

VLANs

Virtual Local Area Networks



VLANs

VLAN (IEEE 802.1Q): mecanismo que permite a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas, a través de la creación de redes virtuales de nivel 2 por software.

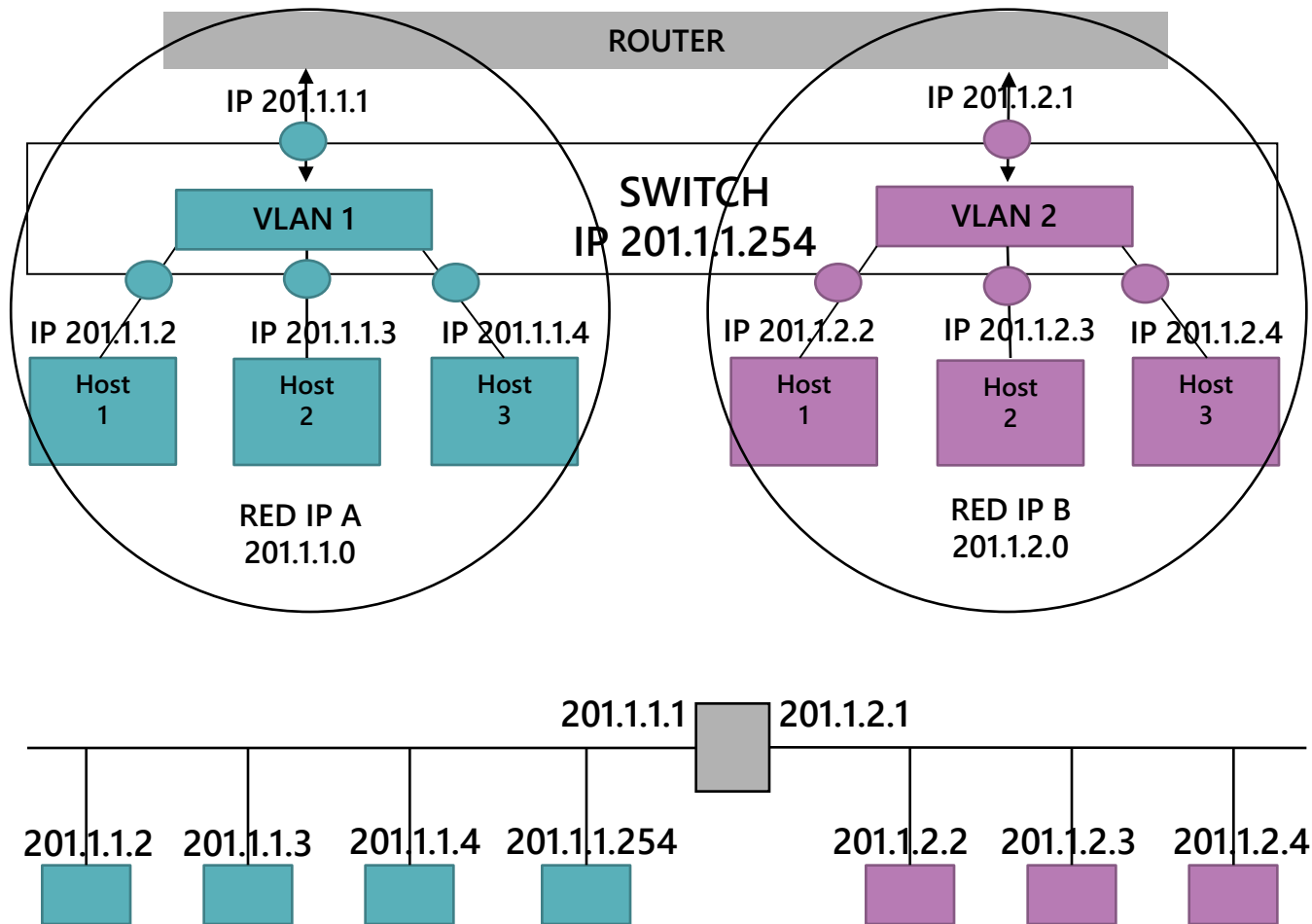
Requisitos

- Switches especiales con capacidad VLAN.
- Compatibilidad con bridges sin capacidad VLAN.
- Altas y bajas de equipos en las VLANs.

Ventajas

- Facilitan la administración de grupos lógicos de PCs que deban comunicarse entre sí.
- Permiten el movimiento físico de equipos.
- Permite a los equipos cambiarse de VLAN.
- Reducción del dominio broadcast.
- El dominio broadcast virtual puede extenderse a diferentes redes físicas (trunking).

VLANs vs LANs

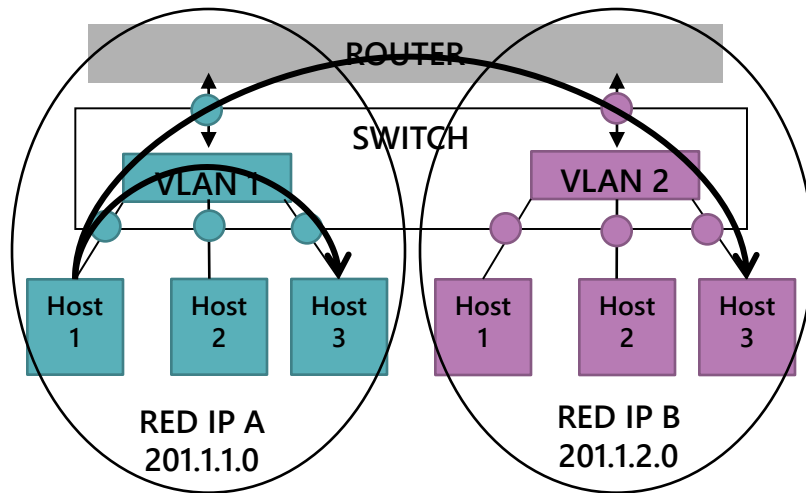


Comunicación entre VLANs

Switches de nivel 2

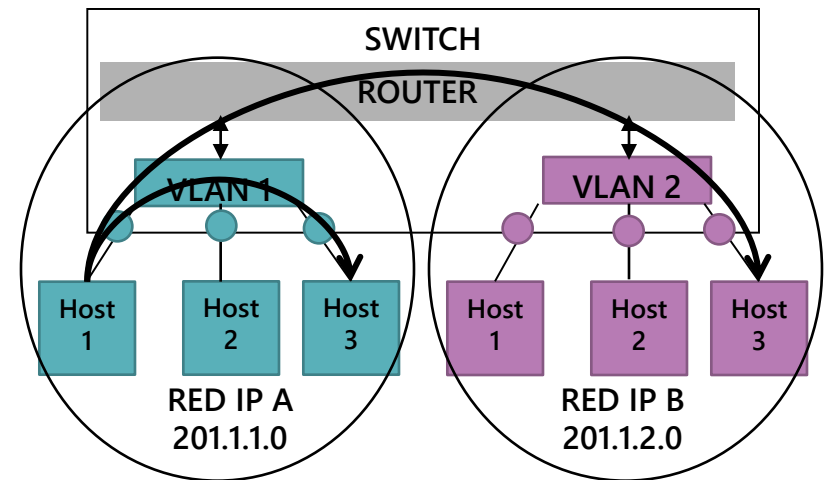
Router externo:

- Con interfaces físicas a cada VLAN.
- Con una única interfaz física soportando trunking.



Switches nivel 2 y 3

Router "interno" al switch, interfaces lógicas a cada VLAN.



Conformación de grupos (membership)

Asignación por ports

- Estática
- Eficiente
- No flexible

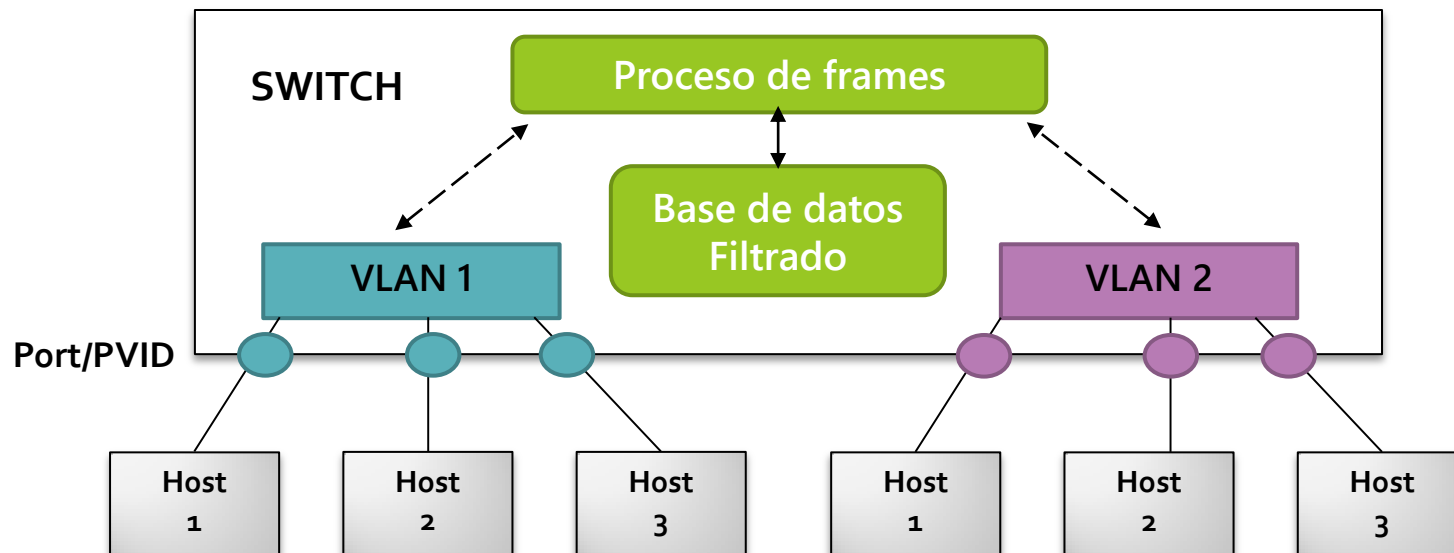
Asignación por dirección MAC

- Flexible
- Dinámica
- Problemas de seguridad (clonado de MACs)

Asignación por información del nivel 3 (Protocolo, red IP, etc)

- Flexible
- Baja performance
- Un equipo puede moverse sin reconfigurar su IP

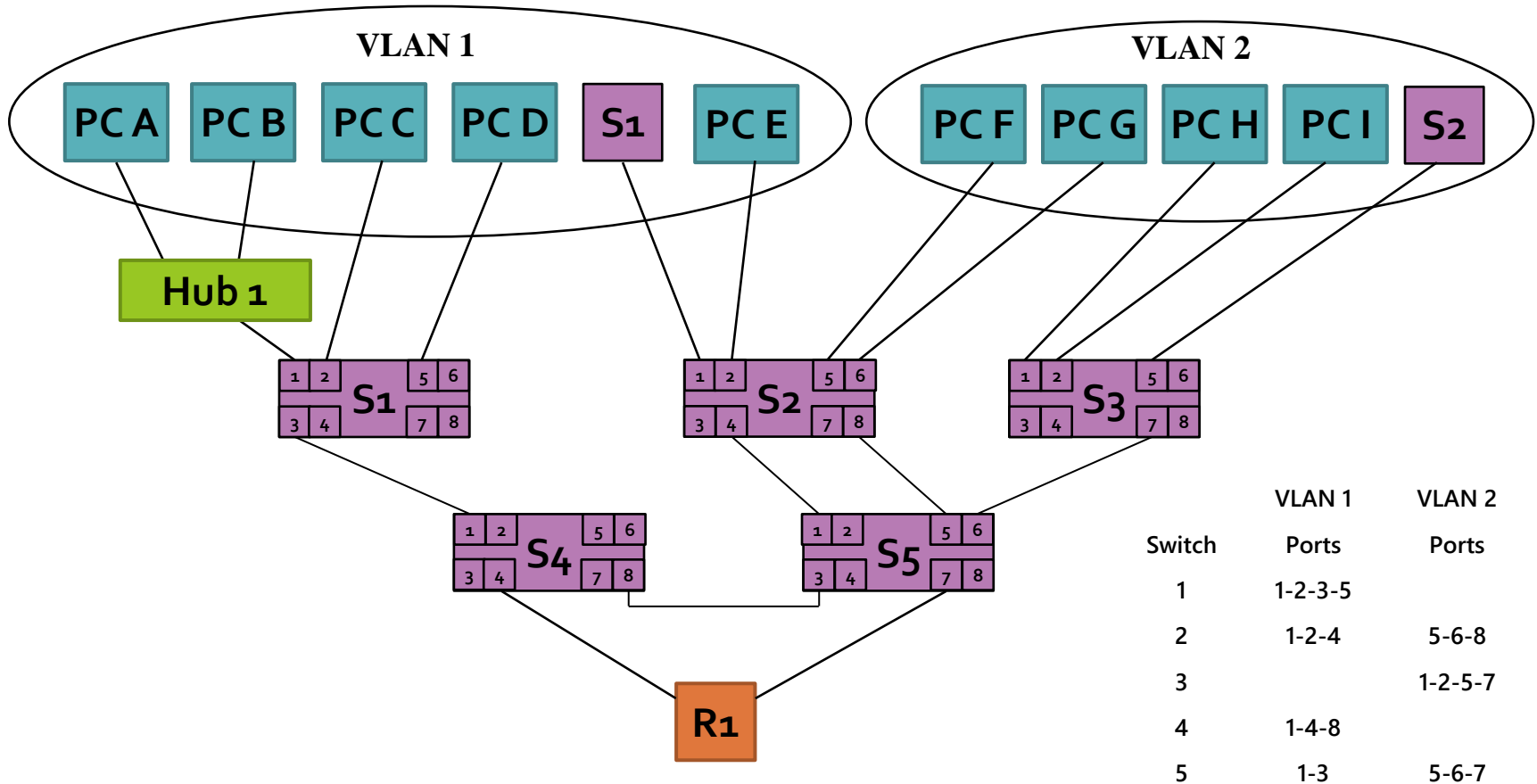
Conformación de grupos (port)



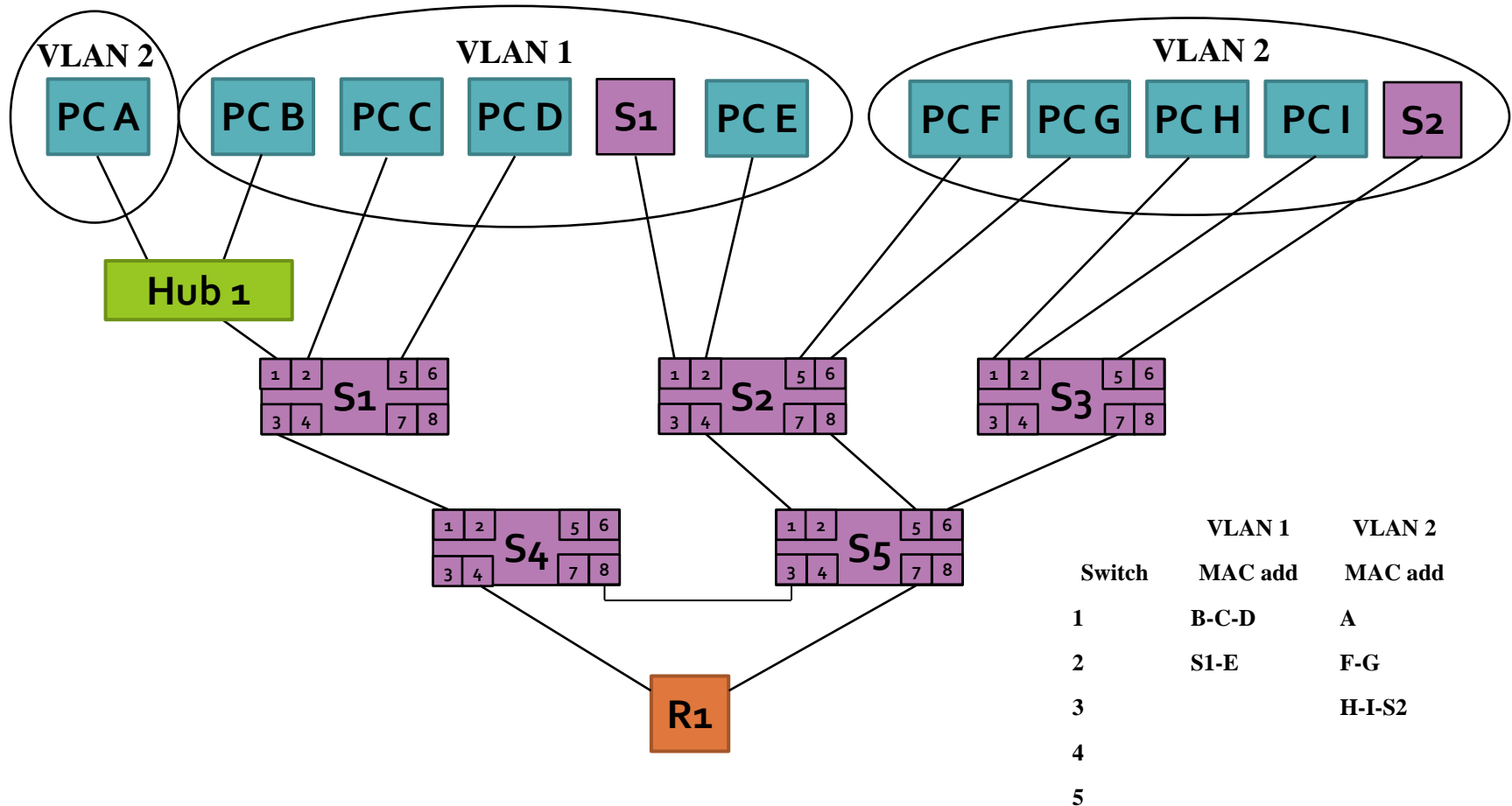
VLANS definidas en función de los ports del switch:

- Base de datos de filtrado: información configurable para definir las VLANs.
- Proceso de frames MAC: reglas que indican cómo se procesará cada frame MAC.
- PVID: identificador de VLAN nativa para cada port.

Conformación de grupos (port)

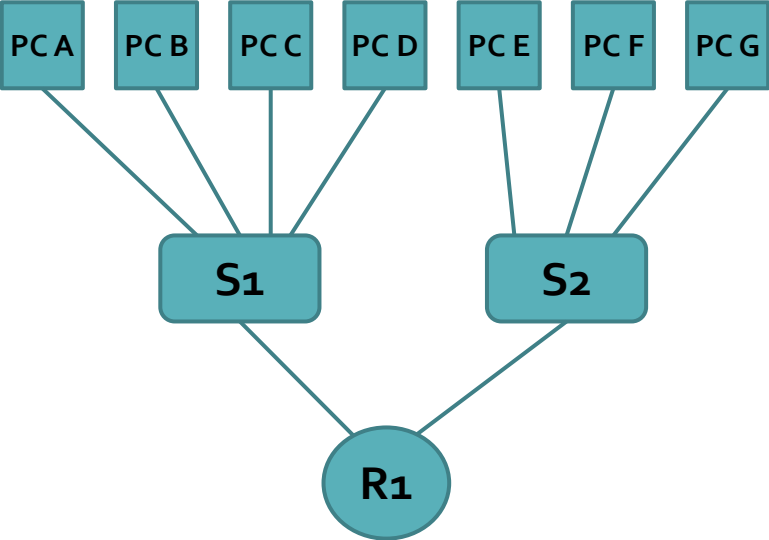


Conformación de grupos (mac addr)

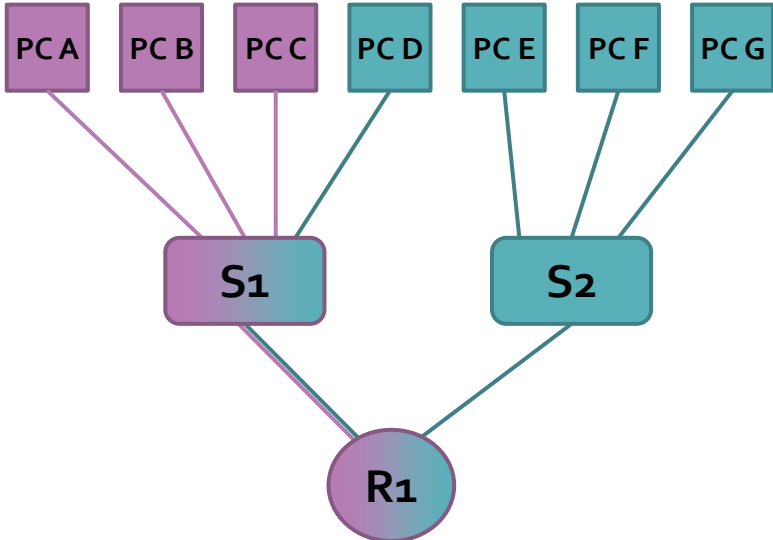


Dominio Broadcast

Sin VLAN



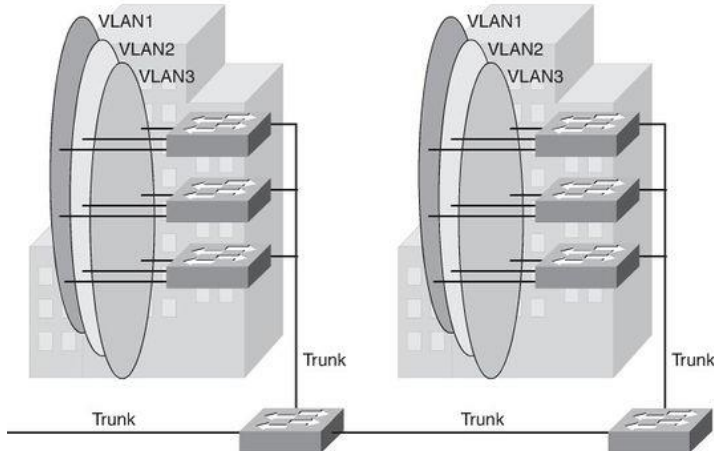
Con VLAN



Alcance de una VLAN

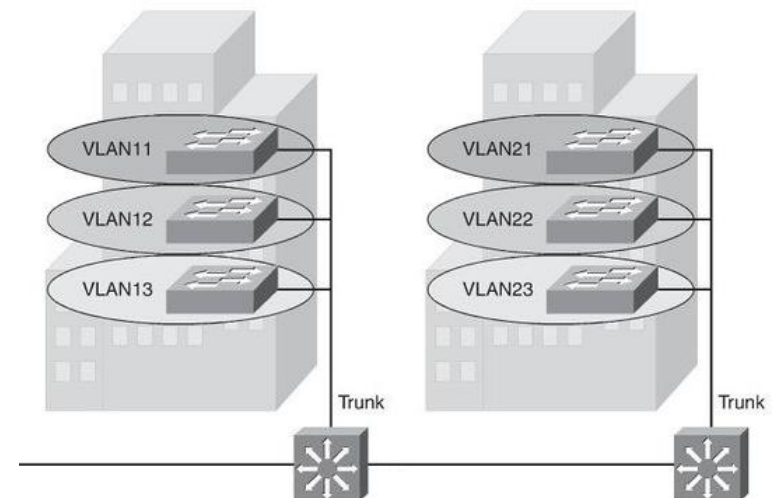
End to end VLAN

- Los equipos de la VLAN pueden estar distribuidos en la intranet
- Provee flexibilidad
- Riesgo de cargar el nivel core
- Requiere trunking



Local VLAN

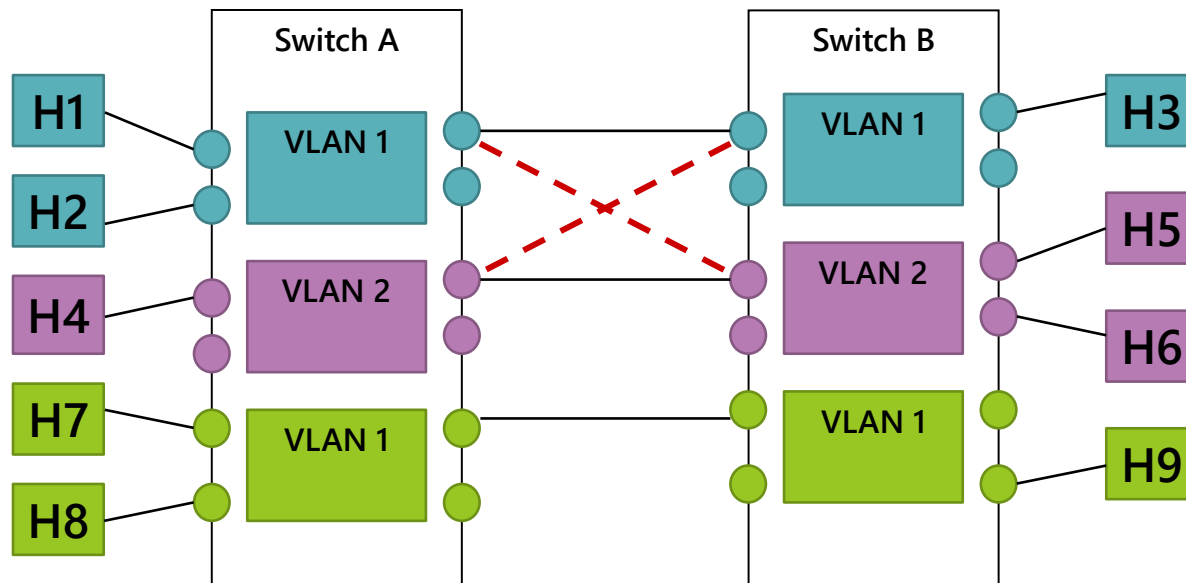
- Los equipos se encuentran físicamente cercanos entre sí
- Mejora eficiencia (separa dominios broadcast)
- Mejora seguridad
- Permite ubicación estratégica de servidores



Múltiples switches: Conexión física

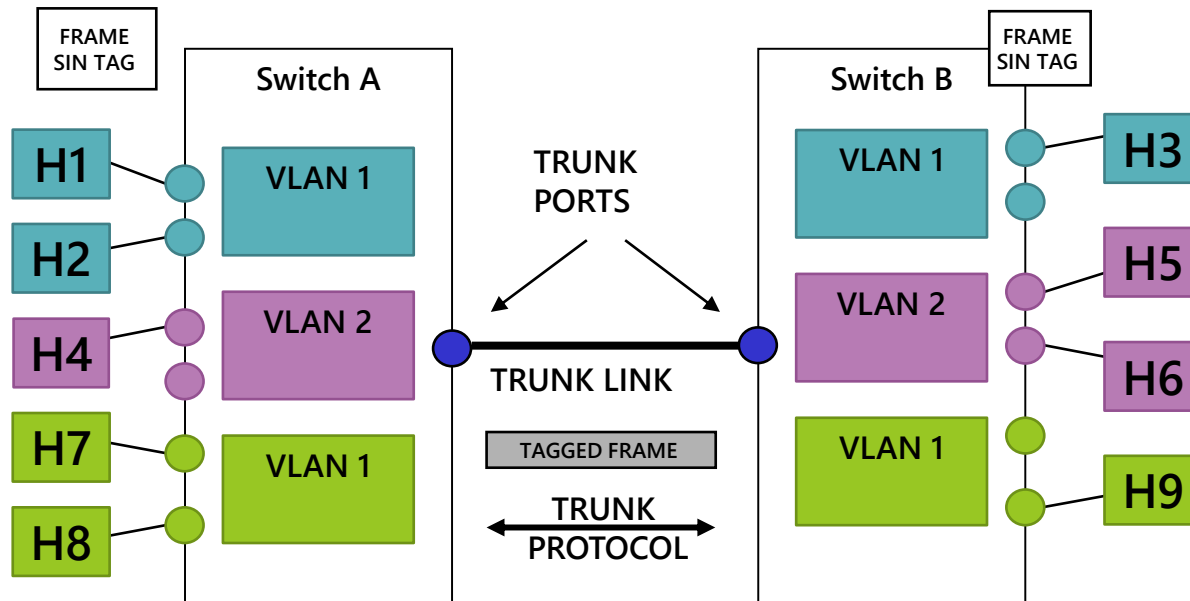
Conexión física de ports asignados a cada VLAN

- Complicado de administrar
- Propenso a errores
- Ports dedicados por VLAN
- Técnicamente posible, pero no recomendado

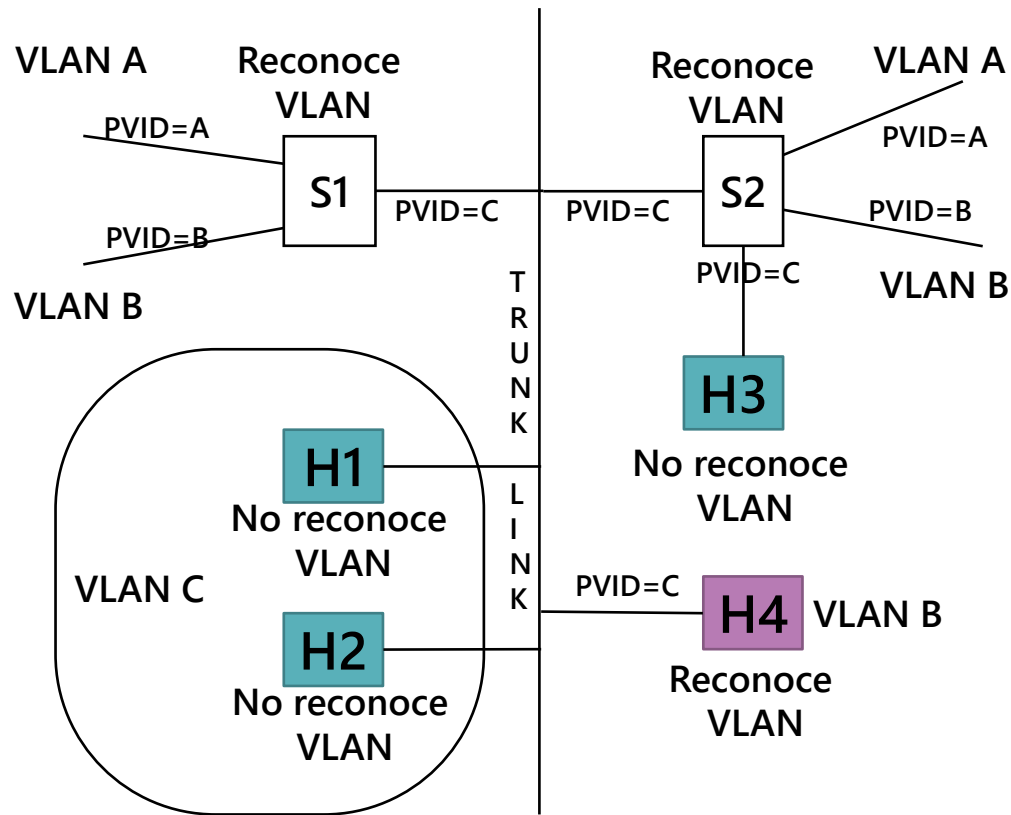


Múltiples switches: Trunking

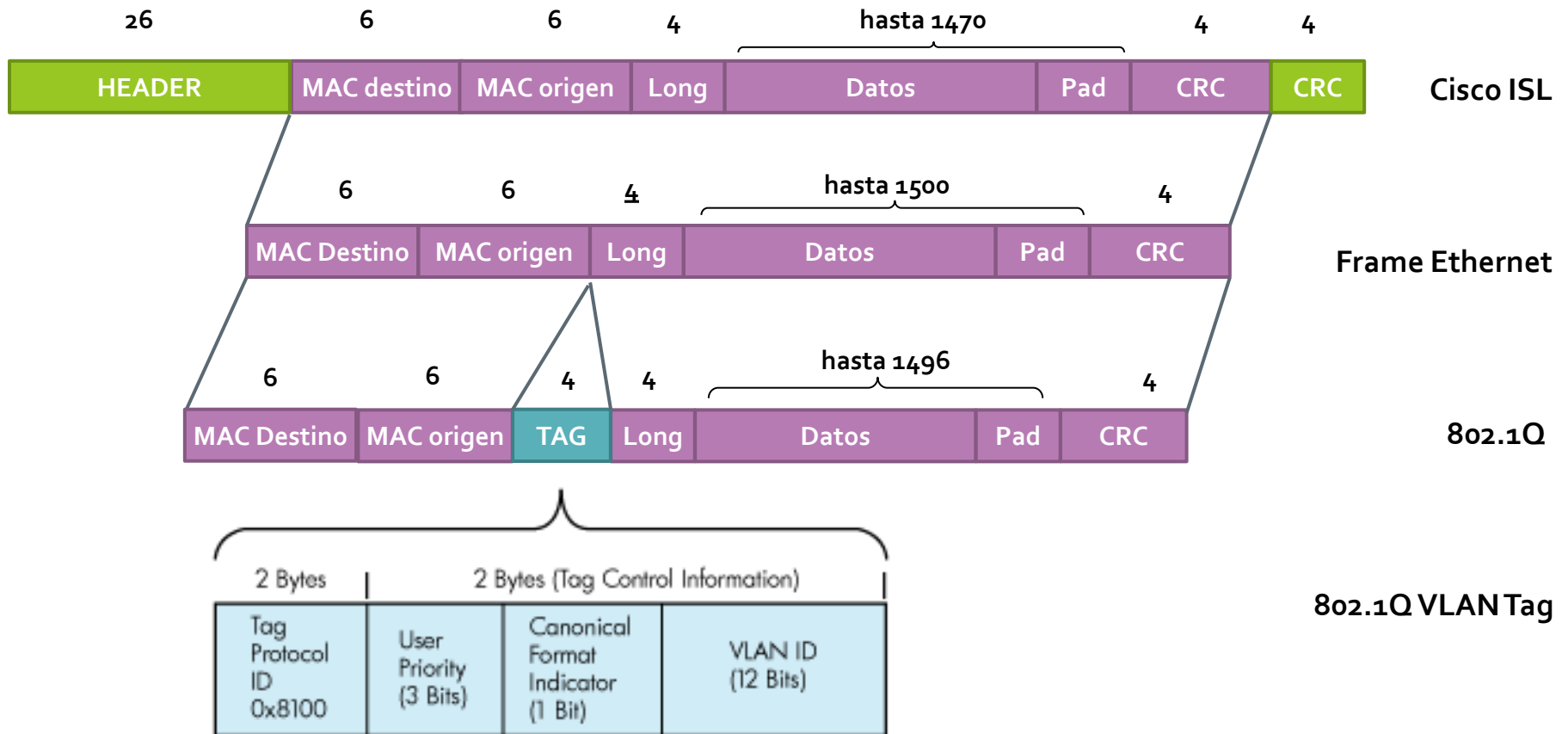
- Access link: Vínculo switch/equipo final, frames sin tag.
- Trunk port: puerto configurado para trunking, de alta velocidad (100Mb, 1GB).
- Trunk link: Vínculo entre switches (entre dos trunk ports), frames con tag, de varias VLANs.
- Tag: indica la VLAN del frame (IEEE 802.1Q, Cisco ISL –Inter switch Link-)
- Trunk protocol: Protocolo para configuración y administración de VLANs (Cisco VTP -VLAN trunk protocol)
- PVID: Port VLAN ID (VLAN activa)



Múltiples switches: Trunking



Tagging



VTP (VLAN Trunking Protocol)

Facilita la administración de las VLANs:

- Configuración desde un único lugar
- Actualizaciones automáticas en los switches
- Reduce el tráfico broadcast en los trunk links
- Modos server, cliente, y transparente

Spanning trees

Alternativas

- Un spanning tree para todas las VLANs: poco flexible, no permite balanceo de carga.
- Múltiples Spanning trees:
 - Uno por VLAN: carga en switches y links, dependiente del número de VLANs.
 - Uno por grupo de VLANs: disminuye la carga y mantiene las propiedades de uno por VLAN.

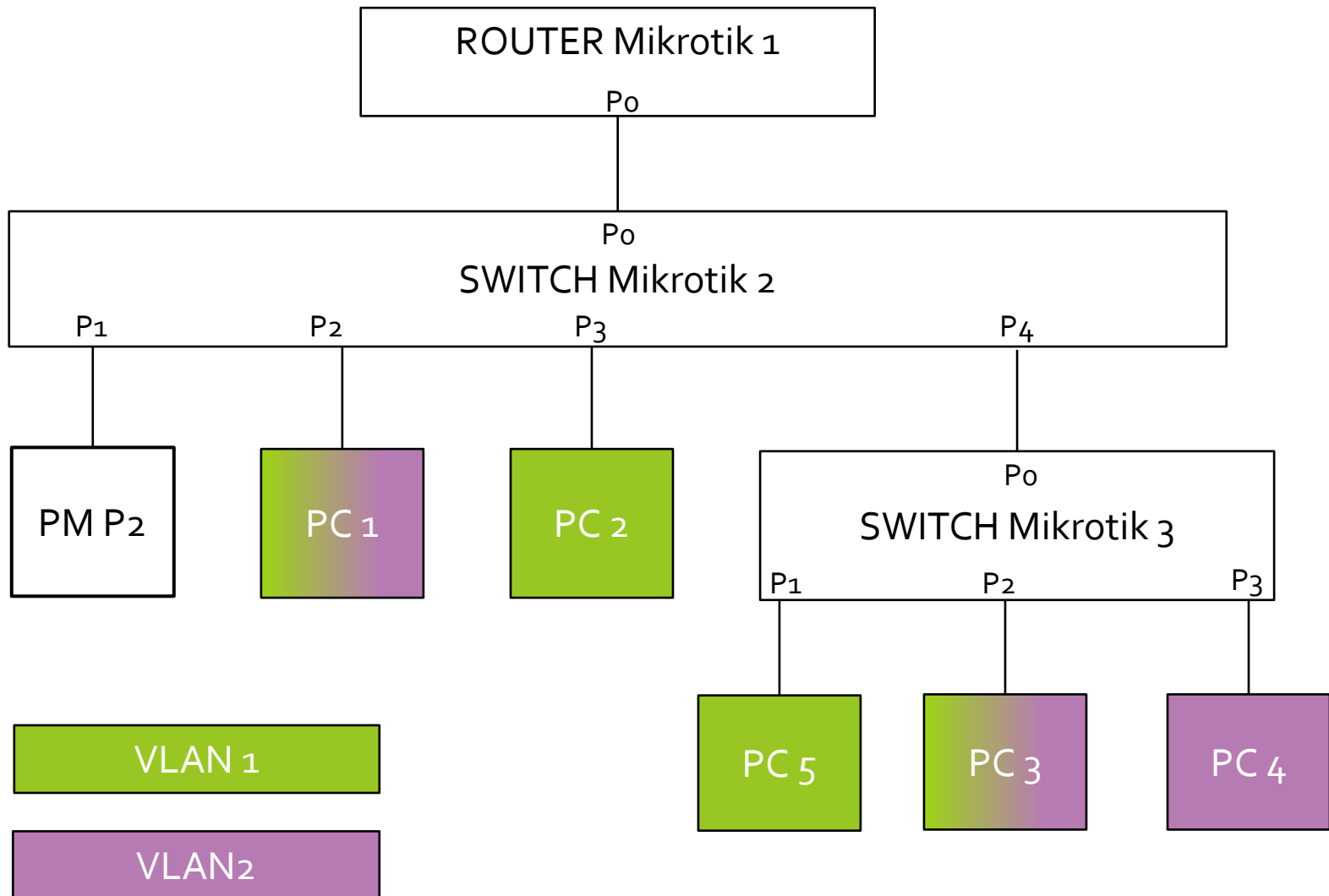
Protocolos spanning tree utilizados

- IEEE
 - STP (Spanning Tree Protocol) IEEE 802.
 - RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w
 - MSTP (Multiple Spanning Tree Protocol)
- Cisco
 - PVST (Per VLAN Spanning Tree protocol)
 - PVST+ (Per VLAN Spanning Tree protocol +)
 - MISTP (Multiple Instance Spanning Tree Protocol)

VLANs

Práctica especial

Ejercicio



Configuración de las VLANs

- Configurar IPs en equipos.
- Crear VLANs en todos los switches.
- Configurar las interfaces de los switches de acuerdo al esquema.
- Analizar los paquetes de los diferentes tipos de links (trunk y access) cuando se comunican equipos conectados a diferentes switches.