Tema 06 - Configuración y administración de switches

1. Configuración de switches

Los **puentes** y los **switches** son dispositivos de comunicación que funcionan en la **capa 2 del modelo OSI**. Por este motivo, se los conoce como dispositivos de enlace de datos.

Los puentes salieron a principios de los 80's y permitían retransmitir tramas entre redes homogéneas. Estos utilizaban las direcciones **MAC** para reenviar selectivamente las **tramas** entre diferentes redes, dividiendo los **dominios de colisión** en dos.

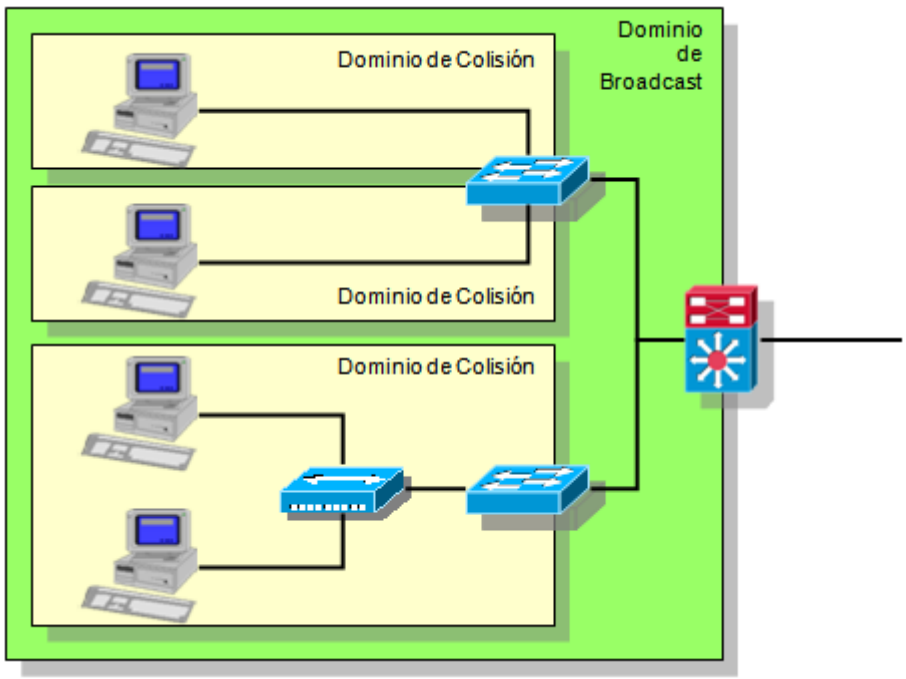
Hoy en día los puentes ya han sido reemplazados por los **switches**, ya que estos son una mejora considerable de **capacidad de puertos** y también tienen **sistema operativo propio**, por tanto se pueden configurar mejor.

1.1 Segmentación de la red

Un **segmento de la red** es cualquier medio de red compartido, por ejemplo, un switch o un hub.

Un **dominio de colisión** es un segmento físico de la red donde los paquetes pueden chocar. Los encargados de minimizar los dominios de colisión son los dispositivos de red de **capa 2 o superiores**, como los switches o routers. Estos dominios son los que provocan problemas de rendimiento en redes ethernet.

Un **dominio de broadcast** es una parte de la red donde todos los dispositivos reciben las **tramas broadcast** enviadas desde una máquina a todas las otras. Los **routers**, al funcionar en **capa 3**, **dividen** los dominios de broadcast. Por tanto, cada dominio de broadcast **forma una red VLAN distinta**.



Dicho esto, cuando hablamos de **segmentación de la red**, estamos hablando de **dividir todos los dominios de colisión en dos o más partes** y así mejorando el rendimiento de la red.

> Un hub tiene un único dominio de colisión, es decir, en el caso que dos dispositivos provoquen una colisión en un segmento asociado a un puerto del hub, todos los otros dispositivos de los otros puertos se ven afectados.

1.2 Switches

Hoy en día, los switches como antes decíamos, han **sustituido** a los puentes. **¿Por qué?** Porque los switches tienen **mejor rendimiento por puerto**, **mayor cantidad de puertos**, **coste inferior** y gran **flexibilidad a la hora de configurarlos**.

1.2.1 Características de los Switches

- Los switches funcionan como los puentes pero con mejor y con más puertos, por tanto, podemos obtener **un único host para cada puerto**.
- Cada puerto del switch constituye un **dominio de colisión**. Cada dominio de colisión es un medio compartido (el cable) con dos dispositivos (host y switch). En este caso, es **aconsejable** configurar las tarjetas de red de ambos dispositivos a modo **full-duplex**. De esta forma, la señal que envía el host y la que envía el switch funcionan de manera **simultánea**.

  > En modo **full-duplex** no existen las colisiones en el medio, ya que **separamos** las comunicaciones entre ambos dispositivos. De esta forma, eliminamos el dominio de colisión.

- Cada switch tiene una **tabla de direcciones MAC**, creando de esta forma la relación **MAC-puerto** para saber por donde tiene que enviar las tramas.

  > En **Cisco IOS**, utilizamos el comando `show mac-address-table` dentro del switch para ver esta tabla.

- De cada switch sabemos la **memoria** que tiene y la **cantidad de direcciones MAC** que puede almacenar. Si se excede el **límite** de direcciones MAC almacenadas, entonces se **retransmitirán** las tramas de los hosts que fueron borradas de la tabla, afectando al **rendimiento** de la red.
- En las redes Ethernet, se utiliza **CSMA/CD** (Carrier Sense Multiple Access with Collision Detection) como protocolo de acceso al medio. Este lo que hace es **consultar** el estado del **medio físico** que quiere comunicarse antes de enviar la trama, y mientras envía las tramas **comprueba** que no se produzcan **colisiones**.

1.2.2 Formas de hacer 'switching'

Los switches pueden '**switchear**' o **conmutar** las tramas entre los distintos puertos mediante **dos filosofías distintas**:

- Almacenamiento y reenvío (store & forward):

  En este modo, el switch **espera** a que la trama le llegue **entera** para enviarla. De esta forma **comprueba si hay errores** recalculando el CRC (Cyclic Redundancy Check) y comparándolo con el almacenado en la trama.

> El hecho de esperar a la trama entera produce un **delay** o **retardo** importante. Además, si tuviese que pasar por dos switches, está comprobación se haría dos veces y el tiempo se **doblaría**.

- Atravesando el router (cut-through):

  En este modo, el switch retransmite los primeros bits de la trama apartir del momento en el que recibe la **dirección MAC de destino** contentida en los **primeros 6 bytes de la trama**. En este caso el switch copia en **buffer** sólo la información **mínima** para leer esa dirección MAC de destino. El problema de no comprobar los errores es que el ancho de banda se satura de manera innecesaria.

> Cuando un **host** recibe una **trama errónea** se encarga de descartar la trama, es decir, no existe peligro de que los hosts reciban errores.

Para solucionar este problema, los switches que funcionan con este método en realidad si que realizan la comprobación de CRC, pero justo **después** de que la trama se haya **conmutado**. Si detecta un error no puede descartar la trama, pero si supera un límite (establecido) de tramas erróneas **cambia al modo de Almacenamiento y reenvío**. Este error se suele dar en cables o tarjetas de red en **malas condiciones**. Aún así, si pasado un tiempo el índex de error por trama **vuelve a bajar del establecido**, vuelve al modo cut-through.

Además de estos dós métodos existen otras alternativas de las cuales no vamos a mencionar aquí.

1.2.3 Switching simétrico y asimétrico

El switching se puede clasificar en **simétrico** y **asimétrico** dependiendo de la **manera de asignar el ancho de banda a los puertos de los switches**.

- El **switching simétrico** proporciona el **mismo ancho de banda** a todos los puertos de un switch.
- El **switching asimétrico** proporciona diferentes anchos de banda a los diferentes puertos **dependiendo del tráfico de cada puerto**. Este método evitaría cuellos de botella en el funcionamiento de la red. El hecho de que los puertos puedan funcionar a distintas velocidades implica que el switch tiene que tener buffers de memoria para almacenar las tramas que tiene que retransmitir, obligando al switch a mantener en memoria las tramas que llegan con una velocidad superior a la que pueden salir.

En la actualidad la mayoría de switches son asimétricos porque proporcionan una mayor flexibilidad.

1.3 Configuración del switch I

Los switches al igual que los routers, son piezas de hardware que se parecen a los PC's en el sentido de que tienen componentes internos que se encargan de hacer **cálculos** (**switching o routing**) y disponen de una serie de **puertos** o **interfaces** para **comunicarse** con el exterior. Para facilitar su uso, utilizan un **sistema operativo**.

En los dispositivos **Cisco** se utiliza el **Cisco IOS** (Cisco Internetwork Operating System).

> Cisco Systems es una de las empresas de Internetworking más importantes en la actualidad. Su nombre es el sobrenombre de la ciudad de San Francisco en los Estados Unidos.

Por **norma general**, se accede al sistema operativo mediante una CLI (Command Line Interface). Dependerá de la versión del sistema el acceso a algunas funcionalidades u otras.

Internamente, el switch consta de los siguientes elementos:

- **Memoria RAM** (Random Access Memory):

  En la RAM es donde se almacenan los datos temporales del dispositivo y, como en los PC's, si hay un **corte de corriente**, la RAM se limpia borrando sus datos. Es aquí donde se almacenan los archivos de configuración.

- **Memoria NVRAM** (Non Volatile RAM):

  Esta memoria almacena **copias de archivos de configuración e inicio del switch** y sus datos no son borrados en el caso de un supuesto corte de luz.

- **Memoria flash**:

  Es la **ROM** que se puede **borrar** y **reconfigurar** que contiene la imagen y el microcódigo del sistema operativo.

- **ROM** (Read Only Memory):

  Contiene el diagnóstico de puesta en marcha del sistema y programas del sistema operativo. Para actualizar la **ROM** hay que **extraer** el circuito integrado y cambiarlo por uno nuevo.

- **Interfaces**:

  Son las conexiones de red por donde entran y se envían las tramas hacia su destino.

El **IOS** está almacenado dentro del dispositivo como un fichero dentro de la memoria flash. Esta memoria como hemos comentado anteriormente no es volátil. Se pueden descargar versiones más nuevas del **IOS** simplemente cargando el fichero en el dispositivo.

Para acceder al sistema operativo del switch tenemos que hacerlo desde un ordenador conectado al switch (no podemos hacerlo sólo con el switch). Para continuar, vamos a ver las diferentes formas de conectarse a un switch.

1.3.1 Conexión por consola

En este método se utiliza el **puerto de consola** que suele estar en al parte posterior del dispositivo de red. Este puerto utiliza una conexión serie de **baja velocidad** para conectar el puerto de consola del switch al puerto serie (COM) del PC, es decir, requiere acceso físico al switch.

Para acceder al switch necesitaremos un **software** para nuestro PC que variará en función de si utilizamos Linux,Mac o Windows: '**Minicom**' para GNU/Linux o '**HyperTerminal**' para Windows.

1.3.2 Conexión por Telnet y SSH

A diferencia de la conexión por consola, mediante **Telnet** o **SSH** establecemos una conexión remota al switch, sin cables y sin tener acceso físico a este. Como bien sabemos de temas anteriores, el protocolo **SSH** es el más seguro y por tanto el recomendado entre estos dos métodos para acceder al switch.

1.4 Trabajo con Cisco IOS

Una de las principales características de **Cisco IOS** es su diversidad de modos:

- **Modo usuario**.
- **Modo de ejecución privilegiada**.
- **Modo de configuración global**.
- **Otros** modos como **configuración de interfaces**, etc.

1.4.1 Modo usuario

El modo usuario es el primero al cual accedemos cuando entramos al **CLI** del **dispositivo Cisco**. Este modo permite ejecutar una serie de comandos muy básicos y limitados, la mayoría de visualización o monitoreo.

> Llamamos **prompt** al texto o caracteres de la **CLI** que indican que el sistema está listo para realizar el siguiente comando. Ejemplo:

> En Windows el **prompt** suele ser `C:\>`

Por defecto, el modo usuario no requiere ninguna contraseña para acceder al dispositivo, aunque se puede configurar. En el modo usuario, el **prompt** es `Switch>` .

1.4.2 Modo de ejecución privilegiada

El modo de ejecución privilegiada permite la configuración y administración del dispositivo.

Para **entrar** al modo privilegiado tenemos que usar el comando `enable` .

El **prompt** de la CLI en modo privilegiado es `Switch#` .

Para **salir** del modo privilegiado usamos el comando `exit` o el comando `disable` .

> Para acceder a los otros modos, se tiene que hacer desde modo de ejecución privilegiada

También podemos configurar una contraseña específica para este modo:

Con `enable secret (contraseña)` la asignamos.

Con `no enable secret` la quitamos.

> Para configurar la contraseña tenemos que acceder al **modo de configuración global** mencionado posteriormente

1.4.3 Modo de configuración global

Desde el modo de configuración global se puede acceder a las **opciones** de **IOS** para **configurar gran parte** del switch, desde el cual también se puede acceder a otros modos como el de **configuración de interfaces**.

Se accede con `configure terminal` desde el modo de ejecución privilegiada.

Prompt: `Switch(config)#`

1.4.4 Modo de configuración de interfaces

En este modo **configuramos** las **características y opciones de cada interfaz** (puerto) del switch. Se accede desde el modo de configuración global mediante el comando `interface (nombre_interfaz)` . Si introducimos el nombre de interfaz correcto, obtendremos el siguiente **prompt**: `Switch(config-if)` indicándonos que está **listo** para empezar a configurar el puerto.

1.5 Ayuda con Cisco IOS

El sistema operativo de **Cisco IOS** ofrece una serie de ayudas a la hora de trabajar.

En primer lugar tenemos el carácter `?` que muestra las ordenes o comandos actualmente disponibles para ejecturase.

> Este carácter también se usa para **autocompletar** cuando estamos escribiendo un comando

1.5.1 Acceso Rápido y comandos abreviados

Estas son las formas abreviadas o rápidas de introducir comandos:

- **Tabulador**.

  La tecla tabulador completa los comandos incompletos.
- **Flechas arriba y abajo**.

  Como en todas las CLI, para aceder a los comandos realizados anteriormente.
- **Ctrl + C**.

  Interrumpe el comando actual y sale del modo de configuración.
- **Ordenes abreviadas**.

  Son comandos abreviados como por ejemplo `configure terminal` se abrevia a `conf t`.

1.5.2 Verificación de sintaxis

La CLI muestra un comentario cuando introducimos un comando erroneo, clasificados en tres tipos:

- **Ambiguous command**:

  Orden de comandos ambigua.
- **Incorrect command**:

  Comando incorrecto.
- **Incomplete command**:

  Comando incompleto.

1.6 Configuración del switch II

Como hemos mencionado anteriormente, el switch tiene diferentes **modos de ejecución**, y cada uno permite ejecutar unos comandos.

1.6.1 Mostrar el estado del switch

Para mostrar el **estado** del switch, disponemos de varios **comandos**. Mediante el comando `show ?` podemos ver todos los comandos de estado disponibles. Entre estos destacamos los siguientes:

- `show arp`

  Muestra la tabla **ARP**.
- `show clock`

  Muestra el **reloj** del sistema.
- `show flash`

  Muestra el contenido de la **memoria flash**.
- `show history`

  Muestra el **historial** de **comandos** ejecutados en la sesión del sistema.
- `show interfaces`

Muestra el **estado** y la **configuración** de las interfaces. Del resultado que nos muestra destacamos el estado de la interfaz (activada o desactivada), la dirección MAC de la interfaz, el ancho de banda de la interfaz, las estadísticas de uso y el modo de configuración (full-duplex o half-duplex).

Si queremos información de una interfaz en **concrecto**, ejecutamos lo siguiente como ejemplo:

`show interface FastEthernet 0/1`

También podemos usar `show ip interface` para mostrar la **IP** y **estado**, `show version` para ver la información del **hardware** del switch y la versión del IOS, `show vlan` para ver la configuración de las **redes locales virtuales** y `show mac-address-table` para ver la **tabla de direccionamiento MAC** entre otros.

En la tabla MAC tenemos cuatro columnas:

- **Vlan**:

  Vlan a que puerto pertenece.
- **Mac address**:

  Dirección **MAC** del host.
- **Type**:
  - **Dynamic**:

    Dirección MAC que el switch ha aprendido analizando las direcciones MAC de origen de las tramas.
  - **Static**:

    Dirección MAC que ha introducido manualmente el administrador.
- **Ports**:

  Puerto del switch al cual está **asociada** la MAC.

1.6.2 Comandos en modo de ejecución privilegiada

Recordamos que en este modo nos daba acceso a la **mayoría** de los comandos de configuración del switch y su **prompt** era `Switch#` .

- `configure terminal`

  Entra en el modo de **configuración global**.
- `copy (origen) (destino)`

  Copia un fichero a otro. Necesita siempre 2 parámetros los cuales pueden ser:
  - `flash`

    Es el fichero de la memoria **flash**.
  - `ftp`

    Es el fichero del servicio **FTP** del sistema.
  - `running-config`

    Es el fichero de **configuración en ejecución**.
  - `startup-config`

    Es el fichero de **configuración de arranque**.

    - `tftp`

      Es el fichero del servicio **trivial FTP** del sistema.

    Un caso que se da mucho es cuando queremos copiar la configuración que hemos cambiado a la que se ejecutará cuando el switch arranque de nuevo. Introduciríamos lo siguiente:

    `copy running-config startup-config`

- `delete flash`

  Sirve para **borrar un fichero de la memoria**. Necesita un nombre como parámetro.

- `dir`

  Muestra la **lista de ficheros** del sistema almacenados en la memoria flash.

- `disable`

  Para **salir** del modo de ejecución privilegiada del usuario.

- `exit`

  Sale de la CLI.

- `reload`

  Reinicia el switch. Carga la `startup-config`.

- `show`

  Comando mencionado anteriormente para mostrar información de estado o configuración del switch.

- `spanning-tree`

  Muestra información sobre el protocolo STP (spanning tree protocol).

- `startup-config`

  Muestra el contenido del fichero de configuración de arranque.

- `vlan`

  Muestra información de las VLAN (Virtual Local Area Network). También sirve para configurar las VLAN.

- `vtp`

  Muestra información sobre el protocolo VTP (VLAN trunking protocol).

1.6.3 Comandos en modo de configuración global

Recordamos que para entrar a este modo introducíamos `configure terminal` y el **prompt** era `Switch(config)#`.

Estos son los comandos más importantes de este modo:

- `access-list`

  Gestiona las **listas de control de acceso** al switch.

- `banner motd (mensaje)`

  Define un mensaje de **motd** (message of the day) de bienvenida al switch. Este mensaje se muestra cuando entramos por primera vez al switch. Toma como parámetro un String.

- `hostname (nombre_dispositivo)`

Con este comando cambiamos el **nombre del switch** que se muestra en el prompt. El nombre tiene que seguir unos requisitos:

  - Tiene que empezar por una letra.
  - Sólo se pueden usar letras, dígitos y guiones.
  - Tiene que acabar con una letra o dígito.
  - No puede tener espacios en blanco.
  - La longitud máxima del nombre es de 60.
  - Hay que respetar el uso de mayúsculas y minúsculas (Case-Sensitive).

  Para volver al nombre por defecto introducimos `no hostname`.

- `interface (nombre_interfaz)`

  Entramos en el modo de configuración de la interfaz específicada. Requiere un parámetro.

1.6.4 Configuración de contraseñas

El switch tiene que tener contraseñas configuradas a nivel local para evitar accesos de usuarios no autorizados al sistema. El **IOS** permite diferentes contraseñas a diferentes niveles jerárquicos:

- **Contraseña de consola**:

  Limita el acceso al dispositivo desde la **conexión de consola**. Para cambiar la contraseña de consola tenemos que ejecutar una serie de comandos:

  ```
  // Configuramos la primera línea de consola
  Switch(config)#line console 0

  // Introducimos la contraseña deseada
  Switch(config-line)#password contraseña

  // Requiere iniciar sesion para cada vez que alguien accede
  Switch(config-line)#login
  ```

- **Enable password**:

  Limita el acceso al **modo de ejecución privilegiada**. Esta contraseña hay que destacar que **no está encriptada**. Para configurarla ejecutamos:

  ```
  Switch(config)#enable password contraseña
  ```

- **Contraseña secreta de enable**:

  Limita el acceso al **modo de ejecución privilegiado** pero con contraseña **encriptada**. Para configurarla ejecutaríamos:

  ```
  Switch(config)#enable secret password contraseña
  ```

- **Contraseña VTY**:

  Limita el acceso mediante **conexión remota**. Ejecutaríamos:

```
Switch(config)#line vty 0
Switch(config-line)#password contraseña
Switch(config-line)#end
```

> Recuerda que siempre podemos ver las **contraseñas** que tiene el switch establecidas con el comando `show running-config`

1.6.5 Configuración de interfaces

Para acceder al modo de configuración de interfaz introducimos `interface (nombre_interfaz)` desde el modo de configuración global. Ejemplo:

```
Switch(config)#interface FastEthernet 0/1
Switch(config-if)#
```

Desde este modo de configuración podemos ejecutar las siguientes ordenes:

- `description (descripcion)`

  Sirve para dar un texto indentificativo a la interfaz. Es como `hostname` pero solo a un puerto del switch. Espera un parámetro. Ejemplo:

  ```
  Switch(config-if)#description Conexion con el router
  Switch(config-if)#exit
  ```

  > **RECUERDA**
  >
  > Para salir de este modo y finalizar la configuración utilizabamos `exit`

- `duplex ({full | half | auto})`

  Permite configurar el modo de la interfaz. Espera un parámetro que puede ser de tres tipos: full, half o auto.

- `mac-address`

  Permite indicar manualmente la dirección MAC de la interfaz. Espera un parámetro.

- `shutdown`

  Deshabilita la interfaz. `no shutdown` la vuelve a habilitar.

- `speed`

  Configura la velocidad del puerto. Espera un entero como parámetro en Mbps (Megabits por segundo). Ejemplo:

  ```
  // Establece 1000Mbps al puerto
  Switch(config-if)#speed 1000
  Switch(config-if)#exit
  ```

2. Administración de los switches

Se pueden realizar una serie de tareas para mejorar el funcionamiento del switch.

2.1 Secuencia de arranque del switch

Cuando el switch se pone en marcha, lo primero que hace es cargar el programa de arranque almacenado en la **ROM**. El **cargador de arranque** ejecuta las siguientes acciones:

- Se encarga de iniciar a bajo nivel la **CPU**.
- Hace una comprobación de la memoria de la **CPU**.
- Inicializa el sistema de archivos **flash**.
- Carga una imagen predeterminada del sistema operativo en la memoria y pone en marcha el switch. A continuación, una vez arrancado el IOS de Cisco, este se encarga de inicializar las interfaces (puertos) consultando los archivos de configuración en la memoria flash.

2.1.1 Inicialización de emergencia

El cargador de arranque proporciona un método para arrancar en el caso de que el sistema operativo no se pueda utilizar. Esto solo permite modificar archivos almacenados en flash mediante una **CLI**. Es como una bios de un PC.

2.2 Configuración de la interfaz de administración

Aunque los switches trabajan en la capa 2, algunos de estos pueden llevar a cabo configuraciones **TCP/IP**. Configurando el switch a nivel de red (capa 3) podemos hacer conexiones remotas con este mediante **Telnet y SSH**.

Para configurarlo, sería como si fuera un host, dándole una IP, máscara de red y un router por defecto. La ip se asigna primero a la VLAN y luego a la LAN. Por defecto, la administración del switch se hace mediante la **VLAN1**, la primera LAN virtual.

2.2.1 Configurar la interfaz de administración

Para configurar la interfaz de administración tenemos que acceder al **modo de configuración de interfaz**, y en este caso de la **VLAN** que queremos configurar:

```
ip address (direccion_ip) (mascara_de_red)
```

Una vez configurada la **dirección IP** y la **máscara** hay que volver a activar la interfaz:

```
no shutdown
```

Un ejemplo completo sería el siguiente:

```
Switch>enable
Switch#configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#ip address 192.168.0.155 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#
```

Una vez hecho esto, tenemos que asigar un puerto para que el switch trabaje desde esta **VLAN**. Accederíamos al modo de configuración de la interfaz correspondiente y utilizaríamos el comando `switchport` que sirve para configurar las características de switching de un puerto. `switchport` puede tomar uno de estos dos parámetros:

- `access`

  Canvia las características del modo de acceso a la interfaz. Permite al puerto en cuestión acceder a la VLAN introducida. Sintaxis:

  `switchport access (vlan) (numero_vlan)`
- `mode`

  Establece el modo de funcionamiento de la interfaz. Este parámetro cuando lo introducimos tenemos que proseguir con otro param. de sus hijos:

  - □ `access`

    Establece el modo de acceso.
  - `trunk`

    Establece el modo a troncal.
  - `dynamic`

    Establece el modo troncal dinámicamente a modo troncal o de acceso.
  - `native`

    Establece las características nativas cuando la interfaz trabaja en modo troncal.
  - `nonegotiate`

    Sirve para decir que la interfaz no utilizará el protocolo de autonegociación del puerto.
  - `port-secuirty`

    Comandos relativos a la seguridad del puerto.

Ahora tenemos que configurar el puerto para funcionar en **modo de acceso** y dar acceso a la **LAN virtual** que hemos configurado. Ejemplo con la interfaz FastEthernet 0/20:

```
Switch#configure terminal
Switch(config)#interface FastEthernet 0/20
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#
```

Si ejecutamos un `show ip interface` podríamos comprobar el estado de la interfaz y mostrar la configuración de las VLAN.

> Recordamos que las **VLAN** (Rede de área local virtual) son redes lógicas que **coexisten en un mismo switch físico** y son las encargadas de **dividir segmentos lógicos de una área local que no deberían de compartir datos entre ellas**. Ejemplo: Un colegio con distintas aulas, se utilizaría una vlan para cada aula para que no compartan información entre ellas pero el switch recibe la información de todas las aulas.

El siguiente paso es configurar el switch para que pueda enviar paquetes IP a otras redes mediante un router. Por eso, hay que configurar un router por defecto (puerta de enlace). **Esta configuración no es necesaria en un switch que no haga conexiones por Telnet o SSH.**

Para ello, desde el **modo de configuración global** utilizamos:

```
ip default-gateway (ip_del_router)
```

Podemos comprobar la conexión al router con un `ping` y listo.

2.3 Configuración Telnet y SSH

Hay veces que si disponemos de muchas redes locales y queremos cambiar la configuración a todos los switches, tenemos que ir uno a uno y realizar una conexión física con cable al puerto de consola para poder configurarlos. Nos interesa configurar todos los switches desde un ordenador conectado a la red.

2.3.1 Configuración Telnet

Con **Telnet** se puede acceder a una terminal virtual (VTY) del switch. Como esta conexión es **insegura**, requiere de una **contraseña** de acceso. Ejemplo:

```
Switch(config)#line vty 0 4
Switch(config-line)#password contraseña12345
Switch(config-line)#login
```

Para configurar la contraseña del switch tenemos que entrar al modo de configuración VTY desde el **modo de configuración global**. De normal los switches tienen **5 entradas de línea** (de la 0 a la 4).

Para acceder al switch mediante Telnet desde un PC se hace así:

```
telnet (ip_del_switch)
```

2.3.2 Configuración SSH

Como ya sabemos, **SSH** es mejor que **Telnet** por temas de **seguridad**, ya que encripta los datos antes de enviarlos a la red. Para funcionar con SSH se tienen que generar **claves RSA**. Para generarlas se utiliza el comando `crypto key generate rsa`. Estos son los pasos para configurar un switch como servidor SSH:

Entrar en el **modo de configuración global**:

```
configure terminal
```

Configurar el **nombre de host** para el switch:

```
hostname (nombre_switch)
```

Configurar el **dominio** del switch:

```
ip domain-name (nombre_dominio)
```

Habilitar el servidor SSH y generar las claves RSA:

```
crypto key generate RSA
```

Seleccionar la **versión de SSH deseada** (se recomienda la versión 2 por tener mejor encriptación):

```
ip ssh version 2
```

Seleccionar el **tiempo de espera**:

```
ip ssh time-out (tiempo_en_segundos)
```

Especificar la **cantidad de veces** que un cliente puede fallar en la autentificación:

```
ip ssh authentication-retries (numero_intentos)
```

Configurar las líneas **TTY** para limitar el acceso por SSH:

```
transport input ssh
```

Y ya estaría el proceso. Esto sería un **ejemplo** completo:

```
Switch#configure terminal
Switch(config)#hostname miswitch
miswitch(config)#
miswitch(config)#ip domain-name rtp.cisco.com
miswitch(config)#crypto key generate rsa
miswitch(config)#ip ssh version 2
miswitch(config)#ip ssh time-out 60
miswitch(config)#ip ssh authentication-retries 2
miswitch(config)#line vty 0 4
miswitch(config-line)#transport input SSH
```

2.4 Administración de las tablas MAC

Los switches son los que determinan si tienen que enviar las tramas por otros puertos analizando el destino de la trama. La dirección la buscan en la tabla interna llamada Tabla de direccionamiento MAC.

Para ver la tabla MAC utilizábamos `show mac-address-table` . Nos damos cuenta de que las direcciones MAC pueden ser de dos tipos:

- **Dinámicas**:

  Aprendidas automáticamente por el switch analizando las direcciones dentro de las tramas. Si el tiempo de expiración es muy corto, las direcciones se pueden borrar de la tabla de manera prematura.

- **Estáticas**:

Configuradas manualmente por el administrador de la red. Estas direcciones nunca expiran y el switch siempre sabe a que puerto enviar cada trama. **Ejemplo** de asignación de una dirección MAC a la tabla de manera estática:

```
Switch(config)mac-address-table static 0060.a014.e06e vlan 1 interface FastEthernet0/3
```

Si escribimos lo mismo pero con un `no` delante, borramos la entrada de la tabla:

```
Switch(config)no mac-address-table static 0060.a014.e06e vlan 1 interface FastEthernet0/3
```

2.5 Administración de los ficheros de configuración

Existen dos ficheros de configuración en los dispositivos Cisco:

- `running-config`

  Este fichero contiene la **configuración actual con la cual se está ejecutando el sistema**. Cualquier cambio que se haga sobre la configuración del sistema mediante comandos de IOS se hara sobre este fichero. Este fichero se situa en la memoria **RAM**, es decir, cuando se apaga el switch el fichero se borra.

- `startup-config`

  Este fichero contiene la configuración inicial del dispositivo. Se situa en la memoria **NVRAM**. Es un fichero persistente y se mantiene cuando el switch se reinicia.

Con `show running-config` podemos ver la configuración del switch cargada.

Cuando el switch se inicia, esta hace una copia del `startup-config` desde la NVRAM sobre el fichero `running-config` en la RAM, es decir, la configuración de arranque se convierte en la de ejecución.

> Cuando configuramos un switch tenemos que **recordar** utilizar el comando `copy running-config startup-config`

Al igual que podemos guardar los cambios, también se pueden deshacer con `copy startup-config running-config` , pero este comando **no sobreescribe por completo** la configuración en ejecución.

A veces, nos puede interesar guardar estos ficheros en el disco, es decir, en la memoria flash:

```
Switch#copy startup-config flash:
Destination filename [startup-config]? configuracio_vlan.bak
```

Introducimos el nombre del fichero con **extensión .bak** y listo.

También podemos **borrar los ficheros de configuración de arranque**:

```
erase startup-config
```

Y si el fichero está en **memoria flash** introducimos `delete flash` y luego de darle a `ENTER` su nombre, confirmamos y listo:

```
Switch#delete flash:
Delete filename []?configuracio_vlan.bak
Delete flash:/configuracio_vlan.bak? [confirm]y
```

Si nos interesara **tener los ficheros de configuración en otro ordenador** entonces tenemos que utilizar **TFTP** (Trivial File Transfer Protocol). Con este podemos hacer copias de seguridad de ficheros de configuración del switch de manera remota y tenerlos en otro ordenador.

Para poder utilizar el cliente de TFTP del switch tenemos que configurar una dirección IP por una interfaz del switch.

Realizar una **copia de seguridad** al TFTP:

```
copy (fichero_origen) tftp:
```

El fichero puede ser `startup-config`, `running-config` o un fichero de la memoria flash.

Ejemplo para **restaurar** del TFTP:

```
copy tftp: flash:
```

2.5 Actualizar el sistema operativo del switch

Con `show version` podemos comprobar la versión del sistema operativo que está ejecutando el dispositivo.

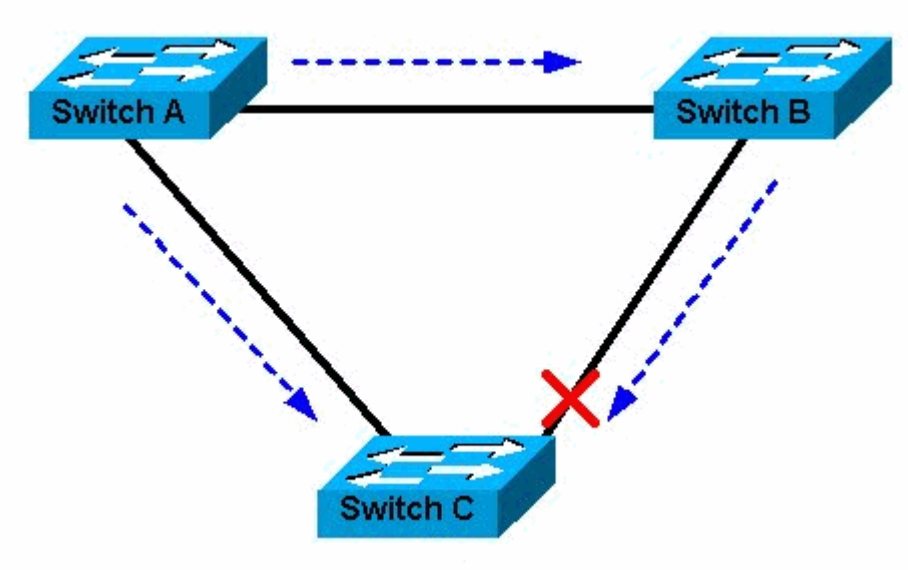
El proceso para actualizar el sistema operativo de un switch consta de tres pasos:

1. Cargar la nueva imagen del sistema operativo en la memoria del switch.
2. Configurar el switch para que cargue la nueva versión cuando se inicie.
3. Reiniciar el switch.

2.6 Configuración del STP (Spanning Tree Protocol)

Cuando en una red **existen varias rutas alternativas hacia un mismo destino se generan bucles**. Estas rutas alternativas son necesarias para proporcionar redundancia y ofrecer fiabilidad a la red en el caso de que un camino falle. El problema es que cuando existen estos bucles, los dispositivos de interconexión de nivel de enlace (los switches) reenvían indefinidamente las tramas broadcast y multicast, creando bucles infinitos y degradando el rendimiento de la red. **Al no existir un TTL** (tiempo de vida) en las tramas de capa 2, estas se quedan atrapadas indefinidamente en estos bucles. **La solución a este problema es el protocolo STP**.

Este protocolo permite que los switches se envien entre ellos información de la topología de las conexiones, paquetes de información llamados tramas BDPU. **Una vez los switches saben que topología de red hay, desactivan las conexiones redundantes eliminando los bucles y garantizando que haya un único camino** para unir todas las redes.



2.6.1 Funcionamiento del protocolo STP

Este protocolo utiliza sus propios algoritmos para determinar que interfaces de los switches se deben de desactivar para romper el bucle. Estos algoritmos se llaman **STA** (Spanning Tree Algorithm).

Los **STA** seleccionan un switch como raíz y lo utilizan como referencia para el cálculo de rutas. Los switches ejecutan el STP e intercambian las tramas **BDPU** donde envian el **identificador del puerto**, también llamado **BID**, el cual tiene estos campos:

- Campo de prioridad del puente
- Campo identificador del sistema extendido
- Dirección MAC

Se determina el **BID** más bajo mediante la combiandción de estos campos y el STA. El switch con el BID más bajo de la red **es el seleccionado para la raíz del árbol de expansión que calcula el algoritmo**. Luego, el algoritmo calcula la ruta más corta para llegar a él desde los otros switches. Cuando se realiza el cálculo, **el STA bloquea los puertos de los switches necesarios para romper los bucles**.

2.6.2 Funcionamiento de los puertos

El **STP** configura los puertos de los switches con diferentes funciones para evitar los bucles en red. Hay cuatro funciones distintas:

- **Puerto raíz**:

  Es el puerto con una ruta mejor hasta el switch raíz.

- **Puerto designado**:

  En el switch raíz, todos los puertos son designados. En un switch que no es raíz, el puerto designado es el que envía tramas hacia el puerto raíz.

- **Puerto no designado**:

  Es el puerto del switch que está bloqueado, de manera que no envia ni recibe tramas.

- **Puerto desactivado**:

  Es un puerto del switch que esta desconectado por el administrador.

2.6.3 Administración del STP en los switches

El STA calcula las mejores rutas y **tiene en cuenta la velocidad de transmisión de los puertos por los que tiene que travesar hasta llegar al switch raíz**.

El administrador del switch puede configurar los costes de atravesar un puerto con el comando `spanning-tree cost (coste)`

También podemos ver las funciones y prioridades de los puertos con las ordenes `show spanning-tree` y `show spanning-tree detail` desde el **modo de ejecución privilegiada** (EXEC)

El administrador puede modificar el resultado del STA y **hacer que un switch sea seleccionado manualmente como switch raíz**. Desde el modo de configuración global:

```
spanning-tree vlan (id_de_la_VLAN) root primary
```

Por ejemplo:

```
Switch(config)#spanning-tree vlan 1 root primary
```

También podemos configurar un switch raíz secundario si el primario falla:

```
spanning-tree vlan (id_de_la_VLAN) root secondary
```

O directamente especificar manualmente el valor de la prioridad que tendrán asignados los switches. El orden es el siguiente:

```
spanning-tree vlan (id_de_la_VLAN) priority (valor)
```

Los valores de la prioridad tienen que ser múltiples de 4096, si no, el IOS dará un error. Ejemplo :

```
Switch(config)#spanning-tree vlan 1 priority 50000
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
Switch(config)#
```

2.8 Configuración de seguridad

...

Apuntes por: Jordi Casesnoves Martín@JorudiSAMA - 17/04/2018