Configuración y administración de protocolos dinámicos.

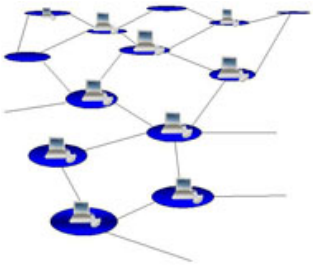
Caso práctico

—Hola Roberto.
—¿Qué tal Tomás?
—¿Qué haces por aquí? Pensaba que estabas fuera, trabajando. — Tomás se acaba de encontrar con un amigo de la infancia que trabaja en una importante empresa de informática.
—Sí, pero tenemos un proyecto aquí y nos han desplazado.
—Me he acordado de ti esta temporada, porque he estado liado con temas de informática y casi me vuelvo loco con tanto protocolo, IP, router, switch, red virtual y qué se yo.
—Es como todo, si estás todo el día con ello te parece algo sencillo pero de lo contrario es un poco complicado. Yo ahora estoy con temas relativos al enrutamiento dinámico en las redes.
— ¡Por el nombre creo que ya me imagino el lío en el que estás!
—No te creas, es más sencillo de lo que parece.
—Vamos a tomar un café y me cuentas un poco más.
Tomás y Roberto pasarán la tarde hablando de los protocolos dinámicos. Tomás empieza a pensar que no ha sido buena idea invitar a Roberto a un café.

Protocolos enrutables y protocolos de enrutamiento.

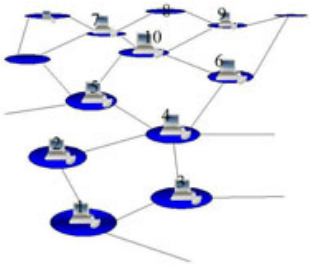
Caso práctico

— ¿Qué protocolos se utilizan en el enrutamiento dinámico?
—Para empezar hay que distinguir entre dos tipos de protocolos, enrutables y de enrutamiento.
—Yo sólo he manejado el IP y casi me desborda.
—No te preocupes verás que no es tan complicado.
—Creo que va a ser una tarde larga, a lo mejor el café se alarga hasta la cena.
Roberto ha empezado a contarle a Tomás los tipos de protocolos con los que trabaja en el enrutamiento dinámico. Veamos si estos protocolos son interesantes.



Los protocolos se pueden clasificar según la capacidad de ser o no enrutables, es decir, tener la propiedad de poder identificar en una red a los dispositivos que forman parte de ella y además asignarles parámetros, que puedan determinar caminos de conexión diferentes entre ellos. Por tanto, una clasificación posible de los protocolos sería:

- **No enrutables.**
- **Enrutables.**



Además, si los protocolos son capaces de encontrar el mejor camino entre dos puntos de la red, se puede decir que son protocolos de enrutamiento.

En la imagen anterior, el protocolo enrutable será el que permita identificar de manera única a cada uno de los ordenadores que están en los círculos, y el protocolo de enrutamiento será el encargado de obtener la ruta óptima entre dos puntos de esa red. Si no se tienen referencias, es imposible crear un camino, por tanto, se necesitará poder distinguir (identificar) cada uno de los elementos de dicha red. Es decir, el protocolo de enrutamiento necesita del protocolo enrutable.

Es evidente, que si identificamos con un número cada uno de los equipos (protocolo enrutable), los podemos distinguir y además podemos determinar diferentes rutas entre dos puntos de la red. En este caso se puede decir que para ir desde el equipo número 1 al equipo número 10 se pueden trazar varias rutas (protocolo de enrutamiento), por ejemplo, son posibles entre otras:

- 1-3-4-6-10.
- 1-2-4-5-10.

La elección de la ruta óptima es una responsabilidad del protocolo de enrutamiento, pero el protocolo de enrutamiento no puede funcionar sin la identificación de los elementos, llevada a cabo por el protocolo enrutable.

Autoevaluación

Un nodo de la red (PC1) se identifica con los números N1 (host) y R1 (red), estos valores se establecen con el protocolo P1 y hacen posible que otro protocolo P2 determine las mejores rutas entre el PC1 y el PC2, identificado con los números N2 y R2, determinados por P1. En esta situación se cumple que:

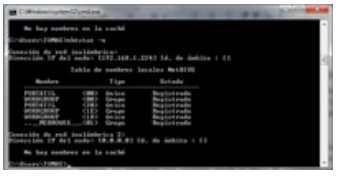
- P1 es un protocolo de enrutamiento.
- P2 es un protocolo de direccionamiento.
- P2 es un protocolo enrutable.
- P1 es un protocolo enrutable.

Protocolos no enrutables.

Los protocolos no enrutables solamente funcionan en un segmento de red, a nivel 2. Un ejemplo de estos protocolos es NetBEUI. Este protocolo es un protocolo previo a la explosión de Internet, en esa época, los programadores no podían ni imaginar la expansión que ha tenido la interconexión de redes por lo que se diseñó para redes pequeñas.

El protocolo NetBEUI hace que los equipos se identifiquen mediante nombres, (nombres NetBIOS), y no tiene la capacidad de asignar una dirección de red a sus paquetes, por lo que estos no pueden atravesar los routers. El comando que permite desde la línea de comandos ver los nombres NetBIOS que reconoce un equipo es:

nbtstat -n



En la imagen se puede ver como después de ejecutar el comando, aparecen varias columnas entre las que se encuentra una que nos proporciona los nombres de los dispositivos reconocidos en ese momento, en este caso PORTATIL y WORKGROUP, nombre del equipo donde se está trabajando y el nombre del grupo de trabajo al que pertenece.

NetBIOS y NetBEUI trabajan conjuntamente y se integran perfectamente con los protocolos TCP/IP. Se puede ver tanto en los sistemas más modernos como en la configuración de las interfaces de red, que se contemplan aspectos de su configuración.

En la imagen se puede apreciar cómo se puede escoger entre distintas configuraciones para NetBIOS y su relación con LMHOSTS.

La configuración que aparece en la imagen es la más adecuada cuando se trabaja conectado a un servidor DHCP, y se obtienen de él todas las configuraciones necesarias para la interconexión. En el caso de que el equipo forme parte de un grupo de trabajo, se puede escoger entre habilitarlo sobre TCP/IP o no, en muchas ocasiones se solucionan problemas con estas dos opciones.

NetBEUI se ocupa de todo el formato que no es capaz NetBIOS, de hecho, la definición es NetBIOS Extended User Interface.

Autoevaluación

El protocolo NetBEUI es un protocolo que se utiliza para identificar nodos en una red, lo que significa que:

- Es un protocolo enrutable porque trabaja a nivel 3.
- Es un protocolo de enrutamiento porque es capaz de especificar una ruta en la red.
- No es un protocolo enrutable porque no incluye la capacidad de identificar direcciones de red.
- Es enrutable porque es capaz de atravesar routers en redes Windows.

Protocolos enrutables o enrutados.

Los protocolos enrutables, al contrario de los no enrutables, son capaces de dar soporte a la capa de red (OSI) o internet (TCP/IP). Un protocolo enrutable debe ser capaz de asignar un número de red y un número de equipo a cada dispositivo de la red. Algunos de estos protocolos solamente incluyen el número de red, como el IPX, que utiliza la dirección MAC de los equipos para identificar a los host. Cuando un mensaje que utiliza estos protocolos llega a un dispositivo como un router, para poder extraer las direcciones de red y de host a partir de las IP, se utilizan las máscaras de red y la operación AND.

En la imagen anterior se puede apreciar cómo funciona la máscara de red para dos direcciones IP, (192.168.0.20 y 192.168.0.10), que pertenecen a la misma dirección de red (192.168.0.0), y cuál es el resultado para una dirección (232.180.119.11), que pertenece a otra red (232.180.129.0). Los routers reconocen como posibles destinos a las direcciones de red, pero al tiempo necesitan conocer las direcciones IP de cada host, cualidades ambas

proporcionadas por los protocolos enrutables.

Estos protocolos son los encargados de incluir la información suficiente para que el router pueda enviar los mensajes de un punto a otro de la red. El protocolo IP en sus versiones IPv4 e IPv6, responsable de las direcciones IP más comúnmente utilizadas, es uno de los protocolos enrutables más utilizado.

IP es un protocolo que facilita el enrutamiento en la red, pero que es no orientado a la conexión y poco confiable, no establece ningún circuito de conexión dedicado y no comprueba si los datos han llegado o no bien al destino, esto no significa que no funcione bien sino que deja esa labor para otros protocolos.

La cualidad de enrutable la tienen porque son capaces de agrupar direcciones dentro de una red, gracias a las direcciones de red, y como son los routers los encargados de dirigir el tráfico hacia una u otra dirección de red, esto permite que no se tengan que conocer todas y cada una de las direcciones individuales de los equipos.

Autoevaluación

Un equipo tiene como configuración en su tarjeta de red los valores 10.0.0.1, 10.0.0.0 y 255.0.0.0 ¿Cuál de ellos determina la ruta por la que es accesible?

- ○ La dirección 10.0.0.1 ya que identifica de manera única al equipo.
- ○ 255.0.0.0 porque es su máscara de red.
- ○ 10.0.0.0 porque es la dirección de red.
- ○ El resultado de la operación AND entre 10.0.0.0 y la máscara de red 255.0.0.0.

Protocolos de enrutamiento.

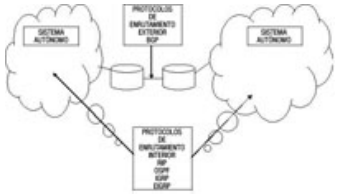
Un **protocolo de enrutamiento** es un conjunto de normas que cumplen los routers cuando se relacionan con otros routers, y se intercambian información necesaria para construir tablas de enrutamiento. Son los encargados de que los routers puedan intercambiarse las **tablas de enrutamiento** y actualizar la información de enrutamiento, determinan la **ruta** que deben seguir los protocolos enrutados.

Los protocolos de enrutamiento que se verán en esta unidad son:

- **RIP: Protocolo de información de enrutamiento.**
- **IGRP: Protocolo de enrutamiento de Gateway interior.**
- **OSPF: Protocolo primero de la ruta libre más corta.**
- **BGP: Protocolo de Gateway fronterizo (BGP).**
- **EIGRP: IGRP mejorado.**

Todos los protocolos de enrutamiento anteriores, se pueden clasificar dependiendo de si operan dentro o fuera de un **sistema autónomo**, en:

- **Protocolos de enrutamiento exterior.**
- **Protocolos de enrutamiento interior.**



En la figura se puede ver claramente la diferencia entre protocolo de enrutamiento exterior e interior y los protocolos de enrutamiento más característicos de cada clase.

Un sistema autónomo es un sistema en el que todo el control de administración lo tiene una sola entidad, es una "pequeña" Internet dentro de Internet.

Para saber más

Puedes encontrar más información sobre los sistemas autónomos en el siguiente enlace.

Sistemas autónomos.

Autoevaluación

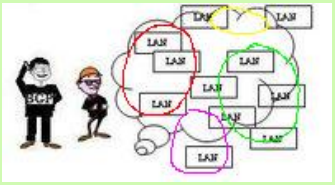
El protocolo IP utilizado en las redes LAN es:

- ○ Un protocolo dinámico de enrutamiento interior.
- ○ Un protocolo de enrutamiento exterior, porque me da las direcciones que hacen posible la conexión a Internet.

- Un protocolo enrutado.
- Un protocolo enrutable dinámico interior.

Protocolos de enrutamiento interior y exterior.

Caso práctico



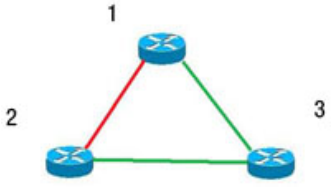
—Pues te voy a decir una cosa, si alguien me hubiera preguntado por un **protocolo de enrutamiento interior**, habría contestado IP.
—Ya, es normal, si no estás familiarizado con el concepto, pero IP es un protocolo enrutable no de enrutamiento.
—Es decir, los protocolos de enrutamiento trabajan con redes más grandes que las redes LAN, pero que a su vez son grupos dentro de Internet y cuya administración no está al alcance de cualquiera. —Algo así, pero no pienses en redes LAN, son grupos mucho mayores que redes LAN, espera un poco y te hablo del enrutamiento interior y exterior.
Roberto le explicará a Tomás en qué consisten los **protocolos de enrutamiento interiores y exteriores**. Esto no se va a solucionar con un café, me parece que tendrán que quedar otro día.

Los protocolos de enrutamiento dinámicos se clasifican en exteriores o interiores, dependiendo de si actúan dentro o fuera de un sistema autónomo, las siglas que suelen emplearse para definir estos dos grupos son IGP (Interior Gateway Protocol) y EGP (Exterior Gateway Protocol). Entre los protocolos EGP más utilizados está BGP, este protocolo intercambia información entre sistemas autónomos a los que se les asigna un número ASN.

Protocolos IGP son RIP, IGRP, EIGRP y OSPF entre otros. Los protocolos IGP utilizan distintas técnicas para determinar el enrutamiento:

a. **Vector distancia.**
b. **Estado de enlace.**
c. **Vector distancia avanzado.**

Cada una de estas técnicas tiene en cuenta un criterio para poder determinar la mejor ruta, la variable que utilizan para calibrar una ruta se denomina métrica.



No todos los **protocolos** utilizan la misma **métrica**, por ejemplo, un protocolo puede tener como métrica el número de saltos y otro la velocidad o el ancho de banda de la comunicación. Elegir la métrica que se va a seguir es como elegir el mejor camino para viajar en coche, hay personas que prefieren recorrer menos kilómetros aunque tengan que ir más despacio y escogen una carretera comarcal en lugar de una autopista.

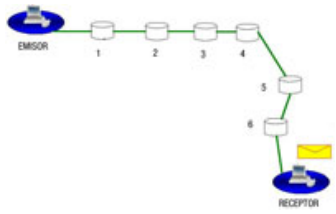
En la imagen se muestran tres routers interconectados, escoger el camino óptimo entre el router 1 y 2 dependerá de la métrica. Si se escoge una métrica donde se valora el número de saltos, (routers que se atraviesan), la ruta óptima será la de color rojo. Si por el contrario se valora el ancho de banda, el retardo o alguna cualidad que tiene la ruta verde pero no tiene la ruta roja, el camino óptimo sería el de color verde.

Protocolos de enrutamiento interior.

Los **protocolos de enrutamiento interior** se configuran en cada uno de los routers incluidos en el sistema autónomo.

La técnica de **vector distancia** que utilizan para encontrar la ruta óptima tiene como principales características:

- **Cada nodo tiene una tabla de encaminamiento que incluye los destinos junto con la distancia a los nodos.**
- **La distancia se expresa como el número de routers que se deben atravesar para llegar al nodo destino.**
- **Cada nodo envía paquetes de sondeo a sus nodos vecinos para mantener actualizado el valor asignado a la distancia con los otros nodos.**
- **Cada nodo estudia la información recibida para conseguir una ruta de menor retardo.**



En la imagen se puede apreciar como el mensaje ha atravesado 6 routers por lo que el número de saltos es 6, este valor sería la distancia que va recorriendo el mensaje y que formaría parte del vector distancia.

El vector distancia correspondiente a la relación entre el equipo 1 y 2 sería:

VectorDistancia(2:17)

La otra técnica utilizada es la que se basa en el **estado del enlace**, cuyas características son:

- **Se calcula el mejor camino a todos los nodos de la red, empleando un algoritmo (Dijkstra).**
- **Las tablas son más complejas que cuando se usa la técnica del vector distancia.**
- **En este caso se envían mensajes a todos los nodos de la red, no solamente a los vecinos como en el caso del vector distancia.**

- **Utiliza el método de inundación para repartir la información del estado del enlace.**

Para saber más

Puedes encontrar más información sobre cómo funciona el algoritmo de Dijkstra en este enlace.

Dijkstra.

IGRP, RIPv1 y RIPv2 utilizan la técnica del vector distancia. OSPF se basa en el estado del enlace y EIGRP utiliza una mezcla que se podría clasificar como**vector distancia avanzado**.

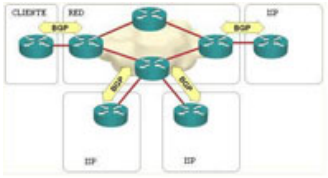
Protocolos de enrutamiento exterior.

Los **protocolos de enrutamiento exterior** (EGP) administran rutas que conectan sistemas autónomos diferentes, un ejemplo de estos es el protocolo BGP.

Para saber más

En el siguiente enlace podrás aprender más cosas sobre el protocolo BGP.

BGP.



El primer protocolo de enrutamiento exterior que se utilizaba era el EGP, cuyas siglas coinciden con las que se utilizan actualmente para denominar a todos los protocolos de enrutamiento exterior. En la actualidad BGP es el protocolo utilizado en Internet en el enrutamiento entre dominios, este protocolo se basa en el **vector distancia**.

Aunque BGP se utiliza entre sistemas autónomos, también se puede utilizar en su interior, en este caso se denomina (IBGP). Para distinguirlos, el exterior se denomina EBGP.

La ruta óptima escogida por BGP viene determinada por el número de sistemas autónomos atravesados para llegar al destino.

En la imagen se puede ver la función que realiza BGP en el entramado de Internet. Se ha representado como un sistema autónomo a toda la red que comunica al proveedor de servicios con el cliente (RED).

BGP clasifica las redes en tres categorías:

- **Redes stub: son las redes que solamente tienen una conexión al entramado BGP y por tanto no se pueden usar para transportar tráfico.**
- **Redes multiconectadas: son redes que pueden soportar el tráfico entre sistemas autónomos, salvo que lo rechacen.**
- **Redes de tránsito: son las redes dorsales, tienen disponibilidad para transportar paquetes de otros sistemas autónomos y normalmente son de pago.**

Autoevaluación

¿Qué protocolo de enrutamiento se utiliza para efectuar la comunicación entre sistemas autónomos?

- RIP.
- Ethernet.
- IGP.
- BGP.

Distancia administrativa.

La distancia administrativa es un parámetro para comparar dos rutas cuyo coste está medido en unidades diferentes. Una de las rutas puede tener un coste 1 utilizando un protocolo RIP y sin embargo, puede tener un coste en EIGRP de 4132768 cuyo valor no se puede comparar porque miden dos cosas diferentes, ya que RIP mide saltos y EIGRP incluye en su cálculo también el ancho de banda por ejemplo. Si lo llevamos al lenguaje coloquial es como comparar manzanas con peras.
Puesto en las redes actuales conviven muchas topologías y protocolos, el parámetro que se utiliza para encontrar la ruta óptima es un número que

se denomina **distancia administrativa**.

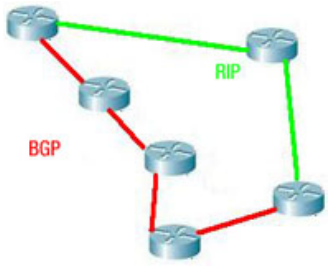
Distancia administrativa de los diferentes protocolos de enrutamiento.

PROTOCOLO	DISTANCIA ADMINISTRATIVA
BGP	20
EIGRP	90
IGRP	100
OSPF	110
RIP	120
EGP	140

De la tabla se puede deducir que si una ruta entre dos puntos de la red, por un camino utiliza un protocolo BGP cuya distancia administrativa es 20 y por otro camino utiliza RIP cuya distancia administrativa es 120, se deberá escoger la ruta que utiliza BGP.

Aunque estos valores vienen definidos por defecto en los routers, el administrador del sistema los puede variar.

```
PAR06(config)#router rip
PAR06(config-router)#distance 90
```



Con los comandos anteriores se cambia la distancia administrativa de RIP al valor 90, en lugar de 120 que es su valor por defecto.

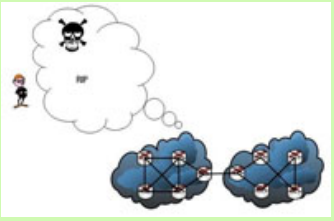
En la imagen se puede ver cómo, a priori, la ruta de color verde parecería ser la más óptima, puesto que hay menos saltos (routers) en el camino, pero si se utiliza como criterio la distancia administrativa, podría resultar que la ruta escogida sea la de color rojo.

Entre los valores que puede tomar la distancia administrativa están 0, 1 y 255.

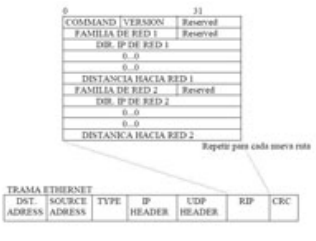
- **El valor 0 se utiliza cuando es una ruta directamente conectada.**
- **El valor 1 se usa si la ruta se alcanza en el siguiente salto.**
- **El valor 255 se emplea si la ruta no es confiable y hay que descartarla.**

El protocolo RIPv2; comparación con RIPv1.

Caso práctico



—Nosotros trabajamos con —Nosotros trabajamos con **protocolos** que gestionan redes más grandes que las locales. — ¿Internet? —Bueno, redes que forman parte de Internet, los sistemas autónomos y los protocolos de comunicación entre ellos, utilizamos protocolos como RIP. — ¡Vaya nombre! Un poco tétrico. —**RIP es un protocolo** que gestiona la comunicación interna de un **sistema autónomo**. Roberto le hablará a Tomás sobre el protocolo RIP de enrutamiento interno y algunas características importantes sobre él. que gestionan redes más grandes que las locales.
— ¿Internet?
—Bueno, redes que forman parte de Internet, los sistemas autónomos y los protocolos de comunicación entre ellos, utilizamos protocolos como RIP.
— ¡Vaya nombre! Un poco tétrico.
—RIP es un protocolo que gestiona la comunicación interna de un sistema autónomo.
Roberto le hablará a Tomás sobre el protocolo RIP de enrutamiento interno y algunas características importantes sobre él.



La diferencia principal entre la versión 1 y la 2 es que RIPv1 no soporta subredes, VLSM ni CIDR, mientras que la versión 2 sí. Ambos actúan de igual manera, cuando eligen una ruta no tienen en cuenta la velocidad del enlace, solamente se fijan en el número de saltos.

FAMILIA DE RED	ROUTE TAG
DIRECCIÓN IP	
MÁSCARA DE SUBRED	
SIGUIENTE SALTO	
DISTANCIA	

Los routers que soportan estas versiones de RIP deben tener la capacidad de crear una ruta alternativa a la óptima para cuando ésta falle, este proceso se denomina convergencia. RIP en sus dos versiones tarda mucho en realizar este proceso, puede tardar hasta tres minutos.

RIPv1 fue diseñado para redes con clase, lo que le permitía conocer la redes conociendo los primeros bits de las direcciones IP, muy poca información, ya que la máscara de red no se incluye. Este protocolo no tenía mecanismos para evitar que un router no autorizado pudiera publicar

rutas erróneas en la red.

RIPv2 si envía máscaras junto con las direcciones IP y además admite autenticación para verificar que los anuncios de las rutas son de routers autorizados.

Los routers diseñados para RIPv2 son compatibles con la versión RIPv1, y los diseñados para RIPv1 si reciben una notificación de RIPv2 la tratan como si fuera RIPv1.

Para asegurar la compatibilidad entre las dos versiones RIPv2 utiliza los campos que RIPv1 tenía a cero para incluir las nuevas funcionalidades.

Autoevaluación

¿Qué ocurre cuando un router que utiliza el protocolo RIPv1 recibe un mensaje de un router que utiliza el protocolo RIPV2?

- En el mensaje no puede haber ninguna información relativa a las direcciones de subred.
- En el mensaje si hay información relativa a las direcciones de subred.
- El mensaje se descarta en el router RIPv1 y es reenviado a un router RIPv2.
- Es imposible que en una misma red convivan routers RIPv1 y RIPv2.

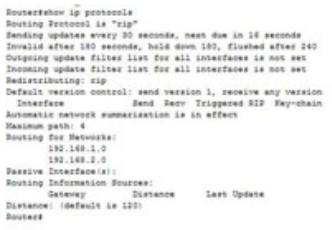
Configuración y administración de RIPv1.

Caso práctico

— ¿Por qué se ha dejado de utilizar RIPv1?
—No se ha dejado de utilizar, digamos que se ha mejorado y ahora se utiliza RIPv2. Internet ha avanzado mucho y con ella el número de direcciones IP y la necesidad de RIPv2.
— ¿Y qué ha pasado con todos los routers que trabajaban con la versión 1?
—Perdona, me he explicado mal. Se sigue utilizando y convive con el RIPv2.
— ¿Al ser más antiguo es más complicado de configurar o qué?
- —No, es muy parecido a la configuración de RIPv2, pero tiene desventajas. Mañana quedamos y te enseño la configuración de los dos.
Roberto enseñará a Tomás a configurar RIPv1 y RIPv2. Estaba visto que con un café no se arreglaba esto. Tomás al llegar a casa se ha puesto a buscar información en Internet sobre la configuración de RIPv1 para que mañana Roberto no le pille por sorpresa con su charla.

Antes de configurar el protocolo RIP es conveniente comprobar los protocolos instalados, para ello, se utiliza el comando:

PAR06#show ip protocols



La salida de este comando será algo así:

Se puede ver en la imagen, como la salida muestra si está instalado el protocolo RIP, en este caso sí.

Además, muestra otro tipo de información, como el tiempo en que tarda en reenviar los paquetes (30 segundos) y las direcciones de red sobre las que actúa (192.168.1.0 y 192.168.2.0).

La configuración de RIP se hace solamente sobre aquellas redes que estén directamente conectadas al router con el que se trabaja. Para configurar el protocolo RIPv1 los pasos son:

a. Entrar en modo privilegiado.
b. Entrar al modo de configuración de enrutamiento RIP.
c. Especificar las redes sobre las que se quiere activar RIP.

Un ejemplo de configuración RIP podría ser el siguiente, donde el comando network se utiliza para especificar las redes que van a soportar RIP.

```
PAR06>enable
PAR06#configure terminal
PAR06(config)#route rip
PAR06(config-router)# network 10.0.0.0
PAR06(config-router)# network 11.0.0.0
```

Configuración y administración de RIPv2.

Caso práctico

—Bueno, no es tan difícil la configuración.
—Es mucho más complicado comprender lo que hace RIP que configurarlo.
—Ahora te enseñaré a configurar la versión RIPv2.
— ¿Hay mucha diferencia?
—No, son casi iguales, hay que incluir un comando para especificar que se va a utilizar RIPv2.
Tomás aprenderá como configurar RIPv2, siguiendo un proceso similar al de la configuración de RIPv1, con la inclusión de alguna variación.

En la configuración de RIPv2 se siguen los mismos pasos que para RIPv1, salvo en el que se especifica la versión del protocolo con el comando **version 2**. El proceso se podría resumir en lo siguiente:

- **Utilizar el comando router rip para entrar en el modo de configuración RIP.**
- **Utilizar el subcomando version 2 para indicar la versión.**
- **Emplear el comando network para habilitar RIP en las interfaces conectadas.**

Con este proceso quedaría configurado el protocolo RIPv2 para todas las interfaces directamente conectadas al router, como el comando **network** configura RIP en toda la red (puede haber más de una interfaz del router para una misma red), para hacer que una de las interfaces que está conectada a esa red no esté configurada con RIP sin modificar la configuración de las demás interfaces se emplea el comando **passive-interface**. Con este comando se puede anular RIP en una interfaz determinada, se evita que se envíen las actualizaciones RIP a través de ese interfaz. La sintaxis sería:

```
PAR06(config-router)#passive-interface FastEthernet 0/0
```

Un ejemplo de configuración RIPv2 sería el siguiente:

```
PAR06#configure terminal
PAR06(config)#router rip
PAR06(config-router)#version 2
PAR06(config-router)#network 192.168.1.0
PAR06(config-router)#network 192.168.2.0
PAR06(config-router)#network 10.0.0.0
PAR06(config-router)#passive-interface FastEthernet 0/1
```

Con la configuración anterior se establece RIP versión 2 para las interfaces conectadas directamente a las redes 192.168.1.0, 192.168.2.0 y 10.0.0.0 (utilizando la máscara definida en cada interfaz), y además, se suprime de la configuración RIP a la interfaz FastEthernet 0/1.

Autoevaluación

La siguiente línea de comandos: PAR06(config-router)#network 192.168.1.32

- No es válida.
- Es válida.
- Faltaría saber la máscara de red para saber si es válida o no.
- Solo es válida en RIPv1.

Para saber más

En el siguiente vídeo puedes ver cómo funciona RIP

RIP

se ha podido cargar el compleme

(Resumen textual alternativo)

Diagnóstico de incidencias en RIPv2.

Caso práctico

— ¿Y cómo sé que el protocolo está funcionando correctamente?
—Bueno, lo más básico es ver que todos los equipos están comunicados perfectamente, pero hay otros métodos.
— ¿Cuáles?

Roberto enseñará a Tomás a interpretar la salida de los diferentes comandos que proporcionan información sobre el estado del enrutamiento.

El primer paso para detectar incidencias es verificar que RIPv2 está configurado, para ello se emplea el comando **show ip protocols**, que vimos en el punto 4. Otro comando muy útil es:

PAR06#show ip route

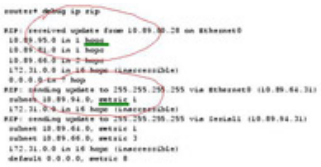
La salida de este comando tiene líneas como:

R 192.168.1.0/24 [120/1] via 10.10.10.254, 00:00:03, Serial0/0/0

Esta salida muestra la dirección de red destino (192.168.1.0) y la dirección IP (10.10.10.254) de la interfaz del siguiente router por la que se accede a la red destino (10.10.10.254), así como la interfaz local por la que se accede a la red (serial0/0/0) y la **distancia administrativa** (120), junto con la métrica (saltos) en este caso 1. Además, aparece una R al comienzo para resaltar que estos datos provienen del enrutamiento RIP. También se puede ver el tiempo que ha transcurrido desde la actualización de la ruta, en este caso 3 segundos.

El siguiente comando utilizado para analizar el funcionamiento de RIP es:

PAR06#debug ip rip



La salida de este comando es del tipo que se muestra en la figura. Se pueden observar mensajes como **sending (enviando)** o **received (recibido)**, acompañados de las direcciones IP de las que provienen y el tipo de interfaz por el que entran, en este ejemplo, la Ethernet0 y la Serial1. A su vez muestra también la métrica o los saltos hacia o desde las diferentes direcciones de red que conoce el router. Se podría interpretar por ejemplo, que el router recibe la información de 10.89.80.28 en la que le dice las redes que conoce y los saltos que tiene hacia ellas (1 salto o hop significa directamente conectado).

También podríamos saber en este momento hacia que redes se está enviando la actualización y desde que interfaces, en este caso desde las interfaces Ethernet0 y Serial1 hacia las redes 10.89.94.0, 10.89.64.0 y 10.89.66.0.

Autoevaluación

Si en la línea de comandos escribimos: PAR06(config-router)#network 192.168.1.0, esto implica que la máscara de red que se está utilizando es:

- 255.255.255.0, la que corresponde a una red de tipo C.
- La que nos indique la subred creada por el protocolo RIPv1.
- La que tenga configurada la interfaz directamente conectada a esta red.
- RIPv2 no es capaz de soportar máscaras de red.

Los protocolos de enrutamiento estado-enlace.

Caso práctico

—Vale, pues no parece tan complicado lo de RIP.
—Bueno, lo complicado es configurar grandes sistemas autónomos y sobre todo hacer que convivan más protocolos.
— ¿Más? ¿Se utiliza algún otro aparte del RIP?
—Muchos más, aunque sobre todo se usa el OSPF.
— ¿Funciona igual que el RIP?
—Igual no, tiene algunas diferencias. Aunque está diseñado para el mismo fin.
— ¿Encontrar la mejor ruta?
—Exactamente, pero con otra técnica.

Roberto explicará a Tomás las características más importantes del protocolo OSPF, representativo de los protocolos IGP basados en el enrutamiento estado-enlace.

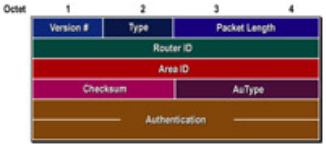
Los **protocolos de enrutamiento estado-enlace** tienen su fundamento en el **envío de mensajes entre los routers** que forman la red, para informar a todos de quienes son sus vecinos y la distancia que les separa de cada uno de ellos. Con toda la información recopilada, se construye una base de datos de información, que se utiliza para determinar los caminos óptimos entre ellos. Uno de los protocolos más representativos que utilizan esta técnica es OSPF (Open Shortest Path First), "abrir primero la ruta más corta".

OSPF es un protocolo del tipo IGP, usado dentro de los sistemas autónomos y se considera un sucesor de RIP. Entre sus características principales están:

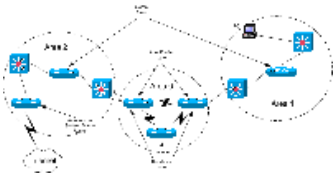
a. **Algoritmo abierto.**
b. **Es capaz de balancear la carga.**
c. **Usa una métrica basada en la distancia física y el retardo.**

Una trama OSPF tiene el aspecto de la figura. Se ve como se incluye un campo para identificar el área sobre el que actúa.

OSPF soporta tres tipos de redes:



- **Líneas punto a punto.**
- **Redes de multiacceso con difusión como las LAN.**
- **Redes de multiacceso sin difusión como las WAN.**



En la imagen se puede ver como es una **topología** que utiliza OSPF. El protocolo OSPF divide los sistemas autónomos en áreas numeradas. Cada sistema autónomo tiene una red dorsal a la que se le asigna el área número 0, todas las demás áreas se conectan a esta dorsal, puede haber equipos que no pertenezcan a ningún área.

Dentro de cada área, cada router, que debe calcular el camino más corto hasta los demás routers del área, maneja la misma base de datos donde se tiene la información de los enlaces, y utiliza el mismo algoritmo para encontrar la ruta óptima.

Los protocolos de enrutamiento estado-enlace I.

Puede ocurrir que haya un enrutador que esté en la frontera de dos áreas diferentes y las comunique, en este caso, deberá tener la base de datos de ambas y utilizar los algoritmos de ambas por separado. De acuerdo con lo anterior, OSPF clasifica los enrutadores en cuatro tipos:

- **Internos: están en el interior del área.**
- **De límite de área: conectan dos o más áreas.**
- **De red dorsal: pertenecen a la red dorsal.**
- **Fronterizos de sistemas autónomos: se comunican con otros sistemas autónomos.**

La información que forma parte de la base de datos que utilizan los enrutadores, se consigue mediante el intercambio de mensajes entre los routers, estos mensajes publican su estado y piden información del estado de los routers que los rodean. En la tabla siguiente se pueden ver los tipos de mensajes que maneja OSPF.

Tipos de mensajes OSPF.

TIPO DE MENSAJE	FUNCIONALIDAD
HELLO	Sondear el entorno.
LINK STATE UPDATE	Publicar el costo del emisor a sus vecinos.
LINK STATE ACK	Confirmación de la recepción de la actualización del estado del enlace.
LINK STATE REQUEST	Solicitar información del estado del enlace.
DATABASE DESCRIPTION	Anunciar que actualización tiene el emisor.

El proceso que sigue el protocolo OSPF es el siguiente:

- **Inundación de mensajes.**
- **Cada router informa a los demás de sus vecinos en el área.**
- **Cada router se construye sus rutas más cortas, tanto en las áreas como en la red dorsal.**
- **Los enrutadores de la red dorsal intercambian información con los routers fronterizos de las áreas.**
- **Los routers fronterizos difunden la información a los routers del interior de las áreas.**

Para saber más

Puedes encontrar más información sobre OSPF en este enlace.

OSPF.

Autoevaluación

El área es un parámetro que se utiliza:

- En el protocolo RIP para dividir el sistema autónomo en subredes.
- En el protocolo OSPF para dividir el sistema autónomo.
- En RIPv1 para poder trabajar con subredes.
- En todos los protocolos IGP.

Para saber más

En el siguiente vídeo puedes ver cómo funciona OSPF.

Funcionamiento de OSPF

se ha podido cargar el compleme

(Resumen textual alternativo)

Configuración y administración OSPF.

Caso práctico

—Pues ya que me enseñaste a configurar RIP, enséñame la configuración de OSPF.
—Es prácticamente igual salvo algún detallito.
— ¿Detallito? Seguro que se complica.
— ¡Qué no! Verás, sólo cambia un poco la línea del comando **network**, con la máscara wildcard y el área.
— ¿Qué? ¿Máscaras? Eso da un poco de miedo.
—Espera, no seas impaciente y verás que sencillo.

Tomás aprenderá con Roberto a configurar un router con OSPF y sobre todo el nuevo concepto de **máscara wildcard**.

La configuración de OSPF sigue un proceso parecido al de la configuración RIP con alguna diferencia en los comandos como es de esperar. La secuencia de comandos es:

a. router ospf <número>
b. network dirección-red máscara-wildcard area <número>

El número que acompaña al comando **router ospf** es un número (entre 1 y 65535), que se asigna al proceso OSPF y que le asigna el propio administrador, ya que pueden convivir varios procesos OSPF.

Al comando **network** le acompañan la dirección de red y la máscara wildcard, además del modificador área y un número que identifica al área en el que estemos configurando OSPF.

Máscara 255.255.255.0 tiene asociada la máscara wildcard 0.0.0.255
Máscara 255.255.255.252 tiene asociada la máscara wildcard 0.0.0.3

Con una máscara wildcard 0.0.0.255, le estamos diciendo al enrutador que solamente se quieren en nuestro segmento OSPF equipos que pertenezcan a la dirección de red coincidente con los tres primeros octetos. Si utilizamos 0.0.0.0 como máscara wildcard se está exigiendo que en el segmento de red solamente sean posibles direcciones que coincidan en todos sus bits, una dirección de host.

En cuanto al área, para redes pequeñas solamente suele haber un área definida, la número 0. Si hubiera que definir más de una, el número 0 se emplearía para la red dorsal. Un ejemplo de configuración OSPF podría ser el siguiente:

```
PAR06#configure terminal
PAR06(config)#router ospf 1
PAR06(config-router)#network 192.168.1.0 0.0.0.255 area 0
```

En el ejemplo anterior, se ha configurado OSPF para que todas las interfaces en la red 192.168.1.0 actúen bajo ese protocolo, se le ha asignado el número de proceso 1 y la configuración actuará sobre el área 0.

Autoevaluación

La siguiente línea de comandos:

network 10.0.0.0 0.0.0.255 area 1

- No es posible porque está mezclando una máscara C con una dirección A.
- Afecta a todos los equipos de la red dorsal.
- Afecta a todos los equipos que pertenezcan a la red 10.0.0.0/24.
- Especifica que los equipos afectados por RIP son 254.

Diagnóstico de incidencias en OSPF.

Caso práctico

— ¿Y cómo sé que está funcionando OSPF?
—Pues de la misma manera que se comprueba el funcionamiento de RIP.
— ¿Los mismos comandos?
—No, parecidos, pero el proceso se hace de igual modo. Aquí se tiene el concepto de área.
— ¿Cómo si fueran áreas de terreno?
—Algo parecido.
— ¿Con esto acabamos ya?
—Bueno, con esto puedes empezar a navegar.

Este es el momento más esperado por Tomás, ya tiene ganas de acabar y descansar un poco de tanto protocolo, pero antes, Roberto intentará que aprenda a verificar el funcionamiento de OSPF.

Las incidencias que se puedan producir en el funcionamiento de OSPF, se pueden observar con el empleo del comando show como en el caso del protocolo RIP, aparte de las combinaciones show **ip protocol** y **show ip route** que se han visto en el punto dedicado a RIP, se pueden emplear las siguientes:

a. **show ip ospf**
b. **show ip ospf interfaces**
c. **show ip ospf neighbors**
d. **show ip ospf database**

El primer comando nos muestra información general sobre el funcionamiento de OSPF, si se quiere saber las interfaces que participan se empleará **show ip ospf interfaces**. Con **show ip ospf neighbors** se listarán todos aquellos routers que son vecinos del router desde donde se ejecuta el comando. El último comando, **show ip ospf database** muestra información sobre el contenido de la base de datos de encaminamiento OSPF de un router, estos datos son los que utilizan los routers de la red para calibrar si una ruta es mejor que otra. Si lo que se quiere es borrar registros de la tabla de enrutamiento se emplea el comando **clear**:

- **clear ip route**
- **clear ip route n.n.n.n**

Con la primera línea de órdenes, se eliminan todas las entradas de la tabla de enrutamiento y con la segunda, se despeja solamente la dirección especificada por n.n.n.n.

Autoevaluación

Se configuran dos routers dentro de un área OSPF única. ¿Cuáles de los siguientes componentes deben configurarse en ambos routers para lograr esto?

- El mismo ID de proceso.
- El mismo ID de área.
- No se pueden tener dos routers en la misma área OSPF.
- El mismo ID del router.

ID del router OSPF.

La **identificación de los routers** en las redes con configuración OSPF es muy importante porque cada uno de ellos intercambia información con todos los demás.
Los enrutadores deben tener la capacidad de distinguirse o de identificarse de manera única, lo consiguen con ID.
Cuando dos routers tienen el mismo ID es posible que el enrutamiento no funcione como debe y que el proceso OSPF no se lleve a cabo en esa área, en estos casos suele aparecer un mensaje de error como el siguiente:

```
%OSPF-4DUP_RTRID1: Detección de router con id duplicadas
```

El ID del router se utiliza para identificar de manera única al router en el área OSPF, este ID se puede establecer de tres maneras:

a. IP configurada con el comando router-id.
b. Dirección más alta de cualquiera de la interfaces loopback.
c. IP activa más alta de cualquiera de sus interfaces físicas.

La configuración de la dirección con router-id se hace de la manera siguiente:

```
PAR06(config)#router ospf 1
PAR06(config-router)#router-id 192.168.1.254
```

La dirección de loopback es una interfaz virtual que se encuentra en estado up de manera predeterminada cuando se configura. Un ejemplo de configuración de loopback es el siguiente.

```
PAR06(config)#interface loopback 0
PAR06(config-if)#ip address 192.168.1.233 255.255.255.255
```

En la configuración la máscara debe ser 255.255.255.255, se denomina una máscara de host, porque la máscara de subred especifica la red de un host. Cuando se solicita que OSPF publique una red loopback, OSPF siempre publica el loopback como una ruta de host con una máscara de 32 bits.

La dirección de loopback en OSPF asegura que el protocolo funcione siempre, si no tenemos configurada una interfaz de loopback puede ocurrir que el router no comience nunca a ejecutar OSPF, la función de la dirección de loopback es asegurar la estabilidad de OSPF.

Si no se tiene configurada una dirección con el comando router-id y tampoco hay una dirección de loopback, el router intentará coger como identificación la IP activa más alta de cualquiera de las interfaces y esto pueden desembocar en problemas de duplicidad, lo más rentable es tener siempre una interfaz de loopback definida.