Lab 5. Switches

1. Introducción

Un switch Ethernet es un dispositivo de nivel 2 que segmenta los dominios de colisiones. La configuración de un switch es totalmente dependiente del fabricante. En este laboratorio vamos a usar switches Ethernet de la gama 2950 de CISCO. Para entrar y configurar el switch seguiremos los mismos pasos que en un router CISCO. Nos conectamos por el puerto consola del switch con un cable rollover y con una aplicación que permita la comunicación asíncrona por el puerto serie del host (ej. hyperterminal o minicom). Una vez conectados entramos en modo setup, o en modo user exec. De modo user exec hemos de entrar a modo privilegiado con el comando "`enable`". En este modo podremos visualizar tablas, ficheros de configuración (running-config), bases de datos del switch, etc. Para configurar cualquier funcionalidad hay que entrar en el modo de configuración global usando el comando "`configure terminal`".

2. Tabla MAC

Cada puerto de un switch es un dominio de colisiones. Para segmentar la red Ethernet, un switch usa la tabla MAC. El switch inicialmente tiene la tabla vacía. Cada vez que una estación envía una trama Ethernet a otro host, el switch "aprende" a que puerto está conectado una dirección MAC. Por ejemplo si una trama Ethernet entra por el puerto del switch e0 con dirección origen MAC=A tiene destino la MAC=B, el switch aprende que la MAC=A está conectada al puerto e0.

A medida que los hosts envían peticiones a otros hosts y estos responden, la tabla MAC se va llenando. Como los hosts pueden cambiar de situación (pasar a estar conectados a otro puerto), no conviene que las entradas de la tabla MAC sean estáticas. Por eso las entradas tienen un tiempo de vida ("age"). Pasado el tiempo de vida, la entrada de la tabla MAC desaparece ("aging out"). Por eso decimos que las entradas son *dinámicas*.

- Verificación:

```
Switch# show mac-address-table
```

Por defecto un switch CISCO de gama 2950 tiene asignado un tiempo de vida de entradas en la tabla MAC de 300 segundos (5 minutos), mecanismo de aprendizaje dinámico y ninguna estrada estática en la tabla.

Para ver la tabla MAC de un switch podemos usar el comando "`sh mac address-table`". Para ver el tiempo de vida se puede usar el comando "`sh mac address-table aging-time`". Para eliminar entradas aprendidas dinámicamente se puede usar el comando "`clear mac address-table dynamic`" (todas las entradas) o "`clear mac address-table dynamic address @MAC`" (eliminar la dirección @MAC de la tabla) o `clear mac address-table dynamic interface IFACE`" (para las MACs de una interfaz) o `clear mac address-table dynamic vlan VLAN-ID`" (todas las MACs de una VLAN).

3. VLANs

Definimos una VLAN como una red broadcast. Cada uno de los puertos de un router es una red broadcast por definición y por tanto una red IP. Para ahorrar puertos de router se pueden crear redes broadcast (redes IP) en un switch mediante software. Eso significa que con un puerto de router conectado al switch vamos a crear tantas VLANs (redes broadcast) como el software del switch nos permita. Un switch CISCO de la gama 2950 permite crear hasta 1024 VLANs.

Es evidente que si un puerto de router debe soportar N VLANs (N redes IP) el puerto deberá tener N direcciones IP, una por cada VLAN creada. También es evidente que para viajar desde una VLAN a otra hay que pasar obligatoriamente por el router. Es decir, no se puede ir desde una VLAN a otra directamente a través del switch, del mismo modo que el tráfico broadcast de nivel 2 (por ejemplo las tramas ARP) no se propagan entre VLANs distintas. Para conseguir esta segmentación de nivel 3 se utiliza un protocolo específico llamado de "trunking". Un enlace en modo trunk pertenece a más de una VLAN, de modo que permite enviar en un solo enlace todo el tráfico de las VLANs del switch al router (esta configuración se conoce con el nombre de *router-on-a-stick*). Las tramas que se envían en el trunk llevan una etiqueta (*tag*) con el número de VLAN a la que pertenece la trama. Existen dos protocolos de trunking: el que se usó por primera vez, propietario de CISCO, conocido como ISL, y el estandarizado por el IEEE: IEEE802.1Q. En los equipos de CISCO podemos encontrar ambos protocolos (los equipos más modernos suelen llevar sólo IEEE802.1Q).

Cuando encendemos un switch CISCO, todos los puertos pertenecen a la VLAN nativa. La VLAN nativa por definición es la VLAN-ID=1. Si se define un VLAN para un uso específico es mejor usar otras VLAN-ID distintos al 1. Para definir VLANs en un switch seguiremos los siguientes pasos:

```
Sw# configure term
Sw(config)# vlan VLAN-ID
Sw(config-vlan)# name NAME
Sw(config-vlan)# exit
```

donde VLAN-ID tiene rango 0001 – 1005, CREAMOS la VLAN con NOMBRE y NUMERO. CUIDADO: VLAN 1, 1002, 1003, 1004 y 1005 son VLANs por defecto para diversos tecnologías de nivel 2 (Ethernet, FFDI, TR, ...)

```
Sw# show vlan
Sw# show vlan id VLAN-ID
```

lista parámetros de todas o una VLAN determinada. Para borrar una VLAN:

```
Sw# configure term
Sw(config)# no vlan VLAN-ID
Sw(config-vlan)# exit
```

Una vez que la VLAN está creada hay que asignar interfaces a la VLAN. Usar el comando switchport para asignar de forma estática puertos a una VLAN:

```
Sw(config)# interface fastethernet0/1
Sw(config-if)# switchport mode access → define VLANs en modo estático
Sw(config-if)# switchport access vlan VLAN-ID → asignar el puerto a la vlan creada vlan-id
Sw(config-if)# exit
Sw(config)# exit
Sw# show running-config interface IFACE → verifica el VLAN membership de la interfaz tal como está en la memoria física
Sw# show interfaces IFACE switchport → lista el modo administrativo (ej.; acceso estático), el modo de acceso de la VLAN (ej..; vlan-id), etc
Sw# show vlan → lista información de las vlans creadas
```

Una vez creada la VLAN en el switch hay que definir el enlace entre el switch y el router como un enlace ("link") de tipo "trunk". Un "link trunk" es un enlace que pertenece a todas las VLANs creadas. Tiene que estar asignada a la VLAN nativa (VLAN=1). Solo interfaces Fast Ethernet pueden ser trunk.

```
Sw(config)# interface fastethernet0/1
Sw(config-if)# switchport mode trunk
Sw(config-if)# exit
Sw(config)# exit
Sw# show interfaces IFACE trunk
```

Ahora el switch ya está configurado. Nos falta configurar el router para que entienda las diferentes VLANs creadas. El enlace del router debe ser un "link trunk" y además debe tener tantas direcciones IP como VLANs creadas. Para ello crearemos subinterfaces en la interfaz Fast Ethernet del router. Cada subinterfaz la asignaremos a una VLAN y le daremos una IP. En el siguiente ejemplo creamos 2 VLANs (VLAN-ID=2 y VLAN-ID=3) en el router. Usamos la interfaz Fast Ethernet 0/0 como interfaz de partida donde crearemos las subinterfaces Fast Ethernet 0/0.1 y Fast Ethernet 0/0.2 y asignamos el VLAN-ID a esa subinterfaz (con el comando *encapsulation*). Finalmente le damos una IP a la subinterfaz:

```
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-ID2
R(config-subif)#  ip address @IP2 MASK2
R(config-subif)#  exit
R(config-if)#  int fastethernet 0/0.2
R(config-subif)#  encapsulation  dot1q  VLAN-ID3
R(config-subif)#  ip address @IP3 MASK3
R(config-subif)#  exit
R(config-if)#  exit
R(config)#  exit
R#  sh ip route
```

Observar que en la tabla de encaminamiento tiene que aparecer una entrada con cada subinterfaz y su subred IP.

4. Puertos seguros

Puede haber situaciones en los que nos interese fijar direcciones MAC en la entrada de la tabla MAC. Por ejemplo, por motivos de seguridad sólo queremos que en un puerto del switch Ethernet se pueda conectar físicamente el host A. Si se conecta otro host con distinta dirección MAC a A queremos que el puerto se deshabilite. Con ello aumentamos la seguridad de nuestra red. A esta solución se le llama puertos seguros. Por defecto la seguridad por puertos está desactivada, para activarla en una interface:

```
Switch(config-if)# switchport port-security
```

Para añadir puertos seguros:

- El puerto debe estar en modo *access*. Para cambiar el modo de un puerto:

```
Switch(config-if)# switchport mode {access | dynamic {auto | desirable} | trunk}
```

Descripción:

Access	Set the port to access mode (either static-access or dynamic-access depending on the setting of the switchport access vlan inteface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that transmits and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
Dynamic auto	Set the interface trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link.
Dynamic desirable	Set the interface trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
Trunk	Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port transmits and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.

The default mode is **dynamic desirable**.

La manera de conseguir un puerto seguro es especificar el número máximo de direcciones MACs que se pueden asociar a un puerto Ethernet y fijar las direcciones MAC que nos interesan como seguras en ese puerto. Pero primero tenemos que vaciar la tabla MAC borrando las direcciones dinámicas que haya podido añadir el switch con el comando:

```
Switch# clear mac address-table {dynamic [address mac-addr | interface interface-id
| vlan vlan-id]}
```

- Para limitar el máximo número de MAC permitidas en una interface:

```
Switch(config-if)# switchport port-security maximum max_addrs
```

Si queremos asignar una MAC segura en una interfaz de una VLAN determinada hay que ejecutar:

```
Sw(config-if)# switchport port-security mac-address @MAC
Sw# show mac-address-table static
```

- A continuación se define la acción a tomar cuando se produce una violación de puertos.

```
Sw(config-if)# switchport port-security violation {protect | restrict | shutdown }
```

donde "protect" significa que se descartan tramas de las MAC que violan el sistema, "restrict" significa que además se envía un trap (aviso) al gestor de red (protocolo SNMP) y "shutdown" (por defecto) significa que se desactiva el puerto.

- Verificación:

```
Switch# show port-security [interface interface-id | address]
Switch# show mac-address-table
Switch# show running-config
```

NOTA:

Al violar la seguridad del puerto, este queda bloqueado. Para reactivarlo, ejecutar:

```
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
```

5. Realización de la práctica

La configuración del lab será de un router conectado a un switch por un enlace Fast Ethernet (tiene que ser Fast Ethernet para soportar *trunking*). A cada switch conectaremos 3 PCs.

5.1. VLANs y trunking

1. Borrar las VLANs creadas por el usuario existentes en el switch. Que pasa si se intenta borrar la VLAN=1?
2. Configura la topología de la Figura 19. Crea las estaciones T_1 y T_2 como pertenecientes a la VLAN=2 y la estación T_3 a la VLAN=3. Configura el router para que acepte VLANs. Apuntar las direcciones IP configuradas en la siguiente tabla:

T1/e1	
T2/e1	
R1/fe1.1	
R1/fe1.2	
T3/e1	

3. Comprueba que puedes hacer un ping a todas las estaciones.
4. Comprueba la tabla MAC del switch. Identifica la dirección MAC y VLAN de todos los PCs en la tabla MAC.
5. Observa la tabla de routing del router. ¿Qué entradas y qué formato tienen?
6. Ejecuta tcpdump en las estaciones para ver el tráfico recibido/transmitido.
7. Haz un ping desde T_1 a T_2. ¿Que dispositivos ven tráfico? ¿Por qué?
8. Haz un ping desde T_1 a T_3. ¿Que dispositivos ven tráfico? ¿Por qué?
9. Usa el comando traceroute entre T1 y T2, y entre T1 y T3. Razona las diferencias.

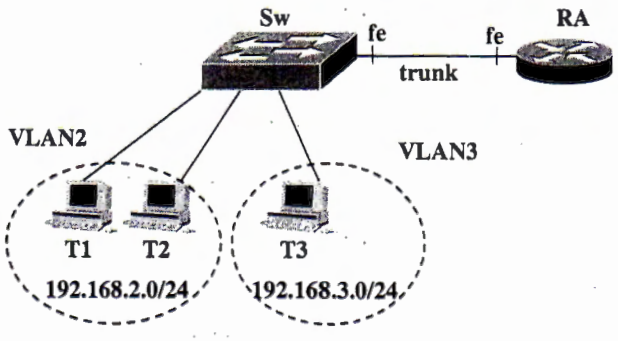
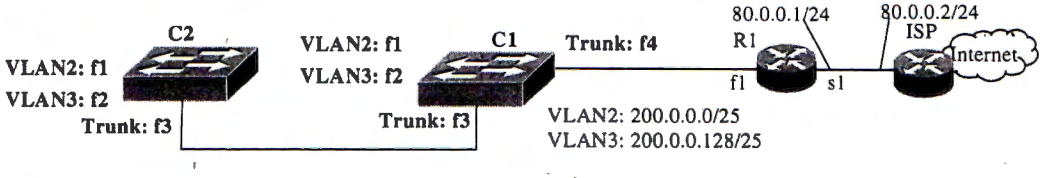


Figura 19

5.2. Puertos seguros

10. Configura un puerto seguro en una de las estaciones (ej. T_1). Configura que la acción por defecto sea deshabilitar el puerto si otra estación se conecta. Desconecta la estación T_1 y conecta la estación T_2. Observa como se deshabilita el puerto y vuelve a conectar la estación original. El comportamiento debe ser el siguiente: si se la acción es *shutdown* del puerto, no aceptará de nuevo la estación original y habrá que habilitarlo manualmente (es decir entrar en la interfaz del switch y ejecutar el comando *shutdown* i *no shutdown*).

6. Informe previ



1. Dóna les comandes per a configurar els commutadors i el router R1 de la figura. Suposa que el hostid del router R1 en cada xarxa és l'adreça numèricament més baixa de la xarxa.
2. Suposa que en el commutador C2 hi ha un PC1 connectat a un port de la VLAN2 i PC2 connectat a un port de la VLAN3. Digues per quins dispositius passaran els paquets si PC1 fa un ping a PC2.