo se escucha para detectar si hay tramas
- **Aprendizaje:** No se envían tramas, se aprenden direcciones
- **Envío:** Tramas enviadas, se aprenden direcciones
- **Desactivado:** No se envían tramas, no se escucha ninguna **BPDUs**

PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE



✦ En la figura, debido a que ambos switches están usando la misma prioridad predeterminada, el que tiene la dirección **MAC** más baja es el **Switch Raíz**. Así, en este ejemplo, el **Switch X** es el **Switch Raíz**, con un Bridge ID de **8000.0C0011111111**. El valor hexadecimal **8000** es la prioridad del bridge (**32768** en decimal). El valor **0C0011111111** es la dirección **MAC** del dispositivo.

✦ Una vez que la BPDU ha sido intercambiada, los estados de los puertos en los switches serían los siguientes:

- Los puertos del **Switch X** (el Switch Raíz), son puertos designados (forwarding). Sólo puede haber un puerto designado por segmento.
- El puerto Fast Ethernet del **Switch Y** es el puerto Raíz (forwarding). Éste posee una ruta de costo superior hasta el Switch Raíz a través del segmento de red Ethernet 10BT, con lo cual queda descartada esta ruta.
- El puerto Ethernet del Switch Y es el puerto no designado (blocking).

PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE

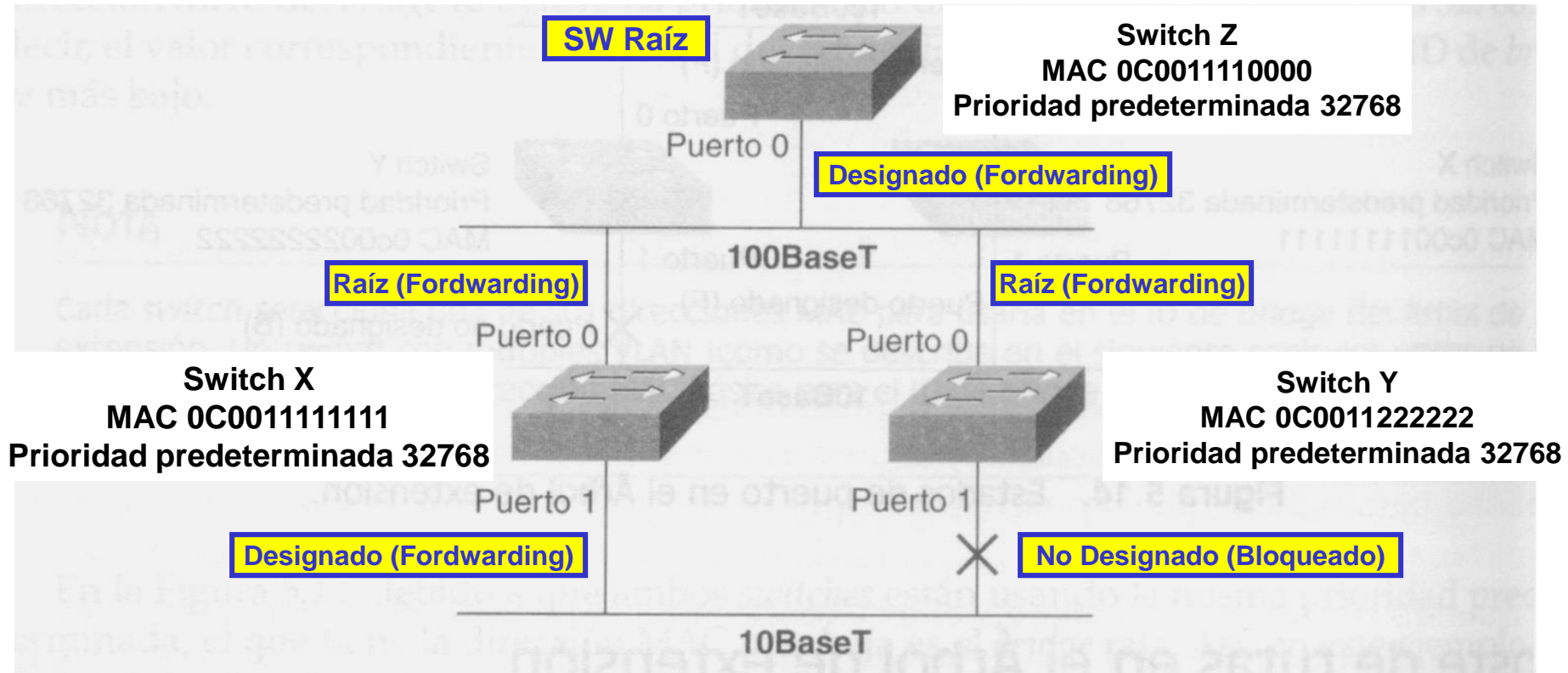
Costos de rutas en el STP

La **métrica de una ruta en el STP** es un costo acumulativo basado en el **ancho de banda** de todos los enlaces que conforman la ruta hacia el **Switch Raíz**. La siguiente tabla nos muestra alguno de los costos de ruta especificados en el estándar **IEEE 802.1d**. Dicha especificación fue objeto de revisión. En la especificación antigua, la métrica se calculaba como **1000 M / ancho de banda**. En la nueva especificación se ha ajustado el cálculo para dar cabida a interfaces de **velocidad superior**, incluidas las de **1** y **10** Gbps.

Tabla de métricas de rutas en el STP

Velocidad del enlace	Métrica (Especificación IEEE revisada)	Métrica (Especificación IEEE previa)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE

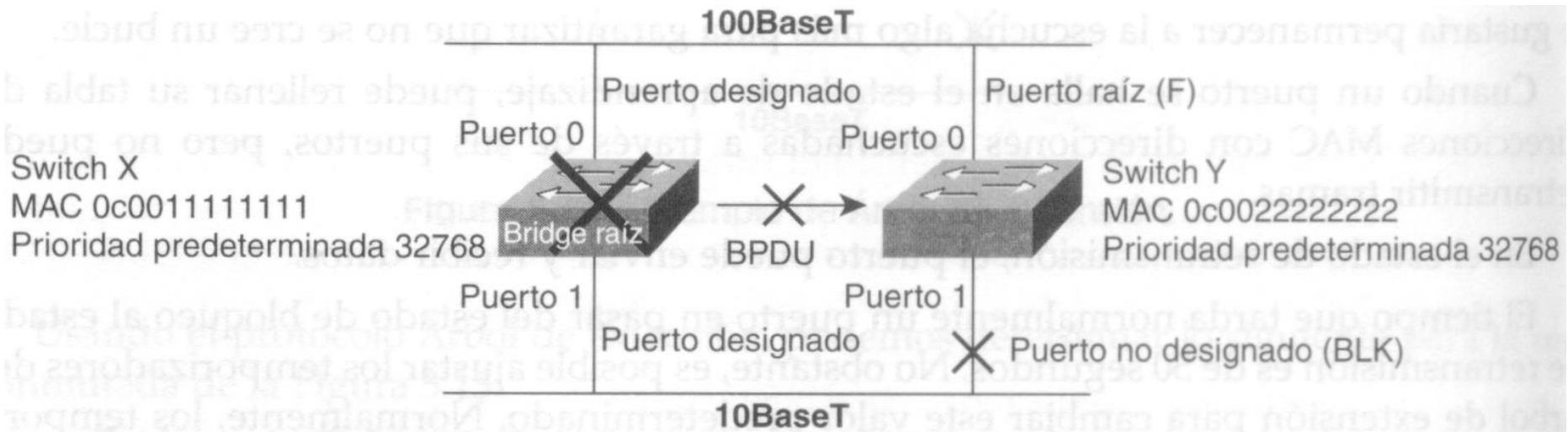


Usando el STP, podemos determinar lo siguiente para la red conmutada de la figura:

- **Switch Raíz.** El switch **Z**, dado que posee el **bridge ID** más bajo (prioridad y dirección MAC)
- **Puerto Raíz.** Puertos **0** de los Switches **X** e **Y**, ya que están en la ruta hacia el Switch raíz de menor métrica.
- **Puerto designado.** Puerto **0** del switch **Z**. El puerto **1** del switch **X** es un puerto **designado**. Dado que el switch **X** como el switch **Y** poseen el mismo costo de ruta hasta el switch raíz, el puerto **designado** ha sido elegido en el switch **X**, dado que posee un Bridge ID inferior que el switch **Y**.
- **Bloqueado.** Puerto **1** del Switch **Y**. Se trata del puerto no designado dentro del segmento.

PREVENCIÓN DE LOOPS - PROTOCOLO SPANNING TREE


Recálculo del Árbol de extensión (STP)



Cuando se produce alguna modificación en la topología debido a un fallo en un switch o en un enlace, el protocolo **STP reajusta automáticamente** la topología de la red para garantizar la **conectividad**, colocando puertos **bloqueados en estado de retransmisión**. En el ejemplo indicado, si el **Switch X (el switch raíz)** tuviera un fallo, el **Switch Y** detectaría la **BPDUs ausente del Switch Raíz**. En consecuencia, uno de los temporizadores del **STP**, denominado **“Duración Máxima” expiraría**. Cuando un temporizador de este tipo **llega a su límite** sin haberse recibido una **nueva BPDUs del entorno próximo**, **se reinicia un nuevo recálculo del STP** en su globalidad. El **Puerto 1** pasaría sucesivamente al estado de **escucha**, después al de **aprendizaje** y finalmente al de **retransmisión**.

Una vez recobrada la **convergencia de la red**, el **Switch Y** se convierte en el **Switch Raíz**. **Éste** retransmite el tráfico entre los dos segmentos cuando sus puertos pasan del estado de retransmisión para convertirse en Puertos designados.

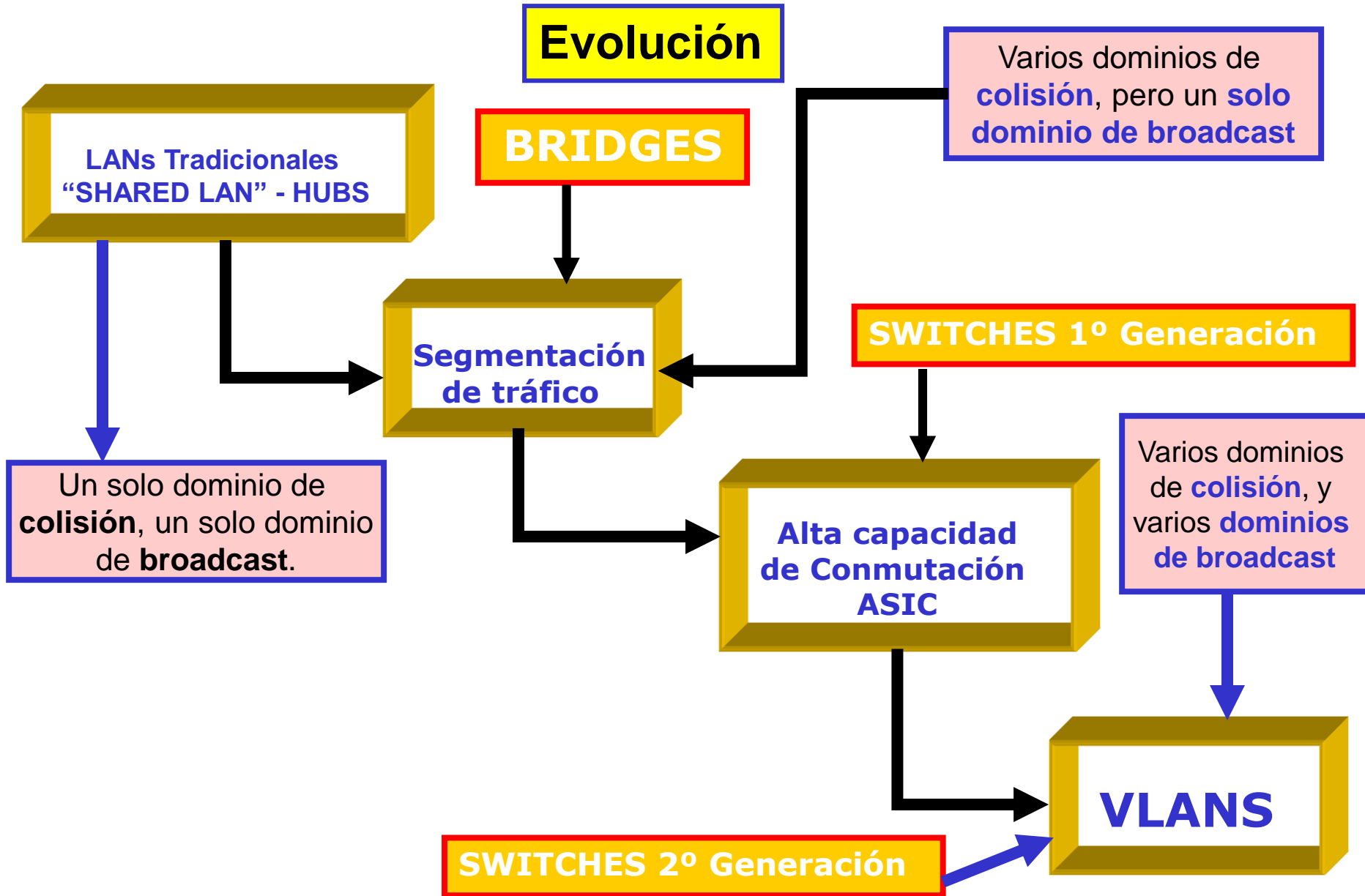
RESUMEN

- 1** Introducción
- 2** Métodos de Interconexión a Nivel Físico: **REPETIDOR y HUB**
- 3** Métodos de Interconexión a Nivel de Enlace: **BRIDGE y SWITCH**
- 4** Prevención de loops - Protocolo Spanning Tree (**STP**)
-  **5** **VLANs**

DEFINICIÓN DE VLAN

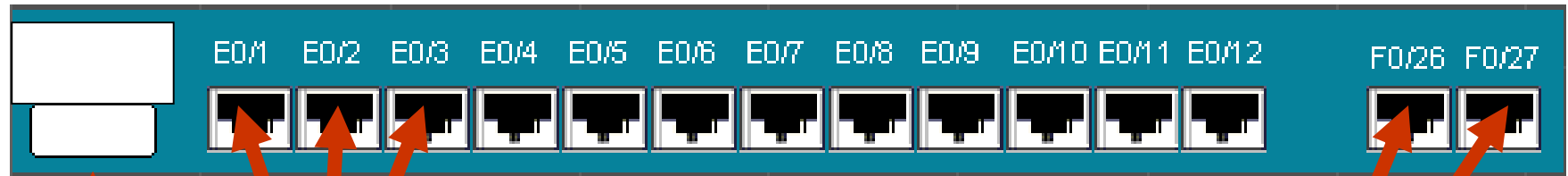
Es la formación de grupos de trabajo (**LANs**) independientemente de **su posición geográfica** que comparten un mismo dominio de **BROADCAST**.

VLANs



VLANs

SWITCHES de 2º GENERACIÓN: IMPLEMENTACIÓN DE VLANs (I)



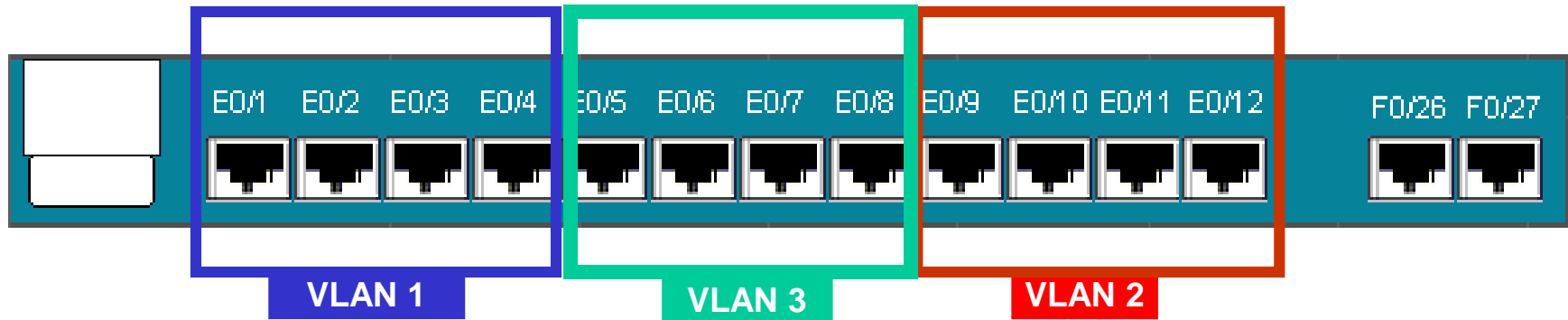
Entrada de consola
para configuración

Puertos de
Acceso **10/100**

Puertos de **TRUNK** (gran ancho de banda),
Típicamente **1 Gbps** para arriba !!
Permiten **cascadear switches** y conectar
las **VLANs** de diferentes switches. Si no
Configuro **VLANs** podría conectar aquí un **Server**

VLANs

SWITCHES de 2º GENERACIÓN: IMPLEMENTACIÓN DE VLANs (II)

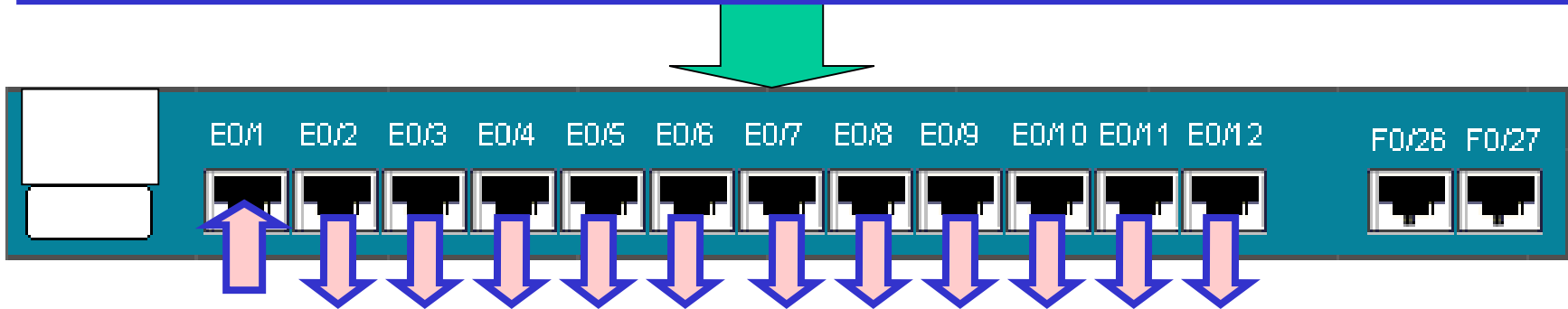


Mediante **comandos de software** se configura **a qué VLAN** pertenece cada puerto del switch. Por ejemplo a la **VLAN 1** pertenecen los **hosts** que se conecten a los **puertos 1, 2, 3 y 4**. La **VLAN 2** estará constituida por los **hosts** que se conectan en los **puertos 9, 10, 11 y 12**. Idéntica situación se dará para la programación de la **VLAN 3** (**puertos 5, 6, 7 y 8**). Cuando un host perteneciente a una **VLAN** realice un **broadcast**, sólo se propagará por los puertos **pertenecientes a dicha VLAN**, por lo tanto hemos logrado **separar dominios de broadcast** empleando un **único dispositivo físico**, de ahí la idea de “**virtual**”, porque es como si se tuviera diferentes **redes físicas**, pero en realidad son **diferentes redes lógicas** soportadas por un mismo medio físico, **el switch**. Cada VLAN podría verse como un switch separado.

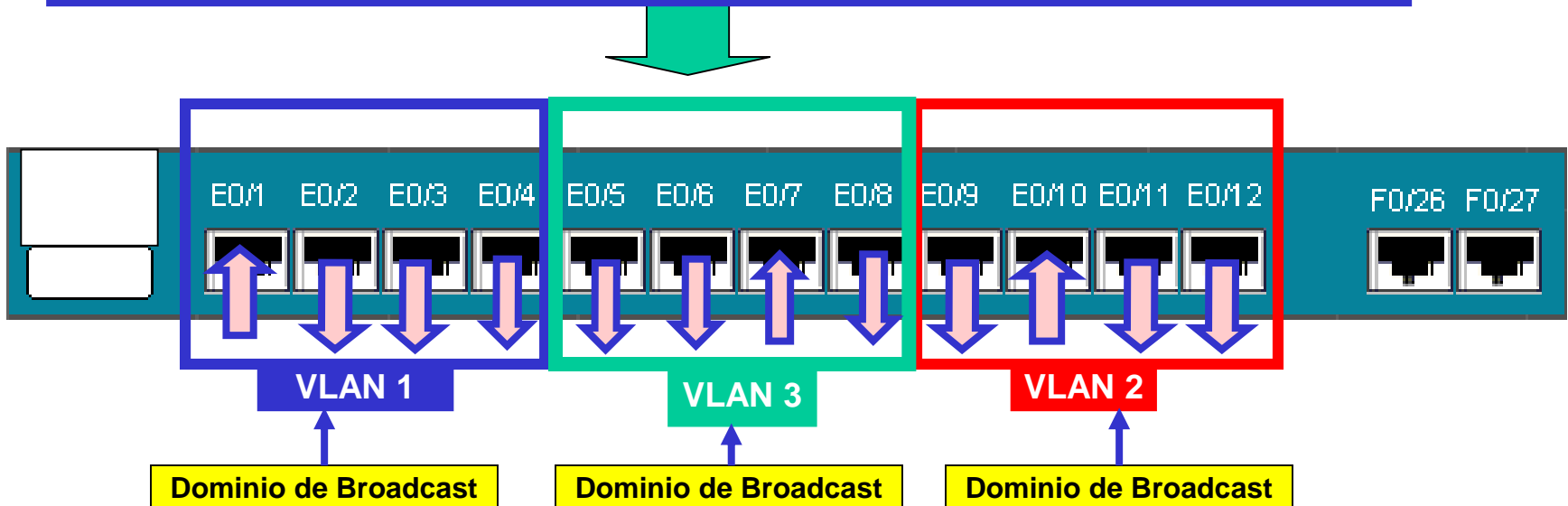
VLANs

SWITCHES de 2º GENERACIÓN: IMPLEMENTACIÓN DE VLANs (III)

ANTES con los Switches de 1º Generación sólo una VLAN o un único dominio de BROADCAST



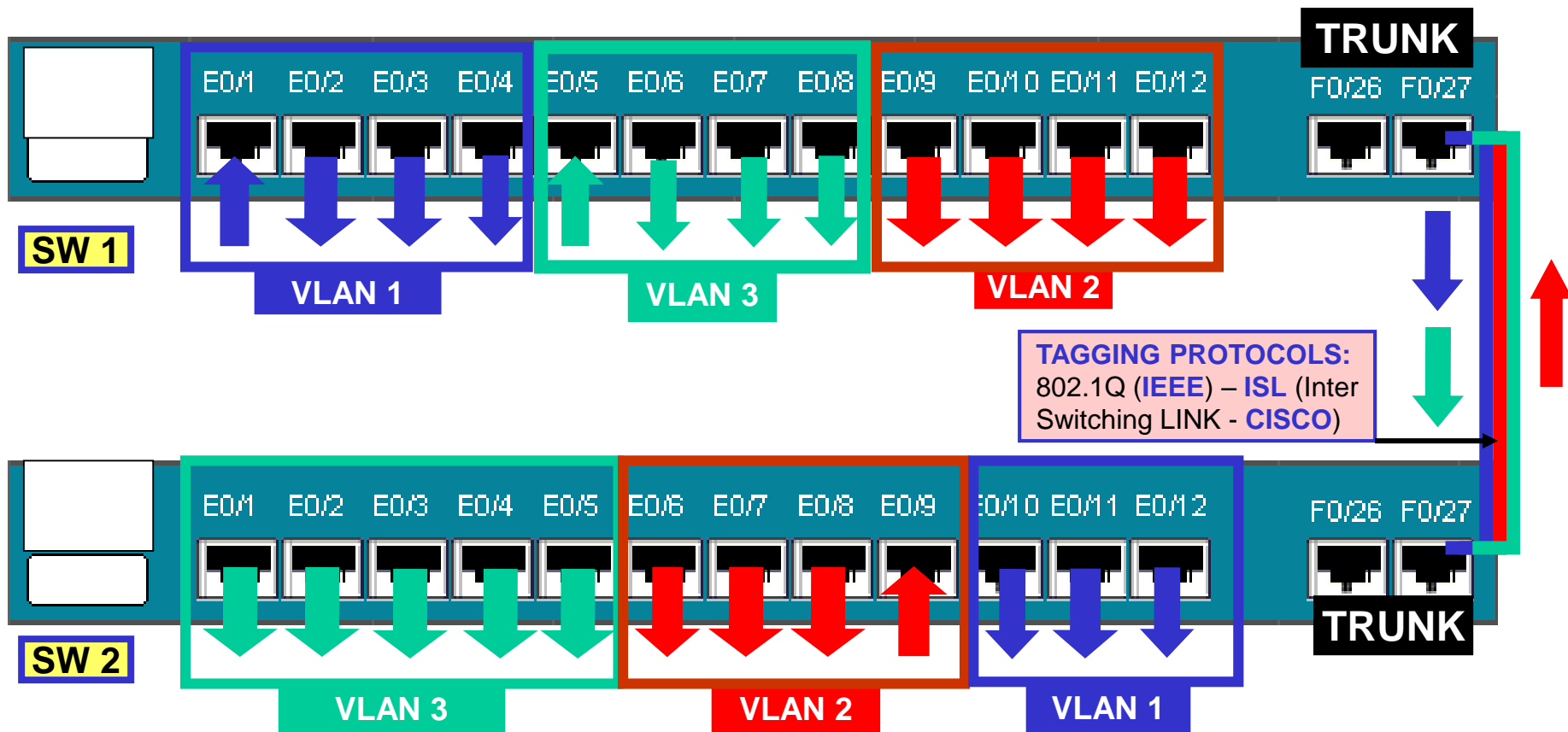
AHORA con la posibilidad de poder implementar VLANs



VLANs

SWITCHES de 2º GENERACIÓN: IMPLEMENTACIÓN DE VLANs (IV)

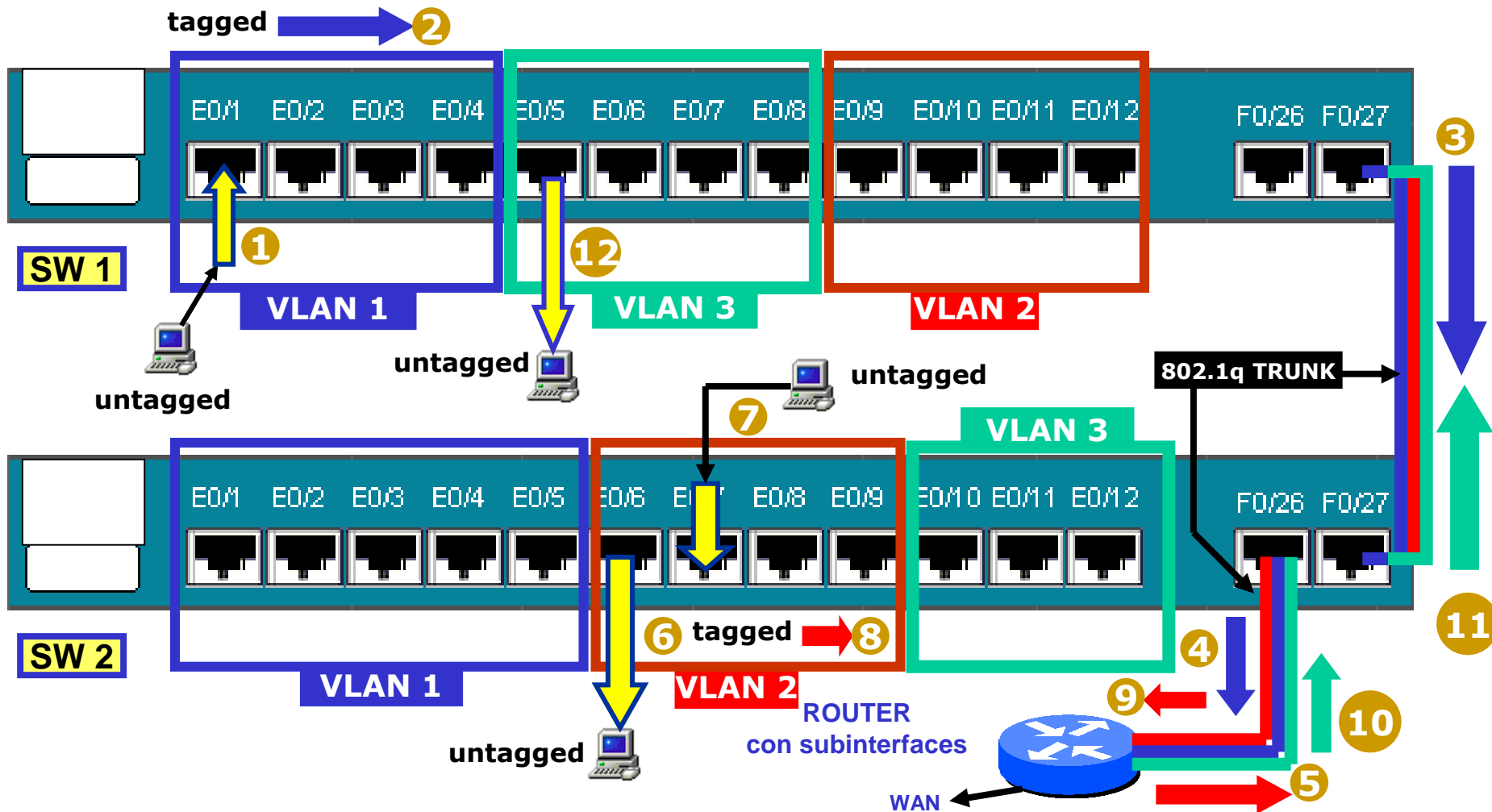
Los puertos de TRUNK se dice que están “tagueados” y por ellos pasan todas las VLANs tagueadas. Los puertos pertenecientes a cada una de las VLANs son puertos no tagueados o “untagged”



VLANs

SWITCHES de 2º GENERACIÓN: IMPLEMENTACIÓN DE VLANs (V)

¿Qué pasa cuándo quiero interconectar dos o más VLANs?

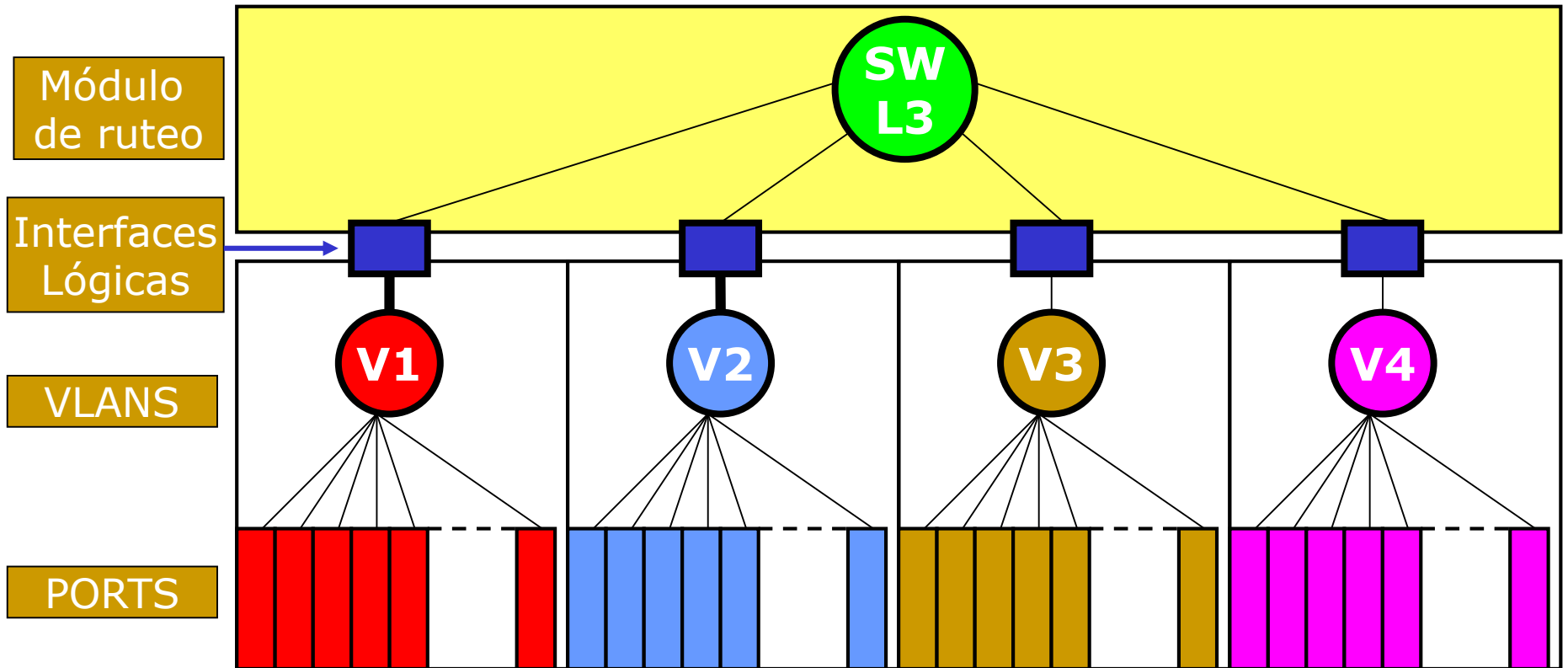


Para comunicarse entre VLANs debo usar un router con una LAN Fast Ethernet (esta es la exigencia de CISCO), o bien un **Switch Layer 3**.

Un Switch L3 es un dispositivo que realiza funciones de N2, pero que se le añade un módulo capaz de rutear N3. También se lo conoce como **Gigaswitch-Router**. Cuando se emplea un router deberá configurarse una subinterface lógica por cada VLAN, cada una con su dirección IP y máscara, y cada subinterface deberá ser asignada a una VLAN.

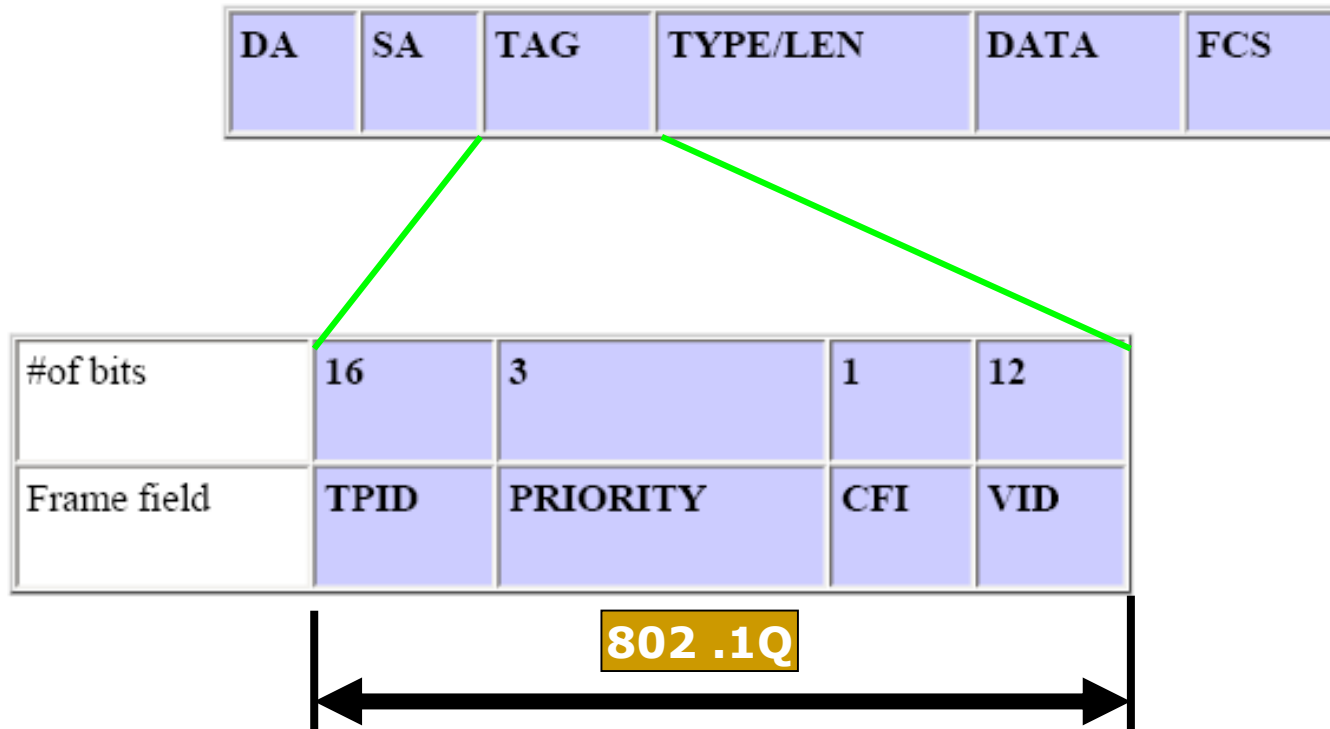
VLANs

Switch Layer 3



VLANs

Trama Ethernet con el agregado del tagging protocol



El detalle de los campos es el siguiente:

TPID: Significa Tag Protocol Identifier. Se le asigna el valor 8100h que identifica a un frame tagueado con 802.1q

Priority: Este campo codifica las clases de servicio (COS que significa Class of Service) y se lo conoce como el estándar 802.1p y tiene que ver con lo que se conoce como QOS (Quality of Service) a nivel de capa 2. El objetivo de este protocolo es la priorización de conmutación de los paquetes en un switch de capa 2 en función del tipo de tráfico.

CFI: Canonical Format Indicator. Este campo consta de un solo bit. Si dicho bit está a 1 entonces la dirección MAC del switch no está en el formato de la dirección canónica. En cambio si este bit está a 0, entonces la MAC address está en el formato canónico.

VID: VLAN Identifier, es un número de 0 a 4095 (12 bits) que caracteriza el número de VLAN.

VENTAJAS DE USAR VLANS:

- + Movilidad**
- + Control de tráfico MULTICAST y BROADCAST**
- + Facilidad de cambios, altas y bajas**
- + Escalabilidad**
- + Seguridad**
- + Posibilidad de gestionar servidores**

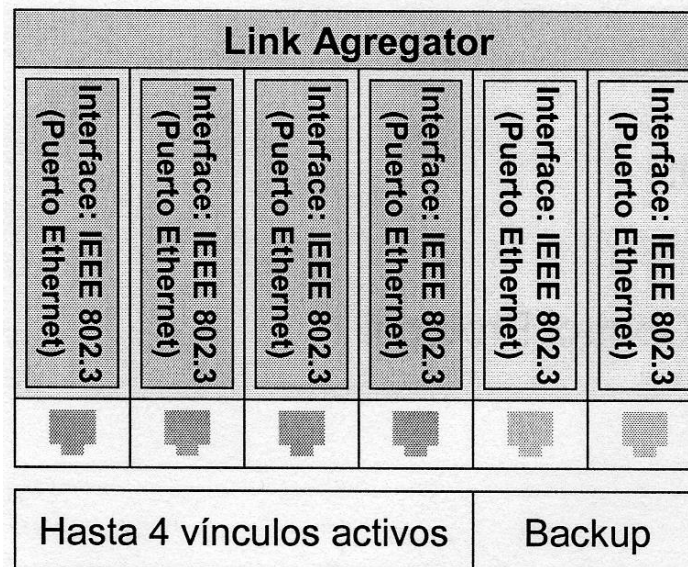
Como desventaja podemos citar tal vez el hecho que se requiere un control administrativo más exhaustivo de la red.

TEMAS ANEXOS DE SWITCHING

LACP

LACP

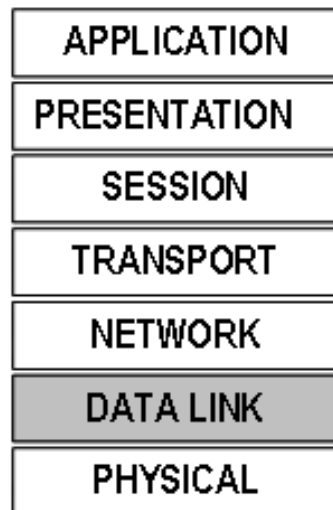
LACP (Link Aggregation Control protocol) es un protocolo normalizado por el IEEE conocido bajo las siglas 802.3ad. La función de este protocolo es la de permitir el incremento del ancho de banda en un switch uniendo varios puertos físicos (hasta 4 puertos más dos puertos de backup) y generando así un único enlace lógico de un ancho de banda equivalente a la suma de los anchos de banda de cada puerto físico. A este enlace lógico que se forma, se lo denomina TRUNK, ya que inicialmente a este protocolo antes de su estandarización se lo conocía como SMART TRUNK. Este protocolo es muy útil cuando se quiere por ejemplo incrementar el ancho de banda entre dos switches que disponen de puertos de 1 Gbps y por razones de coste pasar a un switch con puertos de 10 Gbps sería muy oneroso y además no llegaría a utilizarse tanta potencia de conmutación, entonces este protocolo permite dar una solución sin upgrade de hardware.



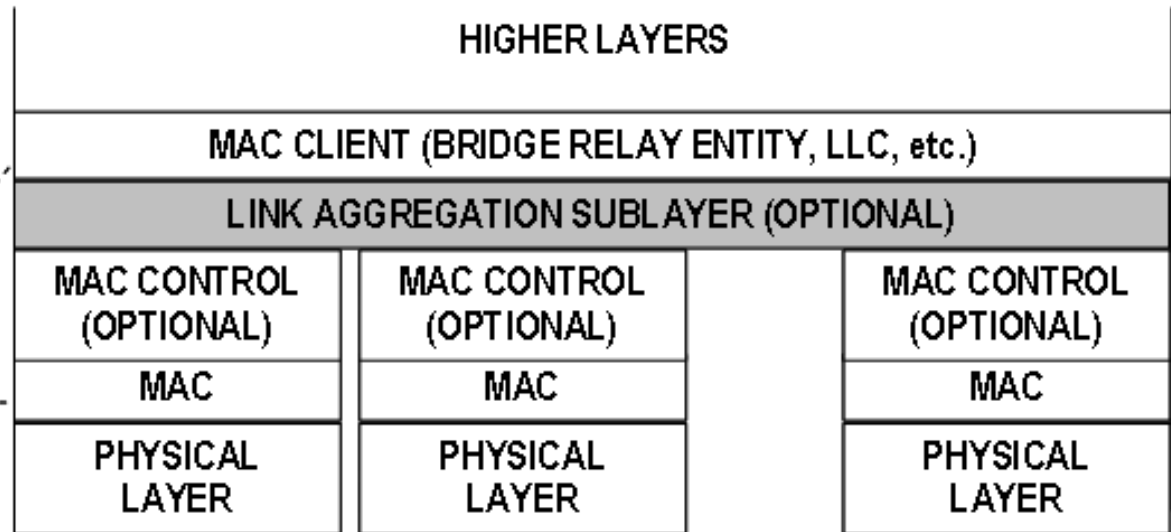
LACP

LACP además de permitir el incremento del ancho de banda de un enlace, uniendo varios puertos físicos, aporta también una mejora en la performance ya que añade redundancia. Si por ejemplo si en un enlace formado por dos links de 100 Mbps (en total 200 Mbps, ó 400 Mbps FULL DUPLEX), un link se corta nos queda un enlace de 100 Mbps, pero la conectividad no se interrumpe. Además LACP admite Spanning tree, el STP considera a cada enlace LACP lógico como si fuera un único vínculo físico. Además LACP también permite hacer un balance de carga entre los links parciales que conforman el TRUNK.

OSI Reference Model Layers



LAN CSMA/CD Layers

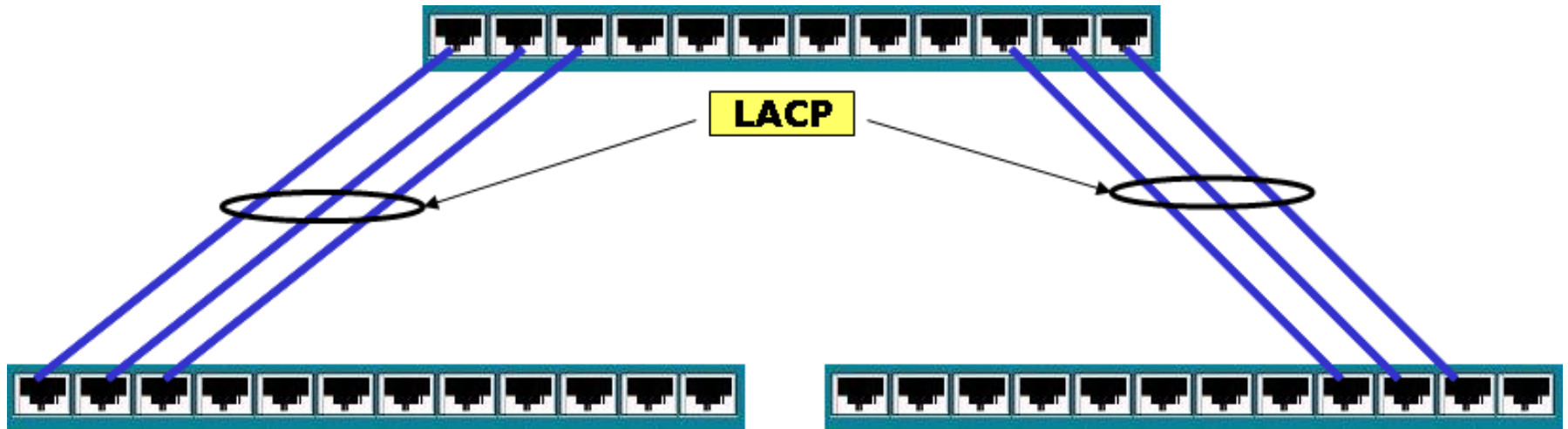


LACP

El esquema anterior nos muestra la relación de **LACP** y el modelo **OSI**. Vemos como entre cada capa MAC individual de cada puerto físico y la capa MAC cliente se agrega la capa denominada LINK AGGREGATION SUBLAYER, que controlará el trunk.

Finalmente para concluir citaremos los tres escenarios de aplicación de LACP:

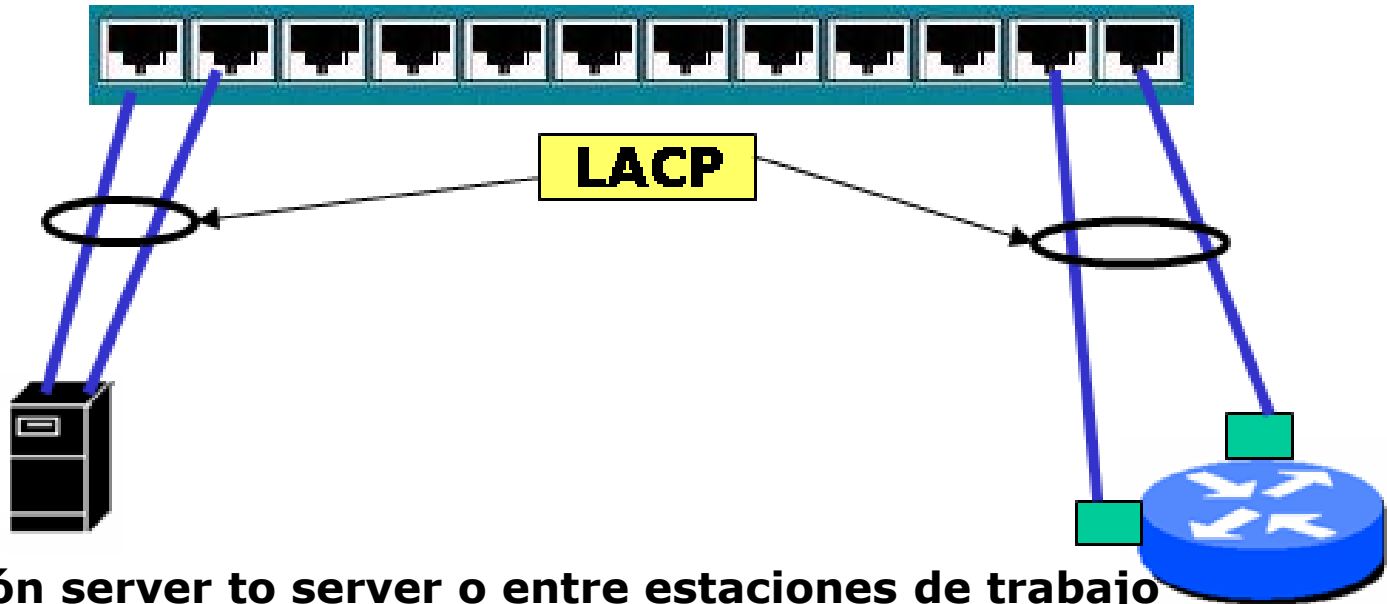
1. Conexiones de switch a switch



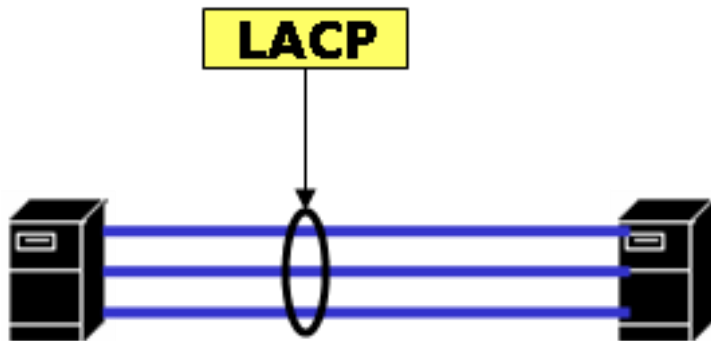
En este escenario varios puertos se nuclean formando un único enlace lógico de mayor ancho de banda. En el ejemplo si los puertos son 100 Mbps cada LACP transporta una capacidad de 300 Mbps.

LACP

2. Conexión switch a Server o Switch a router



3. Conexión server to server o entre estaciones de trabajo



Escenario LACP entre servers o estaciones de trabajo

LACP

Este último escenario es menos utilizado.

Finalmente para concluir se indican una serie de reglas a cumplir para implementar LACP:

1. Los puertos que conformarán parte del LACP deberán configurarse en modo FULL DUPLEX
2. Un vínculo LACP una vez constituido es un enlace que no puede desagruparse, o sea debe tratarse como una unidad lógica indivisible.
3. LACP sólo soporta puertos Ethernet 802.3
4. Todos los links que conforman un LAG (Link aggregation group) deben operar todos a la misma velocidad. Es decir no pueden mezclarse por ejemplo, puertos 1Gbps con fast ethernet.

RATE LIMITING

Esta característica es soportada en algunos switches y lo que permite hacer es regular el ancho de banda que se le asigna a un puerto. Por lo general la granularidad es de 1 Mbps, es decir que éste es el valor más pequeño de ancho de banda que se le puede asignar a un puerto físico. Se suele ir incrementando en pasos de 1 Mbps hasta asignar la totalidad del ancho de banda de 100 Mbps (suponiendo un puerto fast ethernet).

Es útil cuando a algunos usuarios se les quiere limitar el empleo de ciertas aplicaciones que demandan mucho ancho de banda, como por ejemplo algunos programas como el kazaa o el emule. También al limitar el ancho de banda se puede limitar que por ejemplo ciertos usuarios no utilicen por ejemplo tráfico de tiempo real, como audio y video.