PAR03.- Configuración y Administración de Conmutadores.

Caso práctico

Tomás sigue avanzando en su conocimiento sobre redes. Cada vez se siente más animado al comprobar que va entendiendo mejor todos los conceptos que se relacionan con esta materia. Aunque siempre que aprende algo nuevo le surgen nuevas dudas y preguntas, está descubriendo un mundo apasionante.

Esta mañana ha estado visitando las instalaciones de la empresa de telecomunicaciones en la que trabaja Antonia, una antigua amiga suya. Ha quedado impresionado al descubrir los equipos tan avanzados y sofisticados de los que disponen. Antonia le ha explicado muchas cosas y ha contestado a todas sus preguntas.

Segmentación de la red. ventajas que presenta.

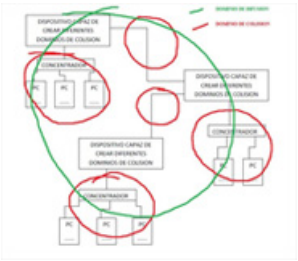
Caso práctico

Tomás ha decidido comprarse una impresora para instalarla en su red LAN. El vendedor le ha recomendado que compre además un **switch para poder conectar la impresora** y que todos los equipos de la red la puedan utilizar. Al preguntarle la razón por la que debe utilizar un switch, el vendedor se ha embarullado en una conversación en la que ha hecho referencia a **evitar colisiones en la red** y a la creación de los dominios de colisión. Tomás no se acordaba del concepto de **dominio de colisión y las ventajas de crear diferentes segmentos en una red** con un conmutador ¿Os ha ocurrido algo parecido alguna vez?

Segmentar una red es crear pequeños dominios de colisión

para minimizar la competencia por el medio entre las distintas estaciones, dando a cada una de ellas un ancho de banda. Esto se consigue gracias a que se aísla el tráfico entre los distintos segmentos de la red. **La segmentación se puede llevar a cabo utilizando puentes, conmutadores o routers.**

Un segmento de red es un conjunto de dispositivos que está en el mismo dominio de colisión. Por ejemplo, cinco PC unidos mediante un hub o concentrador constituyen un único segmento de red porque solamente hay definido un dominio de colisión.



Como se puede apreciar en la imagen anterior, **todos los equipos conectados a un concentrador pertenecen al mismo segmento de red** (un solo dominio de colisión). Varios dominios de colisión pueden estar en el mismo dominio de difusión.

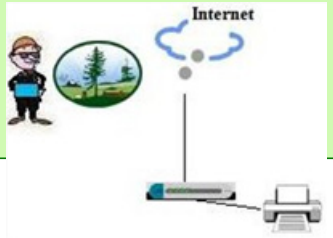
Autoevaluación

Los dispositivos que crean dominios de colisión son:

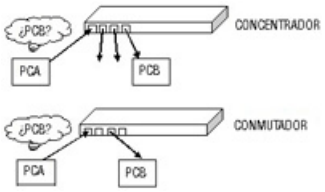
- Routers y concentradores.
- Puentes, conmutadores y routers.
- Solamente los hub.
- Solamente los routers.

Conmutadores y dominios de colision y broadcast.

Caso práctico



La instalación del conmutador en la red ha sido bastante sencilla y parece que la impresora **funciona perfectamente. A Tomás le ha surgido la duda de si podría imprimir desde fuera de su casa a través de Internet**, por ejemplo, cuando se encuentra disfrutando de la montaña durante el fin de semana. Un amigo le ha dicho que es más complicado porque **la impresora pertenece a una red de un dominio de difusión diferente al del ordenador.**



Un **conmutador es un dispositivo de interconexión que es capaz de generar diferentes dominios de colisión.** La diferencia entre un concentrador y un conmutador es que un concentrador recibe información por un puerto y la reenvía por todos los demás mientras que un conmutador reenvía la información solamente por los puertos a los que va dirigida.

Los conmutadores reconocen las direcciones Ethernet de los nodos de cada segmento de la red, y **permiten sólo el tráfico necesario para la comunicación entre los equipos implicados en el mismo dominio de colisión.** Un paquete es recibido por el conmutador, el conmutador examina las direcciones MAC origen y destino y las compara con una tabla de segmentos de la red almacenada en el switch. Después de comparar las direcciones que vienen en el paquete con las almacenadas, el conmutador escoge la ruta apropiada y lo reenvía por el puerto correcto.

Un switch es capaz de aprender el entorno de direcciones MAC que le rodean y crear tablas, es lo que le diferencia del concentrador o hub. Crean canales virtuales de comunicación entre pares de puertos de tal forma que la comunicación entre un par de puertos no se ve afectada por otra comunicación entre cualquier otro par de puertos.

Los conmutadores convencionales pueden conectar redes diferentes a nivel de la capa 1 del modelo OSI pero iguales a nivel de la capa 3, es decir, deben tener direcciones IP de igual clase (igual dominio de difusión). Existen conmutadores que trabajan en el nivel 3, son conmutadores con características de enrutamiento, enrutan los paquetes las direcciones IP de los usuarios. La conmutación IP de los switch es equivalente al enrutado TCP/IPde los routers. Para que los switch puedan realizar enrutamiento se incluye la función router en su hardware. Un conmutador de nivel 3 es capaz de trabajar 10 veces más rápido que un router en la misma red.

Los switches de nivel 3 permiten la unión de segmentos de diferentes dominios de difusión, los switches de capa 3 son particularmente recomendados para la segmentación de LAN's muy grandes, donde la simple utilización de switches de capa 2 provocaría una pérdida de eficiencia de la LAN ya que las difusiones serían muy grandes.

Autoevaluación

Un switch es capaz de comunicar dominios de difusión diferentes:

- Verdadero.
- No existen conmutadores capaces de hacerlo.
- Solamente si incorpora en su hardware la función router.
- Solamente los conmutadores de nivel 2.

La segmentación de redes. Equipos e interconexión.

Caso práctico

Este fin de semana **Tomás tiene que asistir a una convención de profesionales de su sector.** En el folleto de inscripción ha leído que todos los asistentes tendrán la posibilidad de intercambiar información entre sí, porque **van a tener a su disposición una red local creada con varios switches de última generación, que permitirán que la velocidad de intercambio entre los usuarios sea muy alta.** Puesto que asistirán aproximadamente 150 personas ¿Es posible que haya muchas colisiones?

Una correcta segmentación de la red nos ayudará a mejorar los "cuellos de botella" de la red y además contribuirá de manera notable a mejorar la seguridad.

Si la segmentación de la red se lleva a cabo con switches de nivel 2 se hace con las direcciones MAC (conmutación de capa 2), y si se lleva a cabo con conmutadores de nivel 3 (conmutación de capa 3), se emplean también las direcciones IP.

Para segmentar redes se emplean puentes, conmutadores y routers. Todos estos dispositivos funcionan de forma análoga cuando manejan direcciones MAC.

Cuando una trama entra en un conmutador, se contemplan tres casos:

1. **Si la trama entra por el mismo puerto en el cual está el destino de la trama, se ignora.**
2. **Si la trama entra por un puerto diferente al destino se reenvía a ese destino.**
3. **Si no conoce el puerto destino de la trama, se envía por todos los puertos (" inundación").**

El **conmutador básico tiene un funcionamiento similar al puente**, el conmutador actúa por hardware y el puente por software. En cualquier caso, ambos utilizan una tabla de enrutamiento similar:

Tabla de enrutamiento

INTERFAZ	DIRECCIÓN MAC
E0	00-1D-7D-C7-AA-8D
E1	00-1D-7D-C3-BB-4C
E2	00-2C-4A-C2-CC-3A

El interfaz es el puerto del puente o conmutador relacionado con una dirección MAC destino. En la tabla anterior, el equipo cuya dirección MAC es 00-1D-7D-C7-AA-8D es accesible a través del puerto E0.

Estas tablas son las responsables de que los mensajes lleguen a su destino. Cuando una trama llega al dispositivo de interconexión se actúa de la manera siguiente:

1. **La trama** expone su dirección de origen y de destino. "¿Por dónde tengo que salir?
2. **El dispositivo** busca en su tabla esas direcciones. "A ver si te encuentro en la tabla".
3. **Si se encuentra la dirección** buscada en la tabla, se envía la trama por el puerto correspondiente. "Aquí estás, sal por esta puerta".
4. **Si no se encuentra la dirección** buscada, se envía por todos los puertos menos por el que llegó la trama para que se busque en otro segmento de red. "No sé por dónde tendrías que salir, prueba todas las puertas".
5. Una vez que se encuentra la trama y hay una respuesta por parte del destinatario, **se inscribe en la tabla el correspondiente registro para búsquedas posteriores.** "Encontré mi sitio saliendo por esta puerta, recuérdalo".

Estas tablas son las que dan origen a los segmentos de red, **crean caminos lógicos entre el origen y el destino** y así evitan colisiones entre otras comunicaciones.

Los puentes y conmutadores son capaces de aprender del entorno e incorporar a sus tablas de direcciones, las direcciones de los elementos que están conectados a ellos y asociar dichas direcciones a los puertos por donde son accesibles.

Interconexión con PC.

La interconexión de los puentes y conmutadores no necesita de ninguna configuración adicional, solamente nos debe preocupar el tipo de interfaz utilizado (RJ45, coaxial). Los enrutadores por el contrario sí que necesitan de la configuración de direcciones IP ya que son dispositivos que trabajan a nivel de red.

Los tipos de puertos de los que disponen estos dispositivos básicamente son:

- **LAN**
- **Consola**
- **RS232**
- **WAN**

Generalmente, **los puertos vienen identificados y en la actualidad la mayoría utilizan el interfaz RJ45** para la conexión de routers, PC u otros switches. El interfaz RS232 y el puerto Consola se utilizan para acceder a la configuración interna.

Los encaminadores o routers trabajan en el nivel 3 de la arquitectura OSI, gracias a esto son capaces de transmitir datos de un lado a otro de la red utilizando direcciones lógicas o direcciones de red. Además, el router es capaz de determinar la mejor ruta para enviar los datos, basándose en una tabla de enrutamiento que el mismo router es capaz de construir mediante aprendizaje.

Aunque los router se pueden utilizar para segmentar las redes a nivel 2, en sustitución de los conmutadores, lo ideal es utilizar los conmutadores o puentes a nivel enlace y los routers para segmentar las redes a nivel de red (subredes), y así crear diferentes dominios de difusión en una red con varios dominios de colisión creados ya por los conmutadores.

Si solamente queremos una segmentación a nivel 2 podemos escoger entre router o switch, preferiblemente conmutador porque es más efectivo para aumentar el ancho de banda, pero si queremos gestión inteligente de paquetes y acceso a una red WAN, necesitamos un encaminador.

El switch proporciona una velocidad de transmisión de paquetes más rápida a un coste inferior al que proporciona el router, esto es lógico si pensamos que el switch tiene menos circuitería y por lo tanto las tramas están sometidas a menos operaciones dentro de un conmutador.

Autoevaluación

Un administrador de una red LAN sin necesidad de conexión a una red de área extensa escogerá como mejor opción para segmentar dicha red:

- Varios concentradores de nivel 3 puesto que generarán varios dominios de difusión.
- Routers para poder tener una conexión tipo WAN.

- Conmutadores con capacidad de router, enrutan los paquetes de manera inteligente.
- Solamente los conmutadores de nivel 2.

Interconexión entre switches.

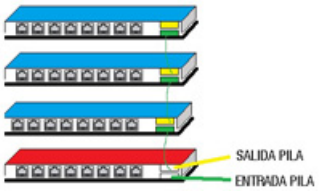
Los switches se pueden conectar entre sí de manera que funcionen como una sola entidad **formando una "pila"**, este mecanismo se conoce como**"apilar switches"**. Se emplea con switches gestionables y nos permite gestionar toda la "pila" utilizando una sola dirección IP y un puerto de acceso para la configuración.

Podemos apilar los switches de tres maneras diferentes:

- **Utilizando los puertos RJ45 y cables de red cruzados.**
- **Utilizando el puerto uplink.**
- **Utilizando el módulo de apilamiento.**

Una pila de conmutadores es un conjunto de conmutadores que deben tener la capacidad "apilable" y que están conectados mediante puertos.

El conmutador que controla el funcionamiento de la pila se denomina "unidad maestra" o "raíz" de la pila. La unidad maestra y los demás conmutadores de la pila son miembros de la pila.



El proceso para crear la pila es el siguiente:

1. **Configurar la protección por contraseña y asignar la dirección IP** de la unidad raíz, la primera unidad de la pila.
2. **Colocar los conmutadores uno encima** de otro con la unidad raíz situada en la parte inferior de ella.
3. **Conectar el cable de apilado de la unidad raíz a su puerto "salida de pila"**, situado en la parte posterior.
4. **Conectar el cable de apilado de la unidad raíz al puerto "entrada de pila"** de la segunda unidad de la pila.
5. La unidad raíz siempre tiene el puerto de entrada de la pila desconectado.
6. Se conecta el puerto **"salida de pila" al "entrada de pila"** de cada unidad superior.
7. El puerto **"salida de pila" de la unidad superior siempre está vacío.**
8. Conectar la corriente eléctrica en sentido descendente, de manera que la unidad raíz sea la última.

Autoevaluación

La diferencia entre varios conmutadores unidos entre sí y una pila de conmutadores es:

- No hay diferencia.
- Los conmutadores que forman la pila están unidos por cables RJ45.
- La pila se puede gestionar desde un solo puerto.
- La pila se puede gestionar desde la IP de cualquiera de los conmutadores que la forman.

Formas de conexión al conmutador para su configuración.

Caso práctico

Efectivamente había muchísimos colegas en la convención y nadie notó que se produjeran colisiones. La curiosidad llevó a **Tomás** al cuarto de telecomunicaciones y **tuvo la ocasión de hablar con el administrador de la red donde le interrogó acerca de los conmutadores gestionables de nivel 3.** El administrador le explicó cómo era uno de esos conmutadores y la forma de acceder a su configuración.

Desde su aparición en el mercado, los conmutadores no gestionables han utilizado una tecnología plug & play, de manera que todo lo que han necesitado saber, lo han "aprendido" de su entorno.

El hardware venía programado de fábrica y no existía la posibilidad de modificar nada. Un switch se conectaba con los equipos utilizando sus interfaces RJ45 y después de un breve tiempo en el que testeaban la red, reconocían a todas las máquinas y creaban su tabla de enrutamiento de direcciones MAC.

El atractivo de los conmutadores para un administrador de red residía en la rapidez que proporcionaban a la red y el menor precio comparado con otros dispositivos como los enrutadores. Si bien, esto sigue estando vigente, la aparición de switches con más prestaciones (nivel 3, gestionables, apilables) ha hecho que la mayoría de las redes LAN de tamaño medio hayan incorporado estos dispositivos.

Los nuevos conmutadores siguen utilizándose, en la mayoría de los casos, sin las prestaciones de enrutamiento nivel 3 y gestión, pero sus compradores los han incorporado en previsión de necesidades futuras.

Entre los switches gestionables, podemos distinguir entre los que se configuran mediante línea de comandos, por SNMP y los que lo hacen por Web.

En general, la administración básica se suele realizar vía línea de comandos (telnet, ssh y/o RS232) y vía WEB.

También existen aplicaciones basadas en el protocolo SNMP que suele utilizarse para monitorizar la actividad del dispositivo. El protocolo SNMP (Simple Network Management Protocol) permite:

- Obtener la cantidad de tramas y el número de bytes por interfaz.
- Ver tablas CAM.
- Ver errores de transmisión.
- Activar y desactivar interfaces.

Para gestionar un conmutador utilizando el protocolo SNMP se han diseñado muchas aplicaciones que permiten un manejo muy intuitivo y amigable por su entorno gráfico.

La dificultad en líneas generales está en identificar cada una de las variables que queremos testear. Las aplicaciones que utilizan el protocolo SNMP varían dependiendo del diseñador, tienen el inconveniente de las licencias y el precio, aunque cada vez aparecen más gratuitas o de libre distribución.

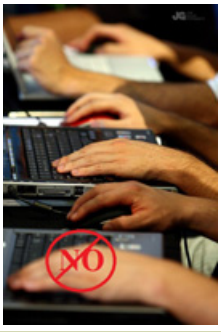
La gestión a través de la línea de comandos con telnet o ssh solamente necesita habilitar el servicio en el equipo, por defecto suele estar desactivado.

Debes conocer

En el siguiente enlace podrás ver un video explicativo de como activar el cliente telnet en Windows 7.

Como habilitar el cliente telnet en Windows 7

Modo usuario y modo privilegiado.



Cuando se trabaja en la **configuración de un conmutador** suelen existir dos formas de hacerlo, dependiendo de los privilegios que tengamos, **usuario y privilegiado.**

El modo usuario me permite solamente consultar el estado de configuración del switch, si quiero cambiar algún parámetro debo acceder en modo privilegiado.

- **Modo usuario. Comprobación del estado (modo sólo comprobar). En la línea de comandos aparece el símbolo:>**
- **Modo privilegiado. También llamado EXEC privilegiado, en este modo se pueden configurar las características del switch. El símbolo que aparece en la línea de comandos es: #**

Al conectarnos con el conmutador, lo hacemos como usuario. En la línea de comandos deberíamos teclear la palabra *enable* para pasar a modo privilegiado:

```
switch>

switch>enable
```

Y el símbolo debería cambiar a:

```
switch#
```

Dentro del modo privilegiado para pasar a configurar debemos ejecutar:

```
switch#configure terminal
```

Con lo que nuestra pantalla quedará:

```
switch(config)#
```

A partir de aquí podemos empezar a cambiar parámetros, por ejemplo, el nombre de nuestro switch lo cambiamos con el comando hostname:

```
switch(config)#hostname ALISAL
```

ALISAL(config)#

Y podríamos comenzar a ejecutar órdenes de configuración en nuestro conmutador. Si utilizamos la vía Web o una aplicación gráfica basada en SNMP, el proceso sería más intuitivo, basado en un sistema de ventanas.

Autoevaluación

Al conectarnos al conmutador vía telnet accedemos a la línea de comandos de configuración en modo:

- Usuario porque se ve el símbolo # en la línea de comandos.
- Exec privilegiado.
- Usuario con símbolo de sistema >.
- Privilegiado con símbolo >.

Conmutadores gestionables por web.

Aunque la conexión al conmutador para su configuración puede variar con el fabricante, se puede decir que los **switches gestionables por Web** tienen las siguientes **características**:

- **No tienen un puerto de consola (COM).**
- **No hay interfaz de línea de comandos.**
- **No son gestionables con SNMP.**
- **Se pueden configurar a través de un navegador.**

Se puede decir que estos conmutadores **se gestionan** a través de una interfaz muy intuitiva accesible **mediante el navegador de Internet**.

Los pasos a seguir para conectarnos a un switch gestionable serán, (suponiendo que ya estén conectados físicamente mediante un cable):

- Conocer la dirección IP asignada al switch. Generalmente suele ser del tipo 192.168.1.1 o 192.168.0.1, depende de cada fabricante.
- Configurar nuestro equipo con una dirección IP de la misma clase que la del switch. Si el conmutador tienen la dirección IP 192.168.1.1, nuestra tarjeta de red tendrá una configuración con una dirección IP 192.168.1.10 como se puede ver en la imagen:

- Escribir la dirección IP del conmutador en la barra de direcciones de navegador. Al ejecutar la orden saltará un cuadro de texto para introducir un usuario y una contraseña que de antemano debemos conocer, el fabricante la suministra en el manual del dispositivo.

- Utilizar el navegador para configurar los parámetros del conmutador que se necesiten.

Conmutadores gestionables por línea de comandos vía telnet o SSH.

Este tipo de conmutadores son **gestionables** mediante órdenes transferidas **por línea de comandos** desde un host conectado por Ethernet al equipo configurable.

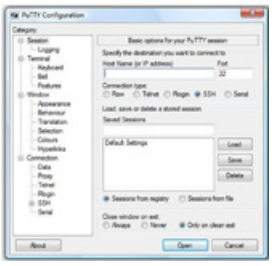
La gestión de este tipo de conmutadores es **más complicada que la gestión por Web** porque hay que conocer las órdenes específicas para configurar cada uno de los parámetros.

Para conectarnos a un conmutador con IP 192.168.1.1, abrimos una consola y tecleamos:

telnet 192.168.1.1

Nos pedirá un nombre de usuario y una contraseña para autentificarnos y acceder al switch. **El protocolo telnet está deshabilitado en muchos dispositivos porque se considera poco seguro** y en la actualidad se **utiliza el ssh** con más frecuencia.

Para utilizar telnet o ssh existen aplicaciones, como PuTTY, que te permitirán conectarme al equipo remoto escogiendo el protocolo que necesite en cada momento. Esta aplicación es gratuita y una vez ejecutada tiene el siguiente aspecto.



Con PuTTY **se puede escoger el protocolo y el puerto** necesarios para la conexión. En las figuras siguientes puedes observar el aspecto de las pantallas al conectar a un dispositivo que tiene una IP 192.168.1.3 y cuyo usuario es "tomas".

Una vez conectados, utilizaremos órdenes en la línea de comandos. Por ejemplo, si queremos cambiar la IP del conmutador, deberíamos introducir una orden del tipo:

ip address 192.168.0.1 255.255.255.0

Si quisiéramos ver la tabla de direcciones MAC almacenada en el conmutador escribiríamos algo como:

show mac-address-table

Todos los comandos de los que se dispone para la configuración se pueden saber tecleando el símbolo:

?

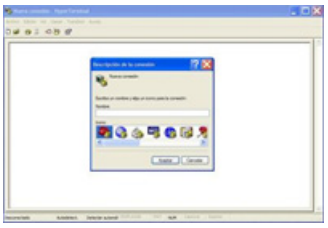
Conmutadores gestionables por puerto de consola.

Otra forma de gestionar el conmutador es la que utiliza el **emulador de terminal por puerto de consola RS-232 (COM1) o RJ45**, la forma de trabajar sería análoga a la línea de comandos.

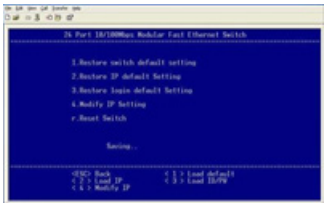
La diferencia estriba en la manera de conectarnos, ya que en esta opción se utiliza el puerto de consola que poseen la mayoría de los conmutadores.

El puerto de consola tiene el aspecto de la figura anterior, conector RS-232, nos conectaríamos utilizando un cable RS-232 (conector serie), aunque también existen adaptadores RS-232/RJ45 que nos permiten conectarnos con un cable de par trenzado válido para redes Ethernet.

Para trabajar de este modo, casi todos los sistemas operativos incorporan un programa de emulación de terminal (en el caso de Windows se llama HyperTerminal).



Para poder conectarnos nos solicitará la dirección IP del conmutador y después de ejecutar nos aparecerá la pantalla de configuración del switch en forma de menús.

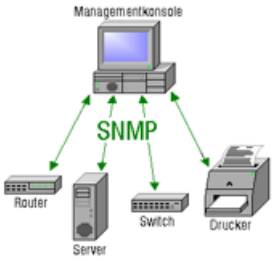


Autoevaluación

La diferencia entre administrar el conmutador por ssh o por telnet está en:

- El tipo de usuario con el que nos conectamos.
- La seguridad de la conexión, ssh es más seguro que telnet.
- Administrar utilizando ssh es más sencillo que por telnet.
- El puerto que se utiliza para conectarnos al switch.

Conmutadores gestionables por SNMP.



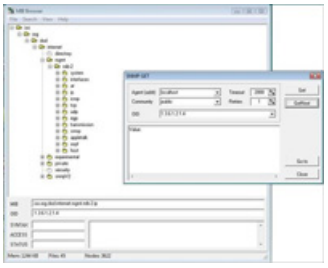
SNMP es una extensión del protocolo de gestión de red para gateways (SGMP), que se convirtió en 1989 en el**estándar recomendado por Internet**. Está dirigido a proporcionar una **gestión de red centralizada** que permita la observación, el control y la gestión de las instalaciones. Utilizando SNMP, un administrador de red puede direccionar preguntas y comandos a los dispositivos de la red.

SNMP se ha convertido, debido al enorme éxito que ha tenido desde su publicación, en el estándar de facto de gestión de redes. Prácticamente todo el equipamiento de redes puede ser gestionado vía SNMP.

El agente de SNMP residente del conmutador permite la gestión remota del mismo mediante IP a través de interfaces Ethernet.

Existen muchas aplicaciones diseñadas para operar con el protocolo de SNMP y poder configurar los dispositivos en un entorno amigable. Cada fabricante suele tener uno específico, pero existen algunos de licencia libre. Una de estas aplicaciones es MIB Browser.

Una vez instalada, la apariencia es la siguiente:



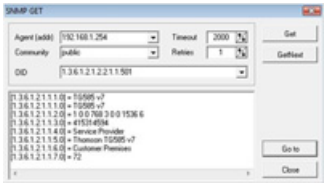
La aplicación tiene una opción de captura SNMP GET que me permite escoger la dirección IP que quiero testear y la variable MIB (casilla etiquetada con OID) a evaluar. Las variables MIB se nombran con números y hay que recurrir al manual de la aplicación para identificar cada una de ellas.

Las aplicaciones SNMP utilizan una base de datos MIB donde se almacenan los parámetros más relevantes de la configuración del equipo.

El Navegador MIB permite visualizar la jerarquía de las variables SNMP MIB en un formato de árbol y le provee con información adicional sobre cada nodo.

Con el Navegador MIB se puede fácilmente cargar (compilar) archivos MIB estándar y propietarios, visualizar y manipular datos, lo cual está disponible vía el agente SNMP.

Todas las aplicaciones incorporan un manual de ayuda explicativo para poder utilizar la herramienta.



Configuración del conmutador.

Caso práctico

Después de gastarse casi 400 euros, **Tomás se ha hecho con un switch gestionable.** La verdad es que no lo necesitaba imperiosamente pero el hecho de que su red sea más rápida y que además pueda modificar la configuración del mismo le ha atraído mucho. Al abrir la caja ha descubierto que el conmutador incluye un magnífico manual en CD e inmediatamente lo ha introducido en su PC para poder ver qué tipo de parámetros va a poder configurar

Sobre los switch **se puede configurar una amplia variedad de funciones** que permiten asegurar el funcionamiento normal, y en caso de fallar, asegurar la calidad del servicio y la seguridad. Entre las funciones configurables para un switch están las siguientes:

Autentificación: Gestionar un switch nos permite crear usuarios y contraseñas para poder acceder al conmutador en distintos niveles de privilegios, así como cambiar parámetros como el nombre del switch.

Configuración de puertos: Las configuraciones posibles sobre los puertos de switch afectan a:

- **La velocidad de comunicación de los puertos.**
- **El tipo de comunicación soportada por los puertos.**
- **El nombre que identifica a cada uno de los puertos.**

La velocidad de los puertos de un conmutador puede variar entre 10, 100 o 1000 Mb/s sobre la puerta RJ45 del switch. La configuración de la velocidad se puede hacer de forma manual (fija) o automática.

El tipo de comunicación soportada por los puertos define si la comunicación es **dúplex o semidúplex**. Normalmente Ethernet funciona en forma semidúplex; para un mejor rendimiento de la red se puede configurar manualmente una comunicación en forma dúplex, aunque lo aconsejable es no asignar este parámetro de forma manual.

Otro de los parámetros configurables de los puertos es el nombre que se les asigna y que sirve para identificarlo con su función o con un elemento conectado a él.

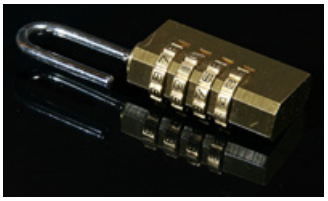
Modificar la tabla de direcciones: Aunque las tablas de direcciones MAC son aprendidas de manera automática, existe la posibilidad de añadir direcciones de forma manual.

Gestionar la seguridad en los puertos: Se indican las direcciones MAC que pueden ser conectadas a un puerto. Si la dirección MAC de origen que llega en la trama es distinta de la especificada en esta configuración, la conexión se rechaza.

Creación de archivos de configuración: Se puede crear un archivo que contenga toda la configuración del conmutador para utilizarlo en una reconfiguración posterior o en otro switch de iguales prestaciones.

Crear VLAN: la función VLAN (virtual LAN) permite dividir la lan en grupos virtuales para limitar el tráfico de multicast y broadcast. Este tema es muy importante y se tratará en próximas unidades de trabajo de manera amplia.

Nombres y contraseñas.



La configuración de un conmutador suele comenzar con la asignación de nombres y contraseñas. Se puede asignar un nombre a un equipo (en este caso ALISAL) y una contraseña. La primera orden que se debe utilizar es *enable*, que nos permite pasar al modo privilegiado:

```
switch>enable

switch#
```

Ahora que estamos en modo privilegiado para configurar utilizamos configure terminal.

```
switch#configure terminal

switch(config)#
```

Para cambiar el nombre del conmutador utilizamos hostname, vamos a darle el nombre de ALISAL.

switch(config)#hostname ALISAL

ALISAL(config)#

Los comandos enable password y enable secret se utilizan para restringir el acceso al modo EXEC privilegiado. El comando enable password establece una contraseña más débil que enable secret.

ALISAL(config)#enable password [nombre de la enable pass]

ALISAL (config)#enable secret [nombre de la enable secret]

Dependiendo de la forma de acceso debemos configurar la línea de comandos de una u otra manera con el comando line y los modificadores console o vty. Si accedemos vía consola utilizaremos:

ALISAL (config)#line console 0

El prompt de la línea de comandos cambia ahora y tiene el siguiente aspecto donde establecemos el login y la contraseña de acceso vía consola.

ALISAL (config-line)#login

ALISAL (config-line)#password [nombre de la pass de consola]

Si accedemos vía telnet utilizaremos para configurar la línea de comandos line vty añadiendo el número de interfaz y la cantidad de conexiones múltiples.

ALISAL (config-line)#line vty 0 4

ALISAL (config-line)#login

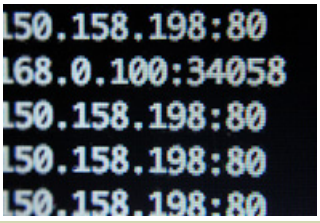
ALISAL (config-line)#password [nombre de la pass de telnet]

Autoevaluación

Si quisiera asignar a nuestro conmutador el nombre curso2011 los comandos a utilizar serían:

- Desde el modo usuario el hostname curso2011.
- Desde el modo privilegiado (#) ejecutar enable.
- Por este orden enable, configure terminal, hostname.
- Con la línea de comandos en modo config-line> utilizar hostname curso2011.

Configuración IP.



La configuración IP **asigna una dirección IP al switch** y además es capaz de asignar una puerta de enlace por si el switch necesita enviar o recibir información a una red diferente a la red desde la que se administra dicho switch.

El comando utilizado es ip address y se utiliza con los modificadores:

- **Netmask: Para especificar la máscara de red.**
- **BOOTP: Para obtener la dirección IP del protocolo de arranque BOOTP.**
- **DHCP: Para obtener la dirección IP del servidor DHCP.**

Si quisiéramos asignar a nuestro conmutador la dirección IP 192.168.1.2 tendríamos que hacer:

ALISAL(config)#ip address 192.168.1.2 255.255.255.0

Si queremos establecer una ruta estática entre nuestro conmutador y otro segmento de red utilizaremos el comando ip default-gateway, con esto podremos administrar nuestro conmutador desde una dirección diferente a la que estamos trabajando.

Si queremos que nuestro conmutador se comunique con un router cuya dirección IP es 192.168.1.5 escribiremos:

ALISAL(config)#ip default-gateway 192.168.1.5

El conmutador también se puede configurar para que obtenga todos los parámetros de configuración IP de un servidor BOOTP o DHCP utilizaremos los modificadores BOOTP y DHCP con el comando ip *address*.p

```
ALISAL(config)#ip address dhcp
```

Autoevaluación

Dispones de un conmutador gestionable, te has conectado a él mediante telnet, después de autentificarte has escrito en la línea de comandos la siguiente órden:

ALISAL(config)#ip address 255.255.0.0

Al ejecutar esta orden:

- Se cambiará la dirección IP del switch.
- La IP del switch será 192.168.1.254 y su máscara 255.255.0.0
- La orden está incompleta, faltaría una dirección IP de clase B (Ipv4).
- La orden estaría incompleta le faltaría la dirección 192.168.1.1.

El switch como servidor DHCP.

¿Te has preguntado por qué en algunas redes no tenemos que emplear ninguna configuración de direcciones IP y es suficiente con tener nuestra tarjeta con la opción "**Obtener la IP automáticamente**"? Gracias a **el protocolo DHCP**, utilizado por los dispositivos de red como un PC o una impresora (clientes DHCP) para obtener la dirección IP, puerta de enlace predeterminada y servidores DNS. En una pequeña red local el servidor DHCP puede ser un conmutador con esta prestación, la mayoría de los switches modernos gestionables de nivel 3 tienen la capacidad de ser servidores DHCP. Para habilitar el servicio DHCP en el switch:

```
ALISAL#conf t dhcp
ALISAL(config-dhcp)#service dhcp
```

Para salir del modo de configuración de DHCP:

```
ALISAL(config-dhcp)#exit
```

Si comenzamos creando el "pool" de direcciones IP:

```
ALISAL#ip dhcp pool TOMAS
```

Agregamos máscara de subred al pool y puerta de enlace predeterminada para los clientes:

```
ALISAL(config-dhcp)#network 192.168.1.0 255.255.255.0
ALISAL(config-dhcp)#default 192.168.1.1
```

Especificar el servidor de nombres de dominio DNS para los clientes:

```
ALISAL(config-dhcp)#dns-server 192.168.1.2
```

Establecer el tiempo en el que las direcciones no cambian para los clientes (2 días, 12 horas y 2 minutos):

```
ALISAL(config-dhcp)#lease 2 12 2
```

Se pueden agregar rangos de direcciones excluidas de DHCP (desde 192.168.1.250 a 192.168.1.254).

```
ALISAL(config)#ip dhcp exclude-address 192.168.1.250 192.168.1.254
```

Después de la configuración podemos testear el funcionamiento de nuestro servidor DHCP:

```
ALISAL#show ip dhcp binding
```

Y también con los siguientes comandos se mostrará la configuración del servidor DHCP y algunas estadísticas relevantes.

```
ALISAL#debug ip dhcp server events
ALISAL#show ip dhcp database
```

Configuración de puertos.

Los puertos de un switch se denominan también "interfaces". Para elegir un puerto a configurar se usa el comando *interface*, en modo de

configuración global:

ALISAL(config)# interface [type] [module/number]

ALISAL(config-if)#

El tipo (type) puede ser FastEthernet, GigabitEthernet, TenGigabitEthernet o Vlan. El módulo (module) es el módulo o slot donde está localizado, para los que no soporten módulos ni slots se usa el módulo 0 (cero) y por último se indica el número de puerto (number) dentro del módulo. Para configurar varios puertos:

ALISAL(config)# interface range type module/primer número – último número.

ALISAL (config)# interface FastEthernet 0/1

Para especificar la velocidad de los puertos empleamos el comando speed. La velocidad varía entre 10, 100 o 1000 Mb/s. También podemos dejar la velocidad en modo auto.

ALISAL(config-if)# speed {10 | 100 | 1000 | auto}

El modo de comunicación del puerto (duplex mode) que puede ser: half-duplex, full-duplex o auto negociado; también se puede especificar. En auto negociación primero se intenta negociar a full-duplex y si falla se queda en half-duplex. Normalmente Ethernet funciona en forma half-duplex. Para un mejor rendimiento de la red se puede realizar en forma full-duplex (Gibabit-Ethernet solo utiliza full-duplex).

Las órdenes que nos permiten configurar estos parámetros serían algo así:

ALISAL(config-if)# duplex [auto | full | half]

ALISAL (config-if)# speed [10 | 100 | auto]

La seguridad de los puertos puede limitar el número de direcciones MAC posibles y también asignar una determinada dirección a ese puerto. En el ejemplo siguiente asigna un máximo de 10 direcciones MAC a un puerto y asigna la dirección 00.0A.1A.3A.A8.15.

ALISAL(config)# interface FastEthernet 0/1

ALISAL(config-if)# switchport port-security maximum 10

ALISAL(config-if)# switchport port-security mac-address 000A.1A3A.A815

Las Sticky secure MAC addresses son direcciones configuradas dinámicamente, almacenadas en la tabla y que no se necesita reconfigurar si el switch se reinicia.

ALISAL(config-if)# switchport port-security mac-address sticky

Autoevaluación

Si quieres especificar que cada puerto solamente acepte una dirección MAC, utilizarás el comando:

- interface FastEthernet 0/1.
- ip address 192.168.1.3 255.255.255.0.
- switchport port-security maximum 1.
- show mac-address-table.

Configuración estática y dinámica de la tabla de direcciones MAC.

Caso práctico

Tomás ha descubierto que la tabla de direcciones MAC es uno de los parámetros más importantes de configuración del switch, al contrario de lo que pensaba, es algo que se puede modificar, lo cual le ha parecido curioso, porque siempre había pensado que el conmutador solamente lo podía hacer de manera automática.

Uno de los elementos más importantes de un conmutador es su tabla de direcciones MAC, permite relacionar las direcciones MAC con el puerto por el cual se alcanzan.

El comando show nos permite ver el contenido de la tabla de direcciones MAC:

```
ALISAL#show mac-address-table
```

El resultado nos muestra la tabla de direcciones del switch. El aspecto que tiene la tabla de direcciones MAC es:

Tabla de direcciones MAC

VLAN	MAC ADDRESS	TYPE	PORTS
All	0100.0CCC.EEEE	STATIC	Ethernet 0/2
All	0100.0CCC.EEEC	STATIC	Ethernet 0/3
All	0180.C211.0000	STATIC	FastEthernet 0/26
All	0100.0CCC.EEEE	STATIC	FastEthernet 0/27
All	0100.0CCC.EEEC	STATIC	FastEthernet 0/26
All	0012.2EEE.CCCC	DYNAMIC	FastEthernet 0/26

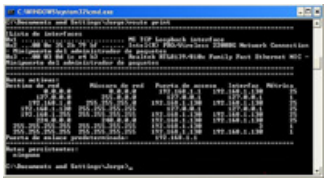
Se puede apreciar como la tabla está formada por direcciones estáticas y dinámicas. En el caso de que solamente se quisieran ver las direcciones aprendidas dinámicamente se usa el comando:

```
ALISAL#show mac address-table dynamic
```

Si queremos refrescar la tabla de direcciones para que el conmutador la "aprenda" de nuevo utilizaremos la orden:

```
ALISAL# clear mac-address-table
```

Agregar direcciones a la tabla.



Los conmutadores construyen las tablas de direcciones MAC por aprendizaje, lo hacen automáticamente, mediante difusiones van aprendiendo las **direcciones MAC** que son accesibles por cada uno de sus puertos. Aunque este proceso sea automático, también se pueden modificar los registros de estas tablas de manera manual.

Si lo que queremos es agregar una dirección estática a la tabla de direcciones MAC lo haremos de la siguiente forma:

```
ALISAL(config)#interface FastEthernet 0/1

ALISAL(config)#mac-address-table static 00E0.2917.1884 interface fastethernet 0/4
```

Con la línea de órdenes anterior hemos asociado la dirección MAC 00E0.2917.1884 al puerto 4 del conmutador y ha quedado grabado en la tabla MAC.

Si dejamos que el switch genere la tabla MAC de manera dinámica, podemos marcar el tiempo de la entrada en la tabla con una orden como:

```
ALISAL(config)# mac-address-table aging-time [time]
```

También podemos hacer que se relacione de manera permanente una dirección MAC con una interfaz determinada:

```
ALISAL(config)# mac-address-table permanet [MAC] [interface]
```

Por lo general un conmutador puede rellenar la tabla de direcciones de forma automática mediante el aprendizaje de las direcciones MAC de las tramas recibidas. Los pasos que sigue son los siguientes:

1. El switch comprueba la dirección MAC origen.
2. Busca en su tabla de direcciones MAC.
3. Si encuentra la dirección la actualiza.
4. Si no encuentra la dirección la agrega a la tabla.

Podemos agregar un contador de "envejecimiento" para las direcciones de la tabla, para que ésta se actualice periódicamente.

```
ALISAL(config)# mac-address temporizador envejecimiento 500
```

Si queremos modificar un registro, por ejemplo, borrar una dirección estática de la tabla:

ALISAL(config)#no mac-address-table static static 00E0.2917.1884 interface fastethernet 0/4

O queremos borrar una entrada de una dirección permanente:

ALISAL(config)# no mac-address-table permanet [MAC] [interface]

Diagnóstico de incidencias del conmutador.

Caso práctico

Después de estar enredando en la configuración del switch, **Tomás ha visto que el funcionamiento de la red no ha mejorado, es más, parece que incluso a veces se ralentiza**. Buscando en Internet posibles causas ha encontrado que existen métodos para **monitorizar el funcionamiento de los conmutadores** y permiten mejorar su rendimiento.

El conmutador como cualquier otro dispositivo de la red **puede tener fallos o defectos en su funcionamiento** producto de agentes externos o de malas configuraciones por parte del usuario administrador. Puesto que es un dispositivo que puede llegar a actuar en los **tres primeros niveles OSI**, lo más adecuado para poder solventar las incidencias es tratar de aislar los problemas clasificándolos por niveles.

Para solucionar posibles problemas es necesario seguir básicamente tres pasos:

1. **Predicción del funcionamiento normal. Hay que saber qué es lo que tiene que hacer la red si funciona correctamente.**
2. **Aislamiento del problema. Intentar determinar dónde comienza el problema y hasta donde funciona correctamente nuestro sistema.**
3. **Analizar las causas de los problemas detectados. Una vez detectado e identificado el problema hay que analizar las causas que lo provocaron para poder proponer una solución los más óptima posible.**

Con el comando show, podemos ver el estado de la configuración actual del equipo utilizando:

ALISAL#show running config

ALISAL#show ip (muestra la dirección IP del switch ALISAL)

ALISAL#show mac-address-table (muestra la tabla de direcciones MAC)

ALISAL#show interfaces status (muestra el estado de configuración de las interfaces)

ALISAL#show interface ethernet 0/1 (muestra las estadísticas de la interface ethernet)

ALISAL#show port-security interface Ethernet 0/1 (muestra las configuraciones de seguridad)

ALISAL#show vlan 1 (muestra información sobre la VLAN)

Otro comando es *debug*, en lugar de mostrar mensajes sobre el estado actual, obliga al conmutador a continuar monitorizando diferentes procesos del mismo. Mientras que el comando *show* muestra mensajes para un único usuario, *debug* muestra mensajes para todos los usuarios interesados en verlos.

El comando *debug* puede generar muchos mensajes en el conmutador por lo que será conveniente antes de usar un comando *show* o *debug* ejecutar una de las dos órdenes siguientes para cancelar todas las depuraciones anteriores, si las hubiera.

ALISAL#no debug all

ALISAL#undebug

Las incidencias más comunes son las relacionadas con los problemas de configuración de tablas y la incompatibilidad de las velocidades y tipo de comunicación dúplex entre los puertos de diferentes conmutadores.

Problemas de velocidad y tipo de comunicación.

Al configurar los interfaces de nuestro conmutador se tiene la **opción de configuración automática para la velocidad y tipo de comunicación (dúplex, semidúplex), configuración de autonegociación. Si se utiliza la opción de autonegociación**, se auto configurará la opción más rápida para la velocidad y comunicación tipo dúplex si es soportada.

Cuando alguno de los dispositivos no tiene configurada la opción de autonegociación, el que utiliza autonegociación, configura sus puertos en modo dúplex o semidúplex dependiendo de velocidad de comunicación que detecte.

Hay tres opciones dependiendo de la velocidad detectada por el conmutador que utiliza autonegociación:

- **Se configura el conmutador con una velocidad de 10 Mbps y comunicación semidúplex, cuando la velocidad se desconoce.**
- **Se configura el switch con un tipo de comunicación semidúplex si la velocidad detectada está entre 10 y 100 Mbps.**

- **Se establece una comunicación dúplex si la velocidad detectada es de 1000 Mbps.**

Algunos switches pueden conocer la velocidad del dispositivo con el que estén conectados utilizando mecanismos de detección de señales eléctricas, incluso si tienen desactivada la autonegociación.

Si uno de los equipos funciona en forma semidúplex y el otro lo hace en dúplex, se pueden ocasionar errores de rendimiento, pérdidas de tramas, desbordamiento en el lado del dispositivo que funciona en semidúplex y como consecuencia un mal funcionamiento de la red.

Es recomendable utilizar siempre el parámetro de autonegociación y no fijar parámetros de velocidad.

Si no utilizamos la autonegociación en ambos extremos se puede dar la no sincronización del establecimiento de enlace.

Si el cable que utilizamos es demasiado largo o está dañado algún par, las notificaciones entre los extremos se pueden distorsionar y uno de los extremos puede interpretar, por ejemplo, que al otro lado la comunicación es semidúplex, por no recibir los impulsos eléctricos suficientes. Si ese extremo está configurado manualmente como dúplex, entonces no se estable el enlace físicamente.

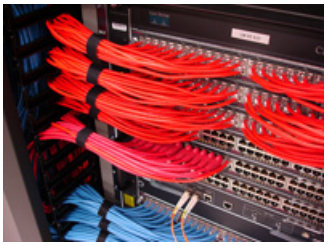
Encontrar una incompatibilidad en el tipo de comunicación (dúplex), es mucho más complicado que encontrar una incompatibilidad en la velocidad ya que no generan una pérdida total del enlace, en esta situación el enlace tendrá un funcionamiento suficientemente bueno como para que no nos alarmemos.

- **El problema es que un dispositivo semidúplex cree que sólo puede hablar un dispositivo a la vez, así que no se comunicará mientras detecte que el dúplex esté transmitiendo.**
- **El dispositivo dúplex cree que ambos dispositivos pueden hablar al mismo tiempo.**
- **Cuando el semidúplex detecta al dúplex detiene su transmisión y espera para poder acceder al medio compartido.**
- **El dispositivo que funciona en dúplex acaba su transmisión y piensa que todo ha ido correcto pero también recibirá un mensaje del semidúplex indicándole que ha habido algún error en la transmisión por lo que añadirá valores a su contador de errores CRC.**
- **El semidúplex iniciará ahora la comunicación al pensar que el canal está vacío, pero ahora es el dúplex el que no hace nada porque no sabe que su comunicación no llegó.**
- **De esta forma, el semidúplex nunca recibe la información.**

Para detectar esto se utiliza el comando show y se controlan los valores asignados a CRC, un número elevado podría ser un síntoma de una mala configuración del tipo de comunicación (dúplex, semidúplex).

```
ALISAL#show interfaces ethernet 0/1
```

Tecnología Auto-MDIX.



Los organismos de estandarización han establecido ya algunas **normas en las configuraciones de los conmutadores**, para evitar las incidencias en el funcionamiento de los mismos. Por ejemplo, de acuerdo con la especificación IEEE, el uso de la Ethernet Gigabit requiere el uso de la auto-negociación, por lo que 1000Mb/s no es una configuración fija válida, en un dispositivo de red que siga fielmente las especificaciones IEEE.

Aparte de las normas que puedan establecer los distintos organismos de estandarización, para solucionar problemas en la comunicación, los conmutadores incorporan tecnologías como Auto-MDIX.

Auto-MDIX permite detectar y corregir automáticamente cruces en los cables Ethernet, y de esta forma adaptarse automáticamente usando el mismo cable, aunque se conecte switch a switch, o switch a dispositivo final.

Con la tecnología **Auto-MDIX** nos olvidamos de la regla que se establecía en redes que decía que para conectar dos dispositivos iguales entre sí había que emplear un cable de red cruzado.

Por ejemplo, si conecto dos ordenadores entre sí sin utilizar ningún elemento de interconexión (hub, switch, router), debo utilizar un cable cruzado.

Hasta la aparición de Auto-MDIX, si quería conectar dos conmutadores entre sí, también tenía que utilizar un cable cruzado.

Esto es lógico si pensamos que para que un dispositivo pueda conectarse con otro el cable que se utiliza para enviar información en uno de los equipos, debe estar conectado al cable que se utiliza para recibir información en el otro equipo y viceversa.

Un ejemplo de configuración de la interfaz para que ejecute Auto-MDIX es el siguiente:

```
ALISAL# configure terminal

ALISAL(config)# interface ethernet 0/1

ALISAL(config-if)# speed auto

ALISAL(config-if)# duplex auto

ALISAL(config-if)# mdix auto

ALISAL(config-if)# end
```

Cómo se puede ver, para que Auto-MDIX funcione correctamente se debe configurar la velocidad y el tipo dúplex en autonegociación.

Si queremos dejar de ejecutar Auto-MDIX deberíamos ejecutar:

```
ALISAL(config-if)# no mdix auto
```

Autoevaluación

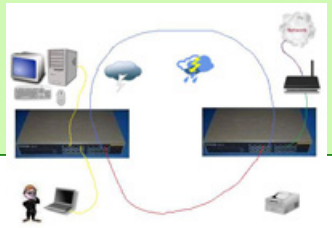
Observa la siguiente secuencia de órdenes:

```
SWITCH(config)# interface ethernet 0/1
SWITCH(config-if)# mdix auto
```

- Falta la orden end para que la configuración sea buena.
- Falta la orden configure terminal.
- Faltaría establecer la autonegociación en velocidad y tipo de enlace.
- Estas órdenes solamente son válidas para FastEthernet.

Las tormentas de broadcast.

Caso práctico



Después de analizar la red y conseguir mejorar el rendimiento, **Tomás ha decidido que como medida de prevención para que su red nunca falle va a comprar otro conmutador igual para poder tener dos caminos diferentes hacia Internet**; unirá los dos conmutadores entre sí. El vendedor, después de cobrarle, le ha alertado sobre el peligro de las "tormentas de broadcast". Tomás no sabe qué tipo de fenómeno atmosférico es ese.

Una tormenta de broadcast es una propagación sucesiva de broadcast. Como consecuencia de esto, los conmutadores ocuparan todo su tiempo en reenviar los broadcast y harán que la comunicación entre los usuarios sea muy lenta e incluso nula.

El origen de las tormentas de broadcast está en la **redundancia de las rutas** (bucles de conmutación). Estas rutas redundantes son convenientes cuando se apilan varios switches para asegurarnos siempre la comunicación frente a fallos en algunos de los conmutadores.

Los switches inundan todas las interfaces, salvo la interfaz por donde llegó la trama de petición, con tramas de difusión hasta que encuentran el destinatario para incorporarlo a su tabla de direcciones con la esperanza de que el destinatario desconocido se encuentre en alguno de los segmentos de red. Si no aparece y además hay bucles en nuestra instalación, esto puede llevar a una "tormenta de broadcast".

Se pueden dar problemas como la recepción de múltiples copias de tramas, al enviarse la trama de un equipo por dos segmentos distintos hacia un mismo equipo receptor, el registro de la dirección MAC de un equipo, recibido por distintos puertos y la saturación de la red.

En la imagen anterior se puede observar como tenemos una red formada por 2 conmutadores (SW1 y SW2) y 2 PC. Con esta topología, tenemos más probabilidades de que la comunicación entre los dos equipos A y B esté siempre activa, pero tiene algunos inconvenientes provocados por los circuitos redundantes (línea verde y línea roja).

Supongamos que tenemos el PC B apagado y que los conmutadores los acabamos de comprar y no conocen el entorno en el que están instalados, es decir, sus tablas de direcciones MAC están vacías.

En un instante habrán reconocido al PC A, pero al B siguen sin conocerle (está apagado). Ahora A envía un mensaje buscando a B, como SW1 no sabe donde está B, inundará todos sus puertos activos con la trama de búsqueda de B (excepto el puerto por el que recibió la petición por parte de A), cuando la trama de búsqueda llega a SW2 preguntará por B, no se obtiene ninguna respuesta por parte de SW2 puesto que no conoce a B. Ahora es SW2 quien inundará todos sus puertos (excepto por el que recibió la trama) con una trama de búsqueda de B y la petición llegará al SW1 de nuevo con lo que estaremos de nuevo en el comienzo del ciclo.

Todo este proceso se repetirá como un bucle hasta provocar un colapso en la red, una tormenta, los conmutadores continuarán preguntándose uno a otro por B sin obtener ninguna respuesta. La solución pasará por desconectar uno de los conmutadores y romper el ciclo.

La estructura de rutas redundantes es necesaria para asegurarnos la confiabilidad de las redes y por lo tanto se han diseñado mecanismos que hacen que este tipo de topologías funcionen como si no tuvieran ningún bucle físico. **Uno de estos mecanismos es el protocolo spanning-tree.**

El protocolo spanning-tree.

Caso práctico

La tormenta de la que el vendedor del switch alertó a Tomás, efectivamente se produjo. Estaba claro que uniendo los dos conmutadores entre sí tendríamos un camino suplementario para nuestro equipo, pero también nos encontramos con un ciclo en la comunicación que en lugar de agilizar entorpeció el funcionamiento de la red.

Menos mal que Tomás descubrió un protocolo que lo arregló todo e hizo que saliera el Sol en su red.

Las rutas redundantes o bucles de conmutación son los causantes de las tormentas de broadcast pero a su vez son sinónimo de confiabilidad, nos aseguran que las probabilidades de perder la comunicación en nuestra red disminuyan, por lo tanto, son necesarias en muchas ocasiones. La necesidad de confiabilidad en nuestra red nos lleva a tener que diseñar mecanismos para que estas rutas existan físicamente pero no funcionen como bucles infinitos; esto se consigue mediante el protocolo "spanning-tree" (STP).

Este protocolo hace que la red funcione como si tuviera una estructura de árbol en lugar de una estructura cíclica, evitando de esta manera los bucles sin salida, físicamente mantenemos los enlaces pero lógicamente funciona sin bucles.

Si en la figura anterior tuviéramos una topología en la que todos los conmutadores estuvieran conectados entre sí, en la que para ir del conmutador 1 al 4 tuviéramos más de 1 camino posible, el protocolo **Spanning Tree** convertiría esa **topología en una topología lógica en la que solamente hubiera un camino entre el switch 1 y el switch 4.**

En esencia el protocolo consiste en designar a uno de los conmutadores como el nodo raíz de un árbol y a partir de este dirigir la comunicación para que no se produzcan bucles, para ello en algunos de los casos se deben inhabilitar puertos para que no haya comunicación a través de ellos.

Cuando los caminos principales están operativos, se deshabilitan los caminos redundantes y cuando falla algún camino principal, se activan los redundantes.

Básicamente la configuración STP se basa en cuatro parámetros:

- **Elegir el nodo raíz. El Bridge ID (prioridad y MAC) más bajo.**
- **Elegir el camino más adecuado hacia el nodo raíz. El coste de Root Path más bajo.**
- **El Bridge ID de origen más bajo.**
- **El puerto (el port ID) de origen más bajo.**

Proceso

La elección del conmutador raíz se hace a través de un proceso entre todos los switches que forman la red.

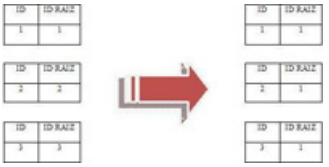
Cada switch tiene un identificador (ID), este indicador consta de dos partes:

- Prioridad: Número entre 0 y 65535 y que por defecto toma el valor 32768. Variando este valor podemos hacer que un conmutador tenga más fácil el ser conmutador raíz.
- Dirección MAC (6 bytes): Es la dirección física del conmutador.

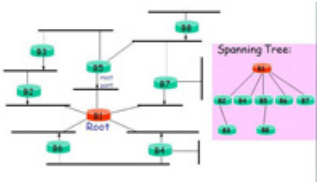
Un switch siempre se considera el raíz, cuando todos los demás hacen lo mismo comienzan a intercambiarse mensajes BPDU.

Los mensajes BPDU incorporan su ID (MAC + prioridad) y un campo que identifica al conmutador raíz con su ID. Como cada conmutador tiene una MAC distinta, el que resulte con un BPDU más bajo será el raíz, la prioridad por defecto es 32768. Si un administrador quiere, puede establecer la prioridad de un switch manualmente a un valor menor que 32768 y hacer que sea el conmutador raíz.

Como cada uno se considera el raíz, al principio todos colocaran su ID en la parte del mensaje reservada para el ID de raíz, a medida que van recibiendo mensajes BPDU de los demás irán cambiando el valor del campo "root bridge ID" por el valor de un ID de switch menor que el que tienen grabado. Normalmente el número que marca la prioridad es igual en todos, así que gana el que tiene una MAC menor.



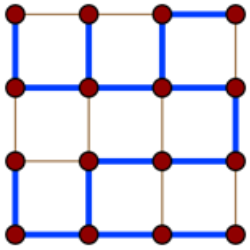
En la figura anterior, supongamos que en cada uno de los tres conmutadores la concatenación de la prioridad y de la MAC es 1, 2 y 3. En principio todos tienen en el campo ID-RAIZ de sus BPDU un valor que les identifica a ellos mismos como conmutadores raíz (todos quieren mandar), después del proceso de intercambios de BPDU se establece que el conmutador raíz es el que tiene el ID igual a 1 como era de esperar.



En la imagen anterior se puede observar una red con 8 dispositivos de interconexión en los que después del intercambio de paquetes BPDU se ha designado al B1 como raíz y se ha trazado la ruta hacia el raíz desde todos los demás.

El funcionamiento lógico de la red pasará ahora a ser en forma de árbol **evitando de esta manera los bucles en la comunicación y de esta manera las tormentas de broadcast.**

Comandos para activar spanning tree



El protocolo spanning tree puede ser activado y desactivado en los conmutadores que tengan esta capacidad, para ello se utiliza el comando:

ALISAL#spanning-tree vlan 1

ALISAL#no spanning-tree vlan 1

Para ver la configuración spanning tree de nuestro switch, utilizaremos:

ALISAL#show spanning-tree

Si queremos saber el switch que actúa como raíz:

ALISAL#show spanning-tree root

Como se puede deducir del punto anterior, básicamente la configuración STP se basa en cuatro parámetros:

- **El Bridge ID (prioridad y MAC) más bajo.**
- **El coste de Root Path más bajo. Costes de puerto hacía el conmutador raíz.**
- **El Bridge ID de origen más bajo. Es el conmutador que tiene menor coste de camino hacia el puente raíz.**
- **El puerto (el port ID) de origen más bajo. En cada conmutador, es el puerto con menor coste de ruta hacía el conmutador raíz.**

Se puede configurar un switch para que sea raíz de manera manual asignándole una prioridad con un valor más bajo de los que hay en la red, para ello necesitamos saber el valor de la prioridad de todos los switches. Para poder cambiar la prioridad tenemos que usar el comando:

ALISAL(config)#spanning-tree vlan Nº-vlan priority Nº-prioridad

Por defecto la prioridad es 32768, pero se pueden usar números de 0 a 65535.

Por ejemplo:

ALISAL(config)#spanning-tree vlan 1 priority 4068

Si queremos especificar el costo de una determinada interfaz del conmutador emplearemos:

ALISAL(config)#interface 0/2

ALISAL(config-if)#spanning tree cost 90

Si en un conmutador queremos establecer una determinada prioridad para un puerto usaremos el comando:

ALISAL(config-if)#spanning-tree port-priority 8

Debes conocer

Aquí podrás ver una simulación de cómo funciona el protocolo spannig-tree.

Spanning tree