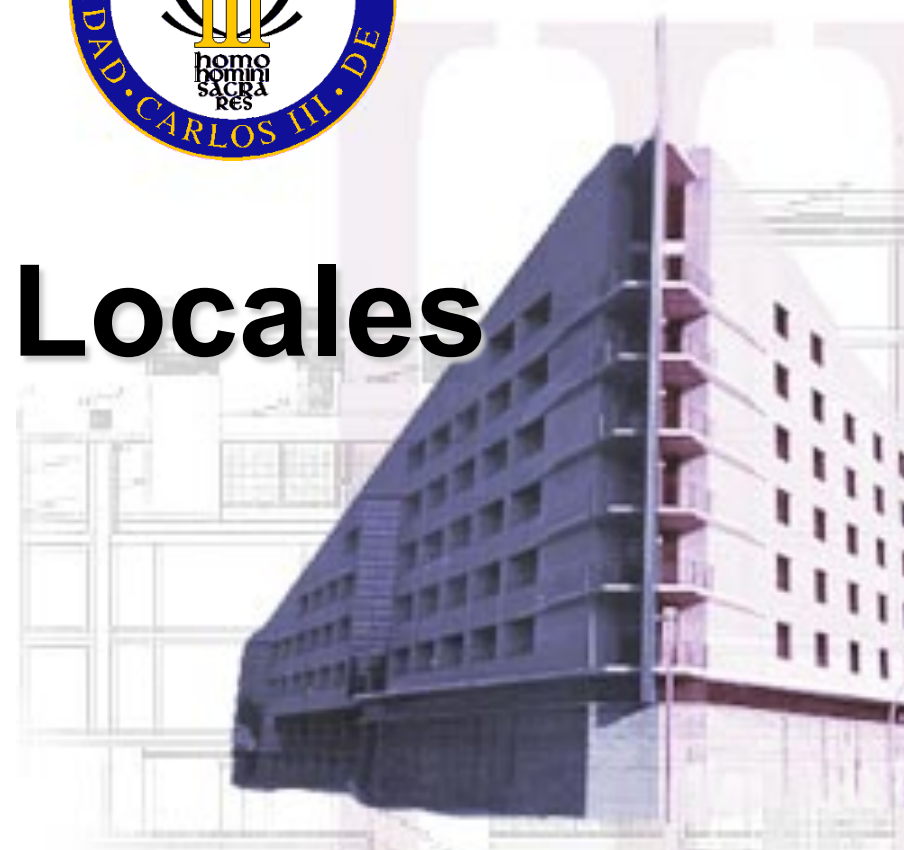




VLAN: Redes Locales Virtuales



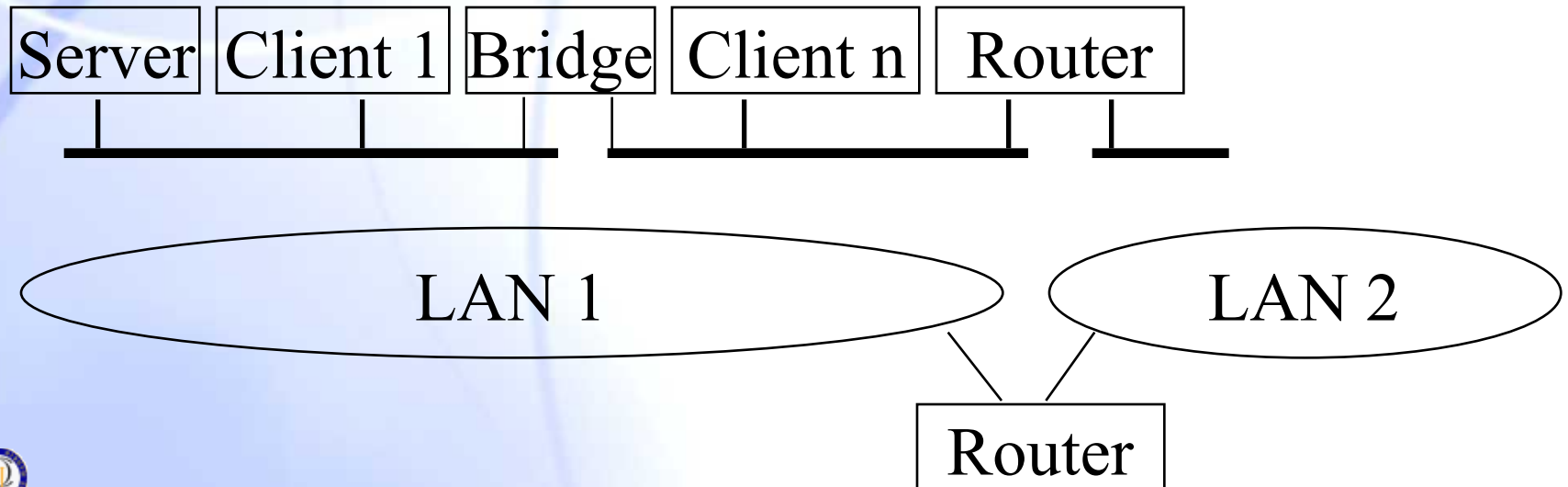
Departamento de Ingeniería Telemática

Universidad Carlos III de Madrid

Concepto de LAN

♦ LANs:

- ❖ Son redes donde se comparte el mismo dominio de difusión
- ❖ Formadas por uno o más segmentos LAN
- ❖ Dispositivos físicamente conectados mediante cableado, repetidores, hubs, bridges o switches
- ❖ Separadas/Interconectadas mediante el uso de routers



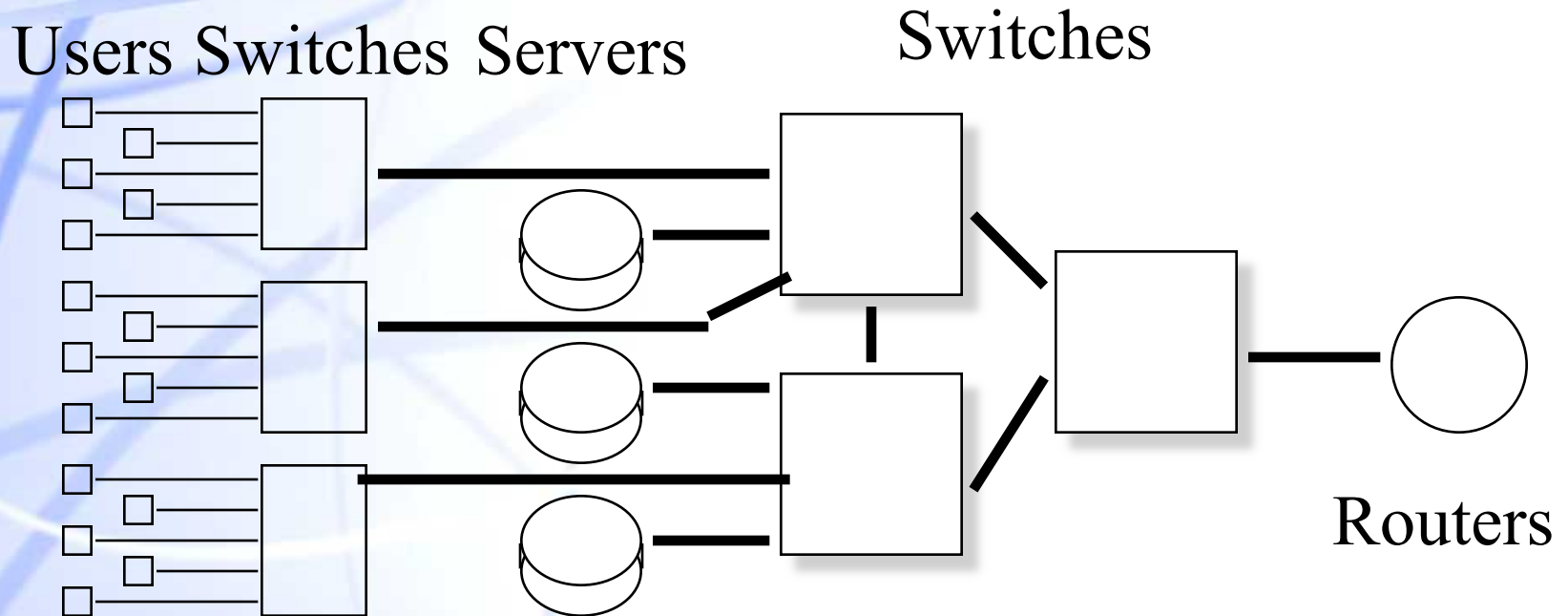
Concepto VLAN

◆ VLANs: “*LANs especiales*”

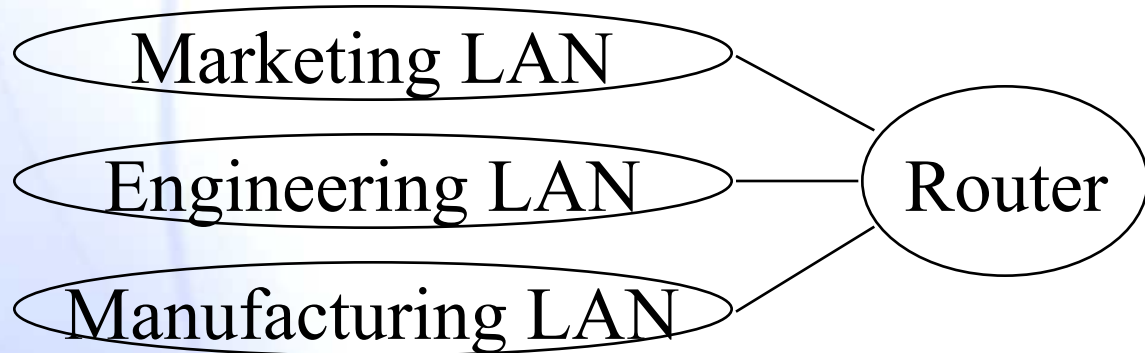
- ❖ Los miembros de la LAN están definidos por el administrador de la red: “VIRTUAL”.
- ❖ Tráfico multicast y broadcast alcanza únicamente miembros de la red.
- ❖ Independiente de situación geográfica y de donde se conecten los miembros.
- ❖ Separadas mediante el uso de routers

Concepto de VLAN

◆ Red Física



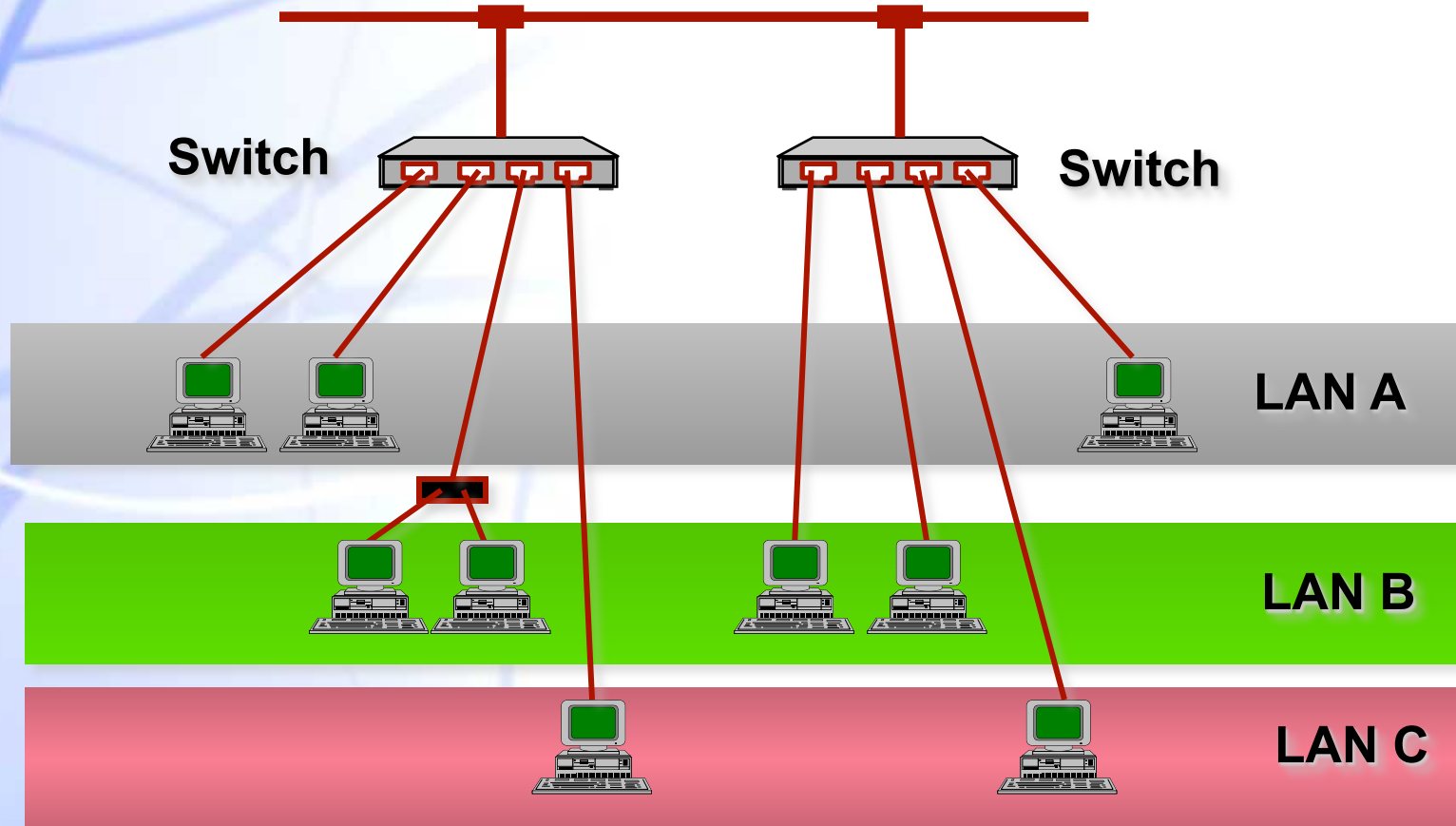
◆ Red Lógica



VLANs

- ◆ ***VLAN: formación de grupos de trabajo (LANs) independientemente de su posición geográfica que comparten un dominio de colisión.***
 - ❖ LAN Física
 - ❖ LAN Virtual
- ◆ **Tipos de VLAN**
 - ❖ basada en puertos
 - ❖ basada en direcciones MAC
 - ❖ basada en protocolo nivel 3
 - ❖ basada en aplicaciones

Escenario



Ventajas de las VLANs

1. Prestaciones:

- ❖ Reduce el envío de tráfico de difusión y multicast a destinos no implicados mediante la construcción de VLANs específicas.

2. Formación de grupos virtuales.

- ❖ Sin necesidad de desplazar a las personas
- ❖ Por tiempo adaptado al grupo
- ❖ Problemas
 - ✓ Recursos compartidos: impresoras
 - ✓ Servidores vs granjas de servidores

Ventajas de las VLANs

3. Administración

- ❖ 70 % del coste de red se debe a añadir, mover o reconfigurar usuarios en la red. VLANs simplifican este proceso. Facilidad para cambios, altas y bajas.
- ❖ Necesario establecer una gestión de grupos virtuales.

4. Reducción de costes

- ◆ Centralización de servidores.

5. Seguridad

- ❖ Información crítica sólo es difundida a los usuarios que pueden acceder a ella.

Inconvenientes de las VLANs

- ❖ **Soluciones propietarias**
- ❖ **Estandarización en marcha**
 - ✓ IEEE 802.10 (Interoperable LAN/MAN security)
 - ✓ IEEE 802.1Q
- ❖ **No es una tecnología plug-and-play**
 - ✓ Hay que configurar los bridges

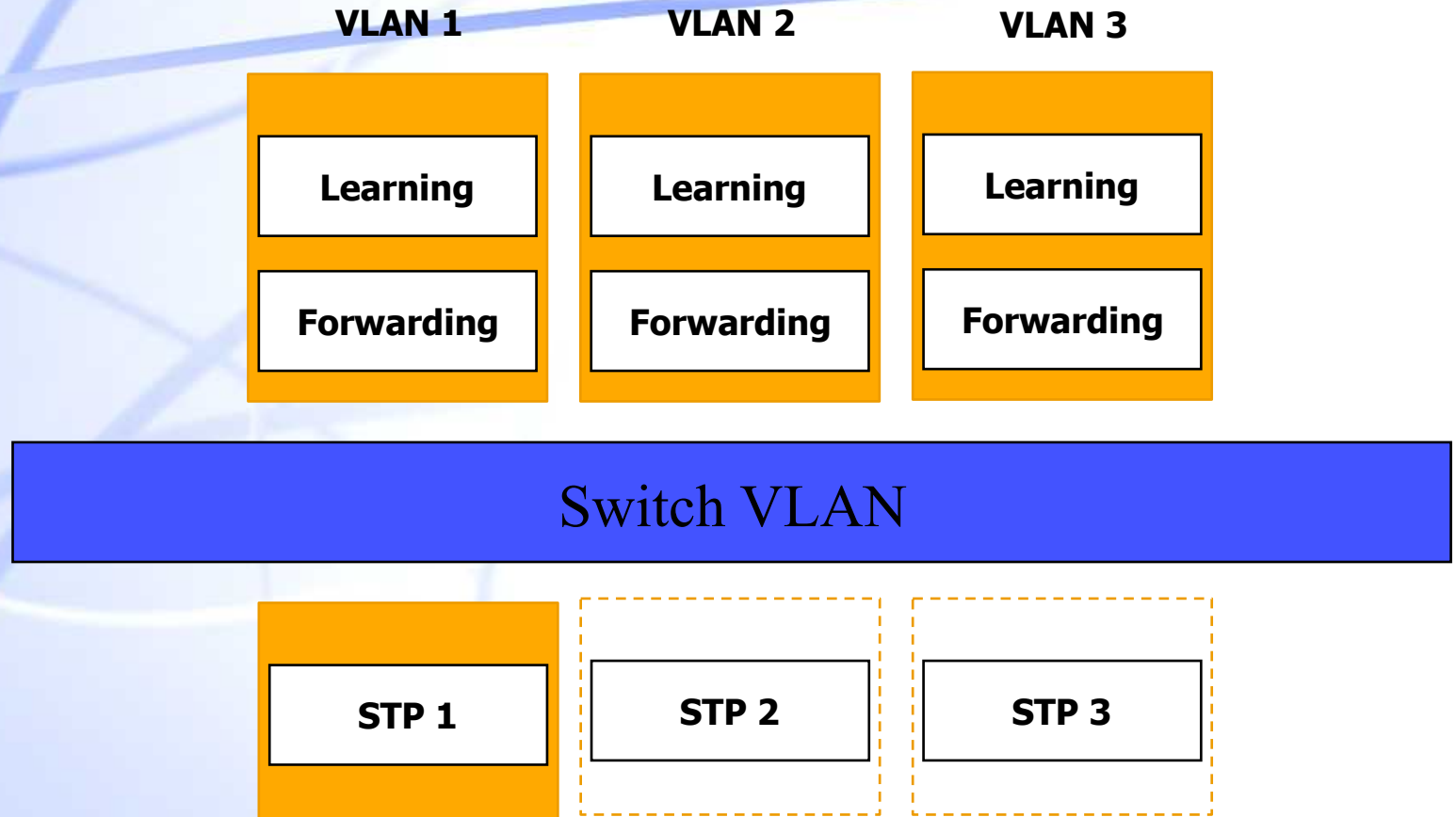
Funcionamiento de las VLANs

- ◆ **Marcado explícito**
 - ❖ **Origen**
 - ❖ **Tipo Ethernet 0x8100**
- ◆ **Marcado implícito**
 - ❖ **Puerto**
 - ❖ **MAC origen**
 - ❖ **IP origen**
 - ❖ **Tipo de protocolo**
- ◆ **El marcado requiere que los bridges/switches mantengan información de filtrado.**

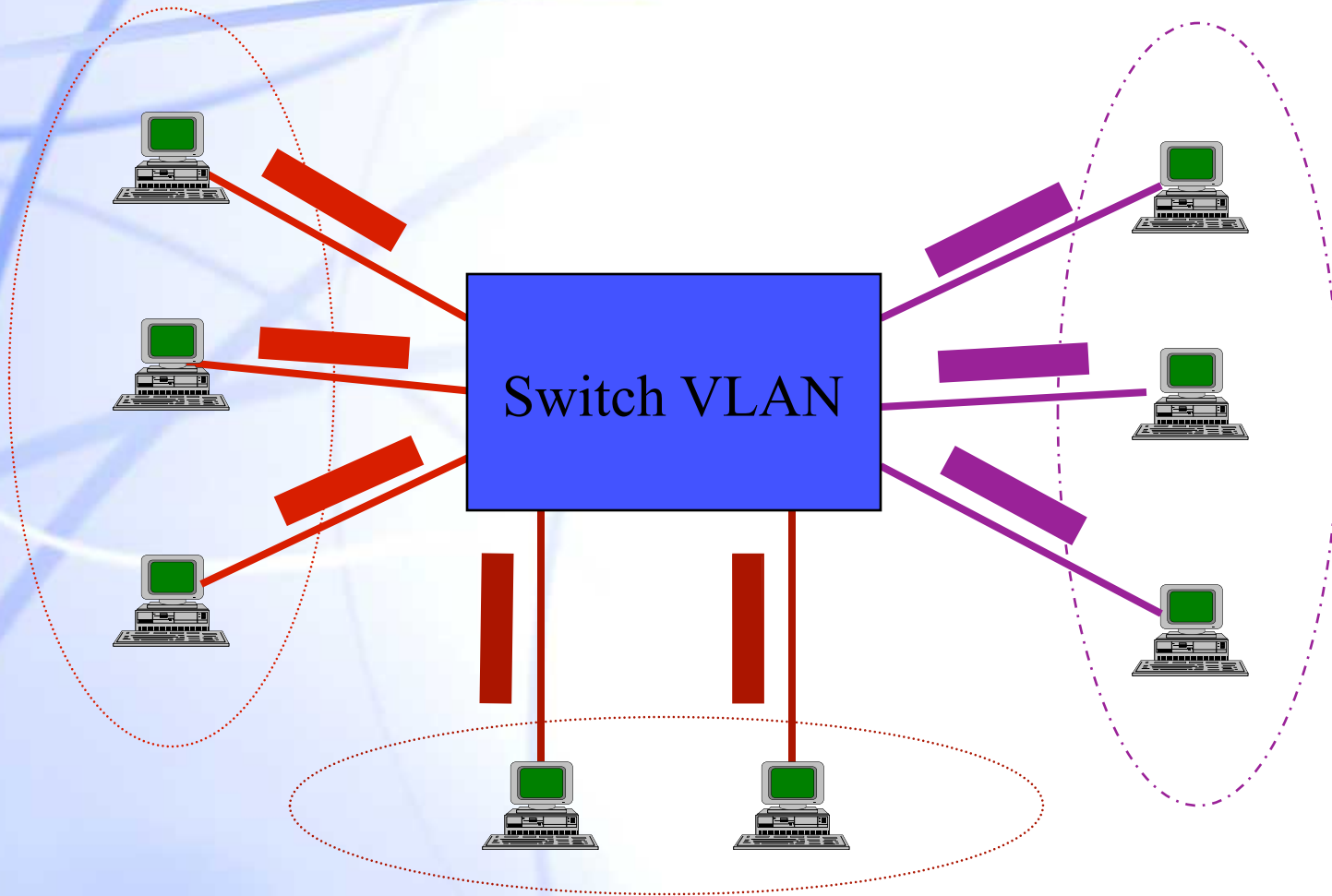
Funcionamiento de las VLANs

- ◆ Si las VLANs se forman en base a puertos debe mantenerse que puertos pertenecen a que VLAN.
- ◆ Todos los bridges de la red deben tener la misma visión.
- ◆ Una vez que el bridge ha decidido donde debe encaminar la trama, esta se encamina como en el caso de redes LAN tradicionales. Si los dispositivos destinatarios son capaces de manejar tramas marcadas (VLAN-aware), el marcado se mantiene. En caso contrario el bridge elimina el marcado.

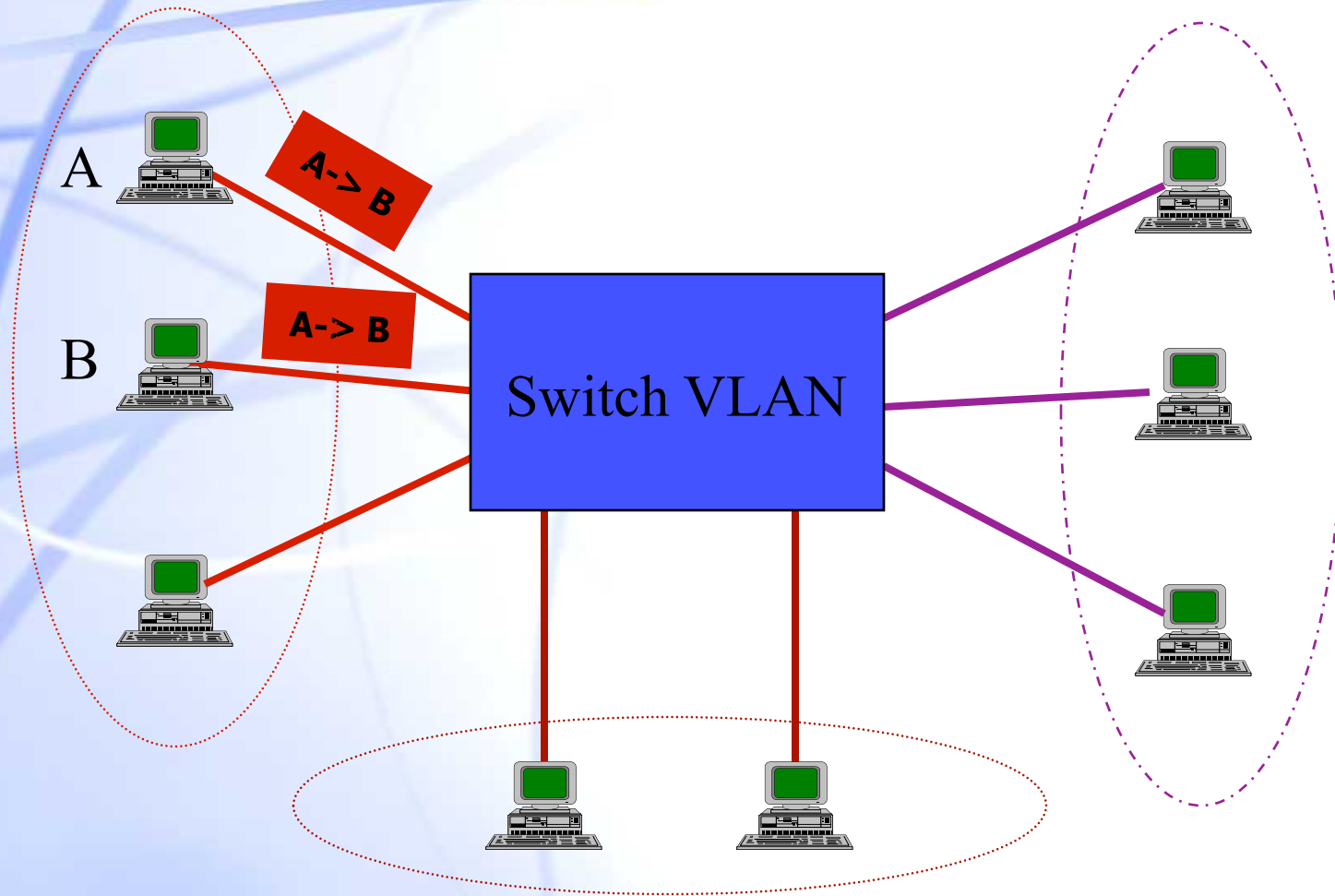
Arquitectura switch con VLAN



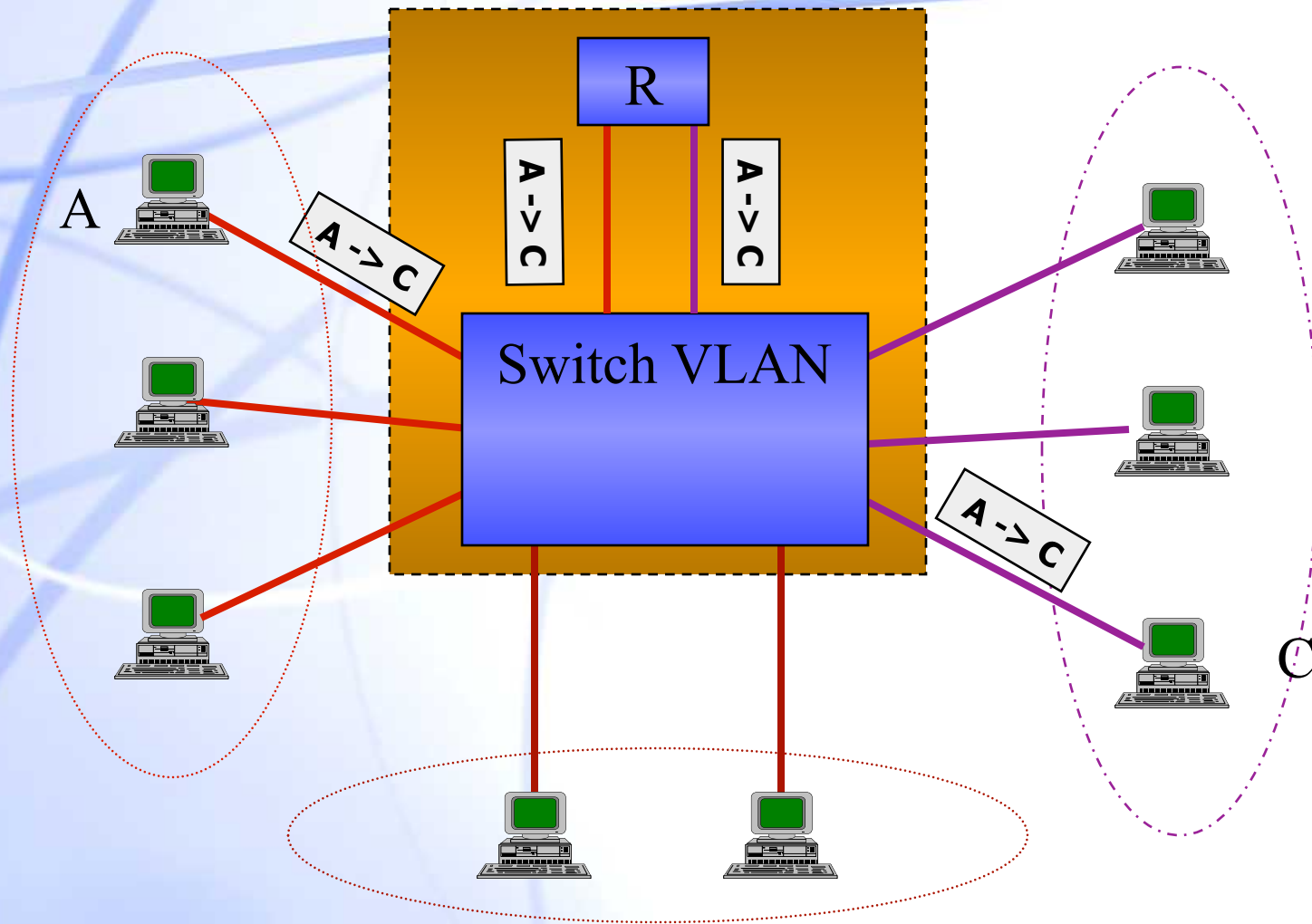
Funcionamiento. Difusión



Funcionamiento. Unicast Interno



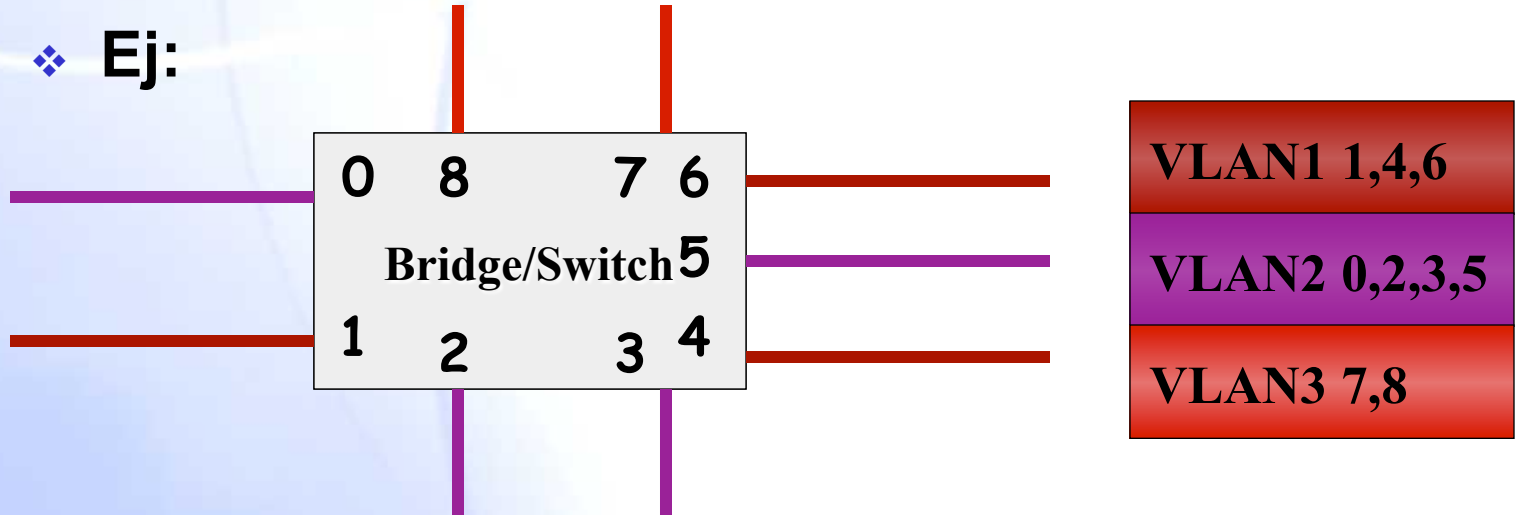
Funcionamiento. Traf.entre VLAN



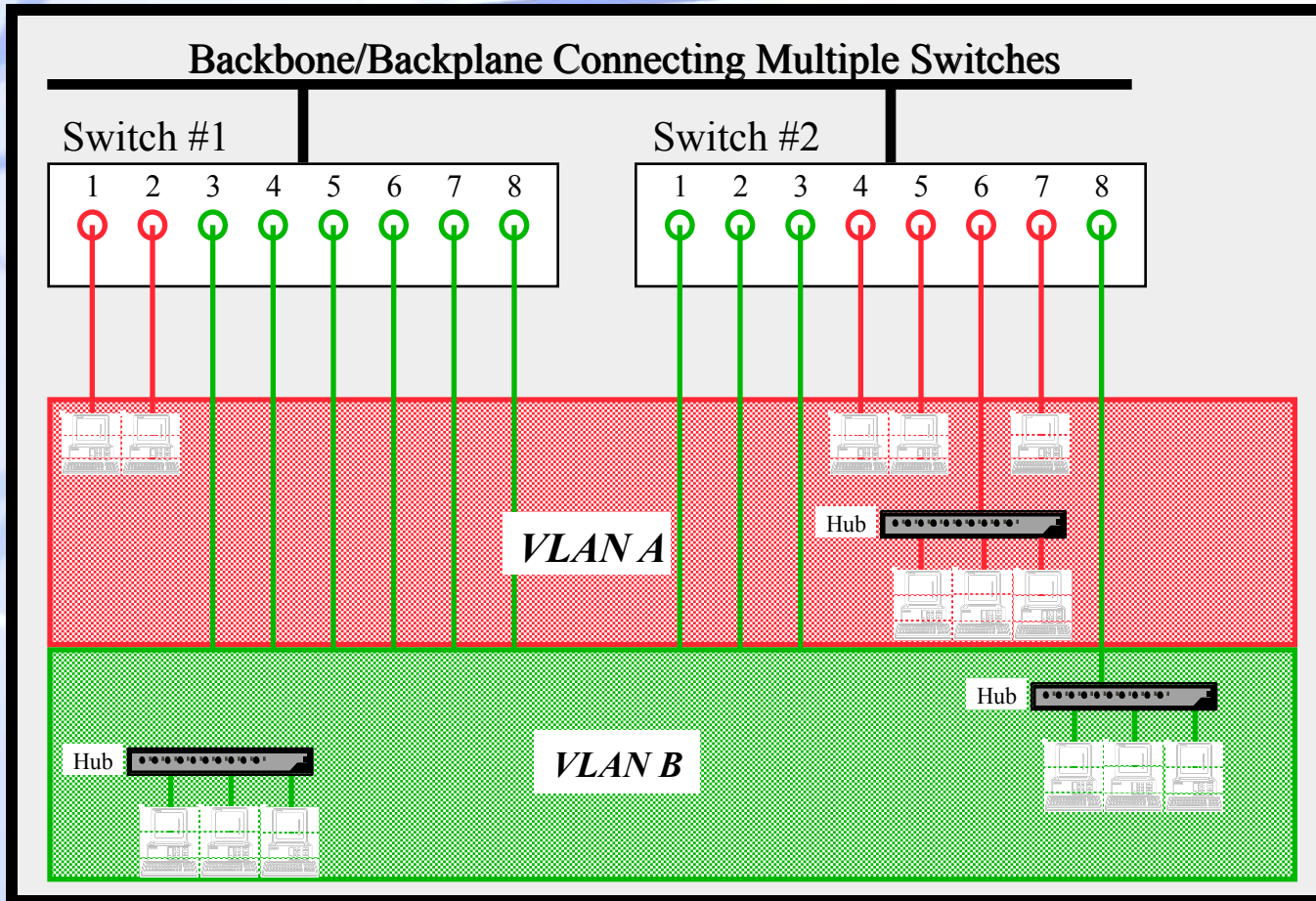
Tipos de VLANs

◆ VLAN de nivel 1: Por puerto

- ❖ Los miembros de la VLAN se especifican en base al puerto en el cual se encuentran conectados a los dispositivos de interconexión.
- ❖ Requiere reconfigurar las VLANs si el usuario se mueve físicamente.
- ❖ Ej:



VLAN por puerto

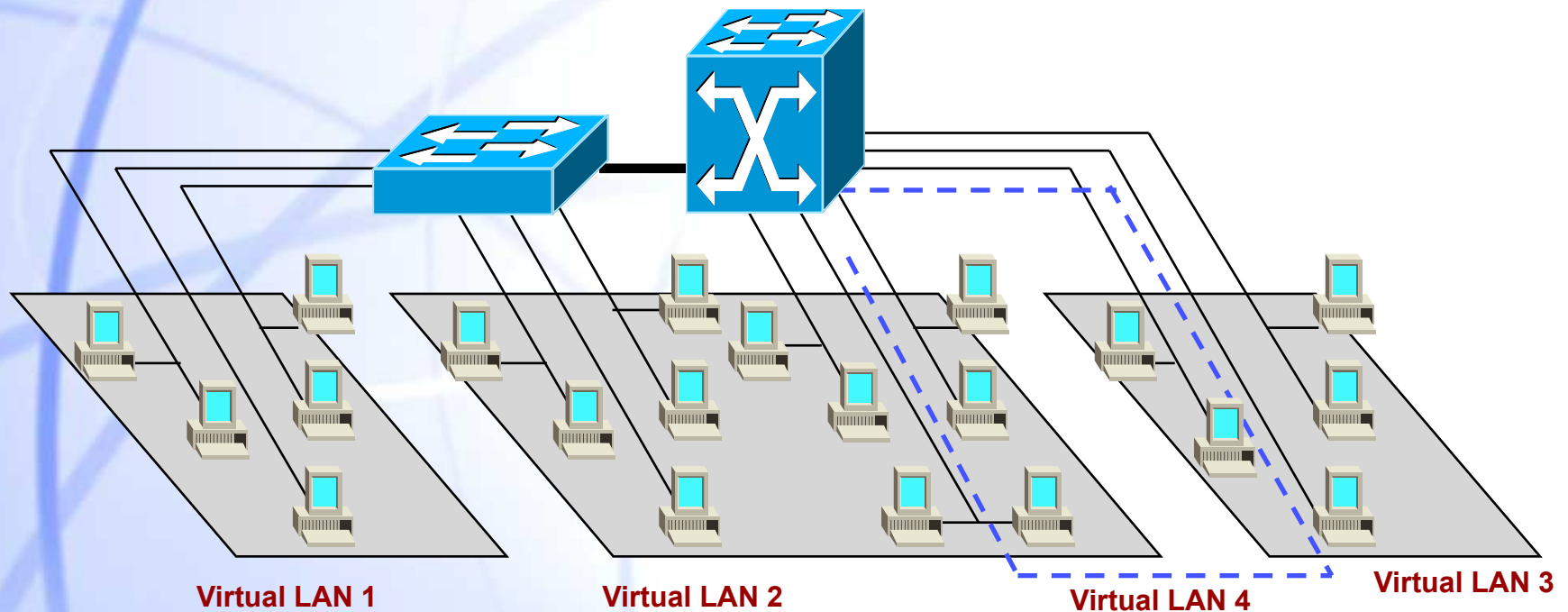


Tipos de VLANs

- ◆ **VLAN de nivel 2: Por dirección MAC**
 - ❖ **Los miembros de una VLAN dependen de la dirección MAC de las estaciones**
 - ❖ **No requiere reconfiguración si las estaciones se mueven físicamente a puertos distintos**
 - ❖ **Los miembros de la VLAN deben asignarse inicialmente. Problemas si existen decenas o cientos de usuarios**
 - ❖ **Problemas para identificar a terminales que poseen varias direcciones MAC**

VLAN1	11:22:33:44:55:66
VLAN2	22:33:44:55:66:77
VLAN3	33:44:55::66:77:88
VLAN1	00:22:33:44:55:66
VLAN3	33:44:55::66:77:99
VLAN3	00:11:55::66:77:88

VLAN por dirección MAC



Tipos de VLANs

◆ VLANs nivel 2: Por tipo de protocolo

- ❖ Basado en el campo tipo de protocolo del nivel 2

VLAN1	IP
VLAN2	IPX

◆ VLANs nivel 3: Direcciones de Subred

- ❖ Basado en la cabecera de nivel 3

VLAN1	138.4.3
VLAN2	163.117.139

- ❖ No tiene nada que ver con routing la cabecera de nivel 3 se utiliza para mapear la VLAN a la que pertenece.
- ❖ Requiere más retardo debido a procesamiento.

◆ VLANs nivel n

- ❖ Basados en otros niveles. Ej: VLAN para ftp,....

IEEE 802.1q

- ◆ **Estándar internacional**
- ◆ **Define VLANs de nivel 1 y 2 y niveles superiores**
- ◆ **Compatible con bridges y switches sin capacidad de VLAN.**
- ◆ **Soporte de medio compartido y LANs conmutadas**
- ◆ **Soporte de configuración estática y dinámica**
- ◆ **Otros:**
 - ❖ **CISCO ISL: Inter Link Switch**
 - ❖ **3COM Virtual LAN Trunking**

Tipos de enlaces

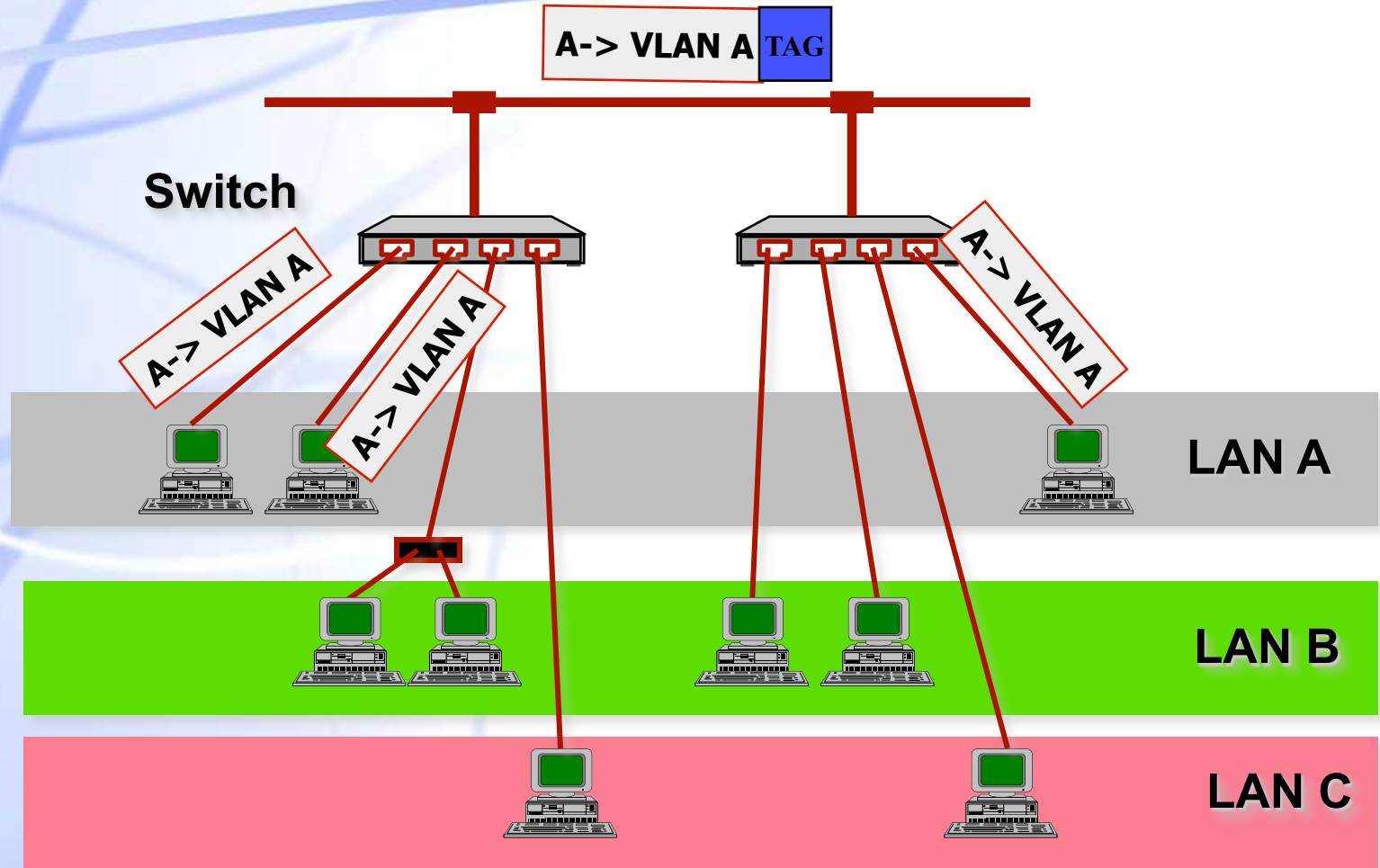
◆ Enlaces de acceso (usuarios)

- ❖ Los switches aprenden o tienen configurados por gestión a que VLAN pertenece dicho enlace

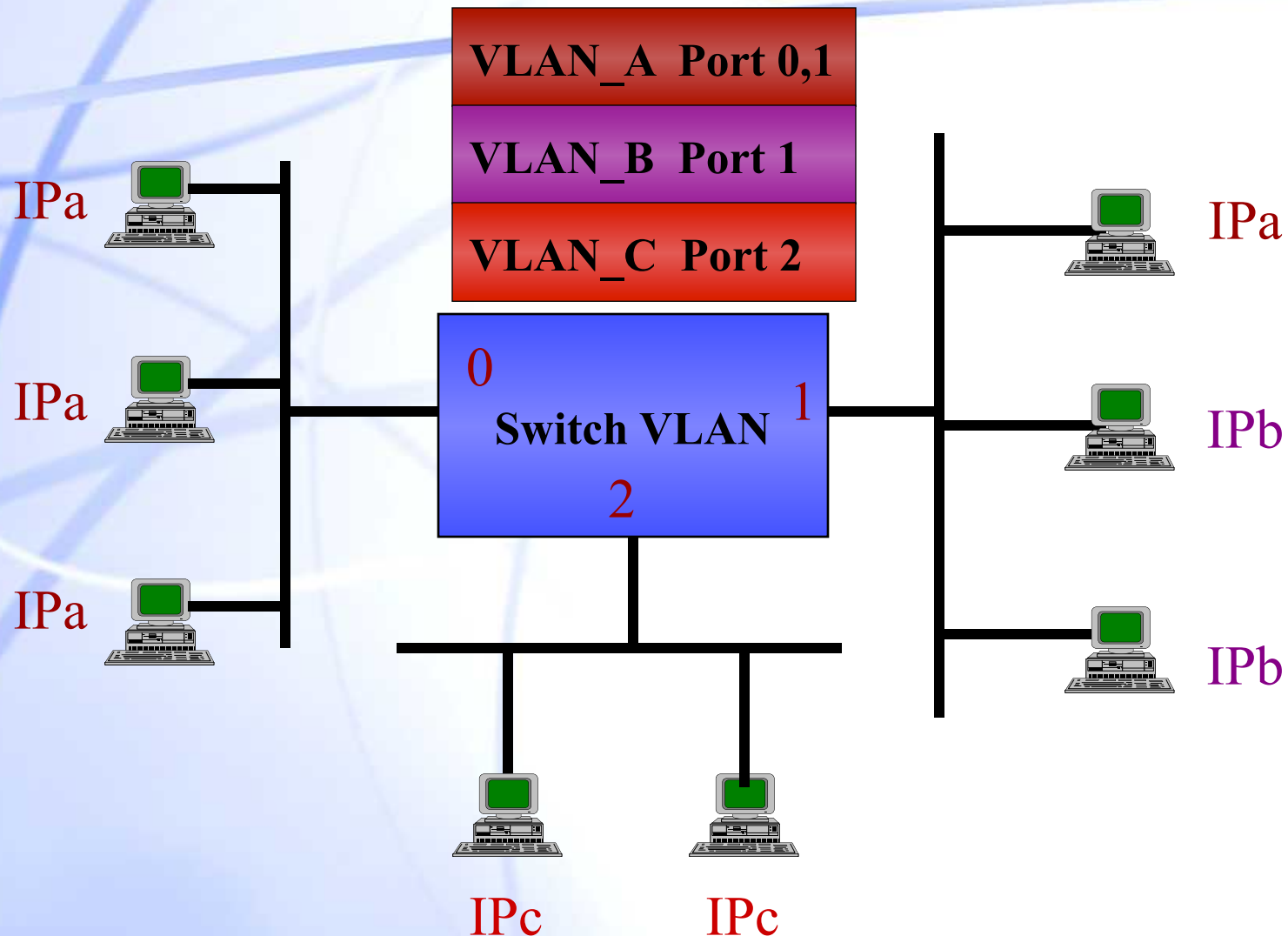
◆ Enlace de interconexión (interswitches)

- ❖ Utilizan un mecanismo de marcado para intercambiar tráfico de VLANs
- ❖ Los switches deben saber que enlaces soportan marcado y cuales no.

Escenario



Aprendizaje basado en Red IP



STP y VLANs

- ◆ **En teoría son tecnologías independientes**
 - ❖ STP devuelve una topología sin bucles
 - ❖ Las VLAN se configuran sobre esta topología
- ◆ **En la practica, casi todos los fabricantes ofrecen mecanismos para “Per VLAN Spanning Tree”**
 - ❖ Se calcula un árbol en cada VLAN
 - ❖ Es posible volver a un “Common Spanning Tree”
 - ❖ Cisco PVST, 802.11s (Multiple Instance Spanning Tree)

Per VLAN spanning tree (PVST)

- ◆ **Multiples Spanning Tree en una misma red fisica**
 - ❖ **Topologías más eficientes**
- ◆ **Configuración de los parámetros de STP en cada VLAN**
 - ❖ **La prioridad por lo menos**
 - ❖ **Aumenta la carga del procesador (gestión de N instancias de STP)**

Conclusiones

- ◆ **VLAN es una tecnología muy utilizada hoy en día**
 - ❖ Muchos casos de uso importantes
- ◆ **Aislamiento de red difícil de conseguir**
 - ❖ VLANs comparten enlaces
 - ❖ Problemas de *broadcast storm* o configuraciones erróneas se repercuten
- ◆ **Posibles alternativas**
 - ❖ L3: routers
 - ❖ L7: firewalls