PRÁCTICA

CONFIGURACIÓN DE CONMUTADORES CISCO

Objetivos

1. Diferenciar las distintas formas de acceso a la interfaz de línea de comandos de un dispositivo Cisco.

2. Comprender el funcionamiento de los conmutadores.

3. Configurar diversos aspectos de los conmutadores Cisco tales como la tabla MAC, la velocidad y el modo dúplex y la seguridad de los puertos.

Materiales

- Ordenadores del Laboratorio ATC2, con sistema operativo Windows.

- Conmutadores Cisco del Laboratorio ATC2.

- Red Docente del Laboratorio ATC2.

Estudio Teórico

Acceso a la CLI en dispositivos Cisco

Existen varias formas de acceder a la interfaz de línea comandos (CLI) de un dispositivo Cisco, concretamente se haría haciendo uso de los siguientes:

1. **CTY** o puerto de consola: accediendo por medio de la interfaz EIA232 desde un PC.
2. **VTY** o terminales virtuales: accediendo desde un host con un cliente Telnet o SSH.

Cada tipo de dispositivo tiene un número concreto de VTYs: los enrutadores poseen 5 y los conmutadores 16.

El acceso a través de telnet al dispositivo se hace por medio de contraseñas y puede utilizar su cliente habitual (por ejemplo el de la línea de comandos de Windows: `c:\>telnet nºIP`) .

La forma de establecer la contraseña en un conmutador es la siguiente (observe que la contraseña es "`class`"):

```
Switch(config)# line vty 0 15
Switch(config-line)#password class
Switch(config- line)#login
```

3. **AUX** o puerto auxiliar: para acceso remoto desde una línea telefónica a través de un modem. Es posible que éste puerto no exista en el dispositivo.

Existen también una interfaz web de acceso a los dispositivos Cisco que, en muchos casos, nada tiene que ver con la CLI y que ofrece un entorno mucho más sencillo que éste último.

Introducción a los conmutadores

Vamos a considerar un conmutador como a un dispositivo de capa 2 que segmenta la red en varios dominios de colisión, enviando las tramas entre segmentos sólo cuando es necesario.

Sus funciones principales son:

- Aprendizaje de direcciones.
- Envío-filtrado de paquetes.
- Anulación de bucles.

En esta práctica trataremos las dos primeras funciones, la tercera se verá en próximos cursos.

Para que un conmutador sea capaz de enviar una trama, sólo por el segmento adecuado, debe asociar las direcciones MACs de las máquinas con los puertos, del propio conmutador, al que está conectado dicha máquina.

Para ello los conmutadores disponen una memoria donde se almacena al menos las duplas (MACs de origen de trama, puerto de

entrada al conmutador), es lo que se llama la **tabla MAC del conmutador**.

He aquí un ejemplo donde se visualiza la tabla Mac de un conmutador Cisco:

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

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

   1    0001.63e5.ed09    DYNAMIC     Fa2/1
   1    0002.4a48.5928    DYNAMIC     Fa0/1
   1    000b.beb1.ec76    DYNAMIC     Fa1/1
   1    0010.111d.8482    DYNAMIC     Fa4/1
   1    0060.705a.3aa0    DYNAMIC     Fa3/1
Switch>
```

Obsérvese que además de la dirección MAC y el puerto del conmutador, aparecen las VLANs y el tipo de asignación (dinámico o estático).

El tipo de asignación más habitual es el dinámico, que consiste en que la MAC se asocia al puerto tras la entrada de una trama por dicho puerto. Se produce entonces lo que se llama el **aprendizaje de la dirección MAC**, que consiste en almacenar la dirección MAC de origen de la cabecera de la trama junto al puerto por el que ha entrado dicha trama.

El tipo de asignación estático era el único que existía en los primeros puentes, y consiste en asociar las direcciones MACs con los puertos por medio de configuración manual. El comando utilizado para ello es `mac-address-table static` *`dir_MAC`* `vlan` *`nº`* `interface` *`nombre-interfaz`*.

Cuando se inicia un conmutador, lo normal es que la tabla MAC de éste esté vacía. Si el conmutador recibe una trama en ese momento la reenviará por todos sus puertos (al igual que hace un concentrador). Actuará así mientras no encuentre en memoria la MAC de destino de la trama y el puerto asociado a ésta.

A este proceso de reenvío de las tramas por todos los puertos se le conoce con el nombre de **inundación** y es objetivo del conmutador evitarlo y que se produzca la segmentación cuanto antes.

Cuando una trama llega al conmutador, y la MAC de destino se encuentra en la tabla, esta se **enviará** por el puerto que tiene asociado dicha MAC. El conmutador no retransmitirá la trama por el resto de los puertos para eliminar posibilidades de colisiones y preservar el ancho de banda. A este hecho se le denomina **filtrado** de tramas.

En el caso de que la trama tenga como destino el mismo puerto por el que ha entrado, lógicamente la trama se descartará.

En muchas ocasiones llegan a los conmutadores tramas con MAC de destino ff-ff-ff-ff-ff-ff (**dirección de broadcast** o de difusión), estas tramas serán reenviadas automáticamente por inundación, es decir por todos los puertos.

Velocidad y modo dúplex

Por defecto los puertos de un conmutador se encuentran en modo de auto-negociación, pero se puede hacer que un puerto vaya a una velocidad concreta y en un modo dúplex concreto (half o full). Para ello se utiliza los comandos `speed` y `dúplex` en el modo de configuración de la interfaz.

Por ejemplo, para obligar a la interfaz Fast Ethernet 0/10 a que sólo funcione a 100 Mbps en modo full dúplex se hace lo siguiente:

```
Switch(config)#interface fa0/10
Switch(config-if)#speed 100
Switch(config-if)#duplex full
Switch(config-if)#exit
```

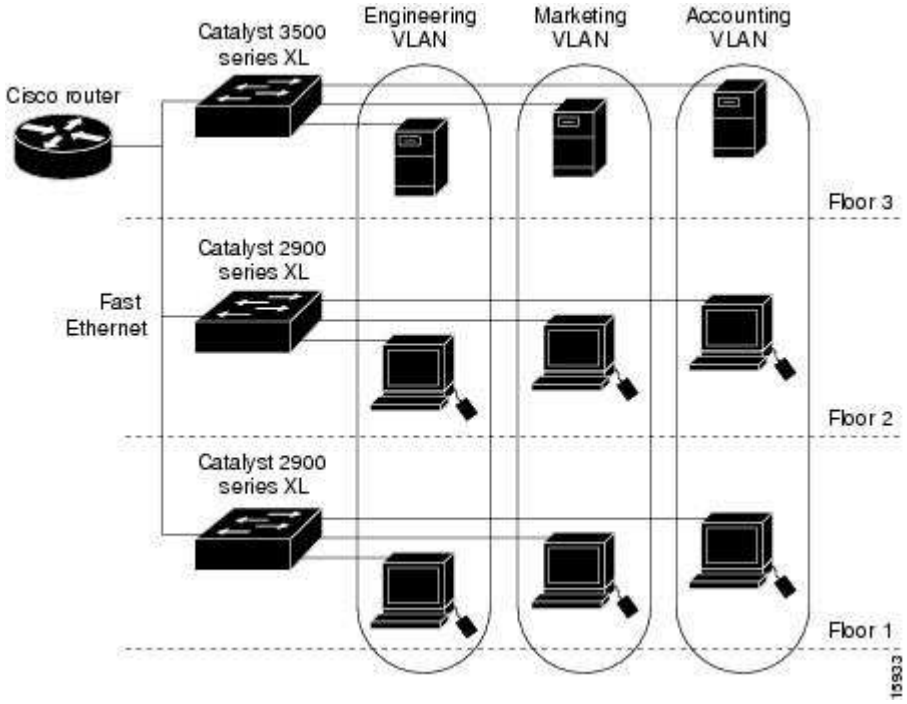
Para visualizar el estado de la interfaz se puede utilizar el comando `show interfaces fa0/10`.

VLANs

Cuando en una red física, formada por un conjunto de conmutadores unidos, se genera una trama de broadcast, ésta pasará por todos los conmutadores y llegará a todos los host de la red. Se dice entonces que la red forma un solo **dominio de difusión** o broadcast.

Lo normal es que el dominio de difusión esté delimitado por dispositivos de capa 3 (enrutadores), pero existe una excepción: las VLANs.

Con las VLANs se consiguen dominios de difusión lógicos en un entorno conmutado:



Las VLANs se pueden extender por distintos segmentos físicos, es decir, que se puede extender por distintos conmutadores. Además cada una de estas VLANs funciona como si fueran conmutadores independientes.

Se pueden crear de múltiples maneras: agrupando direcciones MACs, puertos, protocolos, etc.

No es cometido de ésta práctica configurar VLANs, pero es importante saber que por defecto un conmutador posee una única VLAN (la **VLAN1**) y que todos sus puertos están asociados a ella.

Si se desea configurar algún aspecto genérico del conmutador, entonces se debe configurar dicho aspecto en la VLAN1. Un ejemplo podría ser la configuración de una IP al conmutador.

Bien es sabido que los conmutadores trabajan en la capa de enlace y por tanto no necesitan de IPs para realizar su cometido. No obstante, cabe la posibilidad de acceder a ellos, para configurarlos, a través de telnet, SSH o HTTP (protocolos de la capa de aplicación); y entonces se hace necesario ponerles una IP.

Cuando se habilita esta funcionalidad en el conmutador, realmente lo que se está montando en él es un servidor (telnet, SSH o web).

Para asignar una IP a la VLAN1 de un conmutador, se procede como sigue:

```
Switch(config)# interface VLAN1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Recuerda: las interfaces de tipo VLAN están caídas por defecto y después de configurarlas hay que levantarlas. Para ello se utiliza el comando `no shutdown`.

Configuración de la seguridad de puertos

En los conmutadores Cisco es posible crear restricciones de acceso a los puertos siempre que trabajen en modo acceso. Dichas restricciones se pueden crear de dos formas:

1. Estableciendo el nº máximo de dispositivos que se pueden conectar al puerto, de forma que el conmutador aprende (`sticky`) las MACs de los dispositivos que pueden acceder al puerto.

2. Estableciendo las MACs concretas de los dipositivos que pueden acceder al puerto.

Para establecer una interfaz en el modo de acceso, se utiliza el comando `switchport mode access` en el modo de configuración de la interfaz.

Para habilitar la seguridad de puertos en una interfaz, se utiliza el comando `swicthport port-security` en el modo de configuración de la interfaz concreta a la que se aplicarán las restricciones.

Para restringir el número de MACs que pueden acceder a un puerto se utiliza el comando `switchport port-security maximum` *n* donde n es el número, el cual puede tomar un valor entre 1 y 132.

Por ejemplo, para habilitar la seguridad de puertos en la interfaz Fast Ethernet 0/4 y restringir el acceso a no más de cuatro dispositivos, se podría hacer lo siguiente:

```
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
```

```
Switch(config-if)#switchport port-security maximum 4
Switch(config-if)#switchport port-security mac-address
sticky
Switch(config-if)#end
```

Para visualizar las direcciones asociadas a los puertos se puede utilizar `show port-security address`:

```
Switch#show port-security address
                    Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address    Type                  Ports          Remaining Age
                                                            (mins)
----    -----------    ----                  -----          -------------
1       0001.6429.A440 DynamicConfigured     FastEthernet0/4              -
1       0003.E420.C433 DynamicConfigured     FastEthernet0/4              -
1       0004.9A05.B738 DynamicConfigured     FastEthernet0/4              -
1       00E0.F716.0A55 DynamicConfigured     FastEthernet0/4              -
------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 3
Max Addresses limit in System (excluding one mac per port) : 1024
```

Para visualizar le seguridad de un puerto se puede utilizar el comando `show port-security interface` *`nombre_interfaz`* de la siguiente forma:

```
Switch#show port-security interface fa 0/4
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 4
Total MAC Addresses        : 5
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000C.CF77.2C30:1
Security Violation Count   : 1
```

Cuando se viola la seguridad en un puerto, porque por él ha entrado una trama con una MAC de origen no esperada, el conmutador realiza una acción. Las acciones que puede tomar son:

1. **Protect** (proteger): una vez que el puerto llena la lista de MACs de seguridad, hasta el número máximo de MACs establecido, deja de aprender y no envía ninguna trama cuya dirección de origen no se encuentre en dicha lista.

2. **Restrict** (asegurar): es un caso similar al anterior, sólo que además cuando se produzca la violación, el conmutador enviará

un mansaje a la consola y generará un mensaje de trampa SNMP.

3. **Shutdown** (cerrar): en este caso el conmutador cierra el puerto y éste sólo puede ser levantado por el administrador. También se enviará un mansaje a la consola y generará un mensaje de trampa SNMP.

Por defecto, la acción que se toma es la de cerrar el puerto. Como ejemplo puede observar en el cuadro anterior que se ha producido una violación y se ha cerrado el puerto.

El comando para especificar la acción a tomar es `switchport port-security violation` *`modo`*, donde modo puede ser `protect`, `restrict` o `shutdown`.

Desarrollo

Esta práctica se realizará en pareja y para su desarrollo se requerirán 3 PCs y 2 Switches.

En los primeros ejercicios (hasta el Nº 12), cada componente de la pareja configurará un equipo.

1. Inicia una sesión HyperTerminal a tu conmutador.

2. Borra el archivo de configuración startup-config y, después, reinicia el conmutador. Cancela el diálogo de configuración inicial.

3. Para permitir que telnet y otras aplicaciones, como por ejemplo un navegador web, puedan acceder al conmutador con fines de configuración y administración hay que otorgar al conmutador una dirección IP. Esta dirección hay que configurarla en la interfaz virtual VLAN1.

   Establece la dirección IP y máscara en el conmutador que te corresponda según los datos de la tabla 1:

Nombre de switch	Dirección IP	Máscara
Switch1	192.168.1.2	255.255.255.0
Switch2	192.168.1.3	255.255.255.0

Tabla 1

En el Switch1 se haría de la siguiente manera:

```
Switch1(config)# interface VLAN1
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch1(config-if)#no shutdown
```

```
Switch1(config-if)#end
```

NOTA: Por defecto, todos los puertos del conmutador están asociados a la VLAN1.

4. Asigna un nombre al conmutador según los datos de la tabla 1.

5. Configura la contraseña de acceso al modo privilegiado. La contraseña es `cisco`.

6. Configura la contraseña de acceso a la líneas VTY. La contraseña es `class`. En el Switch1 se haría de la siguiente manera:

```
Switch1(config)# line vty 0 15
Switch1(config-line)#password class
Switch1(config- line)#login
```

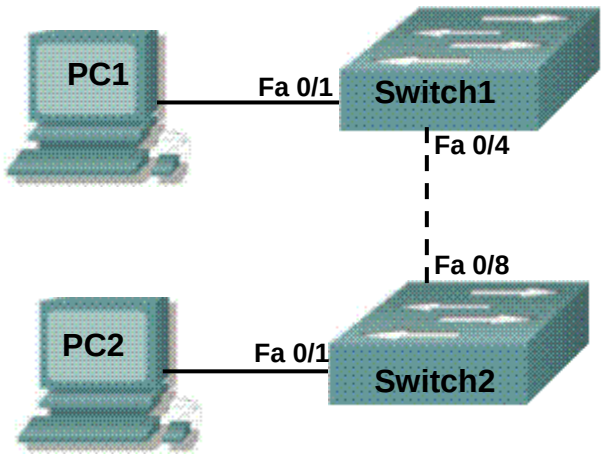
NOTA: Las líneas VTY son las líneas de terminales virtuales y se utilizan para habilitar el acceso remoto al conmutador mediante Telnet. Los conmutadores tienen 16 líneas virtuales: del 0 al 15.

7. Verifica que la configuración activa contiene las últimas modificaciones.

8. Guarda la configuración activa en la NVRAM.

9. Cierra la sesión y desconecta el cable de consola.

10. Realiza las conexiones del siguiente diagrama:



11. Configura el PC que te corresponda con los datos de la tabla 2:

	Dirección IP	Máscara
PC1	192.168.1.4	255.255.255.0
PC2	192.168.1.5	255.255.255.0

Tabla 2

12. Anota la dirección MAC de la tarjeta de red de tu PC.

IMPORTANTE: Los siguientes ejercicios sólo se realizarán en los dispositivos indicados.

13. Para verificar que todos los dispositivos se han configurado correctamente, realiza las siguientes pruebas:

    a. Ping del PC1 al Switch1.
    b. Ping del PC1 al Switch2.
    c. Ping del PC1 al PC2.

14. Inicia una sesión telnet al Switch1. Para ello, ejecuta en windows el siguiente comando: `telnet 192.168.1.2`

15. Enumera y analiza las direcciones MAC que el conmutador ha aprendido.

16. ¿Cuántas entradas dinámicas hay en la tabla CAM?

17. ¿Cómo ha aprendido el conmutador estas direcciones?

18. Supongamos que en el Switch2 hay cinco PCs conectados. ¿Cuántas direcciones MAC se enumerarían en el puerto Fa0/4 del Switch1?

19. Borra la tabla de direcciones MAC con el comando `clear mac-address-table`.

20. ¿Cuántas entradas hay ahora en la tabla CAM?

21. ¿Existe alguna opción del comando `mac-address-table` que permita configurar una dirección MAC estática en la tabla?

22. En la interfaz Fa0/1 del Switch1 configura una dirección MAC estática al PC1.

23. ¿Cuántas entradas hay en la tabla de direcciones MAC? ¿Cuántas son dinámicas? ¿Cuántas son estáticas?

24. Elimina la entrada estática de la tabla.

25. Cualquier persona puede enchufar un PC en un conector del conmutador. Este es un posible punto de entrada de usuarios no autorizados a la red. Para proporcionar seguridad se pueden configurar direcciones MAC estáticas en las interfaces del conmutador, pero es una tarea tediosa y por lo general con una elevada tendencia a errores. Un enfoque alternativo es establecer seguridad de puertos: limitar la cantidad de direcciones que se

pueden aprender en una interfaz. El conmutador se puede configurar para realizar una acción si esta cantidad se supera.

Configura seguridad en la interfaz Fa0/1 del Switch1 para que sólo acepte una MAC. Si se produce una violación de seguridad la interfaz se debe desactivar. En el Switch1 se haría de la siguiente manera:

```
Switch1(config)# interface fa0/1
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security maximum 1
Switch1(config-if)#switchport port-security mac-address sticky
Switch1(config-if)#switchport port-security violation shutdown
Switch1(config-if)#end
```

26. Desde el PC1 haz `ping` al PC2. ¿Ha sido exitoso?

27. Configura un tercer PC al que denominaremos PC3.

	Dirección IP	Máscara
PC3	192.168.1.6	255.255.255.0

28. Desconecta el PC1 del Switch1 y, en el mismo puerto, conecta el PC3.

29. Desde el PC3 haz `ping` al PC2, ¿qué sucede? examina la configuración activa y da una explicación.

    NOTA: Además de la configuración activa también puedes utilizar el comando `show port-security` para verificar el estado de seguridad de puerto.

30. Borra el archivo de configuración startup-config en los dos conmutadores.

31. Cierra la sesión telnet y desconecta los cables.