SESIÓN DE LABORATORIO 2
Configuración básica de switches

Objetivos

- Conocer los aspectos básicos de configuración de los switches.
- Gestionar los diferentes modos de acceso a un switch.
- Establecer las contraseñas de acceso al switch.
- Configurar la seguridad mediante la protección de las interfaces.
- Hacer copias de seguridad de los ficheros de configuración.

Desarrollo

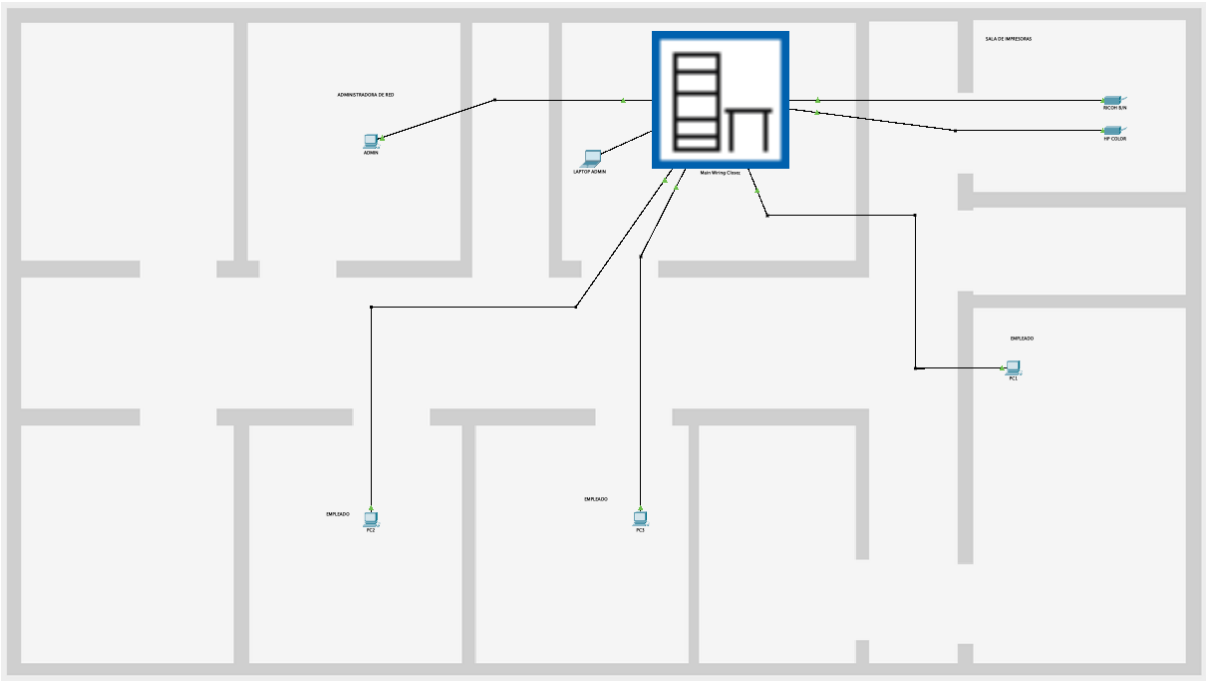
En esta sesión trataremos de diseñar y configurar la red de área local de una pequeña organización. El equipamiento físico de la topología se instala en una única planta de un edificio. Hay una sala de servidores con un armario (rack) en el que se ubica un servidor y un switch Cisco Catalyst 2960. El nombre específico del modelo mostrado es WS-C2960-24TT y puede cambiar con la versión de Packet Tracer.

Según se aprecia en la figura, este modelo de switch dispone de 24 puertos Fast Ethernet (100 Mbps) y dos puertos Gigabit Ethernet (1 Gbps). Los puertos más rápidos suelen usarse para enlaces con alta densidad de tráfico, como servidores o conexiones a otros switches. Sus dimensiones (altura, profundidad y anchura) son 1,75 x 14,50 x 17,5 pulgadas (4,45 x 36,83 x 44,5 cm) y pesa poco menos de 6 kg.

Una particularidad de los switches frente a los routers es que los primeros vienen configurados de fábrica para ser totalmente operativos. De hecho, los switches no suelen tener interruptor de alimentación. Así, basta con desembalar el switch de su caja y conectarlo a la corriente eléctrica. En principio, no hay que hacer nada más. Ahora bien, esta configuración es muy básica y carece de seguridad, por lo que más tarde habremos de configurarlo adecuadamente y establecer un nivel de seguridad apropiado.

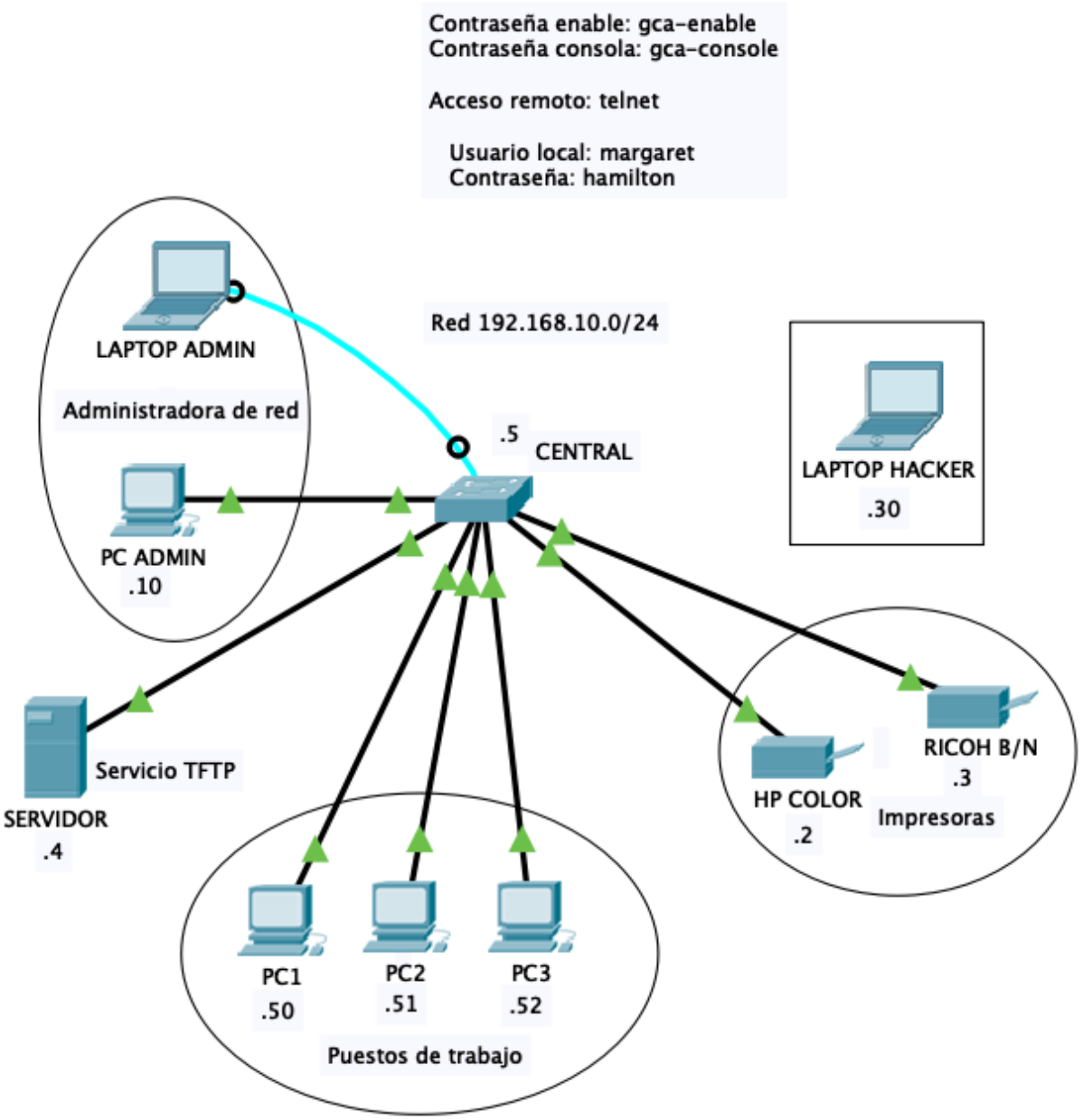
La administradora de red dispone de un PC en su despacho y un ordenador portátil (*laptop*) que utiliza para conectarse al switch a través del cable de la consola. Hay tres despachos con un ordenador personal en cada una de ellos, además de una habitación con dos impresoras para toda la organización, como se puede observar en la siguiente figura que

muestra la vista en planta. Esta vista de la red permite tener en cuenta aspectos físicos como la longitud de los cables.



Es importante considerar las longitudes de los cables cuando se trata de dimensionar físicamente la instalación, principalmente cuando se trata de cable UTP (cobre), el cual suele tener un límite de 100 m. En conexiones que requieran más longitud de cable será necesario emplear fibra óptica.

La visión lógica de esta instalación de red, basada en un único conmutador de red, se muestra en la siguiente figura:



La red de área local tiene el identificador de red 192.168.10.0/24, es decir, se trata de una red de clase C (tres octetos para identificador de red y un octeto para los hosts) que utiliza direcciones privadas (estas direcciones no se podrían emplear para encaminamiento en la red pública). El prefijo /24 es equivalente a especificar la máscara de red mediante los cuatro octetos de una dirección IP que también se puede especificar como 255.255.255.0.

Las direcciones IPv4 de los hosts se indican en la figura con el valor del octeto de menor peso de la dirección, una práctica bastante usual a fin de simplificar la escritura de direcciones.

La siguiente tabla especifica las interfaces del switch ocupadas por los diferentes dispositivos de la topología (hosts), sus nombres y las direcciones IP asignadas. Nótese que todas las interfaces son del tipo Fast Ethernet (ancho de banda de 100 Mbps).

Interfaz switch	Dispositivo	IP
Fa0/1	PC ADMIN	192.168.10.10
Fa0/2	PC1	192.168.10.50
Fa0/3	PC2	192.168.10.51
Fa0/4	PC3	192.168.10.52
Fa0/5	HP COLOR	192.168.10.3
Fa0/6	RICOH B/N	192.168.10.2
Fa0/7	SERVIDOR	192.168.10.4

Finalmente, el switch se configurará más tarde con la dirección IP 192.168.10.5, la cual se usará específicamente para tareas de administración de forma remota, con lo que no hará falta emplear la conexión de consola físicamente más cercana al switch.

El modo privilegiado

Los cambios en la configuración del switch se hacen desde el modo privilegiado. Para entrar en este modo es necesario usar el comando “enable”. El prompt del cursor en IOS cambia de modo usuario (símbolo >) a modo privilegiado (símbolo #). A continuación hay que pasar al modo de configuración global, y de aquí, podremos configurar el resto de características específicas del switch (line, interfaces, vlan).

```
Switch>enable
Switch#configure terminal
Switch(config)#
```

Inicialmente, el switch tiene desactivadas las conexiones remotas, por lo que, necesariamente, el primer acceso a la CLI se tiene que hacer a través del cable de consola, es decir, al menos la primera vez es necesaria la presencia física de la persona que instala y configura el switch.

En los switches actuales existe la posibilidad de conectarse a la consola mediante un cable de tipo USB, aunque tradicionalmente se ha usado un cable serie especial denominado *rollover cable*, y que Packet Tracer lo representa con el color azul claro. Este cable comprendía un conector RJ-45 para la conexión al switch y un conector DB-9 para el computador desde el que se accede al switch. Este es el caso de la conexión del ordenador portátil de la administradora. La siguiente figura muestra un cable con conexión serie y otro con conexión USB.

Evitar peticiones a DNS

Conviene desactivar la búsqueda DNS del switch que se activa cuando nos equivocamos en el nombre del comando, ya que se interpreta como un rango de dominio y el switch comienza a buscar un servidor DNS. La manera de hacerlo es mediante la ejecución del siguiente comando.

```
Switch#configure terminal
Switch(config)#no ip domain-lookup
```

Nombre del dispositivo

El switch se configura con el nombre CENTRAL mediante el comando “hostname” en el modo de configuración global.

```
Switch#configure terminal
Switch(config)#hostname CENTRAL
CENTRAL(config)#
```

Versión de IOS y otras características

El comando “show version” permite saber la versión de IOS (Internetwork Operating System) instalado en el switch (12.2), el tiempo que lleva operativo, el número de interfaces Ethernet y el modelo del dispositivo.

```
CENTRAL#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

ROM: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)

System returned to ROM by power-on
```

```
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of memory.

24 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)

63488K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 0002.4A39.BD9D
Motherboard assembly number     : 73-9832-06
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC103248MJ
Power supply serial number      : DCA102133JA
Model revision number           : B0
Motherboard revision number     : C0
Model number                    : WS-C2960-24TT
System serial number            : FOC1033Z1EY
Top Assembly Part Number        : 800-26671-02
Top Assembly Revision Number    : B0
Version ID                      : V02
CLEI Code Number                : COM3K00BRA
Hardware Board Revision Number  : 0x01

Switch    Ports  Model              SW Version            SW Image
------    -----  -----              ----------            ----------
*    1    26     WS-C2960-24TT      12.2                  C2960-LANBASE-M

Configuration register is 0xF
CENTRAL#
```

También podemos ver el modelo concreto de switch (WS-C2960-24TT), el número total de puertos que tiene el dispositivo (26) y su número de serie.

Autenticación del modo privilegiado

Para acceder al modo privilegiado la contraseña es “gca-enable”.

```
CENTRAL#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CENTRAL(config)#enable secret gca-enable
CENTRAL(config)#
```

Esta contraseña especificada mediante el comando “enable secret” es cifrada automáticamente por el switch y almacenada en el fichero “running-config”. El algoritmo de cifrado empleado es MD5 (Message-Digest Algorithm 5), un algoritmo de reducción criptográfica de 128 bits diseñado en 1991, muy empleado actualmente para detectar posibles cambios en ficheros.

Es importante no confundir esta contraseña, que habilita el paso de modo usuario a modo privilegiado y permite el cambio de la configuración del switch, con las que vamos a establecer a continuación y que sirven para habilitar la conexión al switch bien a través de la consola o bien de forma remota.

Precisamente, debido a la importancia de esta contraseña de acceso al modo privilegiado se sugiere usar siempre el comando “enable secret” y evitar el uso del comando parecido “enable password”, dado que este último no cifra la contraseña.

Autenticación para acceso por consola

Para configurar adecuadamente un switch es necesario acceder físicamente a él y emplear la conexión de consola. La contraseña para acceder a través de la consola es “gca-console”.

```
CENTRAL#configure terminal
CENTRAL(config)#line console 0
CENTRAL(config-line)#password gca-console
CENTRAL(config-line)#login
CENTRAL(config)#
```

El comando “login” sirve para que se exija la contraseña al conectarnos al switch a través de la consola.

Autenticación para acceso remoto (telnet, ssh)

Para acceder de forma remota al switch es necesario asignar una dirección IP de gestión, usada solamente para fines administrativos. Para ello hay que crear una interfaz de red virtual (SVI, *Switched Virtual Interface*) en la VLAN 1 (el 1 es el número por defecto de VLAN nativa).

Además de asignarle la dirección IP es necesario habilitar esta interfaz virtual porque inicialmente está deshabilitada. Para ello es preceptivo emplear el comando “no shutdown”.

Por otro lado, el establecimiento de la dirección IP del router que hace de puerta de enlace por defecto (gateway default) es opcional y se lleva a cabo desde el modo de configuración global porque afecta a todo el switch. Este paso es preceptivo cuando hay routers en la red.

```
CENTRAL#configure terminal
CENTRAL(config)#interface vlan 1
CENTRAL(config-if)#ip address 192.168.10.5 255.255.255.0
CENTRAL(config-if)#no shutdown
CENTRAL(config-if)#exit
CENTRAL(config)#ip default-gateway 192.168.10.1
```

Con esta configuración ya sería posible conectarnos al switch de forma remota mediante la aplicación “telnet”.

A continuación queremos que el acceso remoto se permita solamente para el nombre de usuaria “margaret” y su contraseña es “hamilton”. Para ello hay que dar de alta la usuaria en

el switch. Nadie más podrá conectarse remotamente al switch a no ser que se dé de alta previamente.

```
CENTRAL#configure terminal
CENTRAL(config)#username margaret secret hamilton
```

Por otro lado, hay que configurar el acceso remoto para que se autentique por medio de un usuario local al switch. Esto se consigue usando el comando “login local” dentro de la configuración de las líneas remotas (vty).

```
CENTRAL#configure terminal
CENTRAL(config)#line vty 0 15
CENTRAL(config-line)#login local
CENTRAL(config-line)#exit
```

Finalmente, fijamos el tiempo de inactividad de las sesiones remotas a 5 minutos y 30 segundos. Transcurrido este tiempo sin que la persona operadora no haga ninguna operación, el switch desconecta automáticamente la sesión.

```
CENTRAL#configure terminal
CENTRAL(config)#line vty 0 15
CENTRAL(config)#exec-timeout 5 30
```

Si quisiéramos que la sesión no se cerrase nunca se usa el comando con valores 0 para minutos y segundos, aunque esto no es muy recomendable por motivos de seguridad.

```
CENTRAL(config)#exec-timeout 0 0
```

Configuración de banners: MOTD

El mensaje del día (MOTD, message of the day) es “*Mantenimiento previsto del switch a las 14.30 horas*”. Este mensaje aparecerá cuando nos conectemos al switch a través de la consola (línea console) o bien de forma remota (líneas vty). Su función es publicar mensajes temporales que pueden cambiar con el tiempo.

```
CENTRAL#configure terminal
CENTRAL(config)#banner motd #
Enter TEXT message.  End with the character '#'.
Mantenimiento previsto del switch a las 14.30 horas#
CENTRAL(config)#
```

El delimitador es un carácter cualquiera introducido para marcar el inicio y el fin del mensaje. En este caso hemos hecho uso del símbolo “#”, aunque, como acabamos de decir, podríamos haber hecho uso de cualquier otro.

Configuración de la seguridad en interfaces

Las interfaces no utilizadas se deben deshabilitar para mejorar la seguridad. Esta deshabilitación se lleva a cabo mediante el comando “shutdown” aplicado a un rango de interfaces (así evitamos hacer la misma operación muchas veces).

En nuestro caso hay que deshabilitar las interfaces Fa0/8 hasta Fa0/24 ya que no se usan en nuestra red de interconexión.

```
CENTRAL#configure terminal
CENTRAL(config)#interface range fastEthernet 0/8-24
CENTRAL(config-if-range)#shutdown
CENTRAL(config-if-range)#exit
```

Las interfaces de las impresoras (Fa0/5 y Fa0/6) y del servidor (Fa0/7) se configurarán de modo acceso, y solamente permitirán la dirección MAC de estos dispositivos dado que serán siempre fijas y no se espera que cambien con regularidad; en caso de violación de seguridad las interfaces se deshabilitan.

En este caso no es necesario especificar el comando “switchport port-security violation shutdown” porque es la opción por defecto, pero se incluye para mejor claridad y entendemos que es más adecuado que quede de forma expresa en el fichero de configuración del switch.

Importante: las direcciones MAC anteriores puede que **no coincidan** con las del alumnado, por lo que hay que adaptarlas a los valores específicos en cada caso.

```
CENTRAL#configure terminal
CENTRAL(config)#interface FastEthernet0/5
CENTRAL(config-if)#switchport mode access
CENTRAL(config-if)#switchport port-security
CENTRAL(config-if)#switchport port-security mac-address 0006.2A29.BD09
CENTRAL(config-if)#switchport port-security violation shutdown
CENTRAL(config-if)#exit
CENTRAL(config)#interface FastEthernet0/6
CENTRAL(config-if)#switchport mode access
CENTRAL(config-if)#switchport port-security
CENTRAL(config-if)#switchport port-security mac-address 0050.0F06.33E2
CENTRAL(config-if)#switchport port-security violation shutdown
CENTRAL(config-if)#exit
CENTRAL(config)#interface FastEthernet0/7
CENTRAL(config-if)#switchport mode access
CENTRAL(config-if)#switchport port-security
CENTRAL(config-if)#switchport port-security mac-address 0002.4AA7.CC39
CENTRAL(config-if)#switchport port-security violation shutdown
```

Las direcciones MAC de las interfaces de los PC del personal y de la administradora de red (Fa0/1, Fa0/2, Fa0/3 y Fa0/4) se aprenden de manera dinámica y el switch las definirá de forma estática. En caso de violación se descarta el tráfico y se genera una alerta administrativa (modo “restrict”). En este caso se puede aplicar la misma configuración a un rango de interfaces.

```
CENTRAL#configure terminal
CENTRAL(config)#interface range FastEthernet 0/1-4
CENTRAL(config-if)#switchport mode access
CENTRAL(config-if)#switchport port-security
CENTRAL(config-if)#switchport port-security mac-address sticky
CENTRAL(config-if)#switchport port-security violation restrict
```

Violación de la seguridad en una interfaz

Una vez esté toda la topología configurada, se sugiere desconectar el ordenador personal de la administradora y conectar un portátil (LAPTOP HACKER) que haga de intruso en la misma boca del switch para comprobar cómo se gestiona la política de seguridad en el puerto correspondiente.

Cuando el portátil intruso se conecte, el switch detectará que la dirección MAC no es la que tenía guardada en el fichero de configuración y, aunque no desbloquee la interfaz Fa0/1, lo que hará es descartar el tráfico del intruso, al tiempo que envía un mensaje de alerta (esto último no está implementado en el simulador).

Para comprobar el funcionamiento de la restricción del tráfico se sugiere hacer un ping desde el portátil intruso al servidor y comprobar que no hay acceso.

Guardar el fichero de configuración

Un switch Cisco dispone de cuatro tipos de memoria:

- RAM para la configuración en ejecución (“running-config”) y los procesos,
- FLASH para el sistema operativo IOS (permite hacer actualizaciones),
- ROM (programa de inicio o bootstrap) y
- NVRAM (fichero de configuración inicial “startup-config”).

El fichero de configuración “running-config”, presente en la memoria RAM del switch, se debe copiar en el fichero “startup-config”, que se guarda en la memoria NVRAM y es el fichero que se lee cuando se inicializa el dispositivo.

```
CENTRAL#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
CENTRAL#
```

Así mismo, se debe hacer una copia en el servidor por medio del protocolo TFTP. Para poder llevarlo a cabo es necesario activar, si no lo está ya, este servicio de transferencia de ficheros en el servidor. El fichero guardado en el servidor se llamará "CENTRAL-running-config". Una vez realizada la transferencia es recomendable comprobar que el fichero se ha copiado satisfactoriamente en el servidor.

```
CENTRAL#copy running-config tftp:
Address or name of remote host []? 192.168.10.4
Destination filename [CENTRAL-confg]? CENTRAL-running-config

Writing running-config....!!
[OK - 2366 bytes]

2366 bytes copied in 3.037 secs (779 bytes/sec)
CENTRAL#
```

Servicio de encriptación de contraseñas

Es muy recomendable activar el servicio de encriptación de contraseñas para que no aparezcan como texto plano en los ficheros de configuración del switch. El comando para llevarlo a cabo, dentro del modo de configuración global, es el siguiente:

```
CENTRAL(config)#service password-encryption
```

Lo que hace este servicio es cifrar las contraseñas presentes en el archivo de configuración "running-config" para el acceso por consola y por líneas vty, que anteriormente figuraban como texto plano. Mientras se mantenga activo este servicio todas las contraseñas creadas serán almacenadas con cifrado. La desactivación del servicio simplemente indica que las contraseñas que se creen a partir de ese momento no se cifrarán, pero las que ya hubiera cifradas se quedarán como están.

El objetivo es dotar siempre al switch de la máxima seguridad posible, por lo que la habilitación de este servicio se considera una buena práctica.