CONFIGURACIÓN Y ADMINISTRACIÓN DE CONMUTADORES

Contenido

[Introducción 1](#_Toc431826663)

[Conmutadores y tipos. 2](#_Toc431826664)

[Características de los switchs o conmutadores 4](#_Toc431826665)

[Segmentación de la red 9](#_Toc431826666)

[Conmutadores y dominios de colisión y difusión (broadcast). 10](#_Toc431826667)

[Interconexión entre switchs. 12](#_Toc431826668)

[Formas de conexión al switch para su configuración. 13](#_Toc431826669)

[Switchs gestionables por web. 14](#_Toc431826670)

[Switchs gestionables por línea de comandos vía telnet o SSH. 15](#_Toc431826671)

[Switchs gestionables por puerto de consola. 17](#_Toc431826672)

[Switchs gestionables por SNMP. 18](#_Toc431826673)

[Comandos 19](#_Toc431826674)

[El switch como servidor DHCP. 21](#_Toc431826675)

[Tabla de direcciones MAC. 22](#_Toc431826676)

[Diagnóstico de incidencias 24](#_Toc431826677)

[Tecnología Auto-MDIX. 24](#_Toc431826678)

[El protocolo ARP 25](#_Toc431826679)

[Las tormentas de broadcast 26](#_Toc431826680)

[El protocolo spanning tree 28](#_Toc431826681)

# Introducción

**Caso práctico**

Luisa sigue con su asignatura de redes pero hasta ahora no ha visto ningún dispositivo “en acción”. Se lo comenta a su amigo Juan.

Juan: Pues si has pasado los temas iniciales, que son los más teóricos, ahora viene lo bueno, empezarás a ver el dispositivo más básico y sencillo de las redes, el switch.

Luisa: ¿Sencillo?

Juan: Bueno eso de “sencillo” es relativo, lo hay hasta de nivel tres, pero eso lo verás al final de la asignatura. Básicamente es un dispositivo que conecta a unos ordenadores con otros.

# Conmutadores y tipos.

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

Es importante saber que un switch no proporciona conectividad con otras redes (ni locales ni internet) para ello es necesario un router.

En la actualidad las redes locales cableadas siguen el estándar Ethernet (prácticamente el 100%) donde se utiliza una topología en estrella y donde el switch es el elemento central de dicha topología

Aunque ahora vamos a ver una clasificación de los switch, no existe un consenso en el mundo de las redes para establecer una clasificación clara, cada fabricante establece una clasificación más o menos acorde a su gama de productos. Un ejemplo de la variedad de modelos de switchs es que podemos encontrar en el mercado switchs desde los 10 € hasta los 10.000 € o más.

Tipos de switchs:

**Switchs de configuración fija.**- no se pueden agregar características u opciones al switch más allá de las que originalmente vienen con el switch. Por ejemplo, si se adquiere un switch fijo gigabit de 24 puertos, no se pueden agregar puertos cuando se les necesite. Habitualmente, existen diferentes opciones de configuración que varían en cuanto al número y al tipo de puertos incluidos.



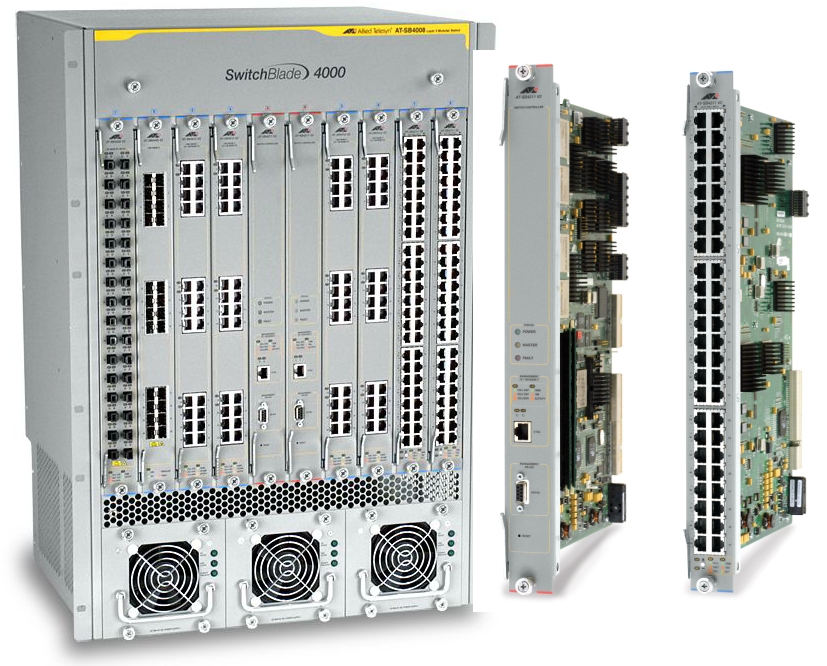
**Switchs modulares.**- ofrecen más flexibilidad en su configuración. Habitualmente, los switchs modulares vienen con chasis de diferentes tamaños que permiten la instalación de diferentes números de tarjetas de línea modulares.



**Switchs apilables.**- Los switchs apilables pueden interconectarse con el uso de un cable especial que otorga rendimiento de ancho de banda entre los switchs.



**Switch troncal / switch perimetral**.- El término switch troncal se refiere a los que se utilizan en el núcleo central (core) de las grandes redes. Es decir, a estos switchs están conectados otros de jerarquía inferior, además de servidores, routers WAN, etc. Por otro lado el término switch perimetral se refiere a los utilizados en el nivel jerárquico inferior en una red local y a los que están conectados los equipos de los usuarios finales.



**Switch desktop o de escritorio.-** Este es el tipo de switch más básico que ofrece la función de conmutación básica sin ninguna característica adicional. Su uso más habitual es en redes de ámbito doméstico o en pequeñas empresas para la interconexión de unos pocos equipos, por lo que no están preparados para su montaje en rack. Estos switchs no requieren ningún tipo de configuración, ya que utilizan el modo de autoconfiguración de Ethernet para configurar los parámetros de cada puerto.



# Características de los switchs o conmutadores

**Número de puertos**

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet. Los switchs de configuración fija admiten hasta 48 puertos.

Un número alto de puertos permite un mejor aprovechamiento de espacio y energía. Si tiene dos switchs y cada uno contiene 8 puertos, se podrían admitir hasta 14 dispositivos porque se necesita un puerto por switch para conectar cada switch al resto de la red y se necesitan dos tomas de corriente. En cambio, un único switch de 48 puertos, admite hasta 47 dispositivos con un sólo puerto para conectar el switch con el resto de la red y sólo una toma de alimentación.

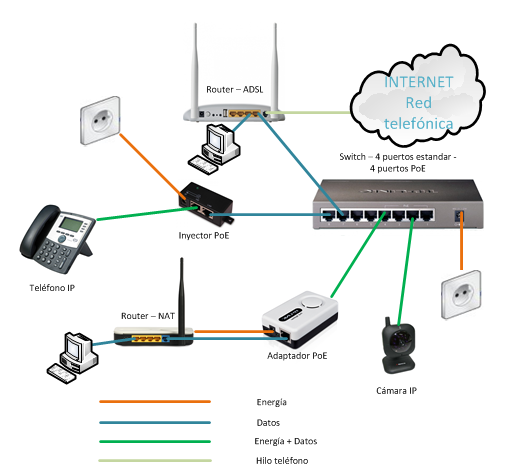
La mayor parte de los switchs de gamas media y alta ofrecen los llamados puertos modulares. Estos puertos realmente no tienen ningún conector específico si no que a ellos se conecta un módulo que contiene el puerto. De esta forma podemos adaptar el puerto al tipo de medio y velocidad que necesitemos. Es habitual que los fabricantes ofrezcan módulos de diferentes tipos con conectores RJ-45 o de fibra óptica. Los puertos modulares proporcionan flexibilidad en la configuración de los switchs.

Existen dos tipos de módulos para conectar a los puertos modulares: el primer tipo de módulo que apareció es el módulo **GBIC** (Gigabit Interface Converter) diseñado para ofrecer flexibilidad en la elección del medio de transmisión para Gigabit Ethernet. Posteriormente apareció el módulo **SFP** (Small Form-factor Puggable) que es algo más pequeño que GBIC (de hecho también se denomina mini-GBIC) y que ha sido utilizado por los fabricante para ofrecer módulos tanto Gigabit como 10GbE en fibra o en cable UTP.



**Power over Ethernet**

Power over Ethernet (PoE) permite que el switch suministre energía a un dispositivo por el cableado de Ethernet existente. Esta característica puede utilizarse por medio de los teléfonos IP y algunos puntos de acceso inalámbricos. PoE permite mayor flexibilidad al instalar los puntos de acceso inalámbricos y los teléfonos IP porque se los puede instalar en cualquier lugar donde se puede tender un cable de Ethernet. No es necesario considerar cómo suministrar energía eléctrica normal al dispositivo. El inconveniente es el incremento de coste.



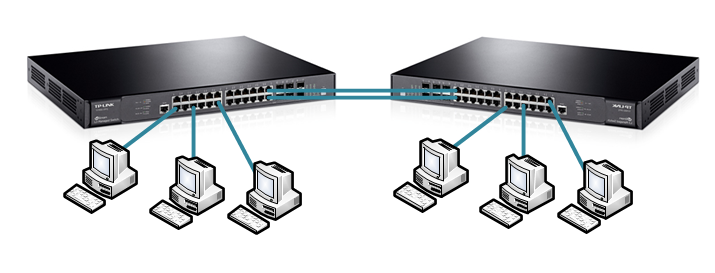
**Velocidad**

Dado que Ethernet permite varias velocidades y medios de transmisión, otra de las características destacables sobre los puertos de los switchs es precisamente la velocidad a la que pueden trabajar sobre un determinado medio de transmisión. Podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares 10BASE-T (con una velocidad de 10 Mbps) y 100BASE-TX (velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar 1000BASE-T (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE-FX y 1000BASE-X.

Por último, los switchs de altas prestaciones pueden ofrecer puertos que cumplan con el estándar 10GbE, tanto en fibra como en cable UTP.

**Agregación de enlaces**

La agregación de enlaces consiste en unir varios puertos entre dos switchs de forma que aumenta el ancho de banda y se eliminan cuellos de botella. Por ejemplo si tenemos 2 switchs con puertos GigaEthernet que comunican dos sectores grandes de la red nos puede interesar conectar 2 puertos entre los switchs de forma que duplicamos la velocidad de la conexión entre ambos.



**Funciones de la Capa 3 / 4**

Normalmente, los switchs operan en la Capa 2 del modelo de referencia OSI, donde pueden ocuparse principalmente de las direcciones MAC de los dispositivos conectados con los puertos del switch.

Los switchs de gama alta utilizados en el troncal de redes Ethernet de mediana y gran envergadura suelen ofrecer capacidades de enrutamiento de paquetes IP. A este tipo de switchs se le conoce como switchs de nivel 3. Un switch de nivel 3 realiza todas las funciones de conmutación de un switch pero además proporciona funciones de enrutamiento IP. Esta característica es especialmente útil para switchs que utilicen VLAN y necesiten comunicar algunas de sus redes LAN virtuales.

Además, pueden existir switchs que ofrezcan características relacionadas con funciones del nivel 4, como control de puertos. A estos switchs se le conoce como switchs de nivel 3 / 4.

**Seguridad de puerto**

La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch

Hay 3 tipos de seguridad de puerto:

* Dinámico: Al configurar la dinámica en un puerto conseguimos que se guarde la dirección MAC de la primera conexión a ese puerto y a partir de ese momento, solo esa dirección MAC tendrá acceso impidiendo que una MAC diferente se conecte. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia.
* Estático: En este caso configuramos manualmente las direcciones MAC que queremos que tengan acceso.
* Persistente: Es similar al dinámico, se aprenden dinámicamente pero con la diferencia de que se almacenan.

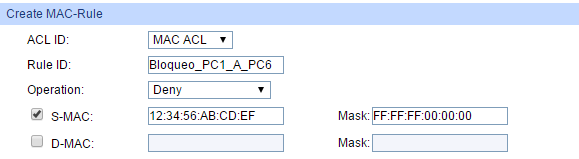
**VLAN**

Una VLAN (‘Red de Área Local Virtual) es un método de crear [redes](http://es.wikipedia.org/wiki/Red_de_computadoras" \o "Red de computadoras) lógicamente independientes dentro de una misma red física. A efectos prácticos es como si dividiéramos el switch en pequeños switchs, uno por cada VLAN definida.

Este tema se verá a fondo en la unidad “Configuración de Redes Virtuales”

**ACL**

Una Lista de Control de Acceso (ACL) permite que el switch impida ciertos tipos de tráfico y autorice otros. Las ACL también permiten controlar qué dispositivos de red pueden comunicarse en la red. El uso de las ACL es un procesamiento intensivo porque el switch necesita inspeccionar cada paquete y observar si coincide con una de las reglas de la ACL definida en el switch



**Tasa de reenvio**

Existen dos técnicas para llevar a cabo la transferencia de los datos entre puertos de un switch:

* **Reenvío directo**(cut-through). En esta técnica, cuando un switch comienza a recibir datos por un puerto, no espera a leer la trama completa para reenviarla al puerto destino. En cuanto lee la dirección de destino de la trama MAC, comienza a transferir los datos al puerto destino.

Esta técnica proporciona unos tiempos de retardo bastante bajos, sin embargo, tiene como inconveniente que sólo puede usarse cuando las velocidades de todos los puertos son iguales.

Otro problema que plantea la técnica cut-through, debido a su forma de funcionamiento, es que los switchs propagan tramas erróneas o tramas afectadas por colisiones. Una posible mejora para evitar la propagación de tramas con colisiones es retrasar el reenvío hasta que se lean los primeros 64 bytes de trama, ya que las colisiones sólo se pueden producir en los primeros 64 bytes de la trama. Esta mejora sin embargo aumenta el tiempo de retardo.

* **Almacenamiento y reenvío**(Store and Forward). En este caso, cuando un switch recibe datos por un puerto, almacena la trama completa en el buffer para luego reenviarla al puerto destino. La utilización de esta técnica permite realizar algunas comprobaciones de error antes de ser enviada al puerto de destino.

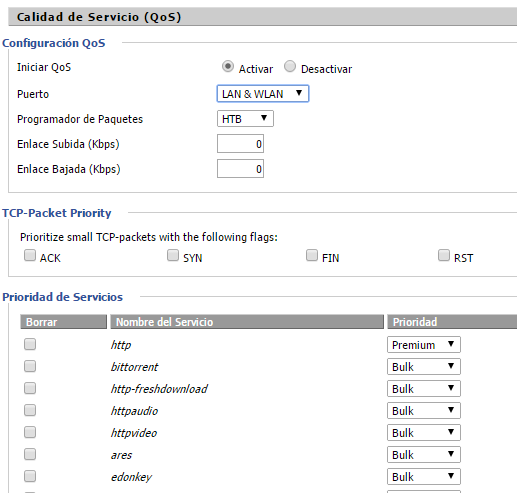
El tiempo de retardo introducido es variable ya que depende del tamaño de la trama, aunque suele ser superior al proporcionado por la técnica cut-through, sin embargo, es imprescindible utilizar esta técnica cuando existen puertos funcionando a diferentes velocidades.

Las tasas de reenvío definen la capacidad de procesamiento de un switch estimando la cantidad de datos que puede procesar por segundo el switch. Un switch que funciona a velocidad de cable completa, si tiene 24 puertos envía a la vez 24 Gb/s de datos.

**Calidad de servicio**

La calidad de servicio (QoS, Quality of Service) hace referencia a la capacidad que tiene un sistema de asegurar que se cumplen los requisitos de tráfico para un flujo de información determinado.

La QoS adquiere mucha importancia cuando hablamos de tráfico que es imprescindible que tenga un determinado ancho de banda asegurado, como por ejemplo la VoIP (Voz sobre IP) o aplicaciones multimedia como videos (si el video no se recibe a la suficiente velocidad se para la imagen)



**Conmutación asimétrica o simétrica**

En un switch simétrico, todos los puertos cuentan con el mismo ancho de banda. En cambio los switchs asimétricos ofrecen mayor flexibilidad porque permiten conectar segmentos de la red a diferentes anchos de banda. Actualmente la mayoría de switchs son asimétricos.



# Segmentación de la red

Segmentar una red es crear pequeños dominios de colisión principalmente para mejorar el rendimiento de la red y mejorar la seguridad

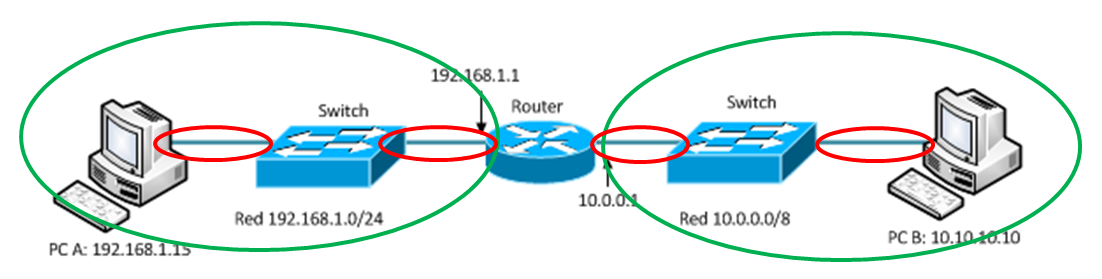
La segmentación aísla el tráfico entre los distintos segmentos de la red.

La segmentación se puede llevar a cabo utilizando puentes, switchs o routers.

Un segmento de red es un conjunto de dispositivos que está en el mismo dominio de colisión.

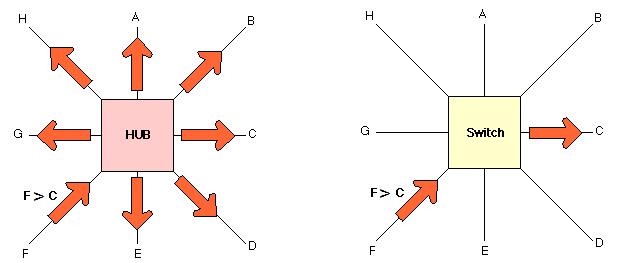
Por ejemplo, cinco equipos conectados en un bus Ethernet constituyen un único segmento de red porque el bus constituye un dominio de colisión.

El router crea dominios de difusión y el switch crea dominios de colisión:



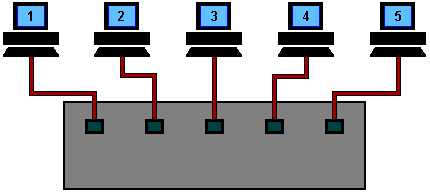
# Conmutadores y dominios de colisión y difusión (broadcast).

Un switch es un dispositivo de interconexión de nivel 2 que es capaz de generar diferentes dominios de colisión. La diferencia entre un hub (concentrador) y un switch (conmutador) es que un hub recibe información por un puerto y la reenvía por todos los demás mientras que un switch reenvía la información solamente por los puertos a los que va dirigida.

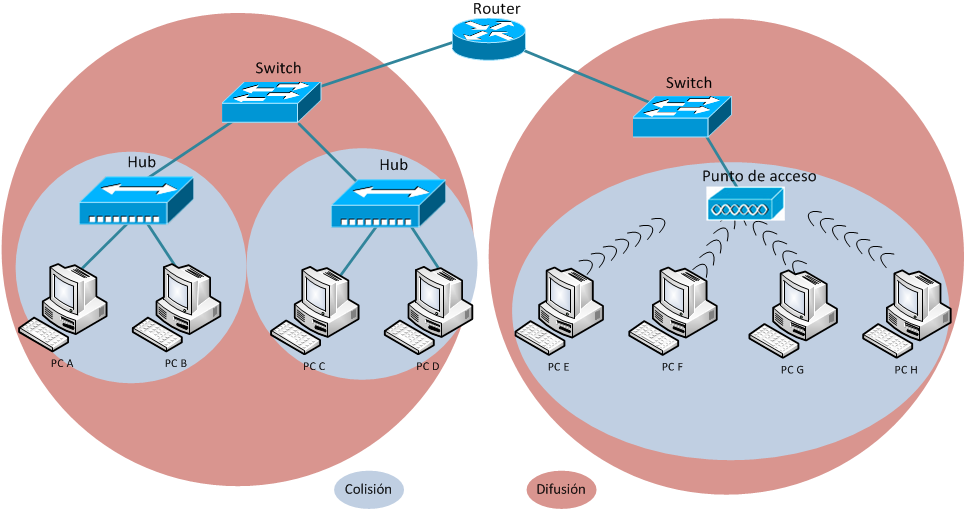


Los switchs reconocen las direcciones Ethernet (MAC) de los nodos de cada segmento de la red, y permiten sólo el tráfico necesario para la comunicación entre los equipos implicados en el mismo dominio de colisión. Un paquete es recibido por el switch, este examina las direcciones MAC origen y destino 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 aprende** del entorno las direcciones MAC que le rodean y crear tablas para recordar donde está cada una, 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.



El switch “normal” no crea dominios de difusión, puesto que esto son segmentaciones a nivel 3, es decir, un dominio de difusión equivale a una red y el dispositivo que separa una redes de otras es el router.



Sin embargo, existen switchs que trabajan en el nivel 3, son switchs con características de routers, enrutan los paquetes a las direcciones IP de los usuarios.

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

https://avanza.educarex.es/cursos/file.php/948/moddata/scorm/12796/icon_autoevaluacionfpd.gifAutoevaluación

Los dispositivos que crean diferentes dominios de colisión son:

* Routers y hubs
* Puentes, switchs y routers. (Correcta)
* Solamente los hubs.
* Solamente los routers.

Retroalimentación:

* No, un hubs es como un cable al que están conectados todos los equipos.
* Enhorabuena, has acertado.
* Falso. Un hub no crea dominios de colisión.
* Incorrecto. El router sí crea dominios de colisión, pero no es el único.

# Interconexión entre switchs.

Los switchs se pueden conectar entre sí de manera que funcionen como una sola entidad, en el caso de los switchs “domésticos” no vienen equipados con ninguna conexión especial para apilarlos (stack), en este caso la única precaución que tenemos que tomar es seguir un orden jerárquico, donde el switch central sea el más veloz.



En el caso switch “profesionales”, un grupo de switchs (stack) puede apilarse (uniéndolos con enlaces de alta velocidad) y comportarse como un único switch con la capacidad de puertos de la suma de todos ellos.

**Stacking** consiste en agrupar diversos switchs de manera que cara la red aparentan ser un solo dispositivo.



Estos switchs profesionales admiten la gestión a través de una IP y desde esta IP se puede gestionar toda la pila. Aunque como hemos estudiado un switch es un dispositivo de nivel 2 y no tiene sentido una IP (nivel 3), esta es exclusivamente para la configuración de forma más cómoda puesto que desde cualquier PC de la red configuramos el stack.

Para apilar los switchs se utilizan puertos específicos para ser enlazados entre sí, empleando conectores dedicados (pueden ser de cobre o Fibra óptica)

Uno de los switchs toma el papel de rector del stack, lo denominamos Master Switch (unidad maestra o raíz), será el switch al que deberemos conectarnos para administrar el conjunto, bien vía IP (web, ssh o telnet) o directamente por conexión de consola. Normalmente otro de los switch toma el papel de Backup, si falla el master switch este tomará el control.



# Formas de conexión al switch para su configuración.

Desde su aparición en el mercado, los switchs no gestionables han utilizado una tecnología plug & play (conectar y funcionar), todo lo que han necesitado saber lo han "aprendido" de su entorno. Es el caso de la mayoría de los switchs para pequeña empresa y hogar.

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.

Pero también podemos encontrar en el mercado switchs con grandes prestaciones, gestionables vía web, apilables, con funcionalidades de nivel 3, etc.



## Switchs gestionables por web.

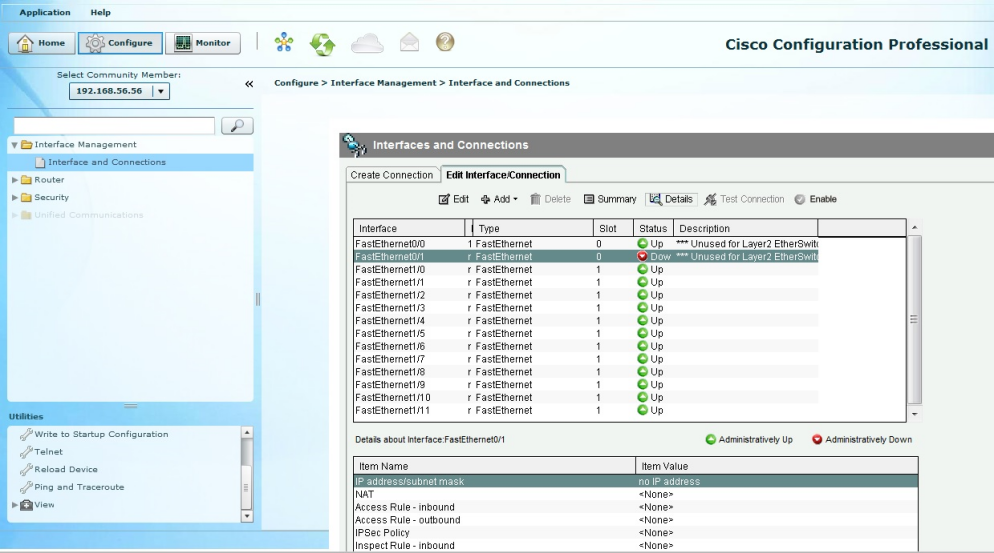
Sin duda alguna la tendencia actual es a administrar los switchs a través de entorno web, desde cualquier PC con un simple navegador se puede gestionar un switch, no se necesitan cables especiales ni software adicional, las pantallas de configuración son intuitivas y no tan tediosas como la linea de comandos (con un simple clic podemos activar o desactivar un puerto).

Normalmente estos switchs no tienen puerto consola (COM) y muchos solo admiten configuración via web, es decir, no tiene configuración por comandos.

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, la IP que trae de fábrica, suele venir indicada en el manual, y se trata de una IP privada tipo 192.168.1.1 o 10.0.0.1, 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 10.10.10.10, nuestra tarjeta de red deberá tener una IP del mismo rango por ejemplo 10.10.10.11.
* Escribir la dirección IP del switch en la barra de direcciones de navegador. Es posible que aquí tengamos que introducir usuario y contraseña (los que traiga de fábrica al ser el primer acceso)

En otras ocasiones el fabricante puede incluir un software adicional, este es el caso de Cisco Systems que incluye su software [Cisco Configuration Professional](http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-professional/index.html)



También en estos enlaces hay simuladores de las pantallas web de configuración de diferentes dispositivos:

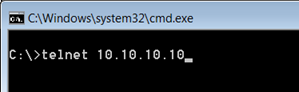
* [Linksys](http://ui.linksys.com/files/)
* [Netgear](http://www.voiproblem.com/emulators/Netgear/)
* [Tp-link](http://www.tp-link.com/en/support/emulators/)
* [Cisco](https://supportforums.cisco.com/community/911/cisco-small-business-online-device-emulators)

## Switchs 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 switch (una vez realizados los mismos pasos que en apartado anterior) abrimos una consola y tecleamos:

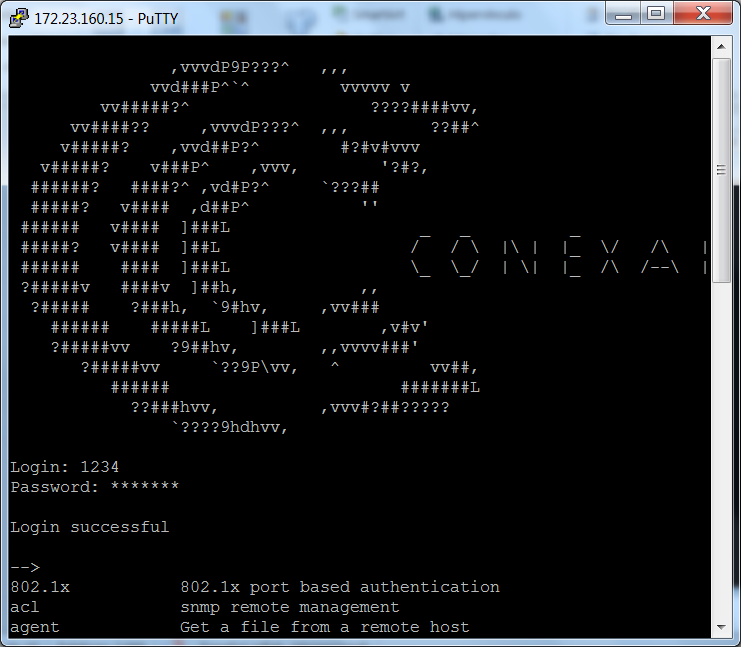


Normalmente, nos pedirá un nombre de usuario y una contraseña para autentificarnos y acceder al switch. El protocolo telnet está deshabilitado en muchos dispositivos porque se considera poco seguro y en la actualidad se utiliza el ssh con más frecuencia.

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:

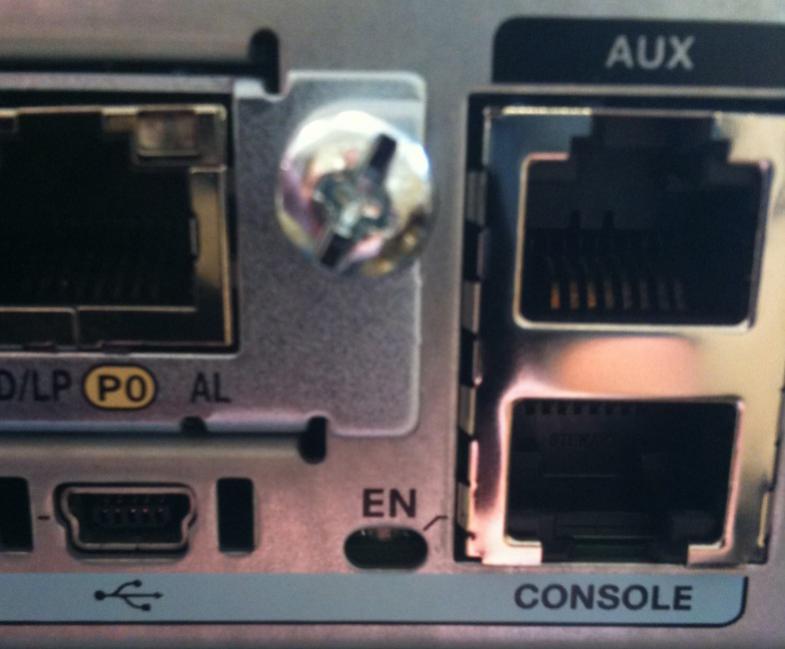


Todos los comandos de los que se dispone para la configuración se pueden saber tecleando normalmente el símbolo ? el comando help man o similar

## Switchs gestionables por puerto de consola.

Muchos dispositivos tienen un puerto o conexión especial llamado puerto de consola, podemos encontrarlo tipo RS-232 (COM1) o RJ45, la forma de trabajar sería análoga a la línea de comandos.

La diferencia estriba en la manera de conectarnos, hay que conectar un cable al puerto de consola, esto ofrece una seguridad adicional ya que para conectarse hay que tener acceso físico al switch (por web solo necesitamos acceder a la red en la que se encuentra).



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

https://avanza.educarex.es/cursos/file.php/948/moddata/scorm/12796/icon_autoevaluacionfpd.gifAutoevaluación

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.

Retroalimentación

* No, el usuario no depende de esto.
* Si, ssh lleva encriptada la información.
* No, utilizando cualquiera de los dos protocolos tenemos que utilizar los mismos comandos.
* No, los dos protocolos pueden utilizar el mismo tipo de puertos.

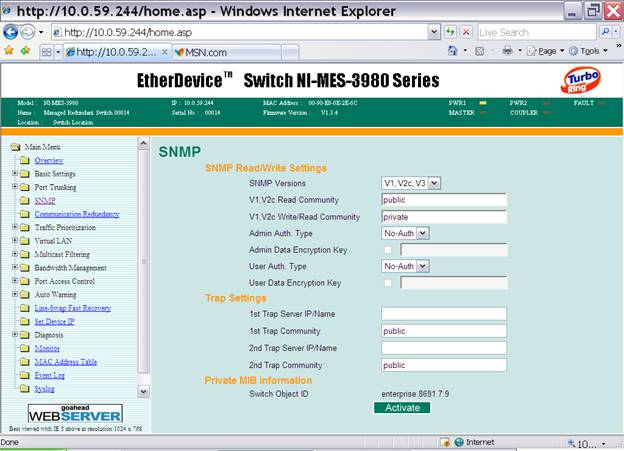
## Switchs gestionables por SNMP.

SNMP (Protocolo Simple de Administración de Red) 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 enviar preguntas y comandos a los dispositivos de la red. SNMP administra la red a través de una base datos MIB (Base de Información Gestionada) estructurada en forma de árbol.

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.

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, pero cada vez aparecen más gratuitas o de libre distribución.



La arquitectura de administración de la red propuesta por el protocolo SNMP se basa en tres elementos principales:

* Dispositivos administrados son los elementos de red (switchs, routers, etc.) que contienen "objetos administrados" que pueden ser información de hardware, elementos de configuración o información estadística;
* Agentes, es decir, una aplicación de administración de red que se encuentra en un periférico y que es responsable de la transmisión de datos de administración local desde el periférico en formato SNMP;
* Sistema de administración de red (NMS), esto es, un terminal a través del cual los administradores pueden llevar a cabo tareas de administración.

# Comandos

A la hora de administrar dispositivos de red a través de comandos, lo habitual es que cada fabricante diseñe su propio sistema con sus comandos, por tanto, vamos a ver los comandos más extendidos que son los comandos del Cisco IOS (Internetwork Operating System) ya que Cisco es una empresa líder en tecnología de redes, de hecho, algunos de los protocolos propios que ha diseñado han acabado convirtiéndose en estándares.

Para trabajar con un dispositivo en IOS hay tres entornos, dependiendo de los privilegios que tengamos, usuario, privilegiado y configuración global

El modo usuario (prompt > ) me permite solamente consultar el estado de configuración, el nivel superior es el modo privilegiado (prompt #), para una configuración completa el modo configuración global (prompt Switch(config)#) y modo configuración de interfaces (prompt switch(config-if)#)

Para cambiar entre los diferentes modos:

switch> enable

switch# configure terminal

switch(config)# interface fa0/0

switch(config-if)# exit

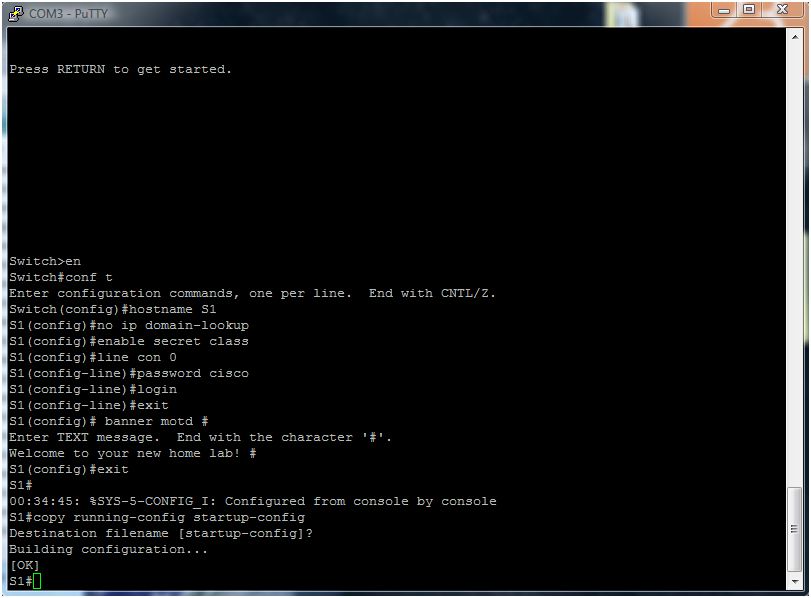
switch(config)# exit

switch# exit

switch>

|  |  |
| --- | --- |
| **Comandos de frecuente uso** | |
| **?** | Nos muestra una lista de los comandos que tenemos disponibles en ese nivel |
| **show running-config** | Nos permite ver la configuración del dispositivo, es decir, desde aquí podemos repasar los comandos que hemos introducido en el dispositivo |
| **hostname** nombre | Permite poner nombre al dispositivo |
| **ip address** IP máscara | Asigna una IP a la interface del dispositivo |
| **no shutdown** | Activar la interface |
| **enable secret** contraseña | Poner contraseña de acceso |

|  |  |
| --- | --- |
| **Comandos para crear un servicio DHCP** | |
| **ip dhcp pool** nombre | Crea el servicio |
| **network** IP\_de\_red máscara | Indica el rango de IPs a asignar |
| **default** IP | IP de la puerta de enlace a asignar |
| **ip address** IP máscara | Asigna una IP a la interface del dispositivo |
| **dns-server** IP | IP del servidor DNS a asignar |



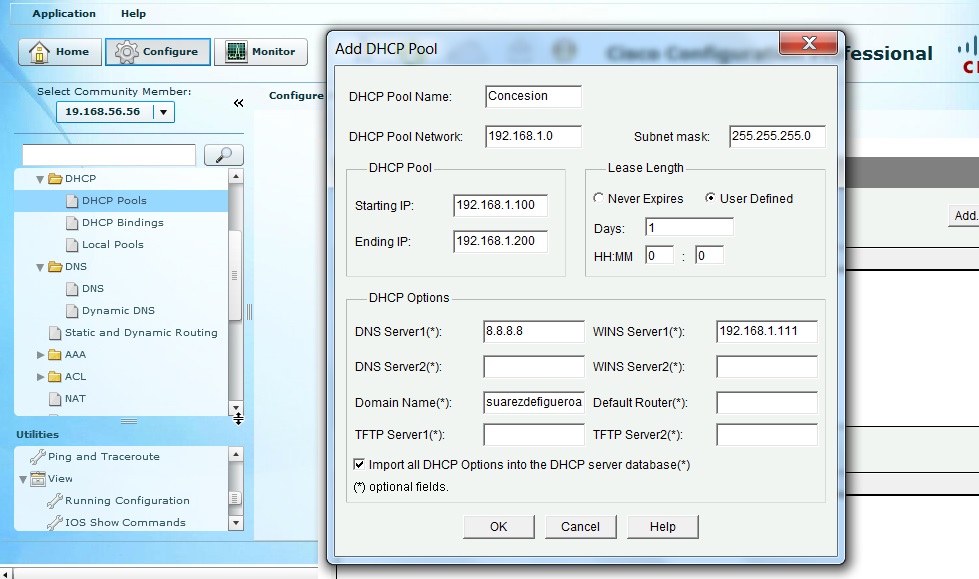
# El switch como servidor DHCP.

Lo habitual en la configuración de terminales de red (PC, Tablets, móviles, …) es que no necesiten ninguna configuración de red, esto sucede porque obtienen la IP automáticamente de un servidor DHCP (dispositivo que ejecuta una aplicación que da servicio DHCP).

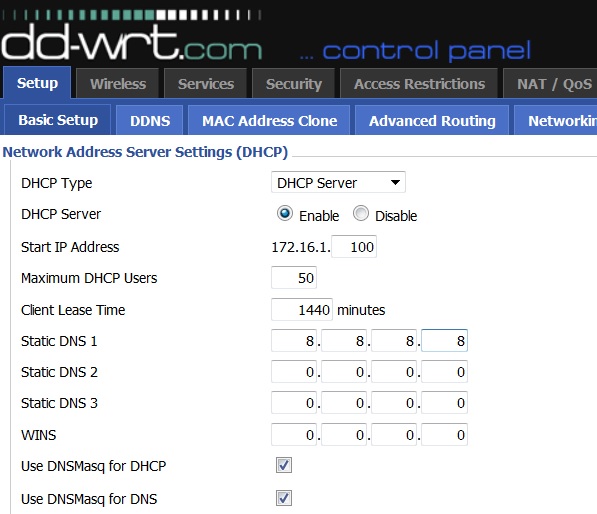
En el servicio DHCP hay dos papeles: cliente y servidor. El cliente es el dispositivo que solicita la configuración IP de red y el servidor es el dispositivo que controla estas asignaciones para evitar, entre otras cuestiones, que no haya dos dispositivos con la misma IP en la red.

Podemos configurar el servicio DHCP a través de comandos (relacionados anteriormente en el tema) pero lo más habitual es configurar el switch a través de web, vemos dos ejemplos:

En [Cisco Configuration Professional](http://www.cisco.com/c/en/us/products/cloud-systems-management/configuration-professional/index.html) donde añadimos una pila de direcciones IPs para la concesión, indicando red, primera IP de la concesión, última IP de la concesión, caducidad de la concesión, servidor DNS, servidor WINS, dominio. Muchos de estos parámetros son opcionales lo único indispensable es indicar la red.



Otro ejemplo lo tenemos en la siguiente pantalla, se trata de [dd-wrt](https://www.dd-wrt.com/site/), un firmware libre que podemos descargar e instalar en nuestros dispositivos de red (hay que consultar la base de dispositivos admitidos). En este caso indicamos la primera IP y el número de IPs que se pueden conceder (50), la caducidad y algunos parámetros.



# Tabla de direcciones MAC.

El elemento principal de un switch es su tabla de direcciones MAC, esta tabla contiene las direcciones MAC de los dispositivos del entorno y a partir de ella el switch conoce el puerto por el que debe envía un determinado paquete de datos.

En el momento inicial, de fábrica, el switch tiene la tabla de direcciones MAC vacía.

Para llenar la tabla de direcciones MAC hay dos formas:

* Dinámicamente, de la información que envían los dispositivos el switch aprende en que puerto esta cada dispositivo y anota en la tabla la dirección MAC del dispositivo y el puerto del switch al que se encuentra conectado directa o indirectamente.
* Estáticamente, a partir de la información introducida en el switch por el administrador de la red.

En este video se puede ver como aprende el switch y rellena su tabla de direcciones MAC

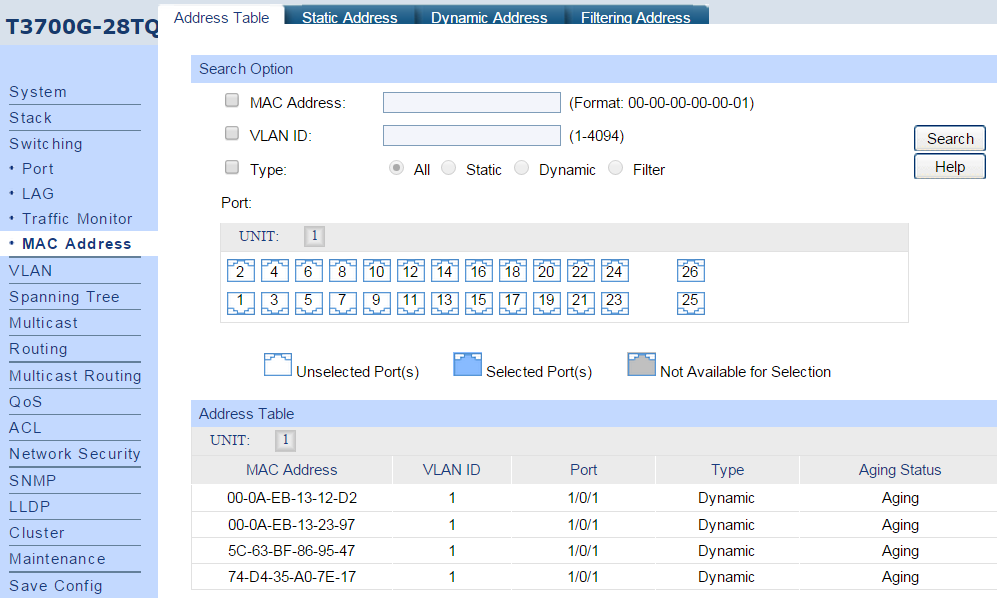
<https://www.youtube.com/watch?v=mnfkwe6ri_E>

Una entrada en la tabla de direcciones MAC se descarta automáticamente o expiran después de un determinado tiempo. La eliminación de entradas antiguas en la tabla de direcciones MAC asegura que la memoria de switch no se llenará y permite garantizar el funcionamiento correcto del switch ya que podrían producirse apagado de equipos, conexión de un equipo en otro puerto del switch, etc.

Se puede asignar una dirección MAC a una interface de forma permanente. Algunas razones para asignar una dirección MAC estática a una interface pueden ser:

* El switch no hace expirar automáticamente la dirección MAC.
* Se pretende mejorar la seguridad y evitar que cualquier máquina pueda conectarse a la red

Los datos que encontramos en una tabla MAC como **mínimo** son: dirección MAC, puerto y tipo (dinámico o estático). En algunos casos podemos ver VLAN u otras informaciones pero eso ya son características adicionales que puede admitir nuestro switch.



# Diagnóstico de incidencias

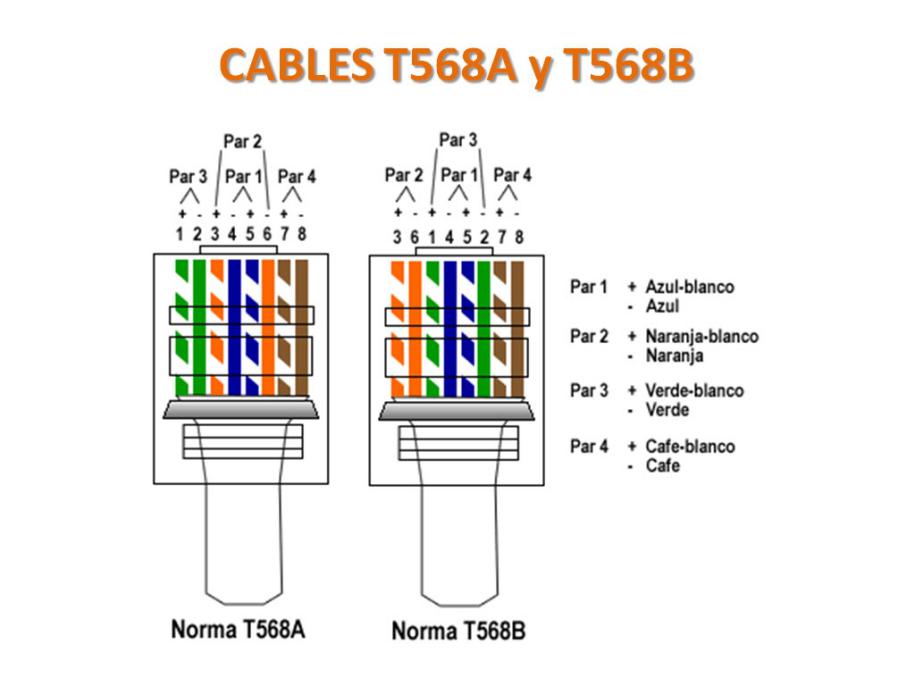
En muchas ocasiones, tenemos una red Gigabit, bien configurada y no sabemos por qué no alcanza ni siquiera los 100MB/s de transferencia, y toda la inversión realizada en switchs o routers gigabit, en cables CAT5E o CAT6, en tarjetas Ethernet Gigabit no vale para casi nada.

Tenemos que tener claro una cosa, Ethernet gigabit es Full-Dúplex, por tanto podemos transmitir y recibir a la vez (de forma simultánea), la tasa de transferencia será la del equipo más lento. Hay que tener en cuenta unas cuantas de consideraciones:

* Lo primero que tenemos que hacer es repasar todo, comprobaremos, por ejemplo, que no hay una roseta que no cumple con la categoría 5e o 6, un cable antiguo, una tarjeta de red FastEthernet, etc. Recordemos que esto producirá un cuello de botella y la transferencia caerá a la velocidad de este elemento más lento.
* Antes de buscar más es aconsejable un reinicio de los dispositivos de red.
* Sobrecarga de la red, no tiene que haber nada mal, sencillamente hay muchos dispositivos transmitiendo a la vez.
* En el caso de conexión inalámbrica habrá que buscar posibles interferencias, evitar elementos metálicos, cambiar el canal, etc.
* Discos duros lentos (la principal causa), o al menos no tan rápidos como nos gustaría, si usamos un disco duro que en el propio equipo se está leyendo o escribiendo, la bajada de rendimiento en la LAN cae radicalmente porque estamos accediendo a distintas partes del disco. Si intentamos transferir de un disco duro, que además contiene el sistema operativo, el rendimiento también bajará porque necesitamos leer y escribir datos para el sistema operativo y otros procesos como el antivirus, y luego también transferir en red…entonces el rendimiento baja.
* Procesadores lentos: Los paquetes se reciben demasiado deprisa para ser procesados (lo que produce que se llene la memoria de entrada). Además puede ser que en la memoria de salida haya demasiados paquetes esperando ser atendidos, entonces se llena la memoria de salida.
* Memoria RAM lenta o escasa: si tenemos muchos procesos abiertos, o si es muy lenta y tiene unos tiempos de latencia altos, la transferencia disminuirá (aunque no es el principal motivo).
* Uso de paquetes JUMBO, los paquetes Jumbo contienen más datos que los paquetes “normales”, aumentaremos significativamente la transferencia si nuestros dispositivos aceptan paquetes Jumbo.

# Tecnología Auto-MDIX.

En principio, para conectar dos dispositivos idénticos (PC a PC, switch a switch) es necesario usar un cable cruzado, es decir, un extremo del cable debe cumplir la norma T568A y el otro extremo la norma T568B.



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.

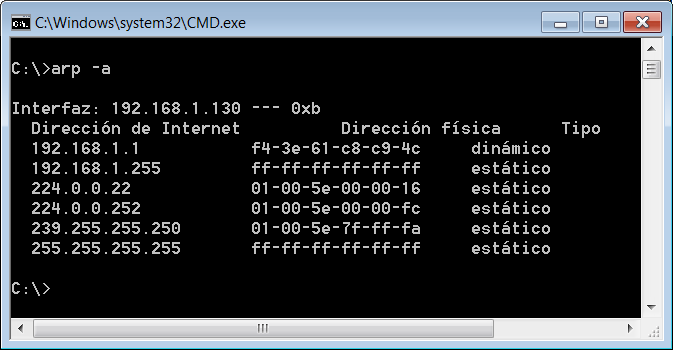
# El protocolo ARP

El protocolo ARP ofrece dos funciones básicas:

* + Resolución de direcciones IPv4 a direcciones MAC
  + Mantenimiento de una caché de las asignaciones.

Cuando un dispositivo quiere comunicar con otro, a nivel de aplicación se suelen manejar nombres (origen y destino) que, por el protocolo DNS, acaban traduciéndose en IPs. Este problema vuelve a aparecer cuando se pasa del nivel IP al acceso a la red, debemos traducir las IPs en MAC, aquí es donde aparece el protocolo ARP, que viene a ser el equivalente al protocolo DNS en un nivel inferior.

Cuando el paquete pasa al nivel de acceso a red, se consulta la tabla denominada tabla ARP o caché ARP. La tabla ARP almacena en la RAM del dispositivo una relación de IPs con sus MACs correspondientes (En Windows podemos ver esta tabla con arp –a). Si el destino se encuentra en la tabla ARP, los datos son enviados a la MAC destino indicada en la tabla, pero si no se encuentra se envía un broadcast (destino MAC: FF-FF-FF-FF-FF-FF) que llega a todos los dispositivos de la red y, al que responderá el dispositivo que tenga la IP que se busca.



La tabla ARP se mantiene dinámicamente, se aprende del tráfico que llega al dispositivo, de broadcast, o de entradas estáticas en la tabla ARP.

Para cada dispositivo, un temporizador de caché de ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado.

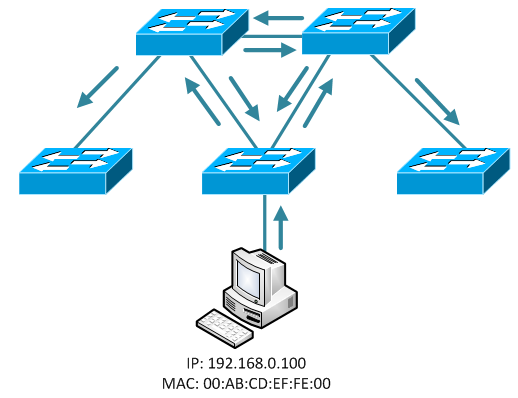
**Protocolo RARP**

El Protocolo de resolución inversa de direcciones (RARP) asocia las direcciones MAC conocidas a direcciones IP. Esta asociación permite que los dispositivos de red encapsulen los datos antes de enviarlos a la red. Es posible que un dispositivo de red, como por ejemplo una estación de trabajo sin disco, conozca su dirección MAC pero no su dirección IP. RARP permite que el dispositivo realice una petición para conocer su dirección IP. Los dispositivos que usan RARP requieren que haya un servidor RARP en la red para responder a las peticiones RARP.

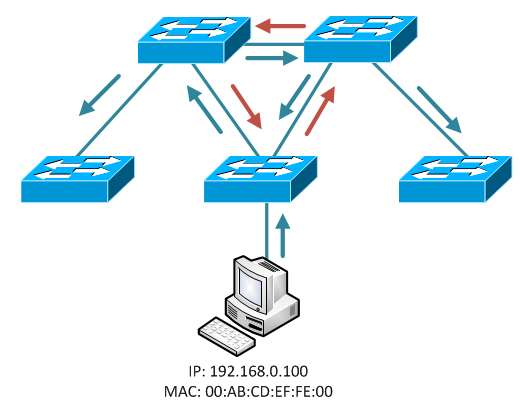
## Las tormentas de broadcast

Como consecuencia de lo que hemos comentado en el apartado anterior hay ocasiones en que el dispositivo no sabe la MAC destino y para conseguir averiguarla envía un paquete a todos los dispositivos de la red (broadcast), si en la red tenemos conexiones entre switchs que formen un circuito cerrado puede suceder que la petición ARP esté dando vueltas y, muchas peticiones de este tipo pueden saturar la red, esto es lo que se denomina tormenta de broadcast.

Supongamos el siguiente esquema, el PC con IP 192.168.0.100 quiere acceder al PC con IP 192.168.0.200, en su tabla ARP no se encuentra una línea asociada a esta IP, desconoce su MAC. Y ahora supongamos que este PC 192.168.0.200 no se encuentra en la LAN, se emitirá una petición ARP de broadcast que se propagará por todos los switchs, cada switchs recibirá la petición y la reenviará por todos sus puertos.



Pero la petición de broadcast no encontrará respuesta y habrá conexiones en las que estará dando vueltas produciendo una tormenta de broadcast.



El origen de las tormentas de broadcast está en la redundancia de las rutas

Los switchs 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".

Una forma de evitar estas tormentas es conectar los switchs de la red en estructura de árbol, donde en la zona troncal colocaríamos los switchs más rápidos.

# El protocolo spanning tree

Este protocolo se encuentra en la capa dos del modelo OSI, la principal función de este protocolo es gestionar los bucles que se encuentren en la topología de la red. (Ojo, el hecho de que haya bucles no significa un mal diseño de red, puede que queramos tener distintas rutas para evitar que una mala conexión bloquee la comunicación de red)

El funcionamiento de STP es calcular una ruta única entre los dispositivos de red y mantiene los enlaces redundantes desactivados, solamente se activarán en caso de un fallo. El protocolo STP utiliza un algoritmo para transforma una red física en malla en una red lógica en árbol.

La especificación de este protocolo está definida por el IEEE 802.1d y aunque hay diferentes tipos, esta especificación es la más aceptada y usada.

La clave en STP es que los conmutadores en la red elijan cual será el “root bridge” este será el foco principal de la red. Todas las decisiones en la red tales como cual puerto bloquear y cual puerto estará en modo de adelanto se hacen desde la perspectiva del “root bridge”. Si estamos trabajando en un ambiente con solo conmutadores se le conoce al “root bridge” como “root switch”.

Entre las evoluciones del protocolo STP encontramos:

* El RSTP (Rapid STP) es un estándar IEEE 802.1w y se podría interpretar como un avance o evolución del el estándar 802.1d, más que una revolución. El RSTP mantiene compatibilidad con el STP pero tiene varias diferencias que amilanan algunas las desventajas del STP, entre estas el tiempo de convergencia.
* La implementación del Multiple Spanning Protocol (MSTP) está definida en el estándar IEEE 802.1s. La convergencia de MSTP cuando hay un cambio de topología es rápida porque va implementada sobre el Rapid Spanning Tree Protocol (RSTP).
* Multi-Chassis Link Aggregation Group (MC-LAG) es una solución propietaria
* Shortest Path Bridging (SPB) es el estándar IEEE 802.1aq y es considerado por la organización como el próximo paso en la evolución de los protocolos “spanning tree”