UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat d'Informàtica de Barcelona

FIB

Xarxes de Computadors

Lab 5
Laboratorio de Switches Ethernet (IOS)

José Suárez-Varela

jsuarezv@ac.upc.edu

Conceptos básicos

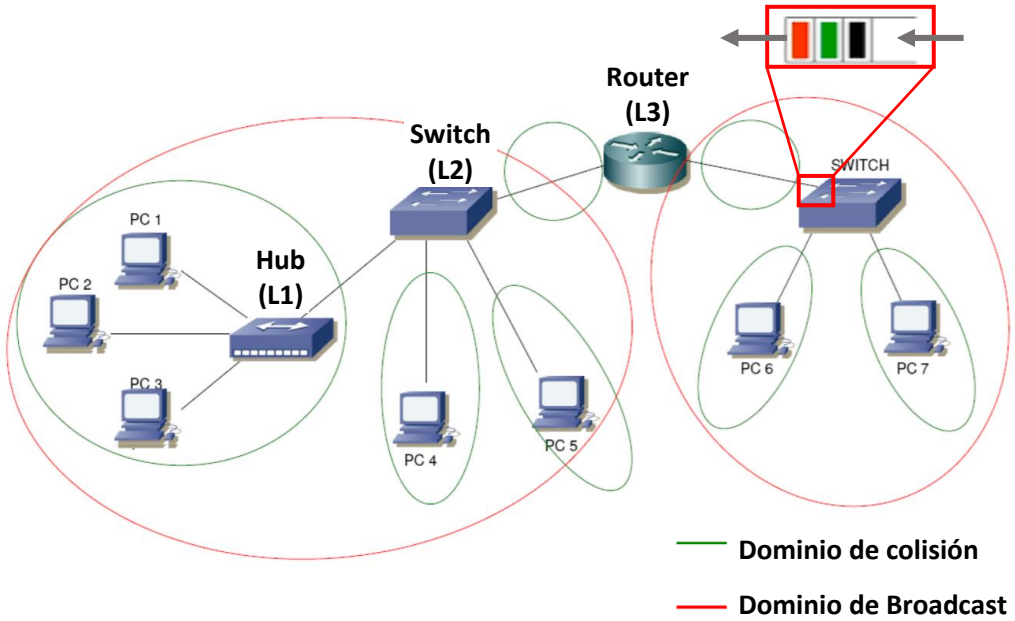
Switch:

- **Capa 2 o de enlace → Local Area Networks (LAN)**
- **Funcionalidades: VLANs y puertos seguros**

Cisco Catalyst 2950 – 24 puertos

Características:

- **Direccionamiento a través de direcciones físicas MAC (únicas)**
- **Cada puerto es un dominio de colisión →** Los equipos en un mismo dominio de colisión comparten ancho de banda (comparten el acceso al medio)



Conceptos básicos

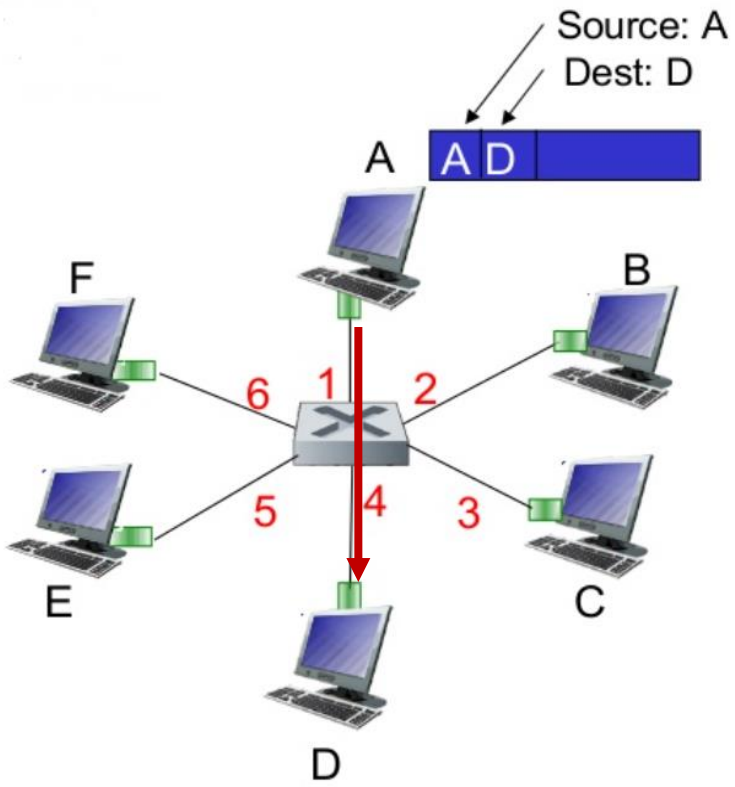
Formato tabla MAC:

VLAN ID	MAC address	Port	Age

Age → Entradas dinámicas (pueden conectarse/desconectarse equipos dinámicamente en la LAN). Por defecto 5 minutos en switches Cisco

Automatic Backward learning:

- Cuando se recibe una trama, se añade una entrada con la MAC de origen y el puerto asociado por el que se recibió la trama
- Si no hay entrada para acceder a la MAC destino se hace *flooding* (se transmite la trama por todos los puertos excepto por el que se recibió)




```
Switch#sh mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0090.21e0.5586    DYNAMIC     Fa0/1
```

MAC address PC_A

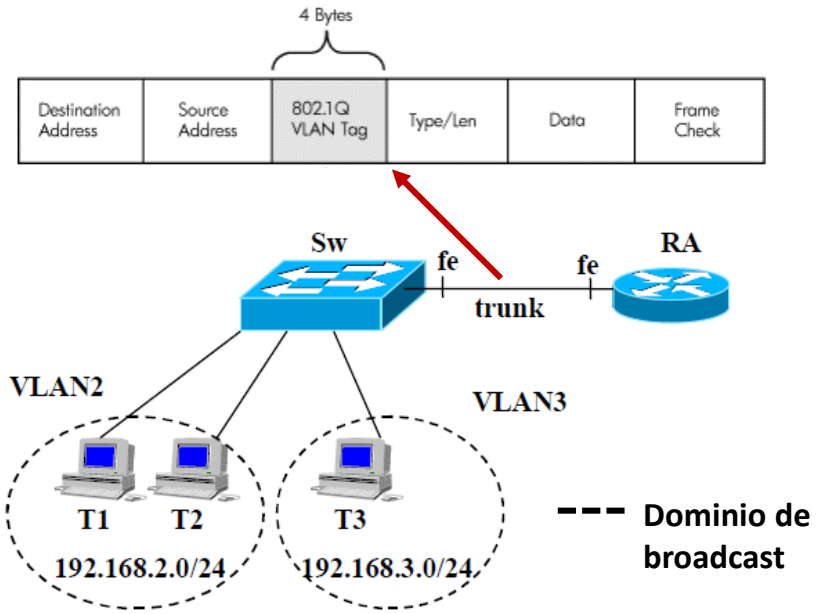
Conceptos básicos

VLANs:

- Una VLAN es equivalente a una Red IP (Capa 3) → Define un dominio de Broadcast
- Cada VLAN agrupa diferentes puertos conectados a un switch
- Permite ahorrar puertos de router → Con un puerto de router conectado al switch se pueden crear tantas VLANs como se desee

Conexión entre hosts de diferentes VLANs a través de router

- ***Trunking*** → Un único puerto *trunk* interconecta todas las VLANs
- *La interfaz trunk* del router debe tener una IP diferente para cada VLAN
  (varias subinterfaces lógicas asociadas a la interfaz física)
- **Sólo en el enlace *trunk* se etiqueta la VLAN en las tramas (IEEE 802.1Q)**
- ***Flooding*** → Sobre los equipos de una misma VLAN y en el enlace trunk



Conceptos básicos

Puertos seguros:

- Asociar una o varias MACs a un puerto físico del switch:

  E.g.: Por seguridad sólo queremos que en un puerto del switch se pueda conectar un host concreto (identificado por la MAC)

- **Posibles acciones** si se conecta un host con distinta dirección MAC:
  - **Protect** → Se descartan las tramas recibidas
  - **Restrict** → Se descartan las tramas y se envía un trap (alarma) al gestor de red (protocolo SNMP)
  - **Shutdown** → Se deshabilita administrativamente el puerto

Comandos básicos

Definir una VLAN:

Sw# *configure terminal*

Sw(config)# *vlan <VLAN_id>* → VLAN 1, 1002, 1003, 1004 y 1005 están definidas por defecto (no utilizar)

Sw(config-vlan)# *name <vlan_name>* → Nombre para identificar más fácilmente la VLAN (e.g., profesores, estudiantes)

Sw(config-vlan)# *exit*

Asignar interfaces a una VLAN:

Sw(config)# *interface <if_name>*

Sw(config-if)# *switchport mode access*

Sw(config-if)# *switchport access vlan <VLAN_id>* → Asigna el puerto a la VLAN

Definir enlace *trunk* (entre switch y router):

Sw(config)# *interface <if_name>*

Sw(config-if)# *switchport mode trunk*

Comandos básicos

Configuración enlace trunk en el router:

R(config)# int fastethernet 0/0

R(config-if)# no ip address

R(config-if)# no shutdown

R(config-if)# int FastEthernet 0/0.1

R(config-subif)# encapsulation dot1q <VLAN-id>

R(config-subif)# ip address <IP> <mask>

} Generar una subinterfaz lógica (FastEthernet 0/0.X) para cada VLAN. Cada una debe tener un prefijo IP (+ máscara) diferente

Configuración puerto seguro en una interfaz del switch:

Sw# *interface <if_name>*

Sw(config-if)# *switchport port-security* → Activar puertos seguros

Sw(config-if)# *switchport mode access* → Configurar puerto en modo "access"

Sw(config-if)# *switchport port-security maximum <max_addrs>* → Definir número máximo de MACs diferentes permitidas

ó

Sw(config-if)# *switchport port-security mac-address <MAC>* → Asociar dirección MAC al Puerto

Sw(config-if)# *switchport port-security violation {protect | restrict | shutdown }* → Acción a realizar cuando se viola el filtro MAC

Comandos básicos

Comandos de consulta de estado y debugging:

Genéricos:

Sw# sh ip interface brief → Aunque las interfaces del switch (capa 2) no tienen IP asignadas, es útil para ver un listado de todas las interfaces

MAC table:

Sw# *show mac-address-table* → Muestra las entradas de la tabla MAC

Sw# *clear mac address-table dynamic* → Borrar entradas dinámicas tabla MAC

VLANs:

Sw# *show vlan* → Muestra las VLANs configuradas en el switch (el switch incluye ya algunas por defecto)

Sw# *show vlan id <VLAN_id>* → Muestra los puertos asociados a una VLAN específica

Sw# *show interfaces switchport* → Comprobar configuración de VLANs y configuración puertos (access, trunk…)

Sw (config)# *no vlan <vlan_id>* → *Borrar VLAN*

Puertos seguros:

Sw# show port-security [interface <if_name> | <address>]

Realización práctica

Pasos a seguir

1) Montar esquema de red (router 1841; Switches 2950-24)

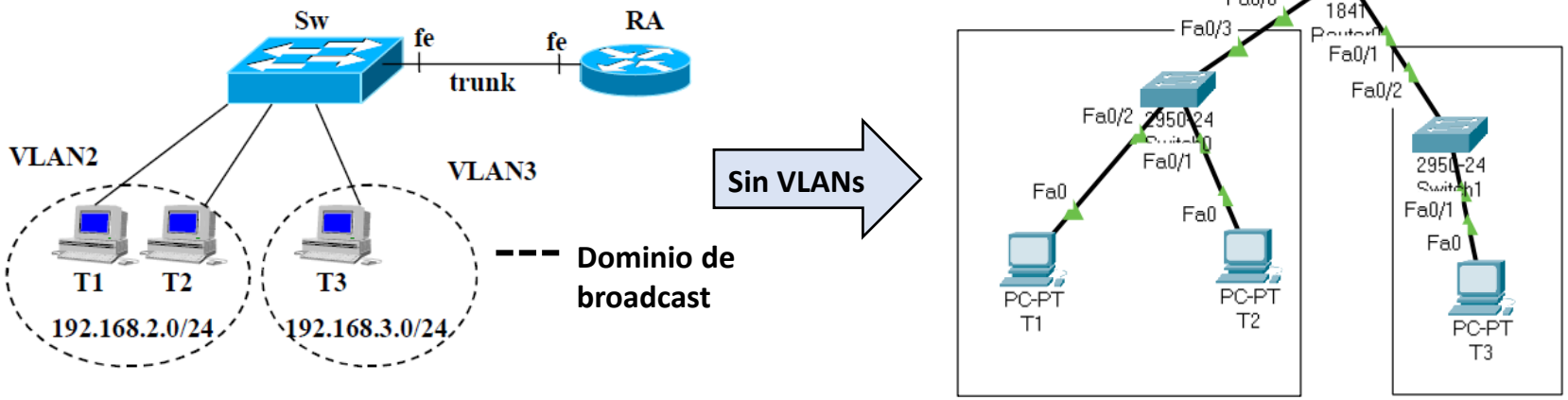
2) Configurar IPs y gateway en PCs (menu "config")

3) Configuración switches y routers (VLANs, puertos seguros)

Nota: Ficheros Packet Tracer con práctica resuelta en el Racó FIB (Sec. 5.1 - VLANs y trunking; Sec. 5.2 – Puertos seguros)

Realización práctica

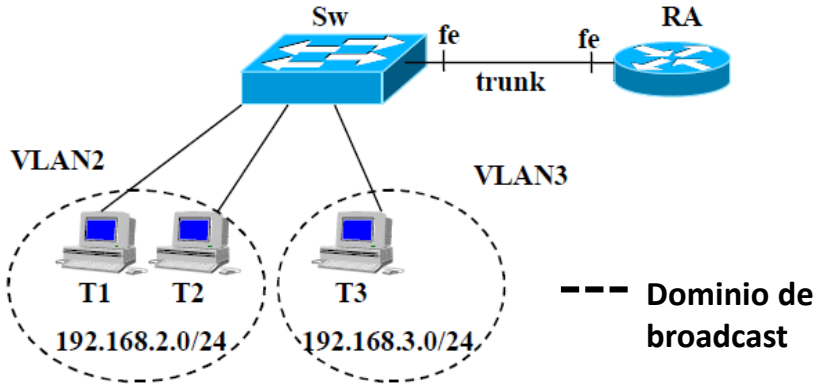
Parte 1: VLANs y trunking



- **Switch** → Configurar VLANs 2 y 3 y puerto *trunk*
- **Router** → Configurar dos subinterfaces lógicas para las dos VLANs (cada una con IP + máscara correspondiente a su red)
- **PCs** → Configurar el gateway a la IP de la subinterfaz correspondiente del router
- No usar *tcpdump* en la práctica (los mensajes broadcast/flooding se envían a los PCs de la VLAN y al enlace trunk)
- Utilizar *tracert (Windows)* en lugar de *traceroute* → *# tracert <ip_dest>*

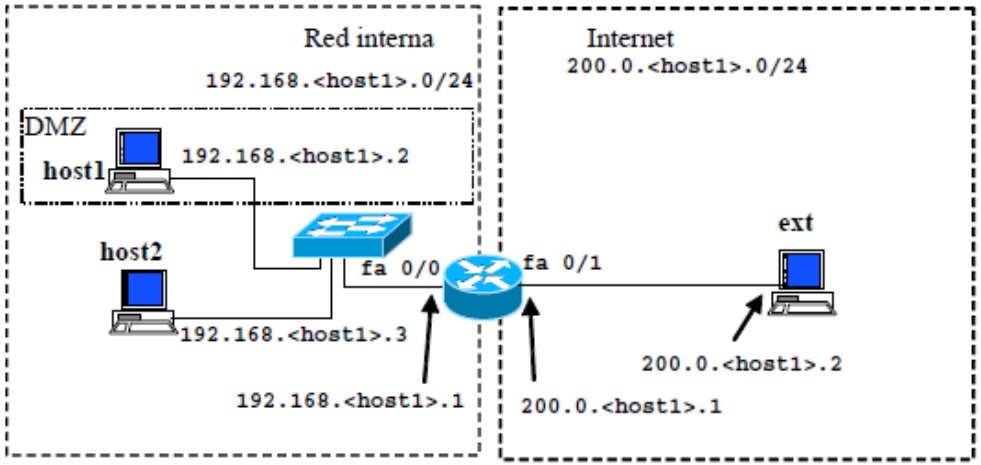
Realización práctica

Parte 2: Puertos seguros



- Configurar puerto con la MAC de un equipo (e.g., T1)
- ***MAC PC:*** *Menú config → interface → FastEthernet0*
- Eliminar enlace y conectar enlace con otro equipo → Usar cable "copper straight-through" para seleccionar interfaz en la que se conecta
- Comprobar conectividad → ***#ping <IP>***
- Acción *shutdown* (luego hay que reestablecer el puerto → #shutdown ; #no shutdown)
- **Configuración** → #show port-security interface <if_name>

Repaso práctica 4



- **NAT** → Estático, dinámico (1:1) y PAT (1:M)

  Direcciones IP: Inside/outside; local/global

  Dinámico y PAT → R(config)# ip nat inside source list < acl #> [pool <name> | interface <int>] [overload]
- **ACLs** → Interfaces "in" y "out"
- **Wildcard vs mask** (0.0.0.255 vs 255.255.255.0)
- **Conectividad de ida y vuelta**

Dudas / preguntas?

Contacto:

José Suárez-Varela
jsuarezv@ac.upc.edu

Minicontrol

- Herramienta WebTest:

  # su

  # root

  # udhcpc -i e0

- **User y password (DNI sin letra)**
- 4 preguntas tipo test (multirrespuesta **o respuesta única**)
- No se puede volver atrás
- No se penalizan respuestas erróneas
- Se puede usar **cuaderno de prácticas y calculadora IPs**
- Quitar móviles de encima de la mesa