Interconexión de redes

Cada topología tiene sus límites en términos de longitud máxima del segmento, número de equipos por segmento, etc. Una de las necesidades actuales es la de aumentar el número posible de equipos de red o interconectar redes del mismo tipo (topología, modo de acceso) o de tipos diferentes.

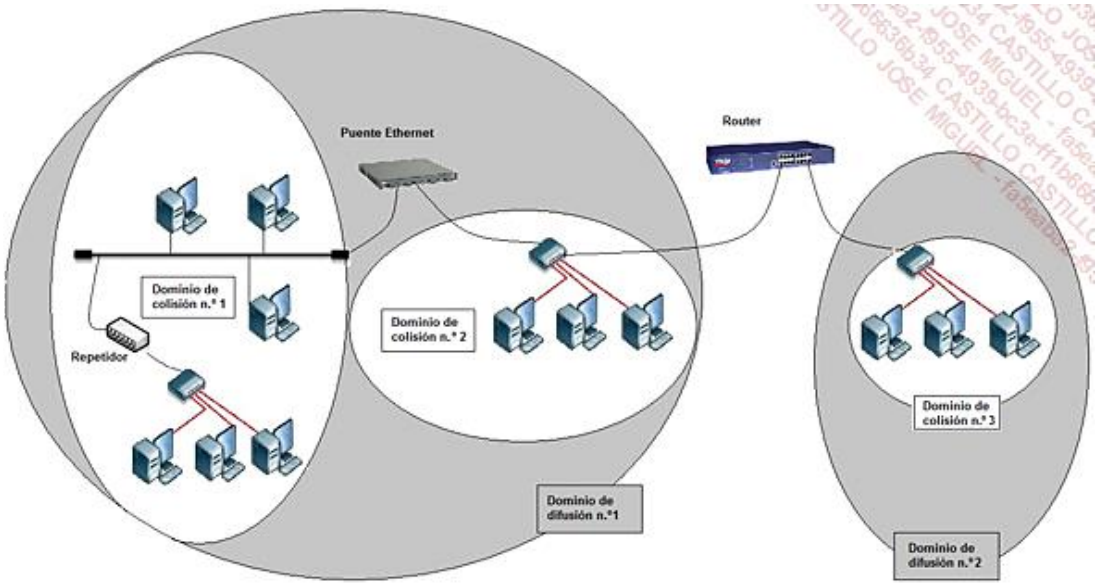
1. Principios

Existe hardware que permite interconectar las redes entre ellas. También permite segmentar las redes de gran tamaño en sectores más manejables.

En una red Ethernet, por ejemplo, el dominio de colisión se refiere a la extensión máxima que alcanza la trama en una red física.

En Ethernet, el hecho de dividir una red en dos dominios de colisión por medio de un puente permite desatascar la red.

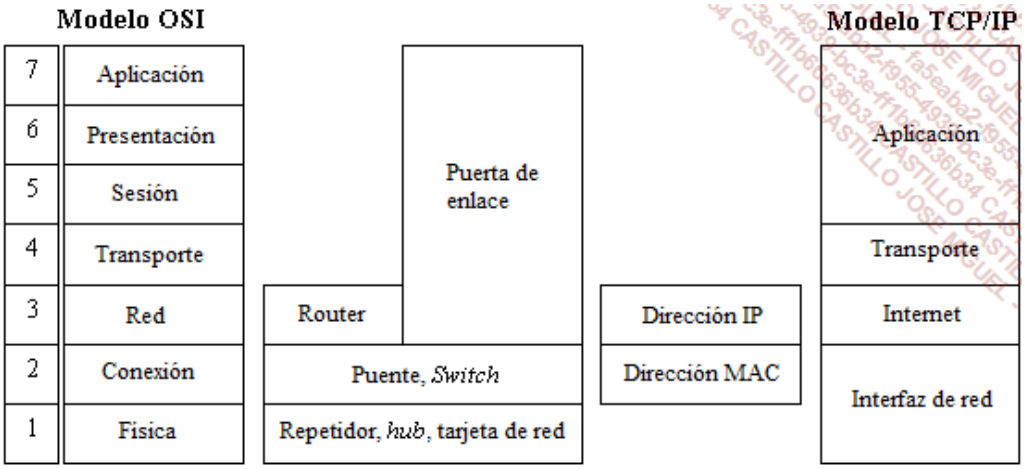
Usaremos la expresión dominio de difusión para identificar las partes de la red sobre las cuales una trama física, cuya dirección MAC es una dirección de difusión (es decir, FF.FF.FF.FF.FF.FF), puede extenderse. Puede ser interesante reducir los dominios de difusión a través de routers, debido a que algunos servicios trabajan solamente por medio de difusiones.



2. Componentes de interconexión y modelo OSI

En primer lugar, es muy importante comprender la relación que existe entre el modelo OSI, TCP/IP y los componentes de interconexión de red.

Según el nivel de funcionamiento de cada componente, podemos distinguir entre los que se basan en la dirección MAC y los que utilizan la dirección IP para filtrar los accesos.



Los conmutadores más avanzados son capaces de manejar los datos en la capa Red, a pesar de no ser esta su función original.

3. Descripción funcional de los componentes

a. El repetidor

Un repetidor (*transceiver*) actúa en la capa física del modelo OSI. Vuelve a empaquetar los datos recibidos y los retransmite con el fin de aumentar la distancia de transmisión. Es necesario transformar la señal en datos y luego los datos en señal, ya que las señales digitales son propensas a una atenuación muy marcada.

Repetidor fibra/par trenzado

Las señales cuadradas tienen una incontenible tendencia a perder amplitud (deteriorarse) y triangularse.

Un repetidor actúa en un mismo soporte físico, salvo si el repetidor asume la interconexión de soportes heterogéneos.

El repetidor no tiene ninguna información de la semántica de los campos de la trama (capa MAC). Se limita a descifrar las señales para reconvertirlas en bits elementales. Por lo tanto, es incapaz de saber si una trama es válida o no. Sin embargo, un repetidor debe ser capaz de detectar una colisión para poder propagarla por el otro lado.

A pesar de trabajar en el nivel 1, tampoco es capaz de interconectar los cables que funcionan a velocidades diferentes. No es aconsejable utilizar un repetidor en casos de mucho tráfico de red. No es posible utilizar un repetidor si los segmentos utilizan modos de acceso diferentes, ya que los modos de acceso se administran en la

capa MAC.

Un concentrador (hub) activo también puede hacer la función de repetidor. Es muy raro encontrar actualmente repetidores que se limiten a esta única función.

b. El puente

Función

Un puente (*bridge*) actúa en la capa Conexión de datos. Permite vincular dos o más soportes físicos diferentes, a condición de que se utilicen en ambos lados los mismos formatos de direcciones MAC.

Puente inalámbrico

Un puente interconecta redes de velocidades diferentes gracias a un funcionamiento de «almacenar y enviar» (*store and forward*). Como contrapartida, puede producirse una saturación de los *buffers* internos, generando una pérdida de tramas. Un puente permite la extensión de una red cuya amplitud máxima se ha alcanzado con repetidores. Las funcionalidades del puente pueden codificarse totalmente en un hardware autónomo.

Actualmente se encuentran a menudo equipos que permiten extender la cobertura de la red Wi-Fi en casa. Este componente actúa como un repetidor inalámbrico. Este tipo de dispositivos generalmente tiene una conexión de red Ethernet que le permite actuar como puente.

Extensión de red Wi-Fi

Acción de filtrado

El puente realiza una acción de filtrado sobre el tráfico que ve pasar. Observando la dirección MAC fuente del paquete que llega, es capaz de saber en qué lugar se encuentra la fuente de emisión (aprendizaje del puente). Algunos puentes son programables, lo que permite efectuar una acción de filtrado en algunos campos del paquete Ethernet. Se pueden utilizar para segmentar una red demasiado cargada.

Además, un puente es capaz de detectar una trama no válida: trama demasiado corta, demasiado larga o que tenga un CRC erróneo.

Aprendizaje

El puente va conociendo poco a poco las direcciones de origen de los dispositivos que originan paquetes y su correspondencia de conexión hacia los puertos (algunos dispositivos, como las impresoras, nunca aparecerán en las tablas de los puentes). A cada dirección de origen se le asocia una duración determinada. Cuando esta duración expira, se suprimen el mapeo de las tablas del puente.

Direccionamiento

En algunos casos, el acceso a las direcciones físicas permite no dejar pasar una trama de la que sabe que el destinatario no está al otro lado.

Por el contrario, cuando el puente no sabe dónde se encuentra el destinatario, deja pasar la trama. Además de transmitir los datos destinados a un único destinatario (*unicast*) si es preciso, el puente deja pasar aquellos destinados a un grupo (multidifusión o *multicast*) o a todos (difusión o *broadcast*).

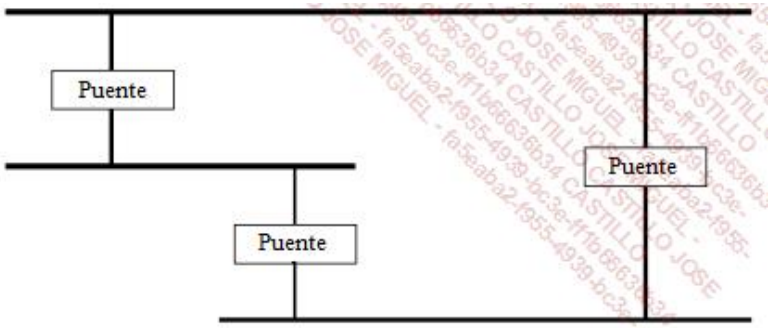
No es necesario asignar direcciones a los puentes, las direcciones de sus interfaces jamás aparecerán en los paquetes, excepto cuando se trata de tramas de servicio intercambiadas entre puentes.

Coherencia del modo de acceso

Al contrario que un repetidor, un puente es capaz de evitar las colisiones sin repetirlas en el otro segmento.

Gracias a sus *buffers*, el puente es capaz de guardar un paquete y de no emitirlo hasta que la red esté dispuesta a recibir la información del otro lado (modo CSMA/CD para Ethernet, o paso de testigo para Token Ring).

Gestión de bucles



Bucle en una red Ethernet

La generalización de las interconexiones de red a través de puentes ha llevado a configuraciones cada vez más complejas. Por ello, los fabricantes han desarrollado un algoritmo de detección de bucle llamado *Spanning Tree Algorithm* (IEEE 802.1D) para Ethernet. En un tipo de configuración bastante particular, si los puentes no detectan el bucle, este genera una circulación continua de tramas que inundan la red. El mismo puente puede detectar el bucle, dirigiendo la trama hacia uno de sus propios puertos mientras está a la escucha de esta trama en otro puerto. En cuanto se detecta el bucle, es necesario desactivar momentáneamente uno de los puertos que participan en el bucle.

Existe una dirección MAC 01.80.C2.00.00.00, definida para que los puentes puedan dialogar entre ellos.

Interconexión de redes

Basta con utilizar un puente con el fin de desatascar el tráfico (demasiadas colisiones, sobre todo en Ethernet) para tener una red segmentada en dos dominios de colisión diferentes.

Un puente, por definición, solo permite interconectar redes que tengan el mismo método de acceso. Por lo tanto, hablaremos de puentes Ethernet o de puentes Token Ring. Sin embargo, existen puentes que integran la transmisión de trama y que permiten la interconexión de topologías que administran modos de acceso diferentes. Hay que tener en cuenta que la dificultad reside en la detección de bucle que se realiza en Ethernet gracias a Spanning Tree, mientras que en Token Ring se aplica el algoritmo del origen del enrutamiento.

Los puentes y las métricas asociadas

Los puentes se pueden dividir según dos características:

- **La capacidad de filtrado**: la capacidad de filtrado corresponde al número de paquetes por puerto que un puente puede tratar, para saber si el paquete se debe transmitir.

Por ejemplo, en Ethernet a 10 Mbps, hay que filtrar 14.880 paquetes por segundo, con *buffers* no superiores a 10 KB.

- **La capacidad de transferencia**: la capacidad de transferencia mide el número de paquetes que se pueden

transferir en un segundo a otro segmento.

Algoritmo de Spanning Tree

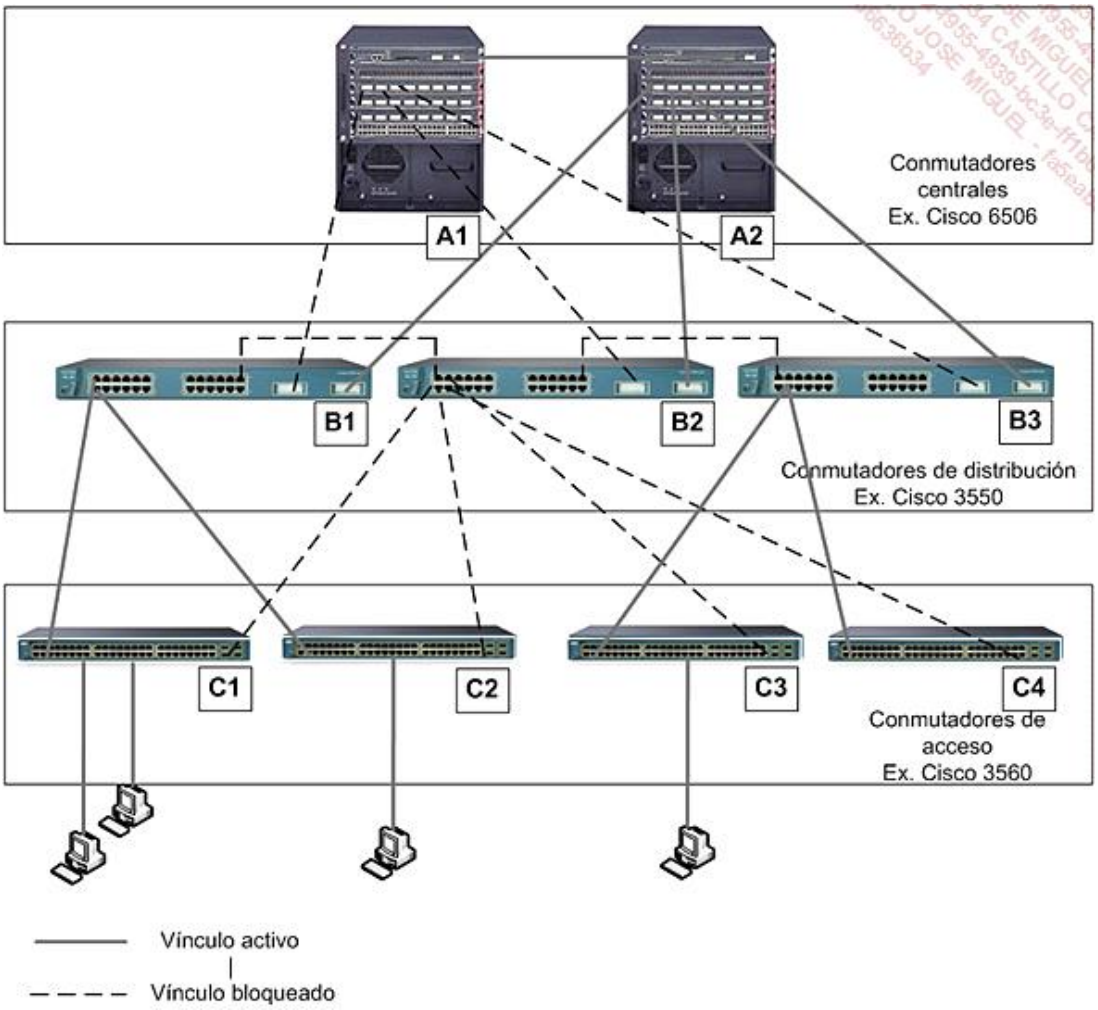
La red se está convirtiendo cada día más indispensable y necesita mecanismos de tolerancia a fallos. La red de nivel 2, al contrario que la de nivel 3, no sabe administrar directamente los múltiples caminos entre un emisor y un receptor. Así, en el caso de los bucles de nivel 2, un conmutador ve que se puede acceder a un ordenador a través de varios de sus puertos (la misma dirección MAC se verá en varios puertos diferentes); en este caso, se generarán tramas duplicadas que pueden llevar al colapso de la red.

El Spanning Tree, literalmente «árbol de expansión», ofrece una solución de neutralización de bucles, que se han introducido voluntariamente en la topología Ethernet para tener mayor tolerancia a fallos.

El algoritmo permite construir, a partir de la topología existente, una arborescencia desde la raíz de un árbol para llegar a cada segmento de la red.

A partir del momento en que el Spanning Tree se ha activado en todos los conmutadores, se opera una neutralización de los bucles calculando el «mejor camino» para el acceso a cada segmento.

En el siguiente esquema, el conmutador central de red A2 ha sido elegido raíz del árbol:



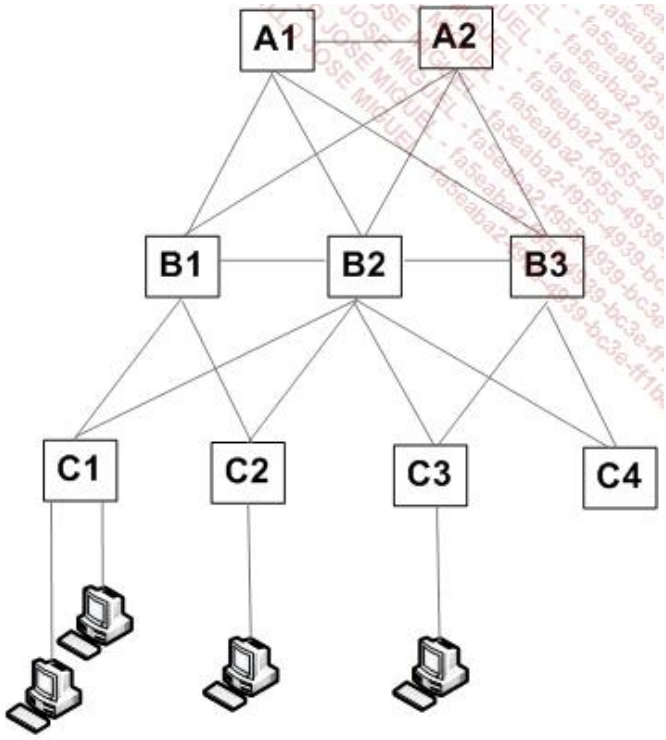
Neutralización de los vínculos por el Spanning Tree

Observe que, en el esquema, se puede acceder directamente a la red troncal principal a través de los núcleos A1 y

A2.

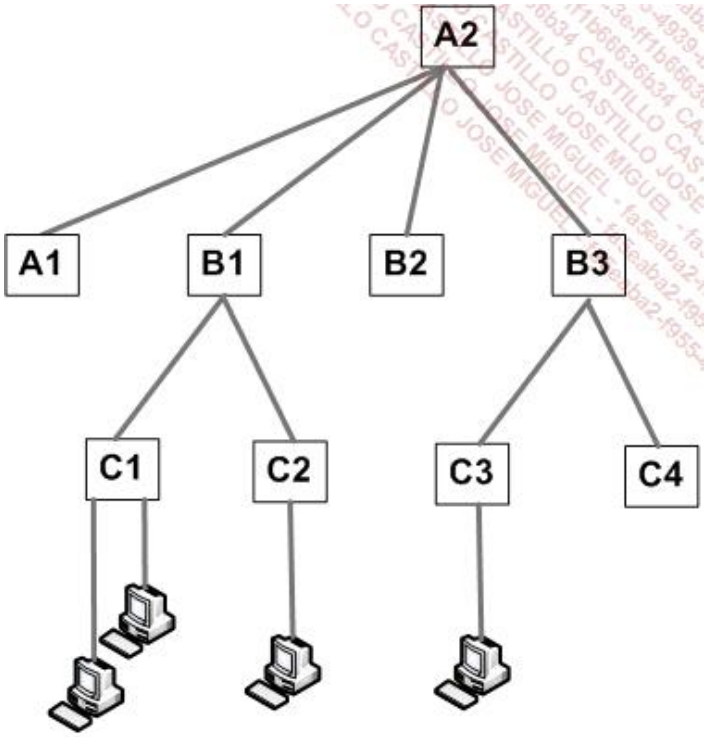
Los servidores de red local están conectados a los servidores de distribución.

Antes de la aplicación de Spanning Tree, el esquema de red era el siguiente:



Esquema de red global

Después de la ejecución de Spanning Tree, el árbol de red equivalente obtenido es el siguiente:



Árbol obtenido por el Spanning Tree

El algoritmo utilizado permite realizar un cierto número de acciones. Para ello se van a intercambiar las tramas entre conmutadores, los mensajes BPDU o *Bridge Protocol Data Unit*, para obtener la información en los conmutadores, así como la topología existente.

Los objetivos contemplados son los siguientes:

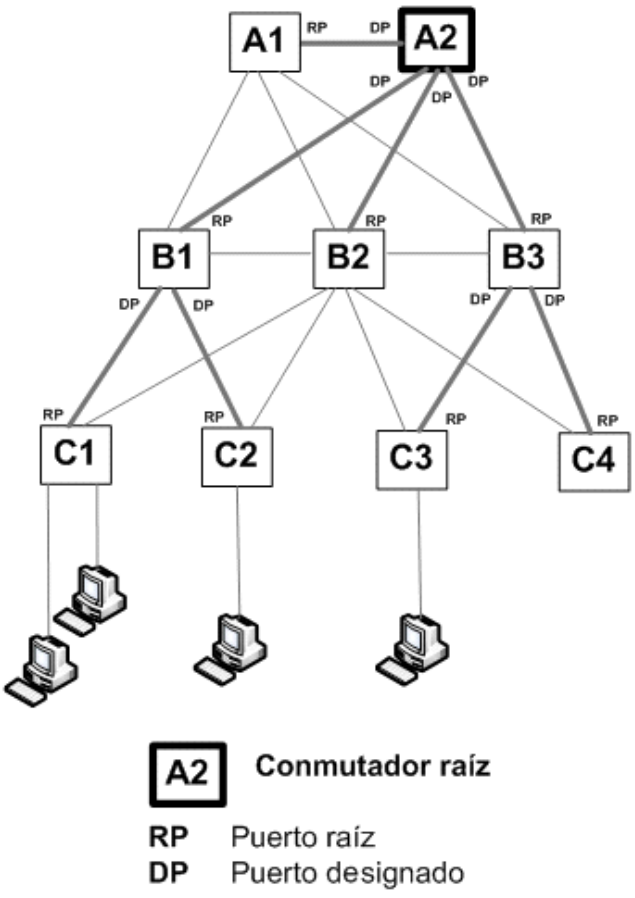
1) Elección de un conmutador raíz del árbol, que disponga de la pareja (prioridad, dirección MAC) más fiable.

2) Designación de otros conmutadores como «conmutadores designados», definiendo un puerto raíz, que necesitará el puerto prioritario para el acceso al conmutador raíz, teniendo en cuenta el camino más corto.

Para esto se asociará un coste a cada puerto en función de la velocidad implementada:

Velocidad	Coste
10 Mbps	2.000.000
100 Mbps	200.000
1 Gbps	20.000
10 Gbps	2.000

El «puerto raíz» del conmutador se relacionará entonces con un «puerto designado» de otro conmutador, «acercándose» al conmutador raíz.



Asignación de «puertos raíces» y «puertos designados»

3) Se atribuirán igualmente los puertos complementarios para implementar la redundancia de Spanning Tree (puerto alternativo, puerto de seguridad, etc.).

Así, los puertos en origen de caminos suplementarios se «bloquearán» para impedir el paso de las tramas, pero no el enrutamiento de los mensajes BPDU.

El algoritmo debe ser capaz de reconsiderar la topología de red en cada evolución (corte de red, introducción de un vínculo suplementario, etc.).

c. El conmutador

Origen

El conmutador (*switch*) apareció en 1990 en Ethernet y en 1994 en Token Ring. Integra a la vez la funcionalidad de un *hub* y de un puente. La gestión de este hardware inteligente la realiza un microcontrolador o incluso un microprocesador.

Hoy en día, el conmutador es un componente clave en las redes locales. En todas las redes modernas, los equipos de trabajo y los servidores están conectados directamente a estos equipos. Actualmente es muy raro utilizar concentradores o puentes.

La red ya no tiene una característica de difusión, sino de conmutación.

Los conmutadores se dividen en función de su capacidad de tratamiento respecto del modelo OSI. Los de nivel 2 (N2) o de grupo de trabajo realizan operaciones hasta la capa de datos. Por ejemplo, pueden operar con direcciones MAC de los ordenadores conectados a sus puertos.

Los de nivel 3 (N3), o conmutadores de fase, pueden trabajar con encabezados de capa 3 (Red). También pueden reconocer las direcciones IP.

Por ejemplo, en una utilización típica de estos conmutadores, un núcleo de red de nivel 3 dirige el conjunto de la red. Los servidores pueden estar conectados directamente. Los equipos de trabajo se conectan a los puertos de conmutadores de nivel 2 que utilizan, como administrador, el núcleo de la red.

Conmutadores Ethernet

Principios

El principio de un conmutador Ethernet es posibilitar un segmento a 100 Mbps (incluso 1 Gbps) por puerto y que cada uno esté conectado a un ordenador. Cuando se transporta una trama a partir de un puerto, el commutador establece un circuito virtual (CV) que corresponde a la dirección MAC origen y a la dirección MAC destino para los puertos especificados.

El conmutador es capaz de almacenar una serie de direcciones MAC por puerto (por ejemplo, 1000 entradas por puerto). Las siguientes tramas se conmutan directamente hacia el destinatario correcto, utilizando el CV previamente establecido.

Se trata de una función de puenteo, si bien la conmutación puede hacerse en paralelo en el conjunto de los puertos gracias a la capacidad del conmutador.

Un conmutador puede tener hasta 48 puertos, más dos de interconexión (mediante cable cruzado o fibra óptica).

Tipos de conmutación

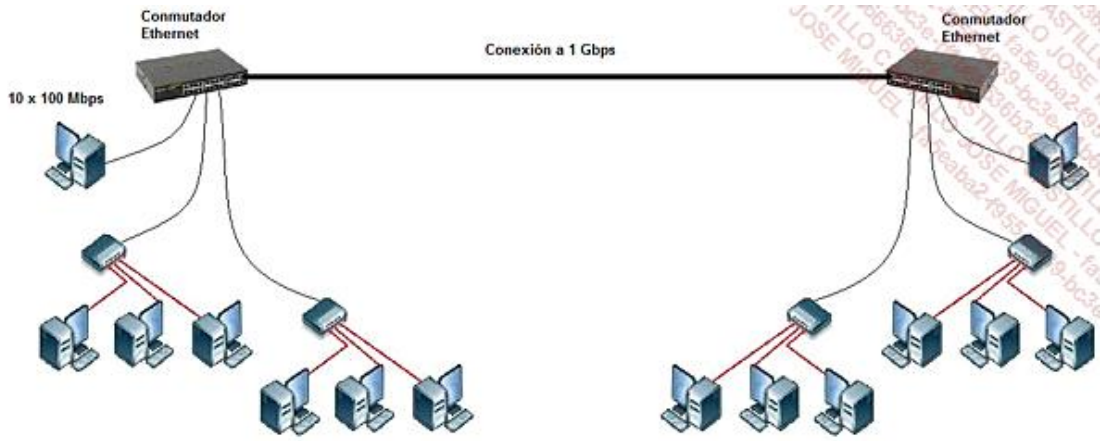
Existen varias clases de conmutación.

La conmutación al vuelo (*on the fly* o *cut through*) responde a un tratamiento simultáneo de tramas, sin almacenamiento intermedio. La ventaja es que el conmutador solo necesita de un pequeño *buffer* y que el tiempo de latencia es inexistente. Sin embargo, deja pasar las tramas erróneas y se transmiten las colisiones.

En la conmutación «almacena y envía» (*store and forward*), se almacena la trama, se analiza y a continuación se encamina hacia el destinatario correcto. Esta técnica tiene la ventaja de eliminar las tramas erróneas.

En Ethernet, el conmutador permite segmentar la red en varios dominios de colisión. En un caso ideal, si se coloca un equipo por puerto, se obtiene una red sin colisión.

La mejora de calidad de los cables cruzados de cobre permite una comunicación a 1 Gbps de bajo coste. Por eso actualmente estas velocidades son normales en las conexiones de red de los servidores y entre conmutadores.

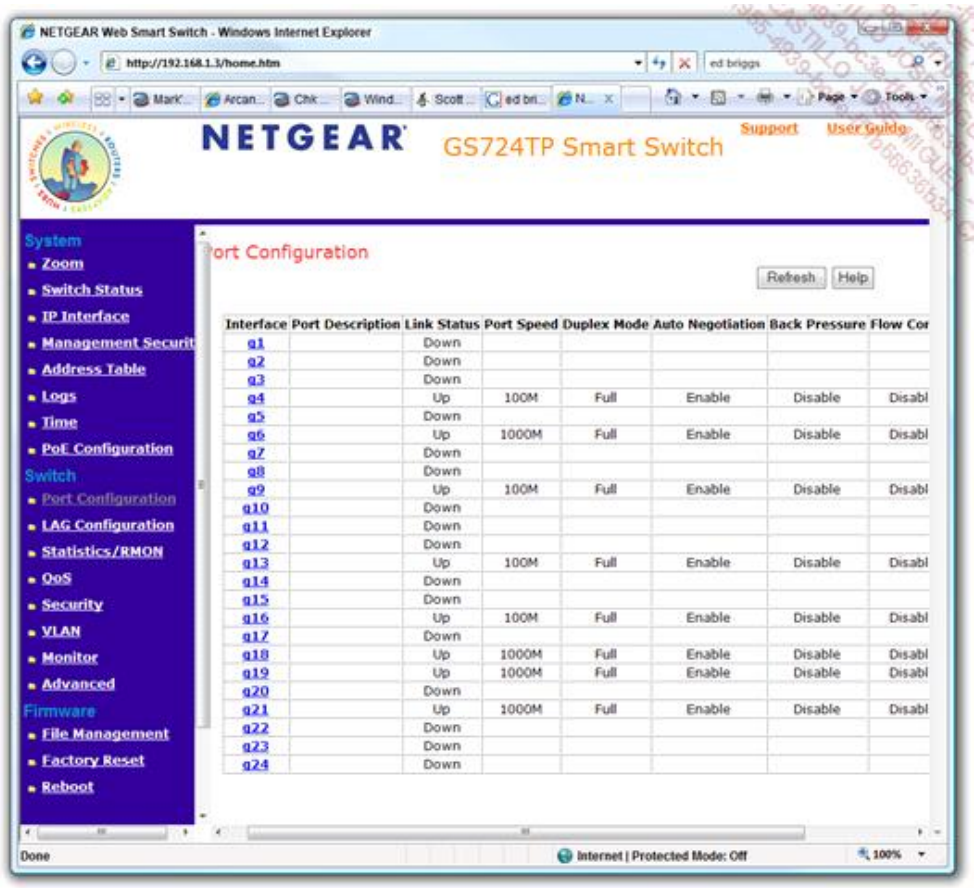


Administración

Muchos conmutadores proporcionan funcionalidades de administración, seguimiento, segmentación de la red y neutralización de bucles (heredada de Spanning Tree, IEEE 802.1D en Ethernet).

En general, disponen de una dirección IP que permite al administrador conectarse a distancia, por Telnet o HTTP, o directamente a través de un terminal serie.

La siguiente pantalla muestra la configuración de los puertos en un conmutador de la marca Netgear.



Administración de un conmutador a través de una interfaz web

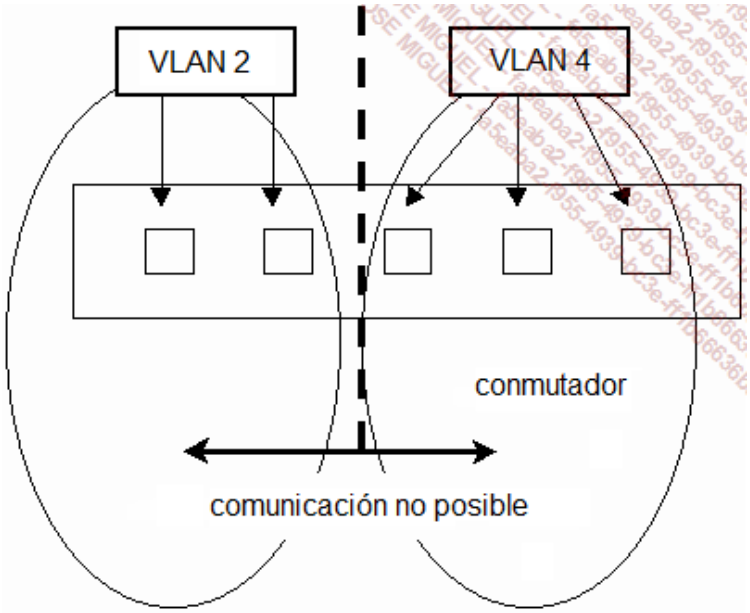
El concepto de VLAN

El objetivo de una red local virtual (VLAN - *Virtual Local Area Network*) es la segmentación lógica de las redes. De este modo, es posible controlar o incluso impedir cualquier diálogo entre equipos interconectados en un mismo conmutador, mediante listas de control de acceso.

La división lógica se puede efectuar de varias maneras. Una VLAN, calificada como implícita, se puede realizar a partir de distintos criterios:

- los números de los puertos del conmutador, capa 1 OSI;
- las direcciones MAC de los dispositivos conectados, capa 2 OSI;
- el protocolo utilizado, capa 3 OSI.

Este último caso se reserva para conmutadores modernos, llamados de nivel 3.



Principio de estanqueidad entre VLAN

Por ejemplo, en una VLAN basada en las direcciones MAC, las que correspondan a una de las VLAN no podrán comunicarse con las que correspondan a otra, salvo si las VLAN están enrutadas.

Un puerto puede pertenecer a varias VLAN.

Tipo de VLAN	Capa OSI	Ventajas	Desventajas
VLAN por puerto	1	• Estanqueidad máxima en caso de intrusión. • Facilidad de configuración por asignación de VLAN en un puerto de un conmutador.	• Configuración pesada a implementar en cada conmutador. • Necesidad de modificar la configuración en cada cambio de puesto. • No hay arquitectura centralizada, cada conmutador dispone de su propia tabla de correspondencia.
Dirección MAC	2	• Posibilidad de centralización de las direcciones MAC para una asignación automática en la VLAN (a través de VMPS o *VLAN Membership Policy Server*).	• Ofrece una seguridad menor que la VLAN por puerto, ya que es posible suplantar una dirección MAC.
Protocolo utilizado	3	• El conmutador asigna automáticamente una máquina a la VLAN en función de su dirección IP extrayendo su IP de origen.	• Las demoras relacionadas con la desencapsulación de las tramas para extraer la dirección IP. • Necesidad de utilizar equipos costosos que aseguren la implementación hasta el nivel 3. • La usurpación de direcciones IP es más fácil de realizar que la usurpación de direcciones MAC.

Existen dos tipos de VLAN: las VLAN implícitas y las VLAN explícitas.

En el funcionamiento de la VLAN implícita, no se modifican las tramas. La pertenencia a una VLAN se basa en el número del puerto, en las direcciones MAC o en un protocolo específico.

En función de esta pertenencia a una VLAN, se rechazará o autorizará la transmisión. Una VLAN implícita sobreentiende una ausencia de marcaje (modificación) de las tramas. Hablaremos entonces de *untagged VLAN*.

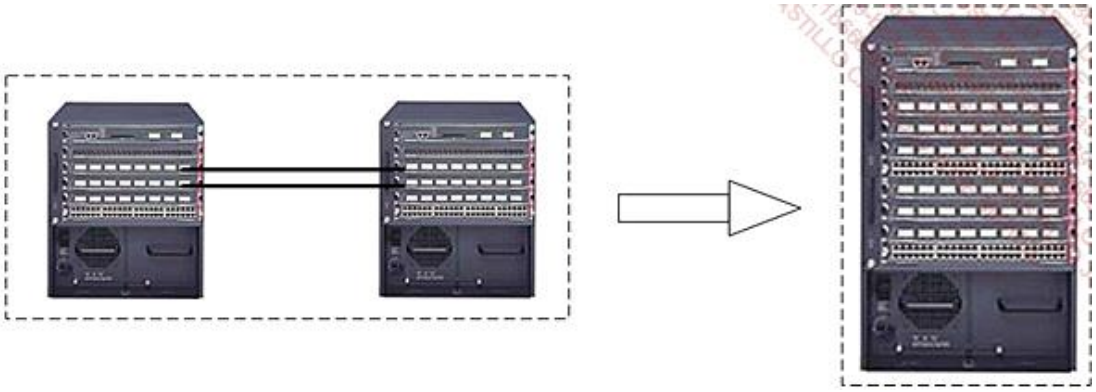
El funcionamiento de VLAN explícita se basa en el marcaje de las tramas (*tagged VLAN*) atendiendo a la norma IEEE 802.1Q.

Este último enfoque permite administrar la segmentación en un entorno de varios conmutadores. Así, se puede rechazar una trama procedente de una *tagged VLAN* de otro conmutador.

Cuando se dispone de varios conmutadores, es posible configurar las conexiones que hay entre los dos dispositivos para optimizar los intercambios. Hablaremos de *Port trunking* para designar la facultad de asociar varias conexiones punto a punto, o de *switch meshing* para designar una malla de conexiones entre un conjunto de conmutadores. Este último enfoque permite poner en práctica una redundancia en conexiones múltiples, designando los mejores caminos entre dos direcciones MAC gracias a distintos criterios, como el tamaño del *buffer* utilizado en cada conmutador y las velocidades asociadas.

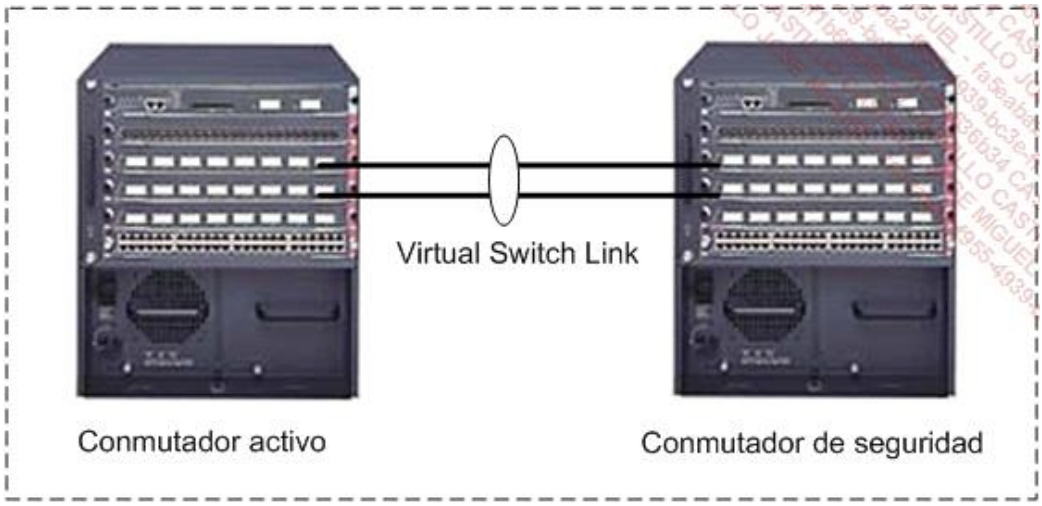
Virtualización de conmutadores: VSS

Virtual Switching System (VSS) o sistema de conmutación virtual es una funcionalidad Cisco que permite ver un solo conmutador lógico en lugar de dos conmutadores físicos desplegados (Catalyst 650X). Esta solución permite remplazar con ventajas el Spanning Tree que a menudo aporta complejidad añadida al entorno de nivel 2 existente.



Equivalente lógico a dos Catalyst 650X con VSS

Cada chasis se puede desplegar en una sala técnica distinta, lo que permite ofrecer una solución con gran tolerancia a fallos.



Conexión de dos conmutadores en VSS

En un sistema VSS, uno de los chasis se designa como conmutador virtual activo y el otro como conmutador virtual secundario. De este modo, solo se elige una de las tarjetas de supervisión como punto de gestión central. De hecho, se puede acceder a las configuraciones de nivel 1, 2 y 3 a través de una configuración única de la tarjeta de supervisión activa.

d. El router

Principio

El router es un dispositivo de interconexión que tiene acceso a toda la información de las capas 1, 2 y 3, en particular, a las direcciones lógicas que son independientes del método de acceso y de la topología física.

El router puede parecer físicamente un conmutador o tener forma de armario:

Conmutador multi-niveles

El router modifica la capa física para cambiar el soporte, la capa MAC, para precisar las nuevas direcciones MAC, la suya y la del próximo periférico intermedio (probablemente otro router), teniendo en cuenta el nuevo modo de acceso. Las direcciones lógicas permiten tener una visión lógica de la intrarred, lo que lleva al router a conocer los distintos caminos posibles para alcanzar un destinatario. El router debe conocer la lista de todas las redes lógicas existentes, que conserva en una tabla. Estos datos se actualizan, ya sea una sola vez al iniciar el dispositivo, lo que llamaremos enrutamiento estático, o bien de manera regular gracias a que los routers se informan entre ellos de las modificaciones de topologías en la intrarred; en este caso se habla de enrutamiento dinámico.

En algunos casos y por razones de seguridad, todas las tablas de enrutamiento pueden ser predefinidas y fijadas.

Una tabla de enrutamiento contiene el conjunto de las direcciones de red conocidas, la manera de conectarse a las otras redes (la dirección lógica del próximo dispositivo que permite llegar a la red del destinatario en el que se encuentra el servidor), los distintos caminos entre routers y los costes vinculados al envío de los datos. Un router también puede hacer la función de barrera de seguridad (cortafuegos) filtrando algunas direcciones lógicas.

El concepto de enrutamiento solo es posible a condición de que los protocolos utilizados sean enrutables, es decir, que administren una dirección lógica compuesta por un número de red y un número de servidor en la red.

Un router, por definición, no deja pasar una difusión (número de redes diferentes).

Un router se puede configurar con un terminal conectado a un puerto DB25 del router, o a través de la red, por ejemplo mediante TELNET en TCP/IP.

Exploración de las rutas

Existen algoritmos de camino único y algoritmos de caminos múltiples que posibilitan una distribución de la carga.

Además, se distingue entre los algoritmos de dominio de enrutamiento plano y los de dominio jerárquico, que evitan que los routers tengan que aprender todas las redes lógicas posibles.

En todos los casos, un router debe elegir el mejor camino posible según distintos criterios. El número de saltos (*hops*) corresponde al número de desvíos para cambiar de red, es decir, el número de routers por los que se debe

pasar. El TICKS da cuenta del tiempo de travesía necesario en la red. El coste de la línea, la densidad del tráfico, la velocidad de las líneas recorridas, así como su fiabilidad, son otros criterios para poder elegir el mejor camino.

Tipos de routers

Estáticos

En este caso, el administrador inicializa manualmente la tabla de enrutamiento (por ejemplo mediante telnet). Los caminos posibles están predefinidos y los routers intermedios no toman ninguna decisión de enrutamiento.

Dinámicos

A menudo, se configura la primera ruta manualmente y se escoge el mejor camino al pasar por cada router de la red.

Elección de una distancia

Vector de distancia

Cada router construye su propia tabla de enrutamiento, en la que combina la información de las tablas de sus vecinos inmediatos.

El inconveniente reside en el hecho de que este tipo de algoritmo genera mucho tráfico en la red. Las tablas de enrutamiento completas se difunden por defecto cada 30 segundos. Además, requiere un tiempo de convergencia bastante largo.

Ejemplo:

IP e IPX aceptan *Routing Internet Protocol* (RIP).

Estados de conexión

La exploración de las rutas se basa en una difusión global inicial, a continuación se difunde cada modificación por separado. Así, las tablas de enrutamiento están permanentemente al día.

Ejemplos:

Open Shortest Path First (OSPF) es utilizado por IP (trabaja a nivel jerárquico).

Podemos citar igualmente los protocolos de enrutamiento IGRP (*Interior Gateway Routing Protocol*) y EIGRP (*Enhanced IGRP*), desarrollados por CISCO. Muy fiables y extensibles, solucionan las limitaciones de RIP.

Ejemplo de protocolos de enrutamiento

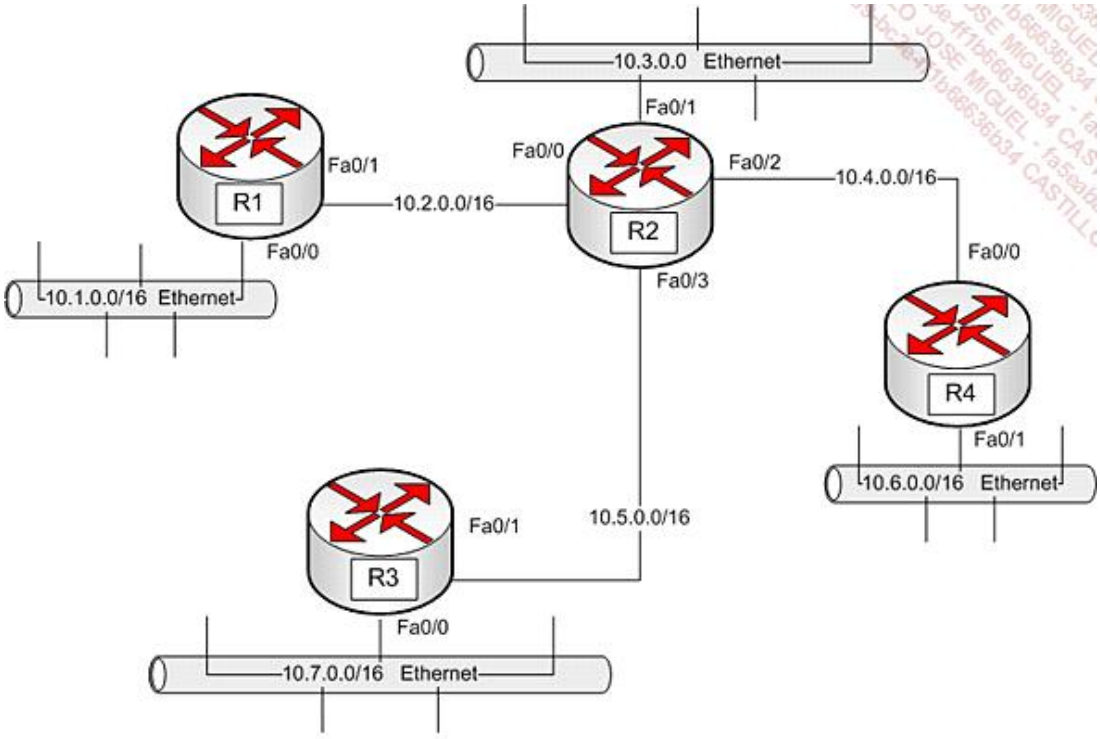
RIP

El protocolo RIP (*Routing Information Protocol*), inicialmente especificado en la RFC 1058 (RIPv1) y posteriormente en la RFC 2453 (RIPv2), es un protocolo de enrutamiento interno y utiliza un algoritmo de vector de distancias.

Utiliza el número de saltos como medida para la selección del camino. Establece como ruta inaccesible un número de saltos superior a 15. Cada router RIP envía el contenido de su tabla de enrutamiento, por defecto cada 30 segundos, a sus vecinos.

Cuando un router recibe una actualización que incluye una nueva subred o una modificación, el router actualiza su

tabla de enrutamiento. A nivel de cada router, el valor del número de saltos se incrementa en una unidad. Después de haber actualizado su tabla de enrutamiento, el router comienza a transmitir las actualizaciones de enrutamiento para informar a los demás routers de la red. El envío de estas actualizaciones, llamadas actualizaciones desencadenadas, es independiente del envío de actualizaciones regulares por los routers RIP.



Entorno de red y RIP

Inicialmente, los routers conocen las redes a las que están conectados. Lo que da:

Router R1	Red	Interfaz	Salto
	10.1.0.0/16	Fa0/0	0
	10.2.0.0/16	Fa0/1	0

Router R2	Red	Interfaz	Salto
	10.2.0.0/16	Fa0/0	0
	10.3.0.0/16	Fa0/1	0
	10.4.0.0/16	Fa0/2	0
	10.5.0.0/16	Fa0/3	0

Router R3	Red	Interfaz	Salto
	10.7.0.0/16	Fa0/0	0
	10.5.0.0/16	Fa0/1	0

Router R4	Red	Interfaz	Salto
	10.4.0.0/16	Fa0/0	0
	10.6.0.0/16	Fa0/1	0

Cuando R1 difunda su tabla de enrutamiento a su vecino R2, R2 descubrirá la existencia de la red 10.1.0.0/16 por su interfaz Fa0/0:

Router R2	Red	Interfaz	Salto
	10.2.0.0/16	Fa0/0	0
	10.3.0.0/16	Fa0/1	0
	10.4.0.0/16	Fa0/2	0
	10.5.0.0/16	Fa0/3	0
	10.1.0.0/16	**Fa0/0**	**1**

A continuación por actualización desencadenada, R3 y R4 descubren la misma red:

Router R3	Red	Interfaz	Salto
	10.7.0.0/16	Fa0/0	0
	10.5.0.0/16	Fa0/1	0
	10.1.0.0/16	**Fa0/1**	**2**

Router R4	Red	Interfaz	Salto
	10.4.0.0/16	Fa0/0	0
	10.6.0.0/16	Fa0/1	0
	10.1.0.0/16	**Fa0/0**	**2**

De manera similar, R3 enviará su tabla de enrutamiento a su vecino R2, que descubrirá que puede acceder a red 10.7.0.0/16 en un salto por su interfaz Fa0/3.

R2 a su vez, propagará la existencia de la red 10.7.0.0/16 a sus vecinos R1 y R4 en dos saltos.

R4 descubrirá a R2 la existencia de la red 10.6.0.0/16. R2 propagará esta información a sus vecinos R1 y R3.

Una vez se ha realizado la convergencia completa de RIP, se obtiene la siguiente información:

Router R1	Red	Interfaz	Salto
	10.1.0.0/16	Fa0/0	0
	10.2.0.0/16	Fa0/1	0
	10.7.0.0/16	**Fa0/1**	**2**
	10.6.0.0/16	**Fa0/1**	**2**
	10.3.0.0/16	**Fa0/1**	**1**
	10.4.0.0/16	**Fa0/1**	**1**
	10.5.0.0/16	**Fa0/1**	**1**

Router R2	Red	Interfaz	Salto
	10.2.0.0/16	Fa0/0	0
	10.3.0.0/16	Fa0/1	0
	10.4.0.0/16	Fa0/2	0
	10.5.0.0/16	Fa0/3	0

	10.1.0.0/16	**Fa0/0**	**1**
	10.7.0.0/16	**Fa0/3**	**1**
	10.6.0.0/16	**Fa0/2**	**1**

Router R3	Red	Interfaz	Salto
	10.7.0.0/16	Fa0/0	0
	10.5.0.0/16	Fa0/1	0
	10.1.0.0/16	**Fa0/1**	**2**
	10.6.0.0/16	**Fa0/1**	**2**
	10.3.0.0/16	**Fa0/1**	**1**
	10.4.0.0/16	**Fa0/1**	**1**
	10.5.0.0/16	**Fa0/1**	**1**

Router R4	Red	Interfaz	Salto
	10.4.0.0/16	Fa0/0	0
	10.6.0.0/16	Fa0/1	0
	10.1.0.0/16	**Fa0/0**	**2**
	10.7.0.0/16	**Fa0/0**	**2**
	10.2.0.0/16	**Fa0/0**	**1**
	10.3.0.0/16	**Fa0/0**	**1**
	10.5.0.0/16	**Fa0/0**	**1**

Las principales ventajas relativas a RIP son las siguientes:

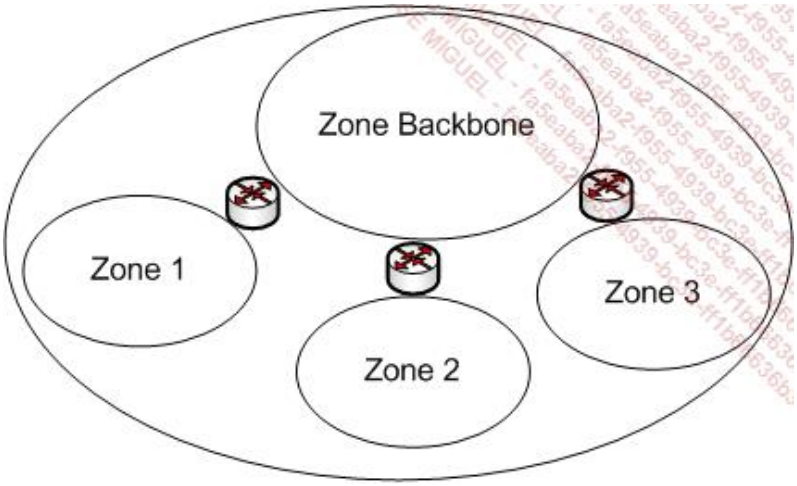
- Funcionamiento simple.
- Protocolo disponible en todas partes.

Los principales inconvenientes de RIP son los siguientes:

- Número de saltos limitado a 15.
- Convergencia lenta.
- Envío de toda la tabla cada vez.

OSPF

El protocolo OSPF (*Open Shortest Path First*) está especificado en la RFC 2328. Se trata de un protocolo abierto, de estado de enlace, que funciona como protocolo interno, dentro de un entorno delimitado (AS o *Autonomous System*).



Autonomous System OSPF

El AS se divide en zonas OSPF (*Área*) que están conectadas a una zona principal o zona *backbone*.

No se aconseja tener más de 50 routers por zona OSPF, lo que representa ya una red muy importante.

Se basa en el algoritmo *Shortest Path First* o SPF para calcular el coste más fiable a un destino en una zona determinada.

El algoritmo utilizado es Dijkstra.

El coste utilizado para el cálculo del camino más corto debe ser inversamente proporcional al ancho de banda utilizado. Se puede definir manualmente o calcular dividiendo por ejemplo 100.000.000 por el ancho de banda en bps:

Red	Velocidad	Coste
Token Ring	16 Mbps	6
Ethernet	100 Mbps	1
Línea T1	1,524 Mbps	65
Línea 56k	56 kbps	1785

Si se tiene en cuenta los 10 Gbps de Ethernet, se puede utilizar una fórmula como 10.000.000.000/ancho de banda en bps para calcular manualmente el conjunto de los costes de red.

En cada una de las zonas se mantiene una tabla de estado de vínculos que se graba en un DR (*Designated Router* o router designado), a continuación se guarda en un BDR (*Backup Designated Router* o router designado de seguridad). Este DR sirve como punto central de los intercambios con todos los routers de la zona.

En OSPF, los routers se informan de la evolución de la topología (desconexión de un vínculo, reconexión, descubrimiento de un nuevo router) enviando únicamente las actualizaciones de enrutamiento al router designado de la zona.

OSPF implementa tres tipos de operaciones: en una zona, entre dos zonas y entre dos AS.

Un router de zona de frontera o ABR (Area Border Router) permite el intercambio de información entre zonas.

Todos los routers mantienen actualizada una base de datos topológica en función de las modificaciones que se van realizando. Cada router recalcula su arborescencia SPF para buscar los nuevos caminos más cortos a cada red. Así actualizan su tabla de enrutamiento en función del mejor camino recalculado.

La convergencia del algoritmo es muy rápida. Además, se encarga de la autenticación de las rutas.

En OSPF, se utilizan tres protocolos:

- Hello.
- Inundación (*flooding*).
- Intercambio.

El protocolo Hello permite a los routers verificar los vínculos con sus vecinos. Los paquetes Hello contienen información, como el identificador del router, el intervalo Hello, los vecinos próximos al router (comparten su información de enrutamiento), el identificador de la zona en la que se encuentra el router, así como la prioridad.

El protocolo de inundación lo utiliza un router que detecta cambios en la red, y que quiere avisar rápidamente a los demás de esta modificación.

El protocolo de intercambio es un mecanismo que permite a los routers intercambiar su información de base de datos topológica. Al finalizar el proceso de intercambio, los routers próximos están completamente sincronizados.

Las ventajas principales de OSPF son:

- Una convergencia rápida.
- El algoritmo tiene un buen rendimiento para neutralizar los bucles de nivel 3.
- Los routers se intercambian información del estado de los vínculos con sus vecinos, lo que permite a cada uno hacerse su propia idea del camino más corto.

Los principales inconvenientes son:

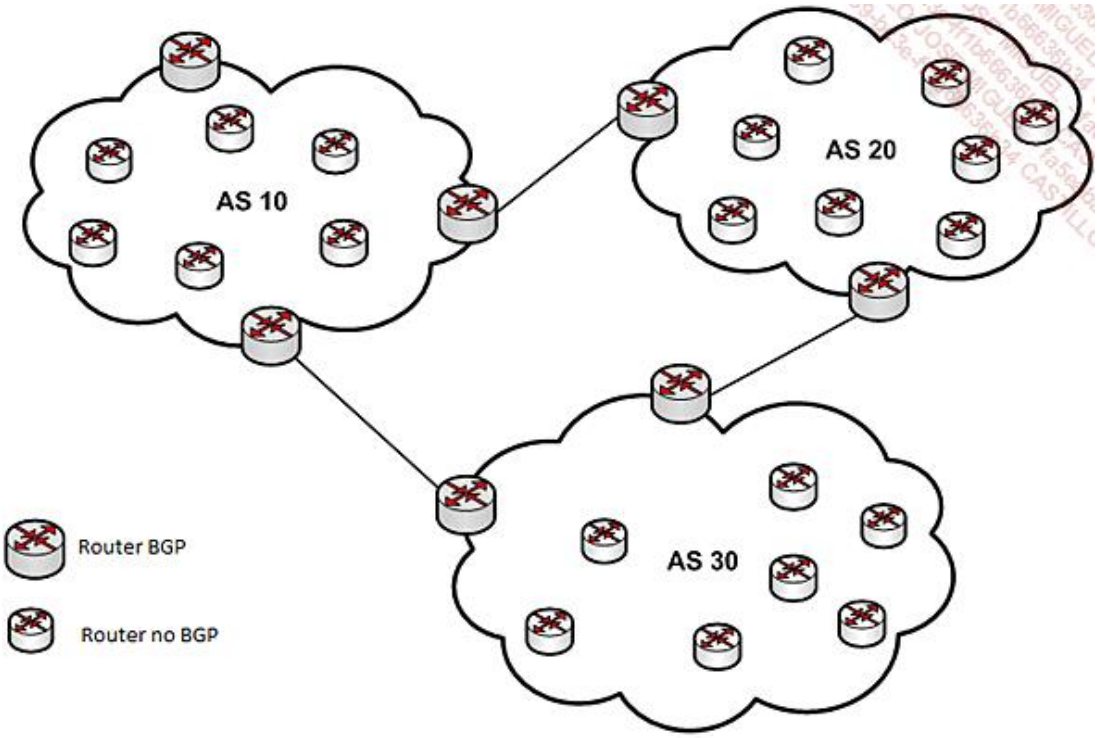
- Un algoritmo complejo de elección de roles específicos para la implementación de OSPF.
- El algoritmo utilizado consume muchos recursos del procesador.

BGP

El protocolo BGP (*Border Gateway Protocol*) en su versión actual, la 4, está descrito en la RFC4271. Se trata de un protocolo externo, es decir, que permite el intercambio de las tablas de enrutamiento entre dos *Autonomous System*. Funciona basándose en reglas de decisión tomadas a lo largo de los AS cruzados, en lugar de utilizar una métrica como en los otros protocolos; en este sentido, está clasificado dentro de los protocolos de tipo **vector de caminos**.

Hoy en día, un AS está codificado en 16 bits y corresponde generalmente a un proveedor de acceso o a una gran empresa. De hecho, a nivel mundial solo puede haber 65535 AS posibles.

BGP relaciona dos AS diferentes para permitir el intercambio de información de enrutamiento. Sin embargo, como cada AS defiende sus propios intereses, es importante poder controlar la información que proviene del otro AS.



Arquitectura BGP

BGP es un protocolo de intercambio entre dos AS y funciona con dos modos posibles de asociación:

- Cliente - proveedor.
- Costes compartidos.

El modo «cliente - proveedor» permite a una gran empresa, que tiene un AS, disponer de conectividad a Internet a través de un proveedor (que tiene igualmente un AS).

El modo «costes compartidos» es una relación de igual a igual, donde cada una de las partes acepta el intercambio de los paquetes a través de un punto de interconexión.

Otra de las particularidades de BGP es que se basa en una conexión TCP (fiable) para realizar los intercambios de las tablas de enrutamiento (TCP 179).

Con BGP se intercambian diversos tipos de mensajes:

- OPEN
- UPDATE
- KEEPALIVE
- NOTIFICATION

La apertura de sesión se realiza a través de un mensaje OPEN. Al principio, los routers BGP se intercambiaban la totalidad de sus tablas. Ahora, se utilizan los mensajes de tipo UPDATE para intercambiar actualizaciones.

La sesión BGP se mantiene a través de mensajes KEEPALIVE.

Finalmente, los mensajes NOTIFICATION permiten generar las excepciones.

BGP, para elegir la mejor ruta con objeto de llegar a una red lejana y propagarla a otro AS, está sujeta a numerosas reglas. Entre ellas podemos encontrar como criterios, por orden de prioridad, las siguientes:

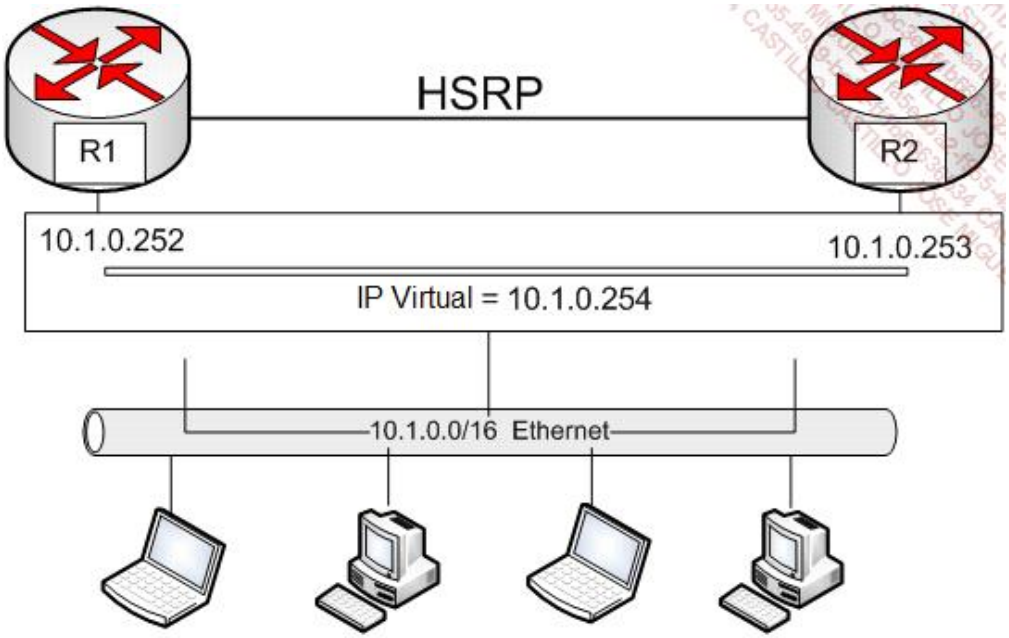
- El peso (preferencia administrativa local).
- La preferencia local (dentro del AS).
- La preferencia de una red cuyo origen es el router local.
- La preferencia de un camino que atraviesa un mínimo de AS.
- La preferencia de un camino aprendido por un protocolo interno en lugar de un protocolo externo.
- La preferencia siguiendo la métrica comunicada por el AS origen.
- La preferencia de las rutas BGP aprendidas por routers externos respecto a routers internos.
- El coste de protocolo interior.
- La asociación BGP para las rutas más estables.
- El identificador del router.

Tolerancia a fallos de una puerta de enlace por defecto: HSRP

Hot Standby Router Protocol o HSRP es un protocolo creado para permitir el restablecimiento transparente en caso de fallo de una puerta de enlace por defecto.

HSRP permite seleccionar, dentro de un grupo de routers, un router activo y un router de emergencia. El router activo es el que se encarga de los paquetes. El router de emergencia es el que se convertirá en activo cuando el falle el principal.

A continuación puede ver una configuración HSRP con dos routers que tienen una interfaz en la red 10.1.0.0/16. Se define como IP virtual para la subred una dirección IP de puerta de enlace por defecto, 10.1.0.254. Cada router dispone de una dirección IP definida para una interfaz en la subred.



Dirección IP virtual y HSRP

La mayor parte de huéspedes IP no disponen más que de una sola dirección IP de puerta de enlace configurada.

Así, cuando se implementa HSRP, la dirección virtual HSRP se configura en los huéspedes, en lugar de una dirección IP de un router físico.

HSRP es útil cuando los huéspedes no incorporan protocolos de descubrimiento de routers como *ICMP Router Discovery Protocol* (IRDP) y no es capaz de bascular a otro router cuando el que tiene configurado no está disponible.

Cuando HSRP se utiliza en un segmento de red, proporciona una dirección MAC virtual, así como una dirección IP que se comparte en un grupo de routers que ejecutan HSRP. Para n routers que ejecutan HSRP, se asignan n+1 direcciones IP y direcciones MAC.

HSRP se basa en un mecanismo de prioridad para determinar qué router HSRP configurado debe ser el router activo. Para definir un router como activo, es necesario asignar la prioridad más elevada entre todos los routers HSRP del grupo.

Los dispositivos HSRP intercambian mensajes Hello multicast para detectar el fallo de un router y para designar el router activo y los routers de emergencia.

Cuando el router activo falla al enviar un mensaje Hello en un periodo de tiempo definido, el router de emergencia que tiene la prioridad más alta se convierte en el router activo. Este mecanismo de transición es completamente transparente para los huéspedes de la red.

e. La puerta de enlace

Es una máquina, generalmente un servidor dedicado o un dispositivo, que opera entre las capas 3 a 7 como traductor de las capas medias y altas, en particular, para la optimización de los datos.

Juniper SRX 5600 - Services Gateway

Con la generalización del uso de TCP/IP, las puertas de enlace se utilizan menos. Las encontraremos, sobre todo, para la interconexión entre estos protocolos y los grandes entornos que utilizan *System Network Architecture* (SNA).

4. Elección de los dispositivos de conexión apropiados

Para facilitar la elección entre los distintos dispositivos de interconexión recién mencionados, examinaremos las distintas características de cada uno. Precisaremos en qué situación nos conviene más un dispositivo que otro.

a. El repetidor

Este actúa en la capa Física del modelo OSI. Permite extender la longitud máxima de un segmento, ampliando la señal, al mismo tiempo que permite interconectar dos soportes físicos diferentes.

No es capaz de trabajar a nivel semántico el contenido de una trama; sin embargo, es capaz de detectar una colisión y de propagarla hacia el otro lado.

A pesar de trabajar en el nivel 1, tampoco es capaz de interconectar cables que funcionen a velocidades diferentes.

Actualmente hablamos de función de repetidor (o concentrador) incorporada a un elemento activo de la red, más que de un componente dedicado.

b. El puente

Posibilita la interconexión de redes que tienen la misma capa de Conexión de datos (el mismo direccionamiento MAC y el mismo modo de acceso) para ejecutar una acción de filtrado basándose en las direcciones físicas, lo que permite desatascar una red sobrecargada.

Deja pasar la multidifusión (*multicast*) y la difusión (*broadcast*), así como las tramas cuya dirección de destino es desconocida. Es capaz de detectar y de administrar los bucles de interconexión.

Actualmente, en las redes locales, estas funcionalidades las implementan los conmutadores.

c. El conmutador

Se comporta como un puente multicable. Permite introducir una arquitectura centralizada de interconexión desde otras LAN. Como se encuentra en el centro de la topología, es un medio privilegiado para seguir la utilización de la red.

En una red Ethernet, permite implementar una red troncal rápida, al mismo tiempo que aislar dominios de colisión distintos, a nivel de cada puerto.

Con un cableado en pares trenzados entre los equipos y el conmutador, es posible trabajar con tarjetas de red directamente en *full-duplex* para duplicar la capacidad global de la red.

El conmutador también se puede utilizar para interconectar dos LAN a 1 Gbps o a 10 Gbps.

d. El router

No deja pasar las difusiones (excepto para algunos routers en que esta opción puede activarse).

Permite elegir el mejor camino posible entre las direcciones lógicas.

No deja pasar un paquete cuya dirección de destino sea desconocida.

Es necesario utilizar un protocolo enrutable, salvo si la función de puente es posible (es el caso de un router puente o b-router).

e. La puerta de enlace

Actúa como una traductora de capas medias y también de las otras: tablas de caracteres, características internacionales o incluso traducción de protocolos.

Evita que se deban instalar componentes de red en cada cliente y ofrece un acceso universal que minimiza la heterogeneidad de la red.