Lab 5. Switches

1. Introducció

Un switch Ethernet és un dispositiu de nivell 2 que segmenta els dominis de col·lisions. La configuració d'un switch és totalment dependent del fabricant. En aquest laboratori utilitzarem switches Ethernet de la gamma 2950 de CISCO. Per entrar i configurar el switch seguirem els mateixos passos que en un router CISCO. Ens connectem pel port consola del switch amb un cable creuat i amb una aplicació que permeti la comunicació asíncrona pel port sèrie del host (ex hyperterminal o minicom). Un cop connectats entrem en mode setup, o en mode user exec. Del mode user exec hem d'entrar al mode privilegiat amb l'ordre "`enable`". En aquest mode podrem visualitzar taules, fitxers de configuració (running-config), bases de dades del switch, etc. Per configurar qualsevol funcionalitat cal entrar en el mode de configuració global usant l'ordre "`configure terminal`".

2. Taula MAC

Cada port d'un switch és un domini de col·lisions. Per segmentar la xarxa Ethernet, un switch utilitza la taula MAC. El switch inicialment té la taula buida. Cada vegada que una estació envia una trama Ethernet a un altre host, el switch "aprèn" a quin port està connectat una adreça MAC. Per exemple, si una trama Ethernet entra pel port del switch e0 amb direcció origen MAC=A té destinació la MAC=B, el switch aprèn que la MAC=A està connectada al port e0.

A mesura que els hosts envien peticions a altres hosts i aquests responen, la taula MAC es va omplint. Com que els hosts poden canviar de situació (passar a estar connectats a un altre port), no convé que les entrades de la taula MAC siguin estàtiques. Per això les entrades tenen un temps de vida ("age"). Passat el temps de vida, l'entrada de la taula MAC desapareix (aging out). Per això diem que les entrades són *dinàmiques.*

- Verificació:

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

Per defecte un switch CISCO de gamma 2950 té assignat un temps de vida d'entrades a la taula MAC de 300 segons (5 minuts), mecanisme d'aprenentatge dinàmic i cap estrada estàtica a la taula.

Per veure la taula MAC d'un switch podem utilitzar l'ordre "`sh mac address-table''`. Per veure el temps de vida es pot fer servir l'ordre "`sh mac address-table aging-time''`. Per eliminar entrades apreses dinàmicament es pot fer servir l'ordre "`clear mac address-table dynamic''` (totes les entrades) o "`clear mac address-table dynamic address @MAC''` (eliminar l'adreça @MAC de la taula) o "`clear mac address-table dynamic interface IFACE''` (per a les MACs d'una interfície) o "`clear mac address-table dynamic vlan VLAN-ID''` (totes les MACs d'una VLAN).

3. VLANs

Definim una VLAN com una xarxa broadcast. Cadascun dels ports d'un router és una xarxa broadcast per definició i per tant una xarxa IP. Per estalviar ports de router es poden crear xarxes broadcast (xarxes IP) en un switch mitjançant per configuració. Això significa que amb un port de router connectat al switch crearem tantes VLANs (xarxes broadcast) com la configuración del switch ens permeti. Un switch CISCO de la gamma 2950 permet crear fins a 1024 VLANs.

És clar que si un port de router ha de suportar N VLANs (N xarxes IP) el port haurà de tenir N adreces IP, una per cada VLAN creada. També és clar que per viatjar des d'una VLAN a una altra cal passar obligatòriament pel router. És a dir, no es pot anar des d'una VLAN a una altra directament a través del switch, de la mateixa manera que el trànsit broadcast de nivell 2 (per exemple les trames ARP) no es propaguen entre VLANs diferents. Per aconseguir aquesta segmentació de nivell 3 s'utilitza un protocol específic anomenat "trunking". Un enllaç en mode trunk pertany a més d'una VLAN, de manera que permet enviar en un sol enllaç tot el trànsit de les VLANs del switch al router (aquesta configuració es coneix amb el nom de router-on-a-stick). Per això, les trames que s'envien al trunk porten una etiqueta (*tag)* amb el número de VLAN a què pertany la trama. Hi ha dos protocols de trunking: el que es va fer servir per primera vegada, propietari de CISCO, conegut com a ISL, i l'estandarditzat per l'IEEE: IEEE802.1Q. Als equips de CISCO podem trobar tots dos protocols (els equips més moderns solen portar només IEEE802.1Q).

3.1. Configuració del switch

Quan encenem un switch CISCO, tots els ports pertanyen a la VLAN nativa. La VLAN nativa per definició és la VLAN-ID=1. Si es defineix un VLAN per a un ús específic és millor utilitzar altres VLAN-ID diferents de l'1. Per definir VLANs en un switch seguirem els passos següents:

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

on VLAN-ID té rang 0001–1005, **creem** la VLAN amb **nom** i **numero**. Nota: VLAN 1, 1002, 1003, 1004 i 1005 són VLANs per defecte per a diverses tecnologies de nivell 2 (Ethernet, FFDI, TR,...)

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

llista paràmetres de totes o una VLAN determinada. Per esborrar una VLAN:

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

Quan la VLAN està creada cal assignar interfícies a la VLAN. Usar l'ordre switchport per assignar de forma estàtica ports a una VLAN:

```
Sw(config)# interface fastethernet0/1
Sw(config-if)# switchport mode access →defineix VLANs en mode estàtic
Sw(config-if)# switchport access vlan VLAN-ID →assignar el port 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 interfície tal com està a la memòria física
Sw# show interfaces IFACE switchport →llista el mode administratiu (ex.; accés estàtic), el mode d'accés de la VLAN (ex.; vlan-id), etc
Sw# show vlan →llista informació de les vlans creades
```

Un cop creada la VLAN al switch cal definir l'enllaç entre el switch i el router com un enllaç ("link") de tipus "trunk". Un "link trunk" és un enllaç que pertany a totes les VLANs creades. Ha d'estar assignada a la VLAN nativa (VLAN=1). Només interfícies Fast Ethernet poden ser trunk.

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

Ara el switch ja està configurat. Ens falta configurar el router perquè entengui les diferents VLANs creades.

3.2. Configuració del router

L'enllaç del router ha de ser un "link trunk" ia més ha de tenir tantes adreces IP com a VLANs creades. Per això crearem subinterfícies a la interfície Fast Ethernet del router. Cada subinterfície l'assignarem a una VLAN i us donarem una IP. Al següent exemple creem 2 VLANs (VLAN-ID=2 i VLAN-ID=3) al router. Fem servir la interfície Fast Ethernet 0/0 com a interfície de partida on crearem les subinterfícies Fast Ethernet 0/0.1 i Fast Ethernet 0/0.2 i assignem el VLAN-ID a aquesta subinterfície (amb l'ordre encapsulation). Finalment donem una IP a la subinterfície:

```
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-ID 3
R(config-subif)# ip address @IP3 MASK3
R(config-subif)# exit
R(config-if)# exit
R(config)# exit
R# sh ip route
```

Observar que a la taula d'encaminament ha d'aparèixer una entrada amb cada subinterfície i la seva subxarxa IP.

4. Ports segurs

Hi pot haver situacions en què ens interessi fixar adreces MAC a l'entrada de la taula MAC. Per exemple, per motius de seguretat només volem que en un port del switch Ethernet es pugui connectar físicament el host A. Si es connecta un altre host amb diferent adreça MAC a A volem que el port es deshabiliti. Amb això augmentem la seguretat de la nostra xarxa. Aquesta solució s'anomena ports segurs. Per defecte la seguretat per ports està desactivada, per activar-la en una interfície:

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

Per afegir ports segurs:

- El port ha d'estar en mode *access.* Per canviar el mode d'un port:

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

Descripció:

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 d'aconseguir un port segur és especificar el nombre màxim d'adreces MAC que es poden associar a un port Ethernet i fixar les adreces MAC que ens interessen com a segures en aquest port. Però primer hem de buidar la taula MAC esborrant les adreces dinàmiques que hagi pogut afegir el switch amb l'ordre:

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

Per limitar el màxim nombre de MAC permeses en una interfície:

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

Si volem assignar una MAC segura a una interfície d'una VLAN determinada cal executar:

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

A continuació es defineix l'acció a prendre quan es produeix una violació de ports.

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

on "protect" significa que es descarten trames de les MAC que violen el sistema, "restrict" significa que a més s'envia un trap (avís) al gestor de xarxa (protocol SNMP) i "shutdown" (per defecte) que es desactiva el port.

Verificació:

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

NOTA: En violar la seguretat del port, aquest queda bloquejat. Per reactivar-lo, executar:

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

5. Realització de la pràctica

La configuració del lab serà d'un router connectat a un switch per un enllaç Fast Ethernet (ha de ser Fast Ethernet per suportar *trunking)*. A cada switch connectarem 3 PCs.

5.1. VLANs i trunking

1) Esborrar les VLANs creades per l'usuari (p. ex: configure term; no vlan 2). Què passa si intenteu esborrar la VLAN=1?
2) Configura la topologia de la Figura 19. Crea les estacions T_1 i T_2 com a pertanyents a la VLAN=2 i l'estació T_3 a la VLAN=3. Configura el router perquè accepti VLANs. Apuntar les adreces IP configurades a la taula següent.

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

3) Comprovar que podeu fer ping entre totes les estacions.
4) Comprovar que les entrades que s'han afegit en la taula MAC s'esborren automàticament després d'un temps.
5) Fer ping entre els PCs fins que totes les adreces MAC estigun en la taula MAC. A continuació identificar l'adreça MAC i VLAN de tots els PCs i del router en la taula MAC.
6) Observar la taula de routing del router. Quines entrades i quin format tenen?
7) Executar tcpdump a les estacions per veure el trànsit rebut/transmès.
8) Fer un ping des de T_1 a T_2. Quins dispositius veuen trànsit? Per què?
9) Fer un ping des de T_1 a T_3. Quins dispositius veuen trànsit? Per què?
10) Usar la ordre traceroute entre T1 i T2, i entre T1 i T3. Raona les diferències.
11) Executa tcpdump en un dels PCs. Observa les trames 802.1D (protocol spanning tree) que arriben cada segon del switch.
12) Descoonecta un dels PCs i torna'l a connectar. Observa que, un cop connectat el PC, el led del switch està primer en taronja durant uns 30 segons, i després verd. Comprova fent ping que mentre el led està en taronja el PC no té connexió. Comprova amb tcpdump que mentre el led està taronja arriben trames 802.1D al PC. Durant aquest temps el protocol spanning tree actua per detectar si hi ha bucles. Comprova que passats els 30 segons, quan el led es posa verd, el PC torna a tenir connexió.

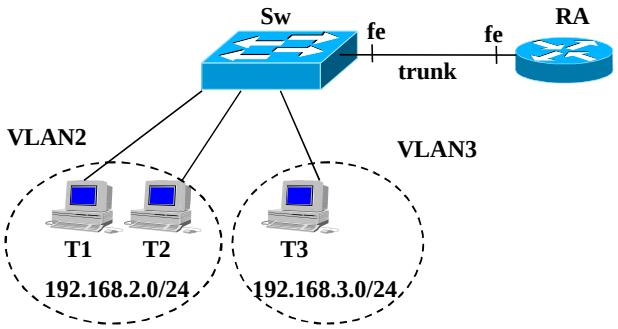
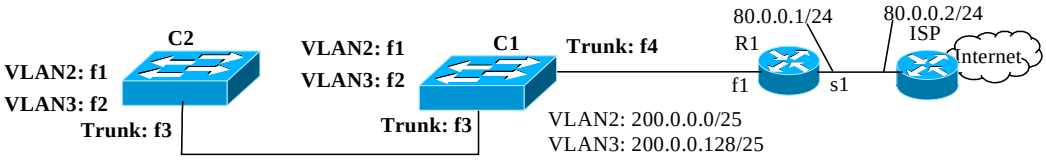


Figura 19

5.2. Ports segurs

13) Configurar un port segur en una de les estacions (ex. T_1). Configura que l'acció per defecte sigui deshabilitar el port si una altra estació es connecta. Desconnecta l'estació T_1 i connecta l'estació T_2. Observa com es desactiva el port i torna a connectar l'estació original. El comportament ha de ser el següent: si l'acció és *shutdown* del port, no acceptarà de nou l'estació original i caldrà habilitar-lo manualment (és a dir entrar a la interfície del switch i executar l'ordre *shutdown* i *no shutdown)*.

6. Informe previ



Respondre a les preguntes següents per a la xarxa de la figura.

1) Posar les ordres per configurar els commutadors i el router R1 de la figura. Suposar que l'hostid del router R1 a cada xarxa és l'adreça numèricament més baixa de la xarxa.
2) Suposar que al commutador C2 hi ha un PC1 connectat a un port de la VLAN2 i PC2 connectat a un port de la VLAN3. Per quins dispositius passaran els paquets si PC1 fa un ping a PC2?