UD3. Configuracion de Switches CISCO

Índice

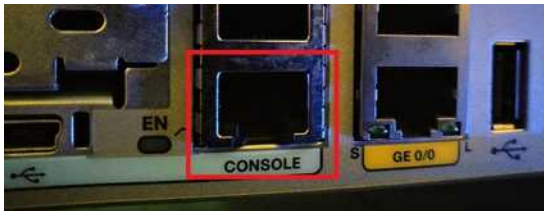
Conexión y modos del conmutador

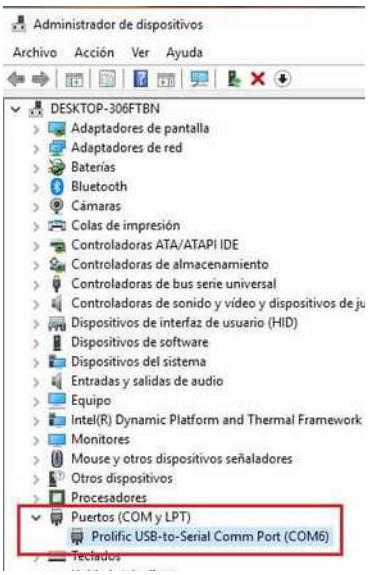
IOS es el S.O de Cisco se maneja fundamentalmente por comandos. Sin embargo, cuando encendemos un switch/router por primera vez, no es posible acceder a ese sistema. Necesitamos proporcionar una configuración inicial. Y para ello, usaremos casi con toda seguridad el cable de consola.

El cable de consola es un cable propio de Cisco y por un lado usa una conexión propia de Cisco y en el otro extremos puede ser:

- USB (hoy en día lo más probable)
- RS-232 (aún muy utilizado, pero está cayendo en desuso)
- RJ-45 (depende del dispositivo)

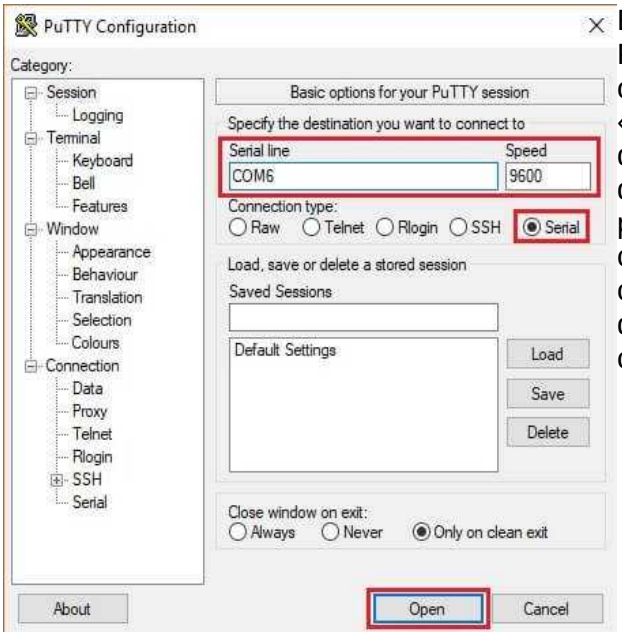
Si nuestro PC no tiene conexión DB9/RS232 vamos a necesitar algún tipo de conversor de DB9/RS232 a USB y bajar los drivers de aquí https://www.youtube.com/watch?v=jIRRsIgfHU8





Una vez todo conectado como el esquema y el router alimentado, nos iremos al PC y suponiendo que

tenemos Windows 10, haremos 'click' con el botón derecho del ratón en el menú de inicio y nos iremos a "Administrador de dispositivos": En la nueva ventana nos iremos al apartado "Puertos (COM y LPT)" y dentro buscaremos el cable USB-Serial, pero sobre todo nos fijaremos el puerto COM que aparece entre paréntesis. En nuestro caso el "COM6".



Este puerto es el que usaremos para conectarnos. Para acceder al sistema operativo necesitaremos un ordenador en el que haya algún programa de tipo «Terminal». Este programa enviará los datos directamente al dispositivo (sin direcciones de origen ni de destino ni nada). Para ello bastará con abrir un programa que nos permita establecer una conexión por consola. Usraemos PuTTY. Así que lo abriremos y lo configuraremos de la siguiente manera: Es vital saber qué velocidades acepta el dispositivo al que nos conectamos. En el caso Cisco, es casi sin excepción:

- Velocidad: 9600 bits por segundo.
- Tamaño de los caracteres de datos: 8 bits.
- Paridad. Es un mecanismo de comprobación de comprobación de errores. Los dispositivos Cisco no usan paridad.
- Bits de stop. En Cisco se usa 1 bits de stop.
- Control de flujo/velocidad. No se usará ninguno.

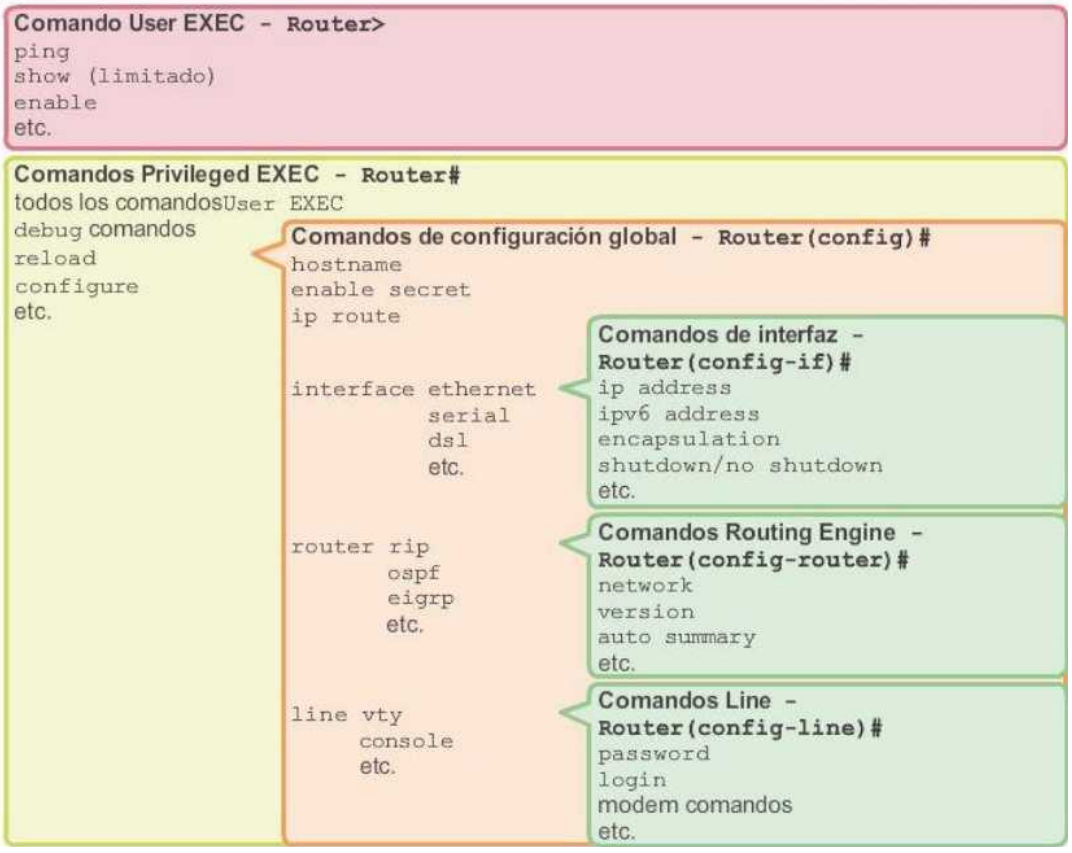
En ocasiones se puede ver algo como 96008N1N. Esto significa «9600 bits/seg», «8 bits de datos», «No paridad», «1 bit de stop» y «No control de flujo».

Una vez que tenemos acceso al sistema operativo, debemos recordar que IOS es un sistema operativo modal.

El sistema operativo arranca en modo usuario. En ese modo lo único que se suele poder hacer es «visualizar», pero no «cambiar» ni «configurar». En suma, se usa el comando **show**

Para pasar al modo «privilegiado» se usa el comando **enable**. Lo normal es que dicho modo tenga una clave. Para volver al modo usuario podemos usar **disable**.

Para pasar al modo «configuración» se usa **configure terminal** desde el modo privilegiado.



El modo usuario

En este modo solo se pueden usar unos pocos comandos show. Por ejemplo:

`show interfaces` muestra la información de todos los interfaces.
`show interfaces Fastethernet 0/1` muestra solo la tarjeta 0/1

Modo privilegiado

Comandos muy típicos:

`show running-config` muestra la configuración en RAM.
`show startup-config` muestra la configuración de arranque.
`show version` muestra información de versión del sistema operativo, número de serie y dirección MAC base (la que usa el switch para comunicarse con otros por ejemplo)
`copy running-config startup-config`. Graba la configuración actual del switch

clock	Comprobación de la fecha y la hora del sistema
ip interface brief	Para ver el estado de las interfaces
interfaces	Muestra información detallada de cada interfaz
logging	Comprueba el estado del registro *syslog*
mac-address-table	Visualiza la tabla MAC
privilege	Para ver el nivel de privilegio del *switch*
running-config	Muestra la configuración actual del dispositivo
sessions	Monitoriza las conexiones remotas activas
spanning-tree	Visualiza la configuración STP del *switch*
terminal	Muestra los parámetros de configuración del terminal
version	Visualiza los parámetros de estado HW y SW del dispositivo
vlan	Comprueba la configuración de las VLAN del *switch*

Modo de configuración global:

`hostname <nombre>`

Configuración parámetros iniciales

Una vez que se enciende el switch Cisco, lleva a cabo la siguiente secuencia de arranque:

1. Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.

2. A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.

3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.

4. El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.

5. Por último, el cargador de arranque ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al IOS.

El cargador de arranque busca la imagen de Cisco IOS en el switch de la siguiente manera: el switch intenta arrancar automáticamente mediante la información de la variable de entorno BOOT. Si no se establece esta variable, el switch intenta cargar y ejecutar el primer archivo ejecutable que puede mediante una búsqueda recursiva y en profundidad en todo el sistema de archivos flash. Cuando se realiza una búsqueda en profundidad de un directorio, se analiza por completo cada subdirectorio que se encuentra antes de continuar la búsqueda en el directorio original. En los switches de la serie Catalyst 2960, el archivo de imagen generalmente se encuentra en un directorio que tiene el mismo nombre que el archivo de imagen (excepto la extensión de archivo .bin).

Luego, el sistema operativo IOS inicia las interfaces mediante los comandos del IOS de Cisco que se encuentran en el archivo de configuración, startup-config, que está almacenado en NVRAM.

CDP

switch# **show cdp neighbors**
switch # **no cdp run**
switch(config-interface)# **no cdp enable**

Recuperación tras un bloqueo del sistema

El cargador de arranque proporciona acceso al switch si no se puede usar el sistema operativo debido a la falta de archivos de sistema o al daño de estos. El cargador de arranque tiene una línea de comandos que proporciona acceso a los archivos almacenados en la memoria flash.

Se puede acceder al cargador de arranque mediante una conexión de consola con los siguientes pasos:

Paso 1. Conecte una computadora al puerto de consola del switch con un cable de consola. Configure el software de emulación de terminal para conectarse al switch.

Paso 2. Desconecte el cable de alimentación del switch.

Paso 3. Vuelva a conectar el cable de alimentación al switch, espere 15 segundos y, a continuación, presione y mantenga presionado el botón **Mode** (Modo) mientras el LED del sistema sigue parpadeando con luz verde.

Paso 4. Continúe oprimiendo el botón **Modo** hasta que el LED del sistema se torne ámbar por un breve instante y luego verde, después suelte el botón **Modo**.

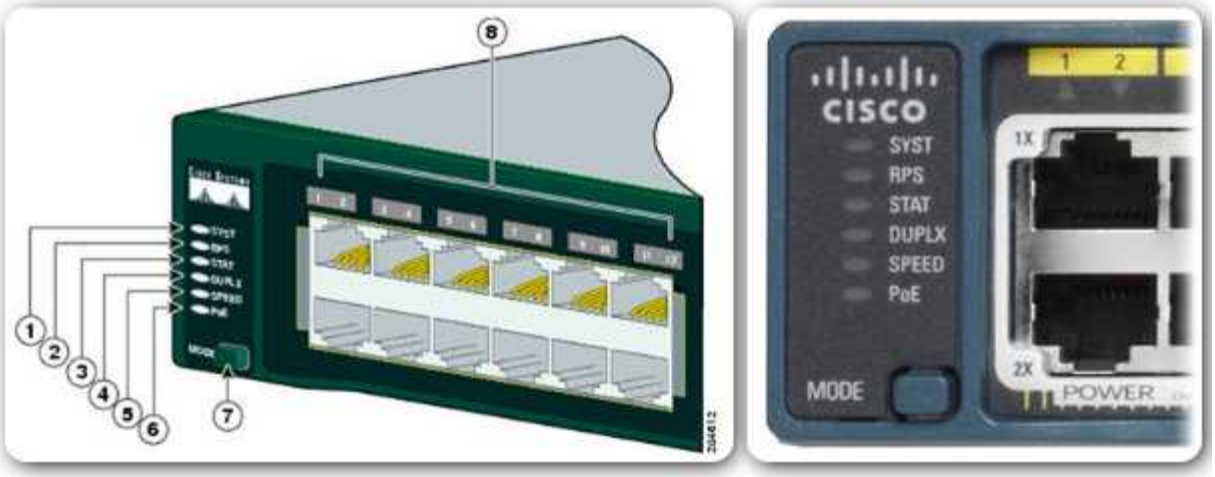
Paso 5. Aparece la petición de entrada **switch:** del cargador de arranque en el software de emulación de terminal en la computadora.

La línea de comandos de **boot loader** admite comandos para formatear el sistema de archivos flash, volver a instalar el software del sistema operativo y recuperarse de la pérdida o el olvido de una contraseña. Por ejemplo, el comando **dir** se puede usar para ver una lista de archivos dentro de un directorio específico.

```
switch: dir flash:
Directory of flash:/
 3 -rwx 1839 Mar 01 2002 00:48:15 config.text
11 -rwx 1140 Mar 01 2002 04:18:48 vlan.dat
21 -rwx 26 Mar 01 2002 00:01:39 env_vars
 9 drwx 768 Mar 01 2002 23:11:42 html
16 -rwx 1037 Mar 01 2002 00:01:11 config.text
14 -rwx 1099 Mar 01 2002 01:14:05 homepage.htm
22 -rwx 96 Mar 01 2002 00:01:39 system_env_vars
17 drwx 192 Mar 06 2002 23:22:03 c2960-lanbase-mz.122-25.FX

15998976 bytes total (6397440 bytes free)
```

Indicadores LED de los switches



LED del switch Catalyst 2960			
1	LED del sistema	5	LED de velocidad del puerto
2	LED de RPS (si el switch admite RPS)	6	LED de estado de alimentación por Ethernet (si el switch la admite)
3	LED de estado del puerto (este es el modo predeterminado)	7	Botón Mode
4	LED de modo dúplex del puerto	8	LED del puerto

En la ilustración, se muestran los LED y el botón Mode de un switch Cisco Catalyst 2960. El botón Mode se utiliza para alternar entre el estado del puerto, el modo dúplex del puerto, la velocidad del puerto y el estado de alimentación por Ethernet (PoE [si se admite]) de los LED del puerto. A continuación, se describe el propósito de los indicadores LED y el significado de los colores:

- **LED del sistema:** muestra si el sistema recibe alimentación y funciona correctamente. Si el LED está apagado, significa que el sistema no está encendido. Si el LED es de color verde, el sistema funciona normalmente. Si el LED es de color ámbar, el sistema recibe alimentación pero no funciona correctamente.
- **LED del sistema de alimentación redundante (RPS):** muestra el estado del RPS. Si el LED está apagado, el RPS está apagado o no se conectó correctamente. Si el LED es de color verde, el RPS está conectado y listo para proporcionar alimentación de respaldo. Si el LED parpadea y es de color verde, el RPS está conectado pero no está disponible porque está proporcionando alimentación a otro dispositivo. Si el LED es de color ámbar, el RPS está en modo de reserva o presenta una falla. Si el LED parpadea y es de color ámbar, la fuente de alimentación interna del switch presenta una falla, y el RPS está proporcionando alimentación.
- **LED de estado del puerto:** cuando el LED es de color verde, indica que se seleccionó el modo de estado del puerto. Éste es el modo predeterminado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, no hay

enlace, o el puerto estaba administrativamente inactivo. Si el LED es de color verde, hay un enlace presente. Si el LED parpadea y es de color verde, hay actividad, y el puerto está enviando o recibiendo datos. Si el LED alterna entre verde y ámbar, hay una falla en el enlace. Si el LED es de color ámbar, el puerto está bloqueado para asegurar que no haya un bucle en el dominio de reenvío y no reenvía datos (normalmente, los puertos permanecen en este estado durante los primeros 30 segundos posteriores a su activación). Si el LED parpadea y es de color ámbar, el puerto está bloqueado para evitar un posible bucle en el dominio de reenvío.

- **LED de modo dúplex del puerto:** cuando el LED es de color verde, indica que se seleccionó el modo dúplex del puerto. Al seleccionarlo, los LED del puerto que están apagados están en modo half-duplex. Si el LED del puerto es de color verde, el puerto está en modo full-duplex.
- **LED de velocidad del puerto:** indica que se seleccionó el modo de velocidad del puerto. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, el puerto funciona a 10 Mb/s. Si el LED es de color verde, el puerto funciona a 100 Mb/s. Si el LED parpadea y es de color verde, el puerto funciona a 1000 Mb/s.
- **LED de modo de alimentación por Ethernet**: si se admite alimentación por Ethernet, hay un LED de modo de PoE. Si el LED está apagado, indica que no se seleccionó el modo de alimentación por Ethernet, que a ninguno de los puertos se le negó el suministro de alimentación y ninguno presenta fallas. Si el LED parpadea y es de color ámbar, no se seleccionó el modo de alimentación por Ethernet, pero al menos a uno de los puertos se le negó el suministro de alimentación o uno de ellos presenta una falla de alimentación por Ethernet. Si el LED es de color verde, indica que se seleccionó el modo de alimentación por Ethernet, y los LED del puerto muestran colores con diferentes significados. Si el LED del puerto está apagado, la alimentación por Ethernet está desactivada. Si el LED del puerto es de color verde, la alimentación por Ethernet está activada. Si el LED del puerto alterna entre verde y ámbar, se niega la alimentación por Ethernet, ya que, si se suministra energía al dispositivo alimentado, se excede la capacidad de alimentación del switch. Si el LED parpadea y es de color ámbar, la alimentación por Ethernet está desactivada debido a una falla. Si el LED es de color ámbar, se inhabilitó la alimentación por Ethernet para el puerto.

Poner una IP de gestión a un switch

De manera predeterminada, el switch está configurado para que el control de la administración del switch se realice mediante la VLAN 1. Todos los puertos se asignan a la VLAN 1 de manera predeterminada. El propósito de esta configuración IP es solamente obtener acceso a la administración remota del switch; la configuración IP no permite que el switch enrute paquetes.

```
#Nos convertimos en administrador
      Switch>enable
#Pasamos al modo de configuración global
      Switch#configure terminal
#Entramos en la VLAN nativa
      Switch(config)#interface vlan 1
#Ponemos una IP y activamos la interfaz
      Switch(config-if)#ip address 192.168.1.2 255.255.255.0
      Switch(config-if)#no shutdown
```

ingresamos al modo de configuración de interfaz.

Configura IP

Habilita la interfaz

Pese a lo anterior, por motivos de seguridad, se recomienda usar una VLAN de administración distinta de la VLAN 1.

En este ejemplo, la VLAN 99 se configura con la dirección IP 172.17.99.11.

La SVI para la VLAN 99 no se muestra como “up/up” hasta que se cree la VLAN 99 y haya un dispositivo conectado a un puerto del switch asociado a la VLAN 99. Para crear una VLAN con la id_de_vlan 99 y asociarla a una interfaz, use los siguientes comandos:

S1(config)# **vlan** *id_de_vlan*
S1(config-vlan)# **name** *nombre_de_vlan*
S1(config-vlan)# **exit**
S1(config)# **interface** *interface_id*
S1(config-if)# **switchport access vlan** *id_de_vlan*

Ingrese al modo de configuración global.	S1# configure terminal
Ingresa al modo de configuración de interfaz para la SVI.	S1(config)# interface vlan 99
Configura la dirección IP de la interfaz de administración.	S1(config-if)# ip address 172.17.99.11 255.255.0.0
Habilita la interfaz de administración.	S1(config-if)# no shutdown
Vuelve al modo EXEC privilegiado.	S1(config-if)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado. El gateway predeterminado es el router al que está conectado el switch. El switch reenvía los paquetes IP con direcciones IP de destino fuera de la red local al gateway predeterminado.

Para configurar el gateway predeterminado del switch, use el comando **ip default-gateway**. Introduzca la dirección IP del gateway predeterminado. El gateway predeterminado es la dirección IP de la interfaz del router a la que está conectado el switch. Use el comando **copy running-config startup-config** para realizar una copia de seguridad de la configuración.

Ingrese al modo de configuración global.	S1# configure terminal
Configura el gateway predeterminado del switch.	S1(config)# ip default-gateway 172.17.99.1
Vuelve al modo EXEC privilegiado.	S1(config)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Para verificar la configuración usamos **show ip interface brief**

Configuración de contraseñas

Se puede poner contraseña a un montón de elementos:

- Contraseña al cable de consola.
- Contraseña de administrador para el modo privilegiado.
- Contraseña al telnet.
- Contraseña SSH.
- Contraseña al puerto auxiliar.

Para poner contraseña a la conexión por cable de consola:

```
Switch>enable
Switch#configure terminal
Switch(config)#line console 0
Switch(config-line)#password sesamo1234
Switch(config-line)#login
```

En lugar de las dos líneas anteriores, puedo poner **login local** para que haya que logarse con un usuario local. Primero deberé haber creado el usuario **username nombre-de-usuario secret contraseña**.

```
Switch(config)#line console 0
Switch(config-line)#username admin secret sesamo1234
Switch(config-line)#login local
```

También podemos poner un timeout de tal forma que si está un tiempo sin teclear nada se cierre la consola. Usamos **exec-timeout minutos**

Switch(config-line)# **exec-timeout 30**

Podemos habilitar el logging síncrono lo que nos permite que si somos interrumpidos por la sallida de un comando mientras estamos tecleando el siguiente nos lo pone en una línea nueva, lo que nos hace la vida más fácil

Switch(config-line)# **logging synchronous**

Para poner una clave al modo de administrador:

```
Switch>enable
Switch#configure terminal
Switch(config)#enable secret Admin1234!
Switch(config)#exit
Switch#copy running-config startup-config
Switch#reload
Switch#service password-encryption
```

El comando Cisco fue durante mucho tiempo «enable password» y de hecho **el comando sigue funcionando**. Sin embargo, `enable password` guarda las claves en la memoria **SIN CIFRAR**.

Hay switches en los que podemos elegir el hash entre MD5 o 9 (scrypt) para ello

Switch(config)# **enable ?**

Aprecerán las opciones password, secret y si está disponible algorithm-type por lo que podremos poner

Switch(config)# **enable algorithm-type scrypt secret admin1234!**

Con **show run | i secret** veremos el número de algoritmo hash que usamos

Acceso por Telnet

Para poner contraseña a Telnet el procedimiento es bastante parecido a lo ya visto:

```
#Nos convertimos en administrador
      Switch>enable
#Pasamos al modo de configuración global
      Switch#configure terminal
#Seleccionamos las conexiones
      Switch(config)#line vty 0 15
#Ponemos una clave de acceso a estas conexiones
      password clave1234!
#Con esto se exigirá el uso de la clave
      login
```

Acceso por SSH

Shell seguro (SSH) es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto. SSH debe reemplazar a Telnet para las conexiones de administración. Telnet es un protocolo más antiguo que usa la transmisión no segura de texto no cifrado de la autenticación de inicio de sesión (nombre de usuario y contraseña) y de los datos transmitidos entre los dispositivos que se comunican. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro cuando se autentica un dispositivo (nombre de usuario y contraseña) y también para los datos transmitidos entre los dispositivos que se comunican. SHH se asigna al puerto TCP 22. Telnet se asigna al puerto TCP 23.

Para habilitar SSH en un switch Catalyst 2960, el switch debe usar una versión del software IOS que incluya características y capacidades criptográficas (cifradas). En la figura 5, use el comando show version en el switch para ver qué IOS se ejecuta actualmente en el dispositivo y el nombre de archivo de IOS que incluye la combinación “k9” que admite características y capacidades criptográficas (cifradas).

Antes de configurar SSH, el switch debe tener configurado, como mínimo, un nombre de host único y los parámetros correctos de conectividad de red.

Paso 1. Verificar la compatibilidad con SSH

Use el comando **show ip ssh** para verificar que el switch admita SSH. Si el switch no ejecuta un IOS que admita características criptográficas, este comando no se reconoce.

Paso 2. Configurar el dominio IP

Configure el nombre de dominio IP de la red mediante el comando **ip domain-name nombre-de-dominio** del modo de configuración global. Configurar claves públicas de un nodo

Los comandos serían estos para configurar las claves públicas de un nodo:

```
ip domain-name midominio.com
```

Paso 3. Generar pares de claves RSA

```
crypto key generate rsa general-keys modulus 2048
```

No todas las versiones del IOS utilizan la versión 2 de SSH de manera predeterminada, y la versión 1 de SSH tiene fallas de seguridad conocidas. Para configurar la versión 2 de SSH, emita el comando **ip ssh version 2** del modo de configuración global. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando crypto key generate rsa del modo de configuración global para habilitar el servidor SSH en el switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. Cisco recomienda un tamaño de módulo mínimo de 1024 bits. Una longitud de módulo mayor es más segura, pero se tarda más. Para eliminar el par de claves RSA, use el comando crypto key zeroize rsa del modo de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

```
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

Paso 4. Configurar la autenticación de usuario

El servidor SSH puede autenticar a los usuarios localmente o con un servidor de autenticación. Para usar el método de autenticación local, cree un nombre de usuario y una contraseña con el comando del modo de configuración global **username nombre-de-usuario secret contraseña**. En el ejemplo, se asignó la contraseña ccna al usuario admin.

Show run | in secret veremos el número de MD5 o 9 del algoritmo hash que estamos usando

Igual que para el enable, podemos teclear **username nombre ?** Y ver si tenemos la opción de algorithm-type para la password del usuario

Paso 5. Configurar las líneas vty

Habilite el protocolo SSH en las líneas vty mediante el comando transport input ssh del modo de configuración de línea. El switch Catalyst 2960 tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al switch a que acepte solo las conexiones SSH. Use el comando line **vty** del modo de configuración global y, luego, el comando **login local** del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

Paso 6. Habilitar la versión 2 de SSH.

De manera predeterminada, SSH admite las versiones 1 y 2. Si se admiten ambas versiones, en el resultado de show ip ssh se muestra que se admite la versión 1.99. La versión 1 tiene vulnerabilidades conocidas. Por esta razón, se recomienda habilitar únicamente la versión 2. Habilite la versión de SSH mediante el comando de configuración global **ip ssh version 2.**

Configuración puertos en capa física

duplex y velocidad

Los puertos de switch se pueden configurar manualmente con parámetros específicos de dúplex y de velocidad. Use el comando **duplex** del modo de configuración de interfaz para especificar manualmente el modo dúplex de un puerto de switch. Use el comando **speed** del modo de configuración de interfaz para especificar manualmente la velocidad de un puerto de switch. En l puerto F0/1 de los switches S1 y S2 se configura manualmente con la palabra clave **full** para el comando **duplex** y la palabra clave **100** para el comando **speed**.

Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese el modo de configuración de interfaz.	`S1(config)# interface FastEthernet 0/1`
Configura el modo dúplex de la interfaz.	`S1(config-if)# duplex full`
Configura la velocidad de la interfaz.	`S1(config-if)# speed 100`
Vuelve al modo EXEC privilegiado.	`S1(config-if)# end`
Guarda la configuración en ejecución en la configuración de inicio.	`S1# copy running-config startup-config`

La configuración predeterminada de dúplex y velocidad para los puertos de switch en los switches Cisco Catalyst 2960 y 3560 es automática. Los puertos 10/100/1000 funcionan en el modo half-duplex o full-duplex cuando se establecen en 10Mb/s o 100Mb/s, y en modo full-duplex cuando se establecen en 1000Mb/s. La autonegociación es útil cuando se desconoce la configuración de dúplex y de velocidad del dispositivo que se conecta al puerto o cuando es posible que cambie. Al conectarse a dispositivos conocidos se recomienda establecer manualmente la configuración de dúplex y de velocidad.

MDI-MDIX

Hasta hace poco, se requerían determinados tipos de cable (cruzado o directo) para conectar dispositivos. Las conexiones switch a switch o switch a router requerían el uso de diferentes cables Ethernet. Mediante el uso de la característica automática de conexión cruzada de interfaz dependiente del medio (auto-MDIX) en una interfaz, se elimina este problema. Al habilitar la característica auto-MDIX, la interfaz detecta automáticamente el tipo de conexión de cable requerido (directo o cruzado) y configura la conexión conforme a esa información. Al conectarse a los switches sin la característica auto-MDIX, se deben usar cables directos para conectarse a dispositivos como servidores, estaciones de trabajo o routers, y cables cruzados para conectarse a otros switches o repetidores.

Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese el modo de configuración de interfaz.	`S1(config)# interface fastethernet 0/1`
Configura la interfaz para autonegociar la comunicación dúplex con el dispositivo conectado.	`S1(config-if)# duplex auto`
Configura la interfaz para autonegociar la velocidad con el dispositivo conectado.	`S1(config-if)# speed auto`
Habilita auto-MDIX en la interfaz.	`S1(config-if)# mdix auto`
Vuelve al modo EXEC privilegiado.	`S1(config-if)# end`
Guarda la configuración en ejecución en la configuración de inicio.	`S1# copy running-config startup-config`

Con la característica auto-MDIX habilitada, se puede usar cualquier tipo de cable para conectarse a otros dispositivos, y la interfaz se ajusta de manera automática para proporcionar comunicaciones satisfactorias. En los routers y switches Cisco más modernos, el comando mdix auto del modo de configuración de interfaz habilita la característica. Cuando se usa auto-MDIX en una interfaz, la velocidad y el modo dúplex de la interfaz se deben establecer en auto para que la característica funcione correctamente.

La característica auto-MDIX está habilitada de manera predeterminada en los switches Catalyst 2960 y Catalyst 3560, pero no está disponible en los switches más antiguos Catalyst 2950 y Catalyst 3550.

Para examinar la configuración de auto-MDIX de una interfaz específica, use el comando show controllers ethernet-controller con la palabra clave phy y el filtro include Auto-MDIX. El resultado indica On (Habilitada) u Off (Deshabilitada)

```
S1# show controllers ethernet-controller fa 0/1 phy |
 include Auto-MDIX
 Auto-MDIX     :  On   [AdminState=1   Flags=0x00056248]
S1#
```

Configuración de puertos de un switch

A continuación se describen algunas de las opciones del comando show que son útiles para verificar las características configurables comunes de un switch.

El comando show interfaces es otro comando de uso frecuente que muestra información estadística y de estado sobre las interfaces de red del switch. El comando show interfaces se usa habitualmente cuando se configuran y se controlan los dispositivos de red.

Muestra el estado y la configuración de la interfaz.	S1# **show interfaces** [*id-interfaz*]
Muestra la configuración de inicio actual.	S1# **show startup-config**
Muestra la configuración de funcionamiento actual.	S1# **show running-config**
Muestra información sobre el sistema de archivos flash.	S1# **show flash**
Muestra el estado del hardware y el software del sistema.	S1# **show version**
Muestra el historial de comandos introducidos.	S1# **show history**
Muestra información de IP de una interfaz.	S1# **show ip** [*id-interfaz*]
Muestra la tabla de direcciones MAC.	S1# **show mac-address-table** O S1# **show mac address-table**

Como ejemplo se muestra el resultado del comando show interfaces fastEthernet 0/18. En la primera línea de la ilustración, se indica que la interfaz FastEthernet 0/18 está “up/up”, lo que significa que está en funcionamiento. Más abajo en el resultado, se muestra que el modo dúplex es full y la velocidad es de 100 Mb/s.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01
(bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is
unsupported
```

Configuración de la tabla MAC

ver la tabla MAC

Para visualizar la tabla de direcciones MAC de un switch se pueden emplear varios comandos Cisco IOS. Por ejemplo, se puede solicitar la tabla completa (o las entradas que han sido generadas exclusivamente de forma estática)

```
switch> enable
switch# show mac-address-table
switch# show mac-address-table static
```

Borrar la tabla MAC

También puede borrarse la tabla completa (o solo las entradas generadas de forma dinámica):

```
switch# clear mac-address-table
switch# clear mac-address-table dynamic
```

También es posible modificar el tiempo de borrado automático de las entradas de la tabla e incluso asignar de forma estática o permanente una entrada concreta:

```
switch> enable
switch# configure terminal
switch (config)# mac-address-table aging-time <segundos>
```

Técnicamente el nombre es «aging» (envejecimiento) pero es muy frecuente oír simplemente «timeout de una entrada».

Para configurar el «timeout» se debe pasar al modo de configuración global y despues entrar en la VLAN para la que queramos cambiar el tiempo. Así, por ejemplo, para cambiar el tiempo que mantenemos algo en la caché ARP a 60 segundos usaremos esto:

```
switch>enable
switch#configure terminal
switch (config)#interface vlan 1
switch (config)#arp timeout 60
switch (config)#no shutdown
```

Asignación estática de una MAC a un puerto

Hay que recordar que en este comando se debe usar obligatoriamente la VLAN. Si no hemos creado ninguna se usa la VLAN por defecto que es la 1. Si por ejemplo queremos indicar que una cierta MAC va enganchada a un cierto puerto podemos usar:

```
switch (config)# mac-address-table static <MAC> vlan <n> interface <N>
switch (config)# mac address-table static 00aa.1122.ccdd vlan 1 interface fastethernet0/3
switch (config)# mac-address-table permanent [MAC] [interface]
```

Borrado de una entrada MAC en la tabla del switch

Es tan sencillo como «negar» el comando anterior. Es decir, tecleamos lo mismo pero poniendo delante un no:

```
switch (config)#no mac address-table static 00aa.1122.ccdd vlan 1 interface fastethernet0/3
```

Trabajo con VLANS

Al configurar redes VLAN de rango normal, los detalles de configuración se almacenan en la memoria flash del switch en un archivo denominado vlan.dat. La memoria flash es persistente y no requiere el comando copy running-config startup-config. Sin embargo, debido a que en los switches Cisco se suelen configurar otros detalles al mismo tiempo que se crean las VLAN, es aconsejable guardar los cambios a la configuración en ejecución en la configuración de inicio.

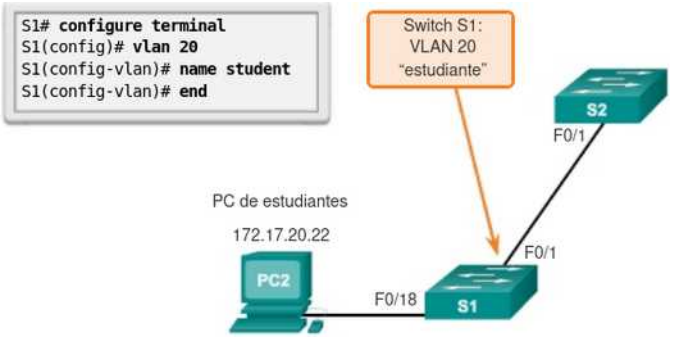
Crear una VLAN

En la figura, se muestra la sintaxis del comando de IOS de Cisco que se utiliza para agregar una VLAN a un switch y asignarle un nombre. Se recomienda asignarle un nombre a cada VLAN en la configuración de un switch.

Ingrese al modo de configuración global.	`S1# configure terminal`
Cree una VLAN con un número de ID válido.	`S1(config)#vlan id-vlan`
Especifique un nombre único para identificar la VLAN.	`S1(config-vlan)#name nombre-vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-vlan)# end`

En la figura se muestra cómo se configura la VLAN para estudiantes (VLAN 20) en el switch S1. En el ejemplo de topología, la computadora del estudiante (PC2) todavía no se asoció a ninguna VLAN, pero tiene la dirección IP 172.17.20.22.

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```



Con el comando **show vlan brief** podemos mostrar el contenido del archivo vlan.dat.

Además de introducir una única ID de VLAN, se puede introducir una serie de ID de VLAN separadas por comas o un rango de ID de VLAN separado por guiones con el comando vlan *id-vlan*. Por ejemplo, utilice el siguiente comando para crear las VLAN 100, 102, 105, 106 y 107:

S1(config)# vlan 100,102,105-107

Asignar una IP a la VLAN

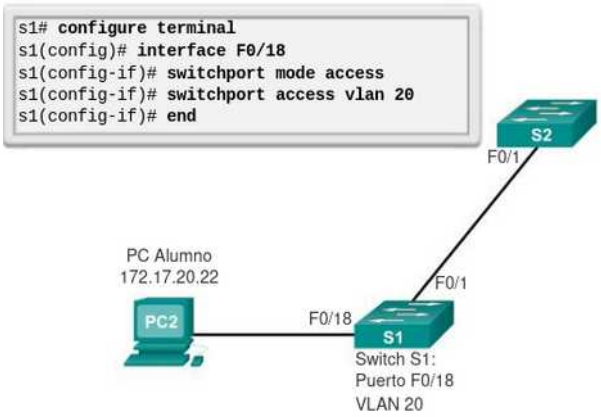
Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Un puerto de acceso puede pertenecer a una sola VLAN por vez; una excepción a esta regla es un puerto conectado a un teléfono IP, en cuyo caso, hay dos VLAN asociadas al puerto: una para voz y otra para datos.

Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface id_interfaz`
Establezca el puerto en modo de acceso.	`S1(config-if)# switchport mode access`
Asigne el puerto a una VLAN.	`S1(config-if)# switchport access vlan id_vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

En la figura se muestra la sintaxis para definir un puerto como puerto de acceso y asignarlo a una VLAN. El comando switchport mode access es optativo, pero se aconseja como práctica recomendada de seguridad. Con este comando, la interfaz cambia al modo de acceso permanente.

Nota: utilice el comando interface range para configurar varias interfaces simultáneamente.

En el ejemplo de la figura, la VLAN 20 se asigna al puerto F0/18 del switch S1; por lo tanto, la computadora de estudiantes (PC2) está en la VLAN 20. Cuando se configura la VLAN 20 en otros switches, el administrador de red sabe que debe configurar las otras computadoras de estudiantes para que estén en la misma subred que la PC2 (172.17.20.0/24).



El comando switchport access vlan fuerza la creación de una VLAN si es que aún no existe en el switch. Por ejemplo, la VLAN 30 no está presente en el resultado del comando show vlan brief del switch. Si se introduce el comando switchport access vlan 30 en cualquier interfaz sin configuración previa, el switch muestra lo siguiente:

% Access VLAN does not exist. Creating vlan 30

Cambio de puertos asignados a una VLAN

Existen varias maneras de cambiar la pertenencia de puertos de una VLAN. En la figura, se muestra la sintaxis para cambiar la pertenencia de un puerto de switch de la VLAN 1 con el comando no switchport access vlan del modo de configuración de interfaz.

Ingrese al modo de configuración global.	S1# **configure terminal**
Elimine la asignación de la VLAN del puerto.	S1(config-if)# **no switchport access vlan**
Vuelva al modo EXEC privilegiado.	S1(config-if)# **end**

La interfaz F0/18 se asignó anteriormente a la VLAN 20. Se introduce el comando no switchport access vlan para la interfaz F0/18. Examine el resultado del comando show vlan brief que le sigue inmediatamente, como se muestra en la figura. El comando show vlan brief muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. El comando **show vlan brief** muestra una línea para cada VLAN. El resultado para cada VLAN incluye el nombre, el estado y los puertos de switch de la VLAN.

```
S1(config)# int fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name              Status    Ports
---- ----------------- --------- -------------------------------
1    default           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                 Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                 Gi0/1, Gi0/2
20   student           active
1002 fddi-default      act/unsup
```

La VLAN 20 sigue activa, aunque no tenga puertos asignados. El resultado del comando show interfaces f0/18 switchport verificaría que la VLAN de acceso para la interfaz F0/18 se haya restablecido a la VLAN 1.

La pertenencia de VLAN de un puerto se puede cambiar fácilmente. No es necesario eliminar primero un puerto de una VLAN para cambiar su pertenencia de VLAN. Cuando se vuelve a asignar la pertenencia de VLAN de un puerto de acceso a otra VLAN existente, la nueva pertenencia de VLAN simplemente reemplaza la pertenencia de VLAN anterior. En la figura, el puerto F0/11 se asignó a la VLAN 20.

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name                 Status     Ports
---- -------------------- ---------- ------------------------------
1    default              active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                     Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                     Fa0/9, Fa0/10, Fa0/12, Fa0
                                     Fa0/14, Fa0/15, Fa0/16, Fa
                                     Fa0/18, Fa0/19, Fa0/20, Fa
                                     Fa0/22, Fa0/23, Fa0/24, Gi
                                     Gi0/2
20   student              active     Fa0/11
```

Eliminación de una VLAN

En la ilustración, se utiliza el comando **no vlan id-vlan** del modo de configuración global para eliminar la VLAN 20 del switch. El switch S1 tenía una configuración mínima con todos los puertos en la VLAN 1 y una VLAN 20 sin usar en la base de datos de VLAN. El comando show vlan brief verifica que la VLAN 20 ya no esté presente en el archivo vlan.dat después de utilizar el comando no vlan 20.

Precaución: antes de eliminar una VLAN, asegúrese de reasignar primero todos los puertos miembro de una VLAN a otra. Los puertos que no se trasladen a una VLAN activa no se podrán comunicar con otros hosts una vez que se elimine la VLAN y hasta que se asignen a una VLAN activa.

```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name                 Status    Ports
---- -------------------- --------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                    Fa0/9, Fa0/10, Fa0/12, Fa0/13
                                    Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                    Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                    Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                    Gi0/2
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

Alternativamente, se puede eliminar el archivo vlan.dat completo con el comando delete flash:vlan.dat del modo EXEC privilegiado. Se puede utilizar la versión abreviada del comando (delete vlan.dat) si no se trasladó el archivo vlan.dat de su ubicación predeterminada. Después de emitir este comando y de volver a cargar el switch, las VLAN configuradas anteriormente ya no están presentes. Esto vuelve al switch a la condición predeterminada de fábrica con respecto a la configuración de VLAN.

Nota: para los switches Catalyst, el comando erase startup-config debe acompañar al comando delete vlan.dat antes de la recarga para restaurar el switch a la condición predeterminada de fábrica.

Comando **show vlan**

Sintaxis del comando de CLI IOS de Cisco	
show vlan [**brief** | **id** *id-vlan* | **name** *nombre-vlan* | **summary**].	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la misma.	**brief**
Mostrar información sobre una sola VLAN identificada por su número de ID. Para la vlan-id, el intervalo es de 1 a 4094.	**id** *id de la VLAN*
Mostrar información sobre una sola VLAN identificada por su nombre. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	**name** *nombre de la VLAN*
Mostrar el resumen de información de la VLAN.	**resumen**

Comando **show interfaces**

show interfaces [*id-interfaz* | **vlan** *id-vlan*] | **switchport**	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	*id de la interfaz*
Identificación de VLAN. El intervalo es de 1 a 4094.	**vlan** *id de la VLAN*
Mostrar el estado de administración y operación de un puerto de conmutación, incluidas las configuraciones de bloqueo y protección del puerto.	**switchport**

Verificación de las VLAN

Una vez que se configura una VLAN, se puede validar la configuración con los comandos show de IOS de Cisco. **Show interfaces switchport | trunk**

Enlaces troncales

Un enlace troncal de VLAN es un enlace de capa 2 del modelo OSI entre dos switches que transporta el tráfico para todas las VLAN (a menos que se restrinja la lista de VLAN permitidas de manera manual o dinámica). Para habilitar los enlaces troncales, configure los puertos en cualquier extremo del enlace físico con conjuntos de comandos paralelos.

Para configurar un puerto de switch en un extremo de un enlace troncal, utilice el comando **switchport mode trunk**. Con este comando, la interfaz cambia al modo de enlace troncal permanente. El puerto establece una negociación de protocolo de enlace troncal dinámico (DTP) para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio. El protocolo DTP se describe en el tema siguiente. En este curso, el comando switchport mode trunk es el único método que se implementa para la configuración de enlaces troncales.

En la figura, se muestra la sintaxis del comando de IOS de Cisco para especificar una VLAN nativa (distinta de la VLAN 1).

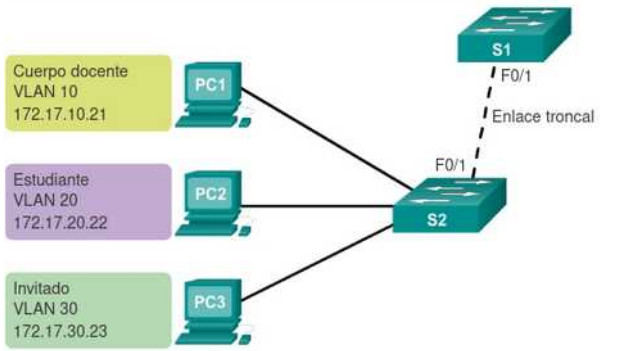
Para extender la VLAN a varios switches debe haberse creado antes en todos ellos

Utilice el comando **switchport trunk allowed vlan lista-vlan** de IOS de Cisco para especificar la lista de VLAN que se permiten en el enlace troncal.

Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface id_interfaz`
Haga que el enlace sea un enlace troncal.	`S1(config-if)# switchport mode trunk`
Especifique una VLAN nativa para enlaces troncales 802.1Q sin etiquetar.	`S1(config-if)# switchport trunk native vlan id_vlan`
Especifique la lista de VLAN que se permitirán en el enlace troncal.	`S1(config-if)# switchport trunk allowed vlan lista-vlan`
Vuelva al modo EXE(	

En la figura 2, las VLAN 10, 20 y 30 admiten las computadoras de Cuerpo docente, Estudiante e Invitado (PC1, PC2 y PC3). La VLAN nativa también se debe cambiar de la VLAN 1 a otra VLAN, como la VLAN 99. De manera predeterminada, se permiten todas las VLAN a lo largo de un enlace troncal. Para limitar las VLAN permitidas, se puede usar el comando switchport trunk allowed vlan.

```
VLAN 10 - Cuerpo docente/Personal -
172.17.10.0/24
VLAN 20 - Estudiantes - 172.17.20.0/24
VLAN 30 - Guest (Default) - 172.17.30.0/24
VLAN 99 - Management and Native -
```



En la figura, el puerto F0/1 en el switch S1 está configurado como puerto de enlace troncal, asigna la VLAN nativa a la VLAN 99 **switchport trunk native vlan numero** y especifica el enlace troncal para que solo reenvíe tráfico para las VLAN 10, 20, 30 y 99.

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30
S1(config-if)# end
```

Nota: esta configuración supone el uso de los switches Cisco Catalyst 2960 que utilizan de manera automática la encapsulación 802.1Q en los enlaces troncales. Es posible que otros switches requieran la configuración manual de la encapsulación. Siempre configure ambos extremos de un enlace troncal con la misma VLAN nativa. Si la configuración de enlace troncal 802.1Q no es la misma en ambos extremos, el software IOS de Cisco registra errores. Habría que poner `switchport trunk encapsulation dot1q`

Restablecimiento del enlace troncal al estado predeterminado

En la figura, se muestran los comandos para eliminar las VLAN permitidas y restablecer la VLAN nativa del enlace troncal. Cuando se restablece al estado predeterminado, el enlace troncal permite todas las VLAN y utiliza la VLAN 1 como VLAN nativa.

Ingrese al modo de configuración global.	`S1# configure terminal`
Ingrese al modo de configuración de interfaz para la SVI.	`S1(config)# interface id_intrfaz`
Establezca el enlace troncal para permitir todas las VLAN.	`S1(config-if)# no switchport trunk allowed vlan`
Restablezca la VLAN nativa al valor predeterminado.	`S1(config-if)# no switchport trunk native vlan`
Vuelva al modo EXEC privilegiado.	`S1(config-if)# end`

En la figura 2, se muestran los comandos utilizados para restablecer todas las características de enlace troncal de una interfaz troncal a la configuración predeterminada. El comando show interfaces f0/1 switchport revela que el enlace troncal se volvió a configurar en un estado predeterminado.

```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<resultado omitido>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
```

En la figura, el resultado de ejemplo muestra los comandos utilizados para eliminar la característica de enlace troncal del puerto F0/1 del switch S1. El comando show interfaces f0/1 switchport revela que la interfaz F0/1 ahora está en modo de acceso estático.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation : natif
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
```

Verificación de la configuración

En la figura 1, se muestra la configuración del puerto F0/1 del switch S1. La configuración se verifica con el comando show interfaces ID-interfaz switchport.

En el área superior resaltada, se muestra que el modo administrativo del puerto F0/1 se estableció en trunk. El puerto está en modo de enlace troncal. En la siguiente área resaltada, se verifica que la VLAN nativa es la VLAN 99. Más abajo en el resultado, en el área inferior resaltada, se muestra que todas las VLAN están habilitadas en el enlace troncal.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<resultado omitido>
```

DTP

Switch(config-if)# **switchport mode {access | trunk | dynamic auto | dynamic desirable}**
Switch(config-if)# **switchport nonegotiate** -- desactiva DTP en la interfaz o rango de interfaces

Trabajo con STP

Ver el estado actual de STP podemos ejecutar este comando en modo administrador:

```
Switch#show spanning-tree
Switch#show spanning-tree detail
Switch#show spanning-tree vlan numero
```

Este comando no solo muestra el spanning-tree sinó que me sirve también para mostrar hacia donde van los paquetes.

Activar STP (si no está ya activada)

```
Switch (config)# spanning-tree vlan <numero>
Switch (config)# spanning-tree mode rapid-pvst
```

Desactivar STP

```
Switch (config)# no spanning-tree vlan <numero>
```

Poner un Switch concreto como raiz

```
switch (config)# spanning-tree vlan <numero> root primary[secondary]
```

Cambiar la prioridad de un switch:

```
Switch> enable
Switch# configure terminal
Switch(config)# spanning-tree vlan <numero> priority <numero>
Switch(config)# spanning-tree vlan <numero>,<numero> priority <numero>
```

Cambiar el coste de un puerto

```
switch (config-if)# spanning-tree [vlan <numero>] cost <numero>
```

Cambiar la prioridad de un puerto:

```
Switch(config-if)# spanning-tree [vlan <numero>] port-priority <numero>
```

PortFast

```
Switch(config-if)# spanning-tree portfast
Switch(config-if)# spanning-tree bpduguard enable
```

Agregación de enlaces (EtherChannel)

Para configurar un Etherchannel tenemos que : poner los interfaces en modo trunk, seleccionar los enlaces, apagarlos y crear el port-channel poniéndolo en modo trunk.

PAgP

PAgP es tecnología Etherchannel propiedad de Cisco. Utiliza la dirección de multidifusión de 01-00-0C-CC-CC-CC para la comunicación.

Los puertos de conmutador/enrutador pueden formar un EtherChannel cuando están en diferentes modos PAgP según los siguientes criterios:

- Un puerto en el modo deseable puede formar un EtherChannel con otro puerto que esté en el modo deseable o automático.
- Un puerto en el modo automático puede formar un EtherChannel con otro puerto en el modo deseable.
- El puerto en modo deseable es aquel que envía solicitudes al otro lado para ver si también está usando PAgP. El puerto en modo automático define el uso de PAgP pero no envía solicitudes.

PAgP Mode	**Desirable**	**Auto**
Desirable	Yes	Yes
Auto	Yes	No

Ejemplo: El Switch1 se configura en modo deseable y el switch2 en modo auto para negociar y formar el Etherchannel.

```
Switch1(config)#interface range Gi0/0-3      (especificamos los interfaces a configurar agregados)
Switch1(config-if-range)#channel-group 1 mode desirable    (Crea el interface port-channel)

Switch2(config)#interface range Gi0/0-3
Switch2(config-if-range)#channel-group 1 mode auto
```

Podemos poner el etherchannel completo en modo trunk

```
Switch2(config-if-range)#interface port-channel 1
Switch2(config-if)#switchport mode trunk
```

LACP

LACP es un protocolo estándar abierto y publicado bajo la especificación 802.3ad. Utiliza la dirección de multidifusión de 01-80-c2-00-00-02.

Los puertos de conmutador/enrutador pueden formar un EtherChannel cuando están en diferentes modos LACP según los siguientes criterios:

Un puerto en modo activo puede formar un EtherChannel con otro puerto que esté en modo activo o pasivo.

Un puerto en modo pasivo no puede formar un EtherChannel con otro puerto que también esté en modo pasivo porque ninguno de los puertos inicia la negociación LACP.

El puerto en modo activo negocia con el otro lado para formar Etherchannel mientras que la interfaz en modo pasivo indica el uso de LACP, pero responde solo a solicitudes y no envía ninguna solicitud.

LACP	**Activo**	**Pasivo**
Activo	Sí	Sí
Pasivo	Sí	No

Ejemplo con un switch1 configurado en modo activo y el switch2 en modo pasivo para negociar el Etherchannel.

```
Switch1(config)#interface range Gi0/0-3
Switch1(config-if-range)#channel-group 1 mode Active
Switch1(config)#interface port-channel 1
Switch1(config-if)#switchport mode trunk

Switch2(config)#interface range Gi0/0-3
Switch2(config-if-range)#channel-group 1 mode Passive
Switch2(config-if-range)#interface port-channel 1
Switch2(config-if)#switchport mode trunk
```

Mode ON

Cuando se utiliza un modo EtherChannel “ ON ”, EtherChannel se creará solo cuando otro grupo de interfaz esté en modo EtherChannel “on”.

Un inconveniente importante de utilizar el modo EtherChannel "ON" configurado manualmente es que cualquier dispositivo de capa uno, como un conversor de medios o un módem entre 2 dispositivos Etherchannel, no podrá diagnosticar la falla del enlace y continuará enviando el tráfico, mientras que los dispositivos configurados con PAgp/LACP detectarán el fallo y responderá a él.

```
Switch1(config)#interface range Gi0/0-3
Switch1(config-if-range)#channel-group 1 mode  on
Switch1(config-if-range)#interface port-channel 1
Switch1(config-if)#switchport mode trunk

Switch2(config)#interface range Gi0/0-3
Switch2(config-if-range)#channel-group 1 mode  on
Switch2(config-if-range)#interface port-channel 1
Switch1(config-if)#switchport mode trunk
```

Ver información del EtherChannel

```
S1# show etherchannel port-channel
S1# show etherchannel summary
S1# show interface port-channel <numero>
S1# show interfaces etherchannel
```