
Cisco | Networking Academy®
Mind Wide Open™
CCNA Exploration 4.0
Conceptos y protocolos de enrutamiento
Tour del curso
Introducción al curso
Iniciar curso

# CAPITULO I – "INTRODUCCION AL ENRRUTAMIENTO Y ENVIO DE PAQUETES"

## 1.0 INTRODUCCION DEL CAPITULO.-

### 1.0.1 INTRODUCCION DEL CAPITULO.-

Las redes de la actualidad tienen un impacto significativo en nuestras vidas, ya que cambian nuestra forma de vivir, trabajar y divertirnos. Las redes de computadoras (y en un contexto más amplio, Internet) permiten a las personas comunicarse, colaborar e interactuar de maneras totalmente novedosas. Utilizamos la red de distintas formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.

En el centro de la red se encuentra el router. En pocas palabras, un router conecta una red con otra red. Por lo tanto, el router es responsable de la entrega de paquetes a través de diferentes redes. El destino de un paquete IP puede ser un servidor Web en otro país o un servidor de correo electrónico en la red de área local. Es responsabilidad de los routers entregar esos paquetes a su debido tiempo. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers de enviar paquetes de la manera más eficiente posible.

En la actualidad, se están incorporando routers a los satélites en el espacio. Estos routers tendrán la capacidad de enrutar el tráfico IP entre los satélites del espacio de un modo muy similar al que se transportan los paquetes en la Tierra, reduciendo así los retardos y ofreciendo una mayor flexibilidad para el trabajo en red.

Además del envío de paquetes, un router también proporciona otros servicios. Para satisfacer las demandas de las redes actuales, los routers también se utilizan para lo siguiente:
Aseguran la disponibilidad las 24 horas del día, los 7 días de la semana. Para ayudar a garantizar la posibilidad de conexión de la red, los routers usan rutas alternativas en caso de que la ruta principal falle.
Proveen servicios integrados de datos, video y voz en redes conectadas por cable o inalámbricas. Los routers dan prioridad a los paquetes IP según la calidad de servicio (QoS) a fin de asegurar que el tráfico en tiempo real, como la voz, el video y los datos esenciales, no se descarten ni retarden.
Disminuye el impacto de gusanos, virus y otros ataques en la red al permitir o denegar el reenvío de paquetes.

Todos estos servicios se construyen en torno del router y de su responsabilidad principal de reenviar paquetes de una red a la siguiente. La comunicación entre los dispositivos de diferentes redes sólo se logra gracias a la capacidad del router de enrutar paquetes entre las redes. Este capítulo será una introducción al router, su función en las redes, sus principales componentes de hardware y software y el proceso de enrutamiento en sí.

1841 Enrutador de servicios integrados

**En este capítulo, aprenderá a:**

- Identificar un router como una computadora con un sistema operativo (SO) y un hardware diseñado para el proceso de enrutamiento.
- Demostrar la capacidad para configurar dispositivos y aplicar direcciones.
- Describir la estructura de una tabla de enrutamiento.
- Describir de qué manera un router determina una ruta y conmuta paquetes.

## 1.1 DEL ROUTER.-

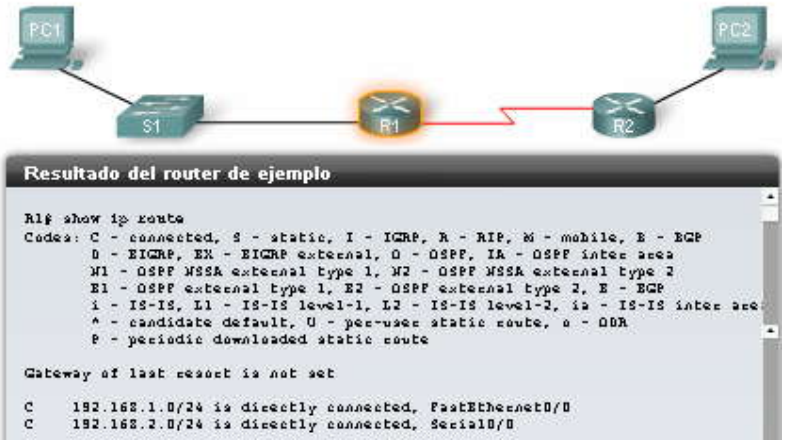
### 1.1.1 LOS ROUTERS SO COMPUTADORAS.-

**Los routers son computadoras**

Un router es una computadora, al igual que cualquier otra computadora; incluso una PC. El primer router, utilizado para la Red de la Agencia de Proyectos de Investigación Avanzada (ARPANET), fue el Procesador de mensajes de interfaz (IMP). El IMP era una minicomputadora Honeywell 316; esta computadora dio origen a la ARPANET el 30 de agosto de 1969.

**Nota:** La ARPANET fue desarrollada por la Agencia de Proyectos de Investigación Avanzada (ARPA) del Departamento de Defensa de los Estados Unidos. También fue la primera red operativa de conmutación de paquetes del mundo y la antecesora de la Internet de la actualidad.

Los routers tienen muchos de los mismos componentes de hardware y software que se encuentran en otras computadoras, entre ellos:
CPU
RAM
ROM
Sistema operativo




**Los routers se encuentran en el centro de la red**

Es posible que los usuarios comunes no estén al tanto de la presencia de numerosos routers en su propia red o en Internet. Los usuarios esperan poder acceder a las páginas Web, enviar mensajes de correo electrónico y descargar música, ya sea si el servidor al que están accediendo está en su propia red o en otra red del otro lado del mundo. Sin embargo, los profesionales de networking saben que el router es el responsable del envío de paquetes de red a red, desde el origen inicial al destino final.

Un router conecta múltiples redes. Esto significa que tiene varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz usar para enviar el paquete hacia su destino. La interfaz que usa el router para enviar el paquete puede ser la red del destino final del paquete (la red con la dirección IP de destino de este paquete), o puede ser una red conectada a otro router que se usa para alcanzar la red de destino.

Generalmente, cada red a la que se conecta un router requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de Redes de área local (LAN) y Redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como PC, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa. Por ejemplo, una conexión WAN comúnmente se usa para conectar una LAN a la red del Proveedor de servicios de Internet (ISP).

En la figura, vemos que los routers R1 y R2 son responsables de recibir el paquete en una red y enviar el paquete desde otra red hacia la red de destino.

**Los routers determinan la mejor ruta**

La principal responsabilidad de un router es dirigir los paquetes destinados a redes locales y remotas al:
Determinar la mejor ruta para enviar paquetes
Enviar paquetes hacia su destino

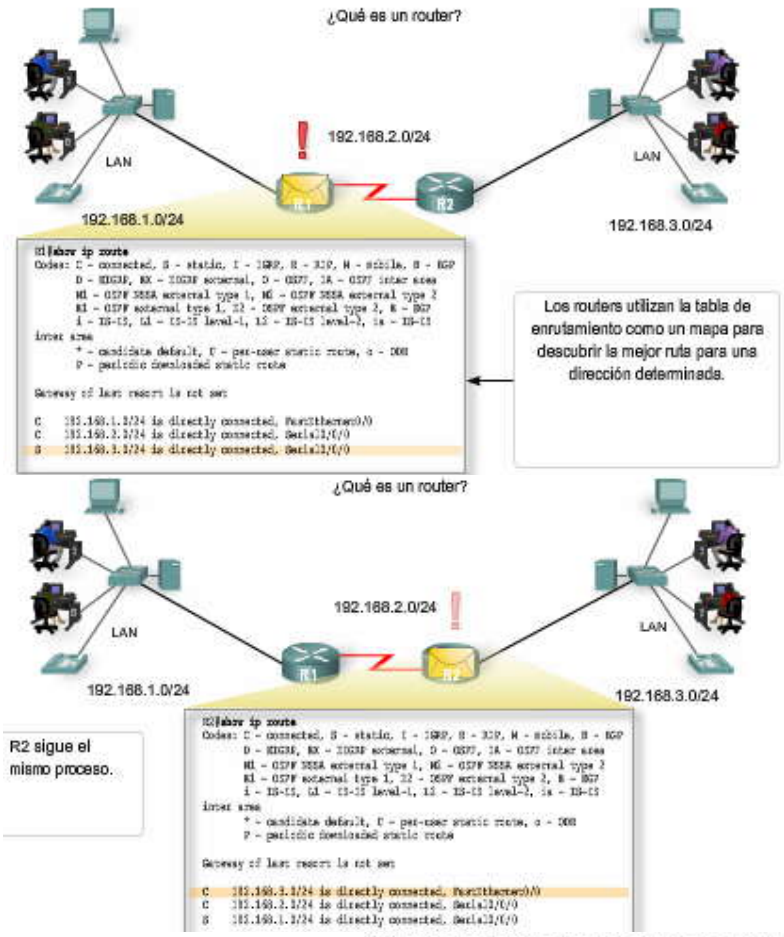
El router usa su tabla de enrutamiento para determinar la mejor ruta para reenviar el paquete. Cuando el router recibe un paquete, examina su dirección IP de destino y busca la mejor coincidencia con una dirección de red en la tabla de enrutamiento del router. La tabla de enrutamiento también incluye la interfaz que se utilizará para enviar el paquete. Cuando se encuentra una coincidencia, el router encapsula el paquete IP en la trama de enlace de datos de la interfaz de salida. Luego, el paquete se envía hacia su destino.

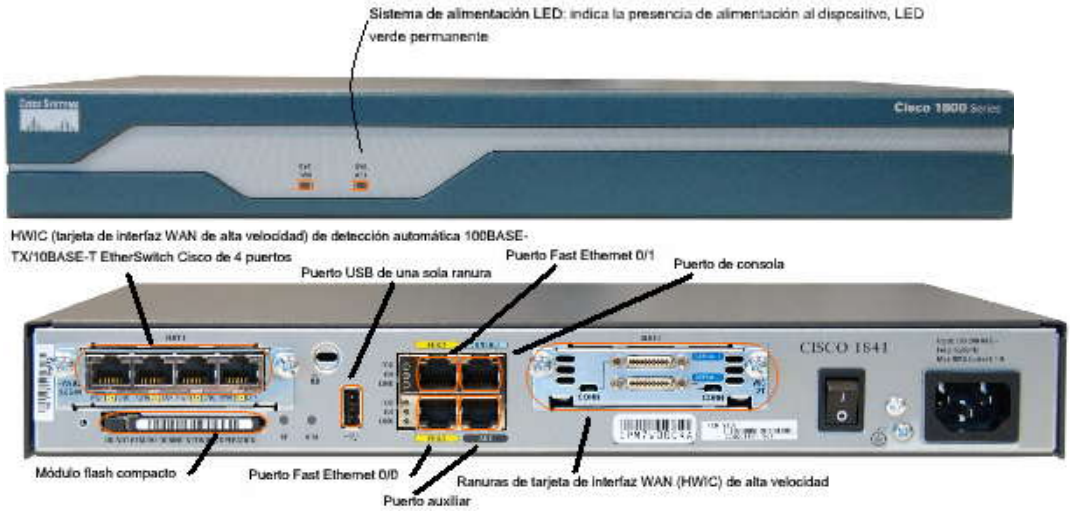
Es muy probable que un router reciba un paquete encapsulado en un tipo de trama de enlace de datos, como una trama de Ethernet, y al enviar el paquete, el router lo encapsulará en otro tipo de trama de enlace de datos, como el Point-to-Point Protocol (PPP). La encapsulación de enlace de datos depende del tipo de interfaz del router y del tipo de medio al que se conecta. Las diferentes tecnologías de enlace de datos a las que se conecta un router pueden incluir tecnologías LAN, como Ethernet, y conexiones seriales WAN, como la conexión T1 que usa PPP, Frame Relay y Modo de transferencia asíncrona (ATM).

En la figura, podemos seguir un paquete desde la PC de origen hasta la PC de destino. Debe observarse que el router es responsable de encontrar la red de destino en su tabla de enrutamiento y enviar el paquete hacia su destino. En este ejemplo, el router R1 recibe el paquete encapsulado en una trama de Ethernet. Después de desencapsular el paquete, R1 usa la dirección IP de destino del paquete para buscar una dirección de red coincidente en su tabla de enrutamiento. Luego de

encontrar una dirección de red de destino en la tabla de enrutamiento, R1 encapsula el paquete dentro de una trama PPP y envía el paquete a R2. R2 realiza un proceso similar.

Los routers usan protocolos de rutas estáticas y de enrutamiento dinámico para aprender sobre redes remotas y construir sus tablas de enrutamiento. Estas rutas y protocolos representan el enfoque principal del curso y se analizarán en detalle en los siguientes capítulos junto con el proceso que usan los routers al buscar en sus tablas de enrutamiento y al enviar los paquetes.

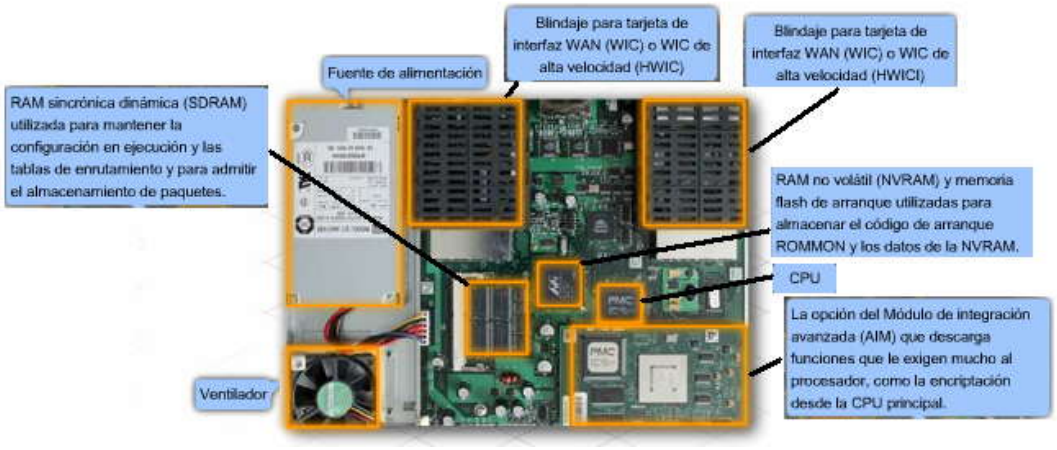



### 1.1.2 MEMORIA Y CPU DEL ROUTER.-

Aunque existen diferentes tipos y modelos de routers, todos tienen los mismos componentes de hardware generales. Según el modelo, esos componentes se encuentran en diferentes lugares dentro del router. La figura muestra el interior de un

router 1841. Para observar los componentes internos del router, es necesario desatornillar la cubierta metálica y retirarla del router. **Normalmente no es necesario abrir el router, a menos que se esté actualizando la memoria.**




**Componentes del router y sus funciones**

Al igual que una PC, un router también incluye:
Unidad de procesamiento central (CPU)
Memoria de acceso aleatorio (RAM)
Memoria de sólo lectura (ROM)

**Coloque el cursor del mouse sobre los componentes en la figura para ver una breve descripción de cada uno.**

**CPU**

La CPU ejecuta las instrucciones del sistema operativo, como el inicio del sistema, y las funciones de enrutamiento y conmutación.

**RAM**

La RAM almacena las instrucciones y los datos necesarios que la CPU debe ejecutar. La RAM se usa para almacenar estos componentes:
**Sistema operativo:** El IOS (sistema operativo Internetwork) de Cisco se copia en la RAM durante el inicio.
Archivo de configuración en ejecución: Éste es el archivo de configuración que almacena los comandos de configuración que el IOS del router utiliza actualmente. Salvo algunas excepciones, todos los comandos configurados en el router se almacenan en el archivo de configuración en ejecución, conocido como running-config.
**Tabla de enrutamiento IP:** Este archivo almacena información sobre redes remotas y conectadas directamente. Se usa para determinar la mejor ruta para enviar el paquete.
**Caché ARP:** Esta caché contiene la dirección IPv4 para la asignación de direcciones MAC, de modo similar a la caché ARP en una PC. La caché ARP se usa en routers que tienen interfaces LAN como las interfaces Ethernet.
**Búfer del paquete:** Los paquetes se almacenan temporalmente en un búfer cuando se reciben en una interfaz o antes de abandonar la interfaz.

La RAM es una memoria volátil y pierde su contenido cuando el router se apaga o reinicia. Sin embargo, el router también contiene áreas de almacenamiento permanente, como la ROM, la flash y la NVRAM.

**ROM**

La ROM es una forma de almacenamiento permanente. Los dispositivos Cisco usan la memoria ROM para almacenar:
Instrucciones de bootstrap
Software básico de diagnóstico
Versión más básica del IOS

La ROM usa firmware, un software incorporado dentro del circuito integrado. El firmware incluye el software que normalmente no necesita modificarse ni actualizarse, como las instrucciones de inicio. Muchas de estas funciones, incluso el software del monitor de la ROM, se analizarán en otro curso. La ROM no pierde sus contenidos cuando se apaga o reinicia el router.

**Memoria flash**

La memoria flash es una memoria de computadora no volátil que puede borrarse y almacenarse eléctricamente. La memoria flash se usa como almacenamiento permanente para el sistema operativo, IOS de Cisco. En la mayoría de los routers Cisco, el IOS se almacena en forma permanente en la memoria flash y se copia en la RAM durante el proceso de arranque, donde entonces es ejecutado por la CPU. Algunos modelos anteriores de routers Cisco ejecutan el IOS directamente desde la memoria flash. La memoria flash está compuesta de tarjetas SIMM o PCMCIA, que pueden actualizarse para aumentar la cantidad de memoria flash.

Esta memoria no pierde sus contenidos cuando se apaga o reinicia el router.

**NVRAM**

La NVRAM (RAM no volátil) no pierde su información cuando se desconecta la alimentación eléctrica. Esto se opone a las formas más comunes de RAM, como la DRAM, que requiere alimentación eléctrica continua para mantener su información. El IOS de Cisco usa la NVRAM como almacenamiento permanente para el archivo de configuración de inicio (startup-config). Todos los cambios de configuración se almacenan en el archivo running-config en la RAM, y salvo pocas excepciones, son implementados inmediatamente por el IOS. Para guardar esos cambios en caso de que se apague o reinicie el router, el running-config debe estar copiado en la NVRAM, donde se almacena como el archivo startup-config. La NVRAM retiene sus contenidos incluso cuando el router se recarga o apaga.

Las memorias ROM, RAM, NVRAM y flash se analizan en la siguiente sección que introduce el IOS y el proceso de arranque. También se analizan con más profundidad en otro curso relacionado con la administración del IOS.

Para un profesional de networking es más importante comprender la función de los principales componentes internos de un router que la ubicación exacta de esos componentes dentro de un router específico. La arquitectura física interna variará de un modelo a otro.

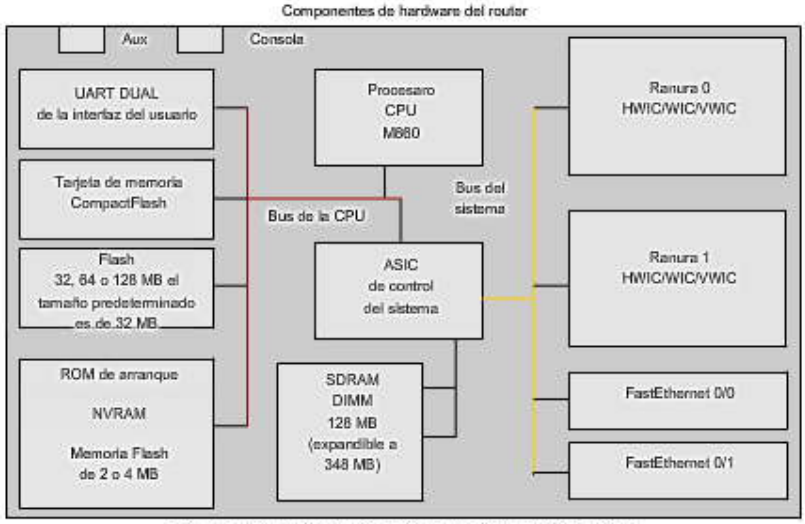


Diagrama lógico de los componentes internos de un router Cisco 1841
Desplácese sobre los componentes para ver una descripción breve.

### 1.1.3 SISTEMA OPERATIVO INTERNETWORK.-

**Sistema Operativo Internetwork**

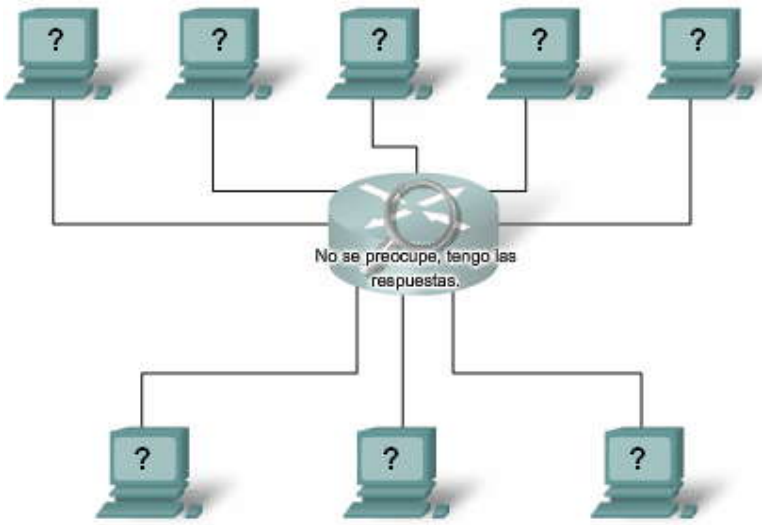
El software del sistema operativo que se usa en los routers Cisco se conoce como Sistema Operativo Internetwork (IOS) de Cisco. Como cualquier sistema operativo de una computadora, el IOS de Cisco administra los recursos de hardware y software del router, incluso la asignación de memoria, los procesos, la seguridad y los sistemas de archivos. El IOS de Cisco es un sistema operativo multitarea que está integrado con las funciones de enrutamiento, conmutación, internetworking y telecomunicaciones.

Aunque el IOS de Cisco puede parecer igual en muchos routers, existen muchas imágenes diferentes de IOS. Una imagen de IOS es un archivo que contiene el IOS completo para ese router. Cisco crea muchos tipos diferentes de imágenes IOS, según el modelo del router y las funciones dentro del IOS. Generalmente, mientras más funciones haya en el IOS, más grande será la imagen IOS; y por lo tanto, más memoria flash y RAM se necesitarán para almacenar y guardar el IOS. Por ejemplo, algunas funciones incluyen la posibilidad de ejecutar IPv6 o la posibilidad del router de realizar NAT (Traducción de direcciones de red).

Como ocurre con otros sistemas operativos, el IOS de Cisco tiene su propia interfaz de usuario. Aunque algunos routers proveen una interfaz gráfica de usuario (GUI), la interfaz de línea de comandos (CLI) es un método mucho más común para configurar los routers Cisco. La CLI se usa a lo largo de este programa de estudio.

En el inicio, el archivo startup-config de la NVRAM se copia en la RAM y se almacena como el archivo running-config. El IOS ejecuta los comandos de configuración en el running-config. Todo cambio ingresado por el administrador de red se almacena en el running-config y es ejecutado inmediatamente por el IOS. En este capítulo, repasaremos algunos de los comandos IOS básicos que se usan para configurar un router Cisco. En capítulos posteriores, aprenderemos los comandos que se usan para configurar, verificar y resolver problemas de enrutamiento estático y distintos protocolos de enrutamiento como RIP, EIGRP y OSPF.

**Nota:** El IOS de Cisco y el proceso de arranque se analizarán con más profundidad en otro curso.




### 1.1.4 PROCESO DE ARRABQUE DEL ROUTER.-

**Proceso de arranque**

El proceso de arranque está conformado por cuatro etapas principales:

1. Ejecución de la POST

2. Carga del programa bootstrap

3. Ubicación y carga del software IOS de Cisco

4. Ubicación y carga del archivo de configuración de inicio o ingreso al modo Setup

**1. Ejecución de la POST**

La prueba de autocomprobación de encendido (POST) es un proceso común que ocurre en casi todas las computadoras durante el arranque. El proceso de POST se utiliza para probar el hardware del router. Cuando se enciende el router, el software en el chip de la ROM ejecuta el POST. Durante esta autocomprobación, el router ejecuta diagnósticos desde la ROM a varios componentes de hardware, entre ellos la CPU, la RAM y la NVRAM. Después de completarse la POST, el router ejecuta el programa bootstrap.

**2. Carga del programa bootstrap**

Después de la POST, el programa bootstrap se copia de la ROM a la RAM. Una vez en la RAM, la CPU ejecuta las instrucciones del programa bootstrap. La tarea principal del programa bootstrap es ubicar al IOS de Cisco y cargarlo en la RAM.

**Nota:** En este momento, si existe una conexión de consola al router, comenzarán a aparecer los resultados en la pantalla.

**3. Ubicación y carga del IOS de Cisco**

**Ubicación del software IOS de Cisco.** El IOS normalmente se almacena en la memoria flash, pero también puede almacenarse en otros lugares como un servidor TFTP (Trivial File Transfer Protocol).

Si no se puede encontrar una imagen IOS completa, se copia una versión más básica del IOS de la ROM a la RAM. Esta versión del IOS se usa para ayudar a diagnosticar cualquier problema y puede usarse para cargar una versión completa del IOS en la RAM.

**Nota:** Un servidor TFTP generalmente se usa como servidor de respaldo para el IOS, pero también puede usarse como punto central para almacenar y cargar el IOS. La administración del IOS y el uso del servidor TFTP se analizará en otro curso.

**Carga del IOS.** Algunos de los routers Cisco más antiguos ejecutan el IOS directamente desde la memoria flash, pero los modelos actuales copian el IOS en la RAM para que la CPU lo ejecute.

Nota:Una vez que el IOS empieza a cargarse, puede verse una secuencia de signos numerales (#), como se muestra en la figura, mientras la imagen se descomprime.

**4. Ubicación y carga del archivo de configuración**

**Ubicación del archivo de configuración de inicio.** Después de cargar el IOS, el programa bootstrap busca en la NVRAM el archivo de configuración de inicio, conocido como startup-config. El archivo contiene los parámetros y comandos de configuración previamente guardados, entre ellos:
direcciones de interfaz
información de enrutamiento
contraseñas
cualquier otra configuración guardada por el administrador de red

Si el archivo de configuración de inicio, startup-config, se encuentra en la NVRAM, se copia en la RAM como el archivo de configuración en ejecución, running-config.

**Nota:** Si el archivo de configuración de inicio no existe en la NVRAM, el router puede buscar un servidor TFTP. Si el router detecta que tiene un enlace activo a otro router configurado, envía un broadcast en busca de un archivo de configuración a través del enlace activo. Esta situación hará que el router haga una pausa, pero finalmente se verá un mensaje de consola como el siguiente:

<El router se detiene aquí mientras envía un broadcast para un archivo de configuración a través del enlace activo>

%Error opening tftp://255.255.255.255/network-confg (Timed out)
%Error opening tftp://255.255.255.255/cisconet.cfg (Timed out)

**Ejecución del archivo de configuración.** Si se encuentra un archivo de configuración de inicio en la NVRAM, el IOS lo carga en la RAM como el running-config y ejecuta los comandos del archivo, de a una línea por vez. El archivo running-config contiene direcciones de interfaz, inicia los procesos de enrutamiento, configura las contraseñas del router y define otras características del router.

**Ingreso al modo Setup (opcional):** Si no puede localizarse el archivo de configuración de inicio, el router indica al usuario que ingrese en el modo Setup. El modo Setup consiste en una serie de preguntas que solicitan al usuario información de configuración básica. El modo Setup no tiene como fin utilizarse para ingresar a configuraciones complejas del router y los administradores de red normalmente no lo usan.

Cuando se inicia un router que no contiene un archivo de configuración de inicio, aparecerá la siguiente pregunta luego de la carga del IOS:

Would you like to enter the initial configuration dialog? [yes/no]: no

El modo Setup no se utilizará en este curso para configurar el router. Ante la petición de entrada del modo Setup, siempre se debe responder no. Si el usuario responde yes (sí) e ingresa al modo Setup, puede presionar Ctrl-C en cualquier momento para finalizar el proceso de configuración.

Cuando no se usa el modo Setup, el IOS crea un running-config predeterminado. El running-config predeterminado es un archivo de configuración básica que incluye las interfaces del router, las interfaces de administración y cierta información predeterminada. El running-config predeterminado no contiene ninguna dirección de interfaz, información de enrutamiento, contraseñas ni otra información de configuración específica.

**Interfaz de línea de comandos**

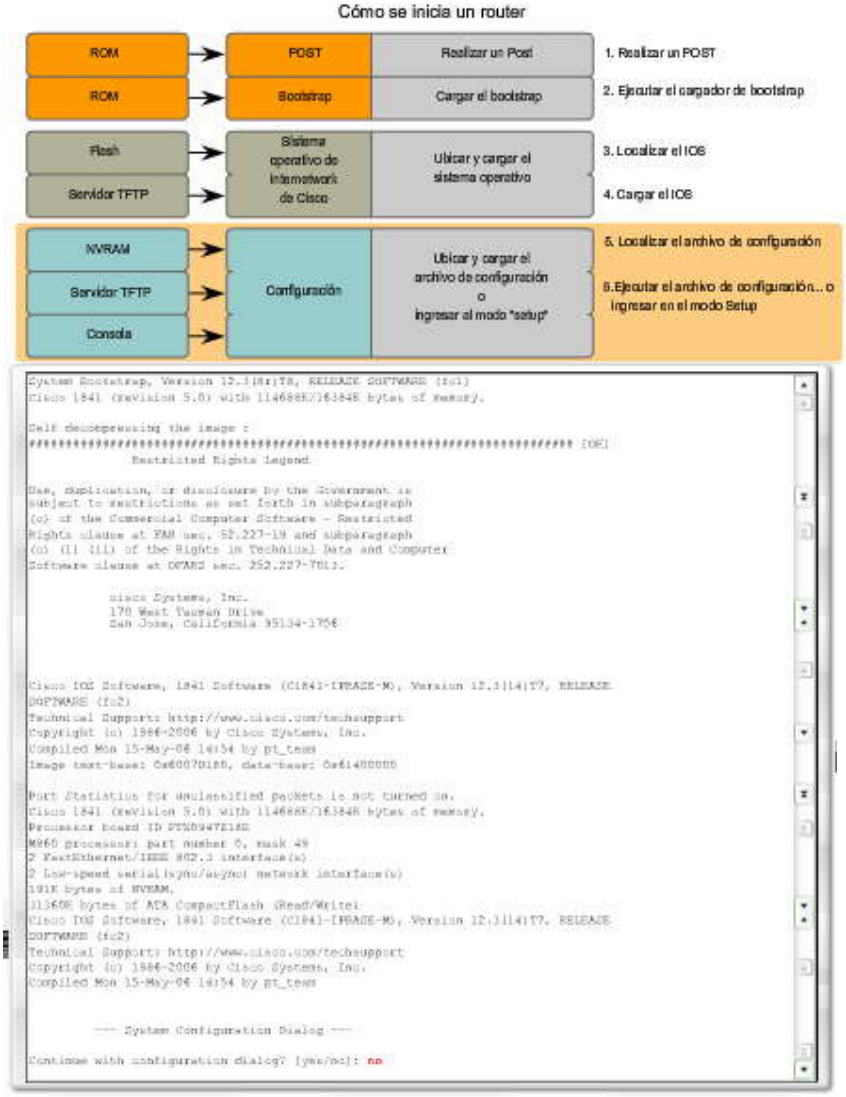
Según la plataforma y el IOS, el router puede realizar la siguiente pregunta antes de mostrar la petición de entrada:

Would you like to terminate autoinstall? [yes]: <Enter>
Press the Enter key to accept the default answer.
Router>

**Nota:** Si se encontró un archivo de configuración de inicio, el running-config puede contener un nombre de host y la petición de entrada mostrará el nombre de host del router.

Una vez que se muestra la petición de entrada, el router ya está ejecutando el IOS con el archivo de configuración actual en ejecución. El administrador de red ahora puede comenzar a usar los comandos del IOS en este ro uter.

**Nota:** El proceso de arranque se analizará con más profundidad en otro curso.




**Verificación del proceso de arranque del router**

El comando **show version** puede usarse para ayudar a verificar y resolver problemas con algunos de los componentes básicos de hardware y software del router. El comando **show version** muestra información sobre la versión del software IOS de Cisco que actualmente se está ejecutando en el router, la versión del programa de bootstrap e información sobre la configuración del hardware, incluso la cantidad de memoria del sistema.

El resultado del comando **show version** incluye:

**Versión IOS**

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)

Ésta es la versión del software IOS de Cisco en la RAM que está usando el router.

**Programa bootstrap de la ROM**

ROM: System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)

Se muestra la versión del software del sistema bootstrap almacenado en la memoria ROM, que se usó en un principio para iniciar el router.

**Ubicación del IOS**

System image file is "flash:c2600-i-mz.122-28.bin"

Se muestra dónde se encuentra el programa bootstrap y dónde está cargado en el IOS de Cisco, además del nombre de archivo completo de la imagen IOS.

**CPU y cantidad de RAM**

cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory

La primera parte de esta línea muestra el tipo de CPU en este router. La última parte de esta línea muestra la cantidad de DRAM. Algunas series de routers, como el 2600, usan una parte de la DRAM como memoria de paquete. La memoria de paquete se usa para paquetes de búfering.

Para determinar la cantidad total de DRAM en el router, sume ambos números. En este ejemplo, el router Cisco 2621 tiene 60 416 KB (kilobytes) de DRAM libre utilizada para almacenar temporalmente el IOS de Cisco y otros procesos del sistema. Los otros 5 120 KB se reservan para la memoria de paquete. La suma de estos números es 65 536 K, o 64 megabytes (MB) de DRAM total.

**Nota:** Posiblemente sea necesario actualizar la cantidad de RAM cuando se actualiza el IOS.

**Interfaces**

2 FastEthernet/IEEE 802.3 interface(s)
2 Low-speed serial(sync/async) network interface(s)

Esta sección del resultado muestra las interfaces físicas en el router. En este ejemplo, el router Cisco 2621 tiene dos interfaces FastEthernet y dos interfaces seriales de baja velocidad.

**Cantidad de NVRAM**

32K bytes of non-volatile configuration memory.

Ésa es la cantidad de NVRAM en el router. La NVRAM se usa para guardar el archivo startup-config.

**Cantidad de memoria flash**

6384K bytes of processor board System flash (Read/Write)

Ésa es la cantidad de memoria flash en el router. La memoria flash se usa para guardar el IOS de Cisco en forma permanente.

**Nota:** Posiblemente sea necesario actualizar la cantidad de memoria flash cuando se actualiza el IOS.

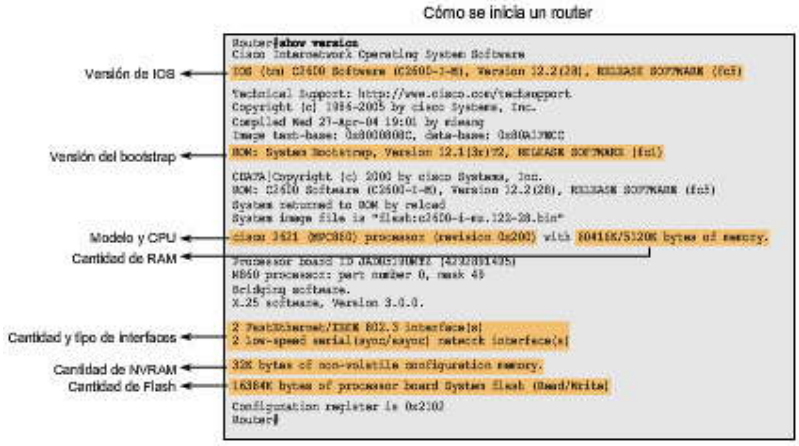
**Registro de configuración**

Configuration register is 0x2102

La última línea del comando **show version** muestra el valor configurado actual del registro de configuración del software en hexadecimales. Si se muestra un segundo valor entre paréntesis, denota el valor del registro de configuración que se usará durante la próxima recarga.

El registro de configuración tiene varios usos, entre ellos la recuperación de contraseña. La configuración predeterminada de fábrica para el registro de configuración es 0x2102. Este valor indica que el router intentará cargar una imagen del software IOS de Cisco desde la memoria flash y cargar el archivo de configuración de inicio desde la NVRAM.

**Nota:** El registro de configuración se analizará con más profundidad en otro curso.




### 1.1.5 INTERFACES DEL ROUTER.-

**Puertos de administración**

Los routers tienen conectores físicos que se usan para administrar el router. Estos conectores se conocen como puertos de administración. A diferencia de las interfaces seriales y Ethernet, los puertos de administración no se usan para el envío de paquetes. El puerto de administración más común es el puerto de consola. El puerto de consola se usa para conectar una terminal, o con más frecuencia una PC que ejecuta un software emulador de terminal, para configurar el router sin la necesidad de acceso a la red para ese router. El puerto de consola debe usarse durante la configuración inicial del router.

Otro puerto de administración es el puerto auxiliar. No todos los routers cuentan con un puerto auxiliar. A veces el puerto auxiliar puede usarse de maneras similares al puerto de consola. También puede usarse para conectar un módem. No se usarán puertos auxiliares en este curso de estudio.

La figura muestra los puertos AUX (auxiliares) y de consola en el router.

**Interfaces del router**

El término interfaz en los routers Cisco se refiere a un conector físico en el router cuyo principal propósito es recibir y enviar paquetes. Los routers tienen muchas interfaces que se usan para conectarse a múltiples redes. Normalmente, las interfaces se conectan a distintos tipos de redes, lo cual significa que se necesitan distintos tipos de medios y conectores. Con frecuencia, un router necesitará tener distintos tipos de interfaces. Por ejemplo, un router generalmente tiene interfaces FastEthernet para conexiones a diferentes LAN y distintos tipos de interfaces WAN para conectar una variedad de enlaces seriales, entre ellos T1, DSL e ISDN. La figura muestra las interfaces seriales y FastEthernet en el router.

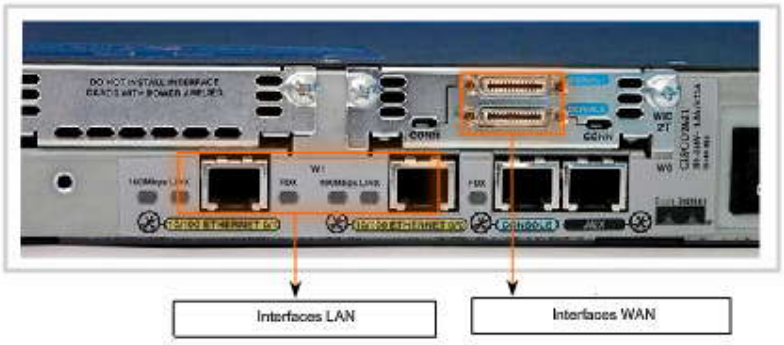
Al igual que las interfaces en una PC, los puertos y las interfaces en un router se encuentran ubicados fuera del router. Su ubicación externa permite la cómoda conexión a los cables y conectores adecuados de la red.

**Nota:** Puede usarse una interfaz única en un router para conectarse a múltiples redes; sin embargo, esto escapa al ámbito de este programa de estudio y se analizará en otro curso.

Al igual que la mayoría de los dispositivos de red, los routers Cisco usan indicadores LED para proveer información de estado. Un LED de interfaz indica la actividad de la interfaz correspondiente. Si un LED está apagado cuando la interfaz está activa y la interfaz está conectada correctamente, puede ser señal de un problema en la interfaz. Si la interfaz está en gran actividad, el LED estará continuamente encendido. Según el tipo de router, puede haber también otros LED. Para obtener más información sobre visualizaciones de LED en el 1841, consulte el siguiente enlace.

Interfaces del router: Representación física

Cada interfaz individual se conecta a una red diferente. Por lo tanto, cada interfaz tiene una máscara/dirección IP de dicha red.




**Las interfaces pertenecen a diferentes redes**

Como se muestra en la figura, cada interfaz en un router es miembro o host en una red IP diferente. Cada interfaz se debe configurar con una dirección IP y una máscara de subred de una red diferente. El IOS de Cisco no permitirá que dos interfaces activas en el mismo router pertenezcan a la misma red.

Las interfaces de router pueden dividirse en dos grupos principales:
**Interfaces LAN,** como Ethernet y FastEthernet
**Interfaces WAN,** como serial, ISDN y Frame Relay

**Interfaces LAN**

Como su nombre lo indica, las interfaces LAN se utilizan para conectar el router a la LAN, así como una NIC Ethernet de la PC se utiliza para conectar la PC a la LAN Ethernet. Del mismo modo que la NIC Ethernet de la PC, la interfaz Ethernet del router también tiene una dirección MAC de Capa 2 y forma parte de la LAN Ethernet al igual que cualquier otro host en esa LAN. Por ejemplo, la interfaz Ethernet del router participa en el proceso ARP para esa LAN. El router mantiene un caché ARP para esa interfaz, envía solicitudes de ARP cuando es necesario y produce respuestas ARP cuando se requieren.

La interfaz Ethernet del router normalmente usa un jack RJ-45 que admite un cableado de par trenzado no blindado (UTP). Cuando un router se conecta a un switch, se usa un cable de conexión directa. Cuando se conectan dos routers directamente a través de las interfaces Ethernet, o cuando una NIC de PC se conecta directamente a una interfaz Ethernet del router, se usa un cable cruzado.

Use la actividad del Packet Tracer al final de esta sección para evaluar sus habilidades de cableado.

**Interfaces WAN**

Las interfaces WAN se usan para conectar los routers a redes externas, generalmente a través de distancias geográficas más extensas. La encapsulación de Capa 2 puede ser de diferentes tipos, como PPP, Frame Relay y HDLC (Control de enlace de datos de alto nivel). Al igual que las interfaces LAN, cada interfaz WAN tiene su propia dirección IP y máscara de subred, que la identifica como miembro de una red específica.

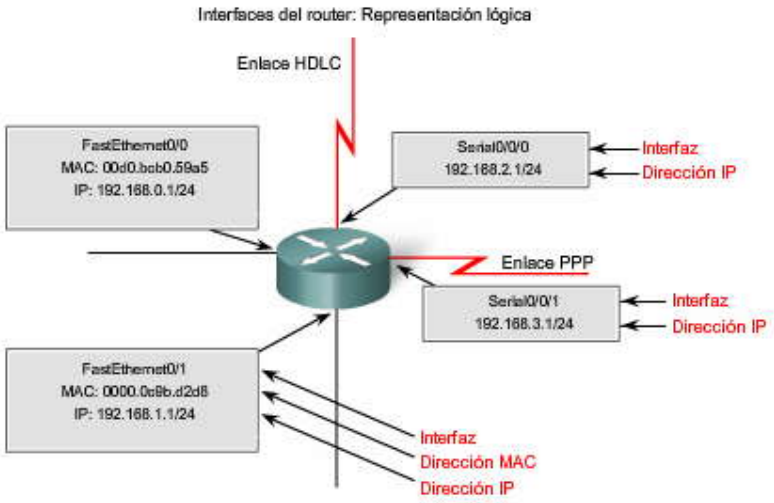
**Nota:** Las direcciones MAC se usan en interfaces LAN, como Ethernet, y no se usan en interfaces WAN. Sin embargo, las interfaces WAN usan sus propias direcciones de Capa 2 dependiendo de la tecnología. Las direcciones y los tipos de encapsulación WAN de Capa 2 se analizarán en otro curso.

**Interfaces del router**

El router en la figura tiene cuatro interfaces. Cada interfaz tiene una dirección IP de Capa 3 y una máscara de subred que la configura para una red diferente. Las interfaces Ethernet también tienen direcciones MAC Ethernet de Capa 2.

Las interfaces WAN usan encapsulaciones de Capa 2 diferentes. La Serial 0/0/0 usa HDLC y la Serial 0/0/1 usa PPP. Estos dos protocolos seriales punto a punto usan direcciones de broadcast para la dirección de destino de Capa 2 cuando encapsulan el paquete IP en una trama de enlace de datos.

En el entorno del laboratorio, existen restricciones respecto de cuántas interfaces LAN y WAN pueden usarse para configurar actividades prácticas de laboratorio. Sin embargo, el Packet Tracer ofrece la flexibilidad de crear diseños de red más complejos.




### 1.1.6 ROUTERS Y CAPA DE RED.-

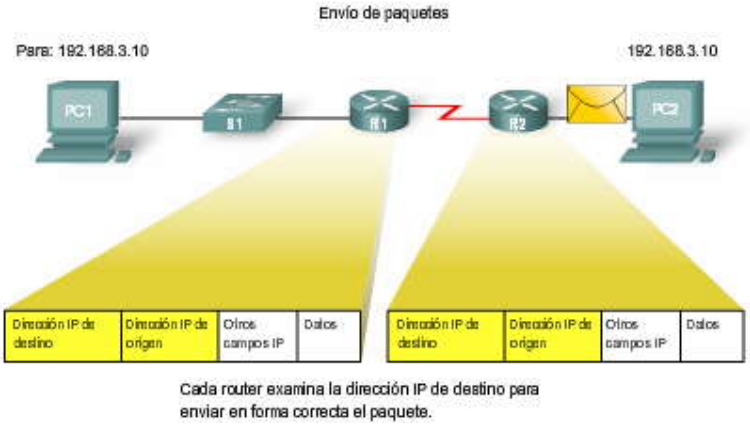
**Routers y capa de Red**

El objetivo principal de un router es conectar múltiples redes y enviar paquetes destinados ya sea a sus propias redes o a otras redes. Se considera al router como un dispositivo de Capa 3 porque su decisión principal de envío se basa en la información del paquete IP de Capa 3, específicamente la dirección IP de destino. Este proceso se conoce como enrutamiento.

Cuando un router recibe un paquete, examina su dirección IP de destino. Si la dirección IP de destino no pertenece a ninguna de las redes del router conectadas directamente, el router debe enviar este paquete a otro router. En la figura, R1 analiza la dirección IP de destino del paquete. Después de buscar en la tabla de enrutamiento,R1 envía el paquete a R2. Cuando R2 recibe el paquete, también analiza la dirección IP de destino del paquete. Luego de buscar en su tabla de enrutamiento, R2 envía el paquete desde su red Ethernet conectada directamente a la PC2.

Cuando cada router recibe un paquete, realiza una búsqueda en su tabla de enrutamiento para encontrar la mejor coincidencia entre la dirección IP de destino del paquete y una de las direcciones de red en la tabla de enrutamiento. Cuando se encuentra una coincidencia, el paquete se encapsula en la trama de enlace de datos de Capa 2 para esa interfaz de salida. El tipo de encapsulación de enlace de datos depende del tipo de interfaz, como por ejemplo Ethernet o HDLC.

Finalmente, el paquete llega a un router que forma parte de una red que coincide con la dirección IP de destino del paquete. En este ejemplo, el router R2 recibe el paquete de R1. R2 envía el paquete desde su interfaz Ethernet, que pertenece a la misma red que el dispositivo de destino, PC2.




**Los routers operan en las Capas 1, 2 y 3**

Un router toma su decisión principal de envío en la Capa 3, pero como mencionamos antes, también participa en procesos de Capa 1 y Capa 2. El router puede enviar un paquete desde la interfaz adecuada hacia su destino después de examinar la dirección IP de destino del paquete y consultar su tabla de enrutamiento para tomar su decisión de envío. El router

encapsula el paquete IP de Capa 3 en la porción de datos de una trama de enlace de datos de Capa 2 adecuada para la interfaz de salida. El tipo de trama puede ser una Ethernet, HDLC u otro tipo de encapsulación de Capa 2, cualquiera sea la encapsulación que se usa en esa interfaz específica. La trama de Capa 2 se codifica en señales físicas de Capa 1 que se usan para representar bits a través del enlace físico.

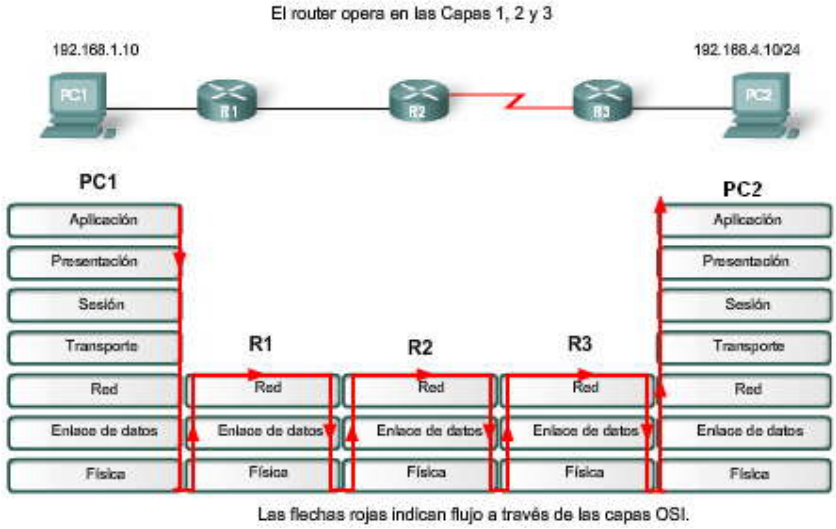
Consulte la figura para comprender mejor este proceso. Observe que la PC1 opera en las siete capas, encapsulando los datos y enviando la trama como un stream de bits codificados a R1, su gateway por defecto.

R1 recibe el stream de bits codificados en su interfaz. Los bits se decodifican y se pasan a la Capa 2, donde R1 desencapsula la trama. El router examina la dirección de destino de la trama de enlace de datos para determinar si coincide con la interfaz receptora, lo cual incluye una dirección de broadcast o multicast. Si hay una coincidencia con la porción de datos de la trama, el paquete IP pasa a la Capa 3, donde R1 toma su decisión de enrutamiento. R1 luego vuelve a encapsular el paquete en una nueva trama de enlace de datos de Capa 2 y lo envía desde la interfaz de salida como un stream de bits codificados.

R2 recibe el stream de bits y el proceso se repite. R2 desencapsula la trama y pasa la porción de datos de la trama, el paquete IP, a la Capa 3 donde R2 toma su decisión de enrutamiento. Luego, R2 vuelve a encapsular el paquete en una nueva trama de enlace de datos de Capa 2 y lo envía desde la interfaz de salida como un stream de bits codificados.

R3 repite este proceso una vez más y envía el paquete IP, encapsulado dentro de una trama de enlace de datos y codificado en forma de bits, a la PC2.

Cada router en la ruta desde el origen al destino realiza este mismo proceso de desencapsulación, búsqueda en la tabla de enrutamiento y nueva encapsulación. Este proceso es importante para comprender la manera en que los routers participan en las redes. Por lo tanto, retomaremos este análisis con mayor profundidad en una sección posterior.



Las flechas rojas indican flujo a través de las capas OSI.

## 1.2 CONFIGURACION Y DIRECCIONAMIENTO DEL CLI.-

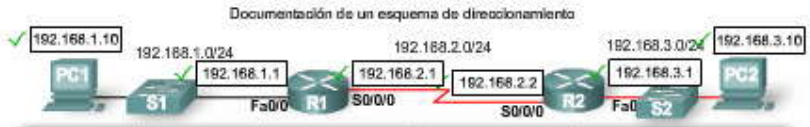
### 1.2.1 IMPLEMETACION DE ESQUEMAS DE DIRECCIONAMIENTO BÁSICOS.-

Cuando se diseña una nueva red o se hacen asignaciones en una red existente, es necesario documentar la red. Como mínimo, la documentación debe incluir un diagrama de topología que indique la conectividad física y una tabla de direccionamiento que mencione la siguiente información:
Nombres de dispositivos,
Interfaces usadas en el diseño,
Direcciones IP y máscaras de subred, y
Direcciones de gateway por defecto para dispositivos finales, como las PC.

Carga de la tabla de direcciones

La figura muestra una topología de la red con los dispositivos interconectados y configurados con direcciones IP. Bajo la topología se observa una tabla que se usa para documentar la red. La tabla está parcialmente completa con los datos que documentan la red (dispositivos, direcciones IP, máscaras de subred e interfaces).

El router R1 y la PC1 host ya están documentados. Termine de completar la tabla y los espacios en blanco del diagrama arrastrando hacia la ubicación correcta el pool de direcciones IP que aparece debajo de la tabla.




| | | | | |
|---|---|---|---|---|
| R1 | Fa0/0 | 192.168.1.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| R2 | Fa0/0 | 192.168.3.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 192.168.2.2 | 255.255.255.0 | N/A |
| PC1 | N/A | 192.168.1.10 | 255.255.255.0 | 192.168.1.1 |
| PC2 | N/A | 192.168.3.10 | 255.255.255.0 | 192.168.3.1 |

### 1.2.2 CONFIGURACION BÁSICA DEL ROUTER.-

**Configuración básica del router**

Cuando se configura un router, se realizan ciertas tareas básicas, tales como:
Asignar un nombre al router,
Configurar contraseñas,
Configurar interfaces,
Configurar un mensaje,
Guardar cambios en un router y
Verificar la configuración básica y las operaciones del router.

Aunque ya debe conocer estos comandos de configuración, haremos una breve revisión. Comenzamos el repaso suponiendo que el router no contiene un archivo startup-config actual.

La primera petición de entrada aparece en el modo usuario. El modo usuario deja ver el estado del router, pero no pe rmite modificar su configuración. Según su utilización en el modo usuario, no se debe confundir el término "usuario" con los usuarios de la red. El modo usuario está destinado a técnicos, operadores e ingenieros de red que tienen la responsabilidad de configurar los dispositivos de red.

Router>

El comando enable se usa para ingresar al modo EXEC privilegiado. Este modo permite al usuario realizar cambios de configuración en el router. El indicador del router cambiará de ">" a "#" en este modo.

Router>enable
Router#

**Nombres de hosts y contraseñas**

La figura muestra la sintaxis del comando de configuración básica del router utilizada para configurar R1 en el siguiente ejemplo. Puede abrir la actividad 1.2.2 del Packet Tracer y seguir los pasos o esperar ha sta el final de esta sección para abrirla.

En primer lugar, ingrese al modo de configuración global.

Router#config t

Luego, asigne un nombre de host único al router.

Router(config)#hostname R1
R1(config)#

Ahora, configure una contraseña que se usará para ingresar en el modo EXEC privilegiado. En nuestro entorno de laboratorio, usaremos la contraseña class. Sin embargo, en entornos de producción, los routers deben tener contraseñas seguras. Consulte los enlaces al final de esta sección para obtener más información sobre la creación y el uso de contraseñas seguras.

Router(config)#enable secret class

A continuación, configure la consola y las líneas Telnet con la contraseña cisco. Una vez más, la contraseña cisco se usa sólo en nuestro entorno de laboratorio. El comando login permite la verificación de la contraseña en la línea. Si no se ingresa el comando login en la línea de consola, el usuario obtendrá acceso a la línea sin ingresar una contraseña.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
```

**Configuración de un mensaje**

Desde el modo de configuración global, configure el aviso de mensaje del día (motd). Al comienzo y al final del mensaje se usa un carácter delimitador, como por ejemplo "#". El delimitador permite configurar un mensaje de varias líneas, como se muestra aquí.

```
R1(config)#banner motd #
Enter TEXT message. End with the character '#'.
*****************************************
WARNING!! Unauthorized Access Prohibited!!
*****************************************
#
```

La configuración de un mensaje adecuado es parte de un buen plan de seguridad. Como mínimo, un mensaje debe prevenir el acceso no autorizado. Nunca configure un mensaje que "invite" a un usuario no autorizado.

**Sintaxis básica del comando de configuración del router**

| | |
|---|---|
| Denominación del router | `Router(config)#hostname name` |
| Configuración de contraseñas | `Router(config)#enable secret password` |
| | `Router(config)#line console 0` |
| | `Router(config-line)#password password` |
| | `Router(config-line)#login` |
| | `Router(config)#line vty 0 4` |
| | `Router(config-line)#password password` |
| | `Router(config-line)#login` |
| Configuración de un mensaje del día | `Router(config)#banner motd # message #` |

**Configuración de la interfaz del router**

A continuación se configurarán las interfaces individuales del router con direcciones IP y otra información. En primer lug ar, ingrese en el modo de configuración de interfaz especificando el número y el tipo de interfaz. A continuación, configure la dirección IP y la máscara de subred:

```
R1(config)#interface Serial0/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
```

Es conveniente configurar una descripción en cada interfaz para ayudar a documentar la información de red. El texto de la descripción tiene un límite de 240 caracteres. En las redes de producción, una descripción puede servir para la resolución de problemas suministrando información sobre el tipo de red a la que está conectada la interfaz y si hay otros routers en esa red. Si la interfaz se conecta a un ISP o proveedor de servicios, resulta útil ingresar la conexión y la información de contacto del tercero; por ejemplo:

```
Router(config-if)#description Ciruit#VBN32696-123 (help desk:1-800-555-1234)
```

En los entornos de laboratorio, ingrese una descripción simple que le ayudará a resolver problemas; por ejemplo:

```
R1(config-if)#description Link to R2
```

Después de configurar la descripción y la dirección IP, la interfaz debe activarse con el comando no shutdown. Es como encender la interfaz. La interfaz también debe estar conectada a otro dispositivo (hub, switch, otro router, etc.) para que la capa Física esté activa

Router(config-if)#no shutdown

**Nota:** Cuando se realiza el cableado de un enlace serial punto a punto en nuestro entorno de laboratorio, se coloca la marca DTE a un extremo del cable y la marca DCE al otro extremo. El router que tiene el extremo DCE del cable conectado a su interfaz serial necesitará la configuración del comando adicional clock rate en esa interfaz serial. Este paso solamente es necesario en un entorno de laboratorio y se explicará con mayor detalle en el Capítulo 2, "Enrutamiento estático".

R1(config-if)#clock rate 64000

Se deben repetir los comandos de configuración de interfaz en todas las otras interfaces que requieren configuración. En nuestro ejemplo de topología, debe configurarse la interfaz FastEthernet.

R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#description R1 LAN
R1(config-if)#no shutdown

**Cada interfaz pertenece a una red diferente**

En este punto, observe que cada interfaz debe pertenecer a una red diferente. Aunque el IOS permite configurar una dirección IP desde la misma red en dos interfaces diferentes, el router no activará la segunda interfaz.

Por ejemplo, ¿qué sucede si se intenta configurar la interfaz FastEthernet 0/1 en R1 con una dirección IP en la red 192.168.1.0/24? Ya se ha asignado una dirección a FastEthernet 0/0 en esa misma red. Si se intenta configurar otra interfaz, FastEthernet 0/1, con una dirección IP que pertenece a la misma red, aparecerá el siguiente mensaje:

R1(config)#interface FastEthernet0/1
R1(config-if)#ip address 192.168.1.2 255.255.255.0
192.168.1.0 overlaps with FastEthernet0/0

Si se intenta habilitar la interfaz con el comando no shutdown, aparecerá el siguiente mensaje:

R1(config-if)#no shutdown
192.168.1.0 overlaps with FastEthernet0/0
FastEthernet0/1: incorrect IP address assignment

Observe que el resultado del comando show ip interface brief muestra que la segunda interfaz configurada para la red 192.168.1.0/24, FastEthernet 0/1, aún está inactiva.

R1#show ip interface brief
<output omitted>
FastEthernet0/1 192.168.1.2 YES manual administratively down down

| Sintaxis básica del comando de configuración del router | |
|---|---|
| Configuración de una interfaz | Router(config)#**interface** *type number* |
| | Router(config-if)#**ip address** *address mask* |
| | Router(config-if)#**description** *description* |
| | Router(config-if)#**no shutdown** |
| Cómo guardar cambios realizados en un router | Router#**copy running-config startup-config** |
| Análisis del resultado de los comandos show | Router#**show running-config** |
| | Router#**show ip route** |
| | Router#**show ip interface brief** |
| | Router#**show interfaces** |

**Verificación de la configuración básica del router**

Como se muestra en el ejemplo, se han ingresado todos los comandos anteriores de configuración básica del router e inmediatamente se almacenaron en el archivo de configuración en ejecución de R1. El archivo running-config está

almacenado en la RAM y es el archivo de configuración que usa el IOS. El próximo paso consiste en verificar los comandos ingresados mediante la visualización de la configuración en ejecución con el siguiente comando:

R1#show running-config

Ahora que se han ingresado los comandos de configuración básica, es importante guardar el running-config en la memoria no volátil, la NVRAM del router. De ese modo, en caso de un corte de energía eléctrica o una recarga accidental, el router podrá iniciarse con la configuración actual. Luego de haber completado y probado la configuración del router, es importante guardar el running-config en el startup-config como archivo de configuración permanente.

R1#copy running-config startup-config

Después de aplicar y guardar la configuración básica, pueden usarse varios comandos para verificar que el router se haya configurado correctamente. Haga clic en el botón correspondiente de la figura para observar una lista del resultado de cada comando. Todos estos comandos se tratarán en mayor detalle en los siguientes capítulos. Por el momento, comience a familiarizarse con el resultado.

R1#show running-config

Este comando muestra la configuración actual en ejecución almacenada en la RAM. Salvo unas pocas excepciones, todos los comandos de configuración que se usaron se ingresarán en el running-config y el IOS los implementará de inmediato.

R1#show startup-config

Este comando muestra el archivo de configuración de inicio almacenado en la NVRAM. Ésta es la configuración que usará el router en el siguiente reinicio. Esta configuración no cambia a menos que la configuración actual en ejecución se guarde en la NVRAM con el comando copy running-config startup-config. Observe en la figura que la configuración de inicio y la configuración en ejecución son idénticas. Esto se debe a que la configuración en ejecución no ha cambiado desde la última vez que se guardó. Observe también que el comando show startup-config muestra además cuántos bytes de NVRAM está usando la configuración guardada.

R1#show ip route

Este comando muestra la tabla de enrutamiento que está usando el IOS actualmente para elegir la mejor ruta hacia sus redes de destino. En este punto, R1 solamente tiene rutas para sus redes conectadas directamente, a través de sus propias interfaces.

R1#show interfaces

Este comando muestra todos los parámetros y estadísticas de configuración de la interfaz. Parte de esta información se analizará más adelante en este curso de estudio y en CCNP.

R1#show ip interface brief

Este comando muestra información abreviada de configuración de la interfaz, como por ejemplo la dirección IP y el estado de la interfaz. Este comando es una herramienta útil para la resolución de problemas y un método rápido para determinar el estado de todas las interfaces del router.

show running-config

```
R1#show running-config
!
version 12.3
!
hostname R1
!
interface FastEthernet0/0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
banner motd ^C
**************************************************
WARNING!! Unauthorized Access Prohibited!!
**************************************************
^C
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

show interfaces

```
R1#show interfaces

FastEthernet0/0 is up, line protocol is up (connected)
  Hardware is Lance, address is 0007.eca7.1511 (bia 00e0.f7e4.e47e)
  Description: R1 LAN
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00,
  Last input 00:00:08, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Serial0/0/0 is up, line protocol is up (connected)
  Hardware is HD64570
  Description: Link to R2
  Internet address is 192.168.2.1/24
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

show ip route

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

show startup-config

```
R1#show startup-config
Using 728 bytes
!
version 12.3
!
hostname R1
!
interface FastEthernet0/0
 description R1 LAN
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R2
 ip address 192.168.2.1 255.255.255.0
 clock rate 64000
!
banner motd ^C
**********************************************
WARNING!! Unauthorized Access Prohibited!!
**********************************************
^C
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
!
end
```

show ip interface brief

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/0/0            192.168.2.1     YES manual up                    up
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

## 1.3 CONSTRUCCION DE LA TABLA DE ENRRUTAMIENTO.-

### 1.3.1 INTRODUCCION DE LA TABLA DE ENRRUTAMIENTO.-

**Introducción de la tabla de enrutamiento**

La función principal de un router es enviar un paquete hacia su red de destino, que es la dirección IP de destino del paquete. Para hacerlo, el router necesita buscar la información de enrutamiento almacenada en su tabla de enrutamiento.

Una tabla de enrutamiento es un archivo de datos en la RAM que se usa para almacenar la información de la ruta sobre redes remotas y conectadas directamente. La tabla de enrutamiento contiene asociaciones entre la red y el siguiente salto. Estas asociaciones le indican al router que un destino en particular se puede alcanzar mejor enviando el paquete hacia un router en particular, que representa el "siguiente salto" en el camino hacia el destino final. La asociación del siguiente salto también puede ser la interfaz de salida hacia el destino final.

La asociación entre la red y la interfaz de salida también puede representar la dirección de red de destino del paquete IP. Esta asociación ocurre en las redes del router conectadas directamente.

Una red conectada directamente es una red que está directamente vinculada a una de las interfaces del router. Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz pasa a ser un host en esa red conectada. La dirección de red y la máscara de subred de la interfaz, junto con el número y el tipo de interfaz, se ingresan en la tabla de enrutamiento como una red conectada directamente. Cuando un router envía un paquete a un host, como por ejemplo un servidor Web, ese host está en la misma red que la red del router conectada directamente.

Una red remota es una red que no está directamente conectada al router. En otras palabras, una red remota es una red a la que sólo se puede llegar mediante el envío del paquete a otro router. Las redes remotas se agregan a la tabla de enrutamiento mediante el uso de un protocolo de enrutamiento dinámico o la configuración de rutas estáticas. Las rutas dinámicas son rutas hacia redes remotas que fueron aprendidas automáticamente por el router utilizando un protocolo de enrutamiento dinámico. Las rutas estáticas son rutas hacia redes manualmente configuradas por un administrador de red.

Nota: La tabla de enrutamiento con sus redes conectadas directamente, las rutas estáticas y las rutas dinámicas se introducirán en las siguientes secciones y se analizarán con mayor profundidad aún a lo largo de este curso.

Las siguientes analogías pueden ayudar a aclarar el concepto de rutas conectadas, estáticas y dinámicas:
**Rutas conectadas directamente:** para visitar a un vecino, lo único que tiene que hacer es caminar por la calle donde vive. Esta ruta es similar a una ruta conectada directamente porque el "destino" está disponible directamente a través de su "interfaz conectada", la calle.
**Rutas estáticas:** un tren siempre usa las mismas vías en una ruta específica. Esta ruta es similar a una estática porque la ruta hacia el destino es siempre la misma.
**Rutas dinámicas:** al conducir un automóvil, usted puede elegir "dinámicamente" una ruta diferente según el tráfico, el clima y otras condiciones. Esta ruta es similar a una ruta dinámica porque puede elegir una nueva ruta en muchos puntos diferentes en su trayecto hacia el destino.

**El comando show ip route**

Como se indica en la figura, la tabla de enrutamiento se muestra con el comando show ip route. Hasta ahora, no se han configurado rutas estáticas ni se ha habilitado ningún protocolo de enrutamiento dinámico. Por lo tanto, la tabla de enrutamiento de R1 sólo muestra las redes conectadas directamente del router. Para cada red enumerada en la tabla de enrutamiento, se incluye la siguiente información:
**C:** la información en esta columna denota el origen de la información de la ruta, la red conectada directamente, la ruta estática o del protocolo de enrutamiento dinámico. La C representa a una ruta conectada directamente.
**192.168.1.0/24:** es la dirección de red y la máscara de subred de la red remota o conectada directamente. En este ejemplo, las dos entradas en la tabla de enrutamiento, 192.168.1./24 y 192.168.2.0/24, son redes conectadas directamente.
**FastEthernet 0/0:** la información al final de la entrada de la ruta representa la interfaz de salida y/o la dirección IP del router del siguiente salto. En este ejemplo, tanto la FastEthernet 0/0 como la Serial0/0/0 son las interfaces de salida que se usan para alcanzar estas redes.

Cuando la tabla de enrutamiento incluye una ruta para una red remota, se incluye información adicional, como la métrica de enrutamiento y la distancia administrativa. La métrica de enrutamiento, la distancia administrativa y el comando show ip route se explican con mayor detalle en los siguientes capítulos.

Las PC también tienen una tabla de enrutamiento. En la figura se observa el resultado del comando route print. El comando revela las redes de broadcast, multicast, loopback o de gateway por defecto que están configuradas o adquiridas. El resultado del comando route print no se analizará durante este curso. Se muestra aquí para destacar que todos los dispositivos IP configurados deben tener una tabla de enrutamiento.


```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
```

Origen: rutas conectadas

```
C:\>route print
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 11 25 af 40 9b ...... Intel(R) PRO/1000 MT Mobile Connection
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.1.1    192.168.1.1      10
        127.0.0.0        255.0.0.0      127.0.0.1      127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.1    192.168.1.1      10
    192.168.1.10    255.255.255.0      127.0.0.1    192.168.1.1      10
        224.0.0.0        240.0.0.0    192.168.1.10   192.168.1.10     10
  255.255.255.255  255.255.255.255    192.168.1.10   192.168.1.10      1
Default Gateway:    192.168.1.1
===========================================================================
Persistent Routes:
  None
```

Ruta por defecto para R1 en 192.168.1.1

### 1.3.2 REDES CONECTADAS DIRECTAMENTE.-

**Incorporación a la tabla de enrutamiento de una red conectada**

Como se mencionó en la sección anterior, cuando se configura la interfaz de un router con una dirección IP y una máscara de subred, la interfaz pasa a ser un host en esa red. Por ejemplo, cuando la interfaz FastEthernet 0/0 en R1 en la figura se configura con la dirección IP 192.168.1.1 y la máscara de subred 255.255.255.0, la interfaz FastEthernet 0/0 pasa a ser miembro de la red 192.168.1.0/24. Los hosts que están conectados a la misma LAN, como la PC1, también se configuran con una dirección IP que pertenece a la red 192.168.1.0/24.

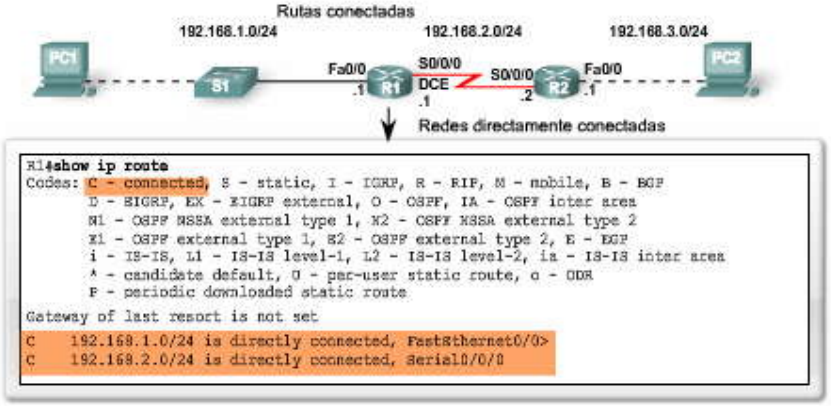
Cuando se configura una PC con una dirección IP host y una máscara de subred, la PC usa la máscara de subred para determinar a qué red pertenece ahora. El sistema operativo realiza esto mediante el proceso ANDing en la dirección IP host y en la máscara de subred. Un router utiliza la misma lógica al configurar una interfaz.

Una PC normalmente se configura con una sola dirección IP host porque tiene una única interfaz de red, generalmente una Ethernet NIC. Los routers tienen múltiples interfaces; por lo tanto, cada interfaz debe ser miembro de una red diferente. En la figura, R1 es miembro de dos redes diferentes: 192.168.1.0/24 y 192.168.2.0/24. El router R2 también es miembro de dos redes: 192.168.2.0/24 y 192.168.3.0/24.

Después de que se configura la interfaz del router y se activa la interfaz con el comando no shutdown, la interfaz debe recibir una señal portadora desde otro dispositivo (router, switch, hub, etc.) antes de que el estado de la interfaz se considere "activo". Una vez que la interfaz está "activa", la red de esa interfaz se incorpora a la tabla de enrutamiento como red conectada directamente.

Antes de configurar cualquier enrutamiento estático o dinámico en un router, éste solamente conoce a sus propias redes conectadas directamente. Éstas son las únicas redes que se muestran en la tabla de enrutamiento hasta que se configure el enrutamiento estático o dinámico. Las redes conectadas directamente son de fundamental importancia para las decisiones de enrutamiento. Las rutas estáticas y dinámicas no pueden existir en la tabla de enrutamiento sin las propias redes del router conectadas directamente. El router no puede enviar paquetes desde una interfaz si la misma no está habilitada con una dirección IP y una máscara de subred, del mismo modo que una PC no puede enviar paquetes IP desde su interfaz Ethernet si la misma no está configurada con una dirección IP y una máscara de subred.

**Nota:** El proceso para configurar las interfaces del router e incorporar direcciones de red a la tabla de enrutamiento se analizará en el próximo capítulo.



### 1.3.3 ENRUTAMIENTO ESTÁTICO.-

**Enrutamiento estático**

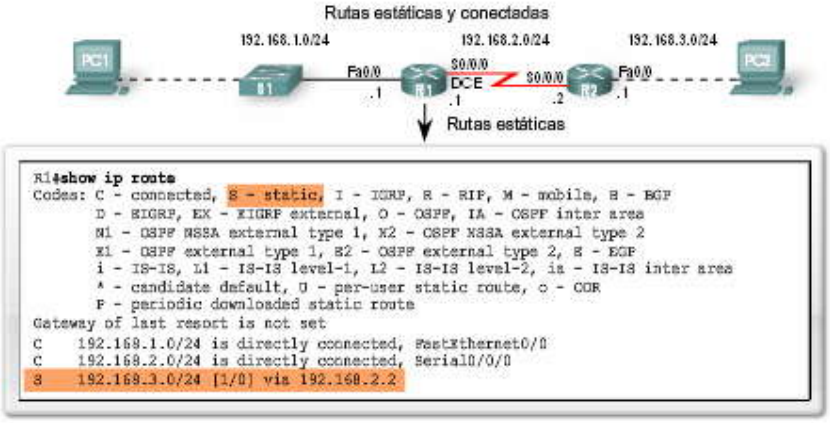
Las redes remotas se agregan a la tabla de enrutamiento mediante la configuración de rutas estáticas o la habilitación de un protocolo de enrutamiento dinámico. Cuando el IOS aprende sobre una red remota y la interfaz que usará para llegar a esa red, agrega la ruta a la tabla de enrutamiento siempre que la interfaz de salida esté habilitada.

Una ruta estática incluye la dirección de red y la máscara de subred de la red remota, junto con la dirección IP del router del siguiente salto o la interfaz de salida. Las rutas estáticas se indican con el código S en la tabla de enrutamiento, como se muestra en la figura. Las rutas estáticas se examinan en detalle en el próximo capítulo.

**Cuándo usar rutas estáticas**

Las rutas estáticas deben usarse en los siguientes casos:
**Una red está compuesta por unos pocos routers solamente.** En tal caso, el uso de un protocolo de enrutamiento dinámico no representa ningún beneficio sustancial. Por el contrario, el enrutamiento dinámico agrega más sobrecarga administrativa.
**Una red se conecta a Internet solamente a través de un único ISP.** No es necesario usar un protocolo de enrutamiento dinámico a través de este enlace porque el ISP representa el único punto de salida hacia Internet.
**Una red extensa está configurada con una topología hub-and-spoke.** Una topología hub-and-spoke comprende una ubicación central (el hub) y múltiples ubicaciones de sucursales (spokes), donde cada spoke tiene solamente una conexión al hub. El uso del enrutamiento dinámico sería innecesario porque cada sucursal tiene una única ruta hacia un destino determinado, a través de la ubicación central.

Generalmente, la mayoría de las tablas de enrutamiento contienen una combinación de rutas estáticas y rutas dinámicas. Sin embargo, como mencionamos antes, la tabla de enrutamiento debe contener primero las redes conectadas directamente que se usan para acceder a estas redes remotas antes de poder usar cualquier enrutamiento estático o dinámico.




### 1.3.4 ENRUTAMIENTO DINÁMICO.-

**Enrutamiento dinámico**

Las redes remotas también pueden agregarse a la tabla de enrutamiento utilizando un protocolo de enrutamiento dinámico. En la figura, R1 ha aprendido automáticamente sobre la red 192.168.4.0/24 desde R2 a través del protocolo de enrutamiento dinámico, RIP (Routing Information Protocol). El RIP fue uno de los primeros protocolos de enrutamiento IP y se analizará en detalle en los siguientes capítulos.

Nota: La tabla de enrutamiento de R1 en la figura muestra que R1 ha aprendido sobre dos redes remotas: una ruta que usó el RIP dinámicamente y una ruta estática que se configuró en forma manual. Éste es un ejemplo de cómo las tablas de enrutamiento pueden contener rutas aprendidas dinámicamente y configuradas estáticamente y no necesariamente implica la mejor configuración para esta red.

Los routers usan protocolos de enrutamiento dinámico para compartir información sobre el estado y la posibilidad de conexión de redes remotas. Los protocolos de enrutamiento dinámico ejecutan varias actividades, entre ellas:
Descubrimiento de redes

Actualización y mantenimiento de las tablas de enrutamiento

**Descubrimiento automático de redes**

El descubrimiento de redes es la capacidad de un protocolo de enrutamiento de compartir información sobre las redes que conoce con otros routers que también están usando el mismo protocolo de enrutamiento. En lugar de configurar rutas estáticas hacia redes remotas en cada router, un protocolo de enrutamiento dinámico permite a los routers aprender automáticamente sobre estas redes a partir de otros routers. Estas redes, y la mejor ruta hacia cada red, se agregan a la tabla de enrutamiento del router y se denotan como una red aprendida por un protocolo de enrutamiento dinámico específico.

**Mantenimiento de las tablas de enrutamiento**

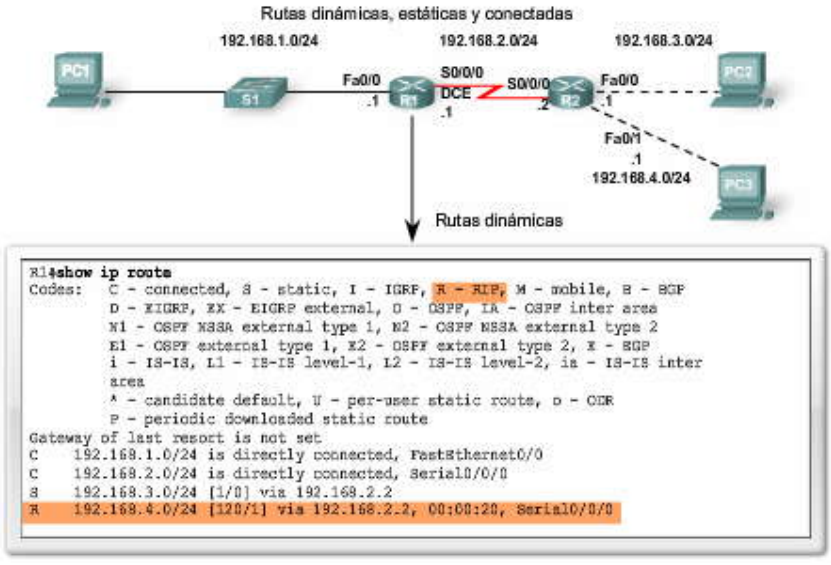
Después del descubrimiento inicial de la red, los protocolos de enrutamiento dinámico actualizan y mantienen las redes en sus tablas de enrutamiento. Los protocolos de enrutamiento dinámico no sólo deciden acerca de la mejor ruta hacia diferentes redes, también determinan la mejor ruta nueva si la ruta inicial se vuelve inutilizable (o si cambia la topología). Por estos motivos, los protocolos de enrutamiento dinámico representan una ventaja sobre las rutas estáticas. Los routers que usan protocolos de enrutamiento dinámico automáticamente comparten la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin requerir la participación del administrador de red.

**Protocolos de enrutamiento IP**

Existen varios protocolos de enrutamiento dinámico para IP. Éstos son algunos de los protocolos de enrutamiento dinámico más comunes para el enrutamiento de paquetes IP:
RIP (Routing Information Protocol)
IGRP (Interior Gateway Routing Protocol)
EIGRP (Enhanced Interior Gateway Routing Protocol)
OSPF (Open Shortest Path First)
IS-IS (Intermediate System-to-Intermediate System)
BGP (Border Gateway Protocol)

Nota: En este curso se analizan el RIP (versiones 1 y 2), el EIGRP y el OSPF. El EIGRP y el OSPF también se explican en mayor detalle en CCNP, junto con IS-IS y BGP. El IGRP es un protocolo de enrutamiento heredado que ha sido reemplazado por el EIGRP. El IGRP y el EIGRP son protocolos de enrutamiento patentados por Cisco, mientras que todos los demás protocolos de enrutamiento enumerados son protocolos estándares, no patentados.

Una vez más, recuerde que en la mayoría de los casos, los routers contienen una combinación de rutas estáticas y rutas dinámicas en las tablas de enrutamiento. Los protocolos de enrutamiento dinámico se analizarán con mayor profundidad en el Capítulo 3, "Introducción a los protocolos de enrutamiento dinámico".




### 1.3.5 PRINCIPIOS DE LA TABLA DE ENRUTAMIENTO.-

**Principios de la tabla de enrutamiento**

En algunas secciones de este curso haremos referencia a tres principios relacionados con las tablas de enrutamiento que lo ayudarán a comprender, configurar y solucionar problemas de enrutamiento. Estos principios se extraen del libro de Alex Zinin, Cisco IP Routing.

1. Cada router toma su decisión en forma independiente, según la información de su propia tabla de enrutamiento.

2. El hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los otros routers tengan la misma información.

3. La información de enrutamiento sobre una ruta desde una red a otra no suministra información de enrutamiento sobre la ruta inversa o de regreso.

¿Cuál es el efecto de estos principios? Observemos el ejemplo en la figura.

1. Después de tomar su decisión de enrutamiento, el router R1 envía al router R2 el paquete destinado a la PC3. R1 sólo conoce la información de su propia tabla de enrutamiento, que indica que el router R2 es el router del siguiente salto. R1 no sabe si R2 efectivamente tiene o no una ruta hacia la red de destino.

2. Es responsabilidad del administrador de red asegurarse de que todos los routers bajo su control tengan información de enrutamiento completa y precisa de manera tal que los paquetes puedan enviarse entre cualquiera de las dos redes. Esto puede lograrse mediante el uso de rutas estáticas, un protocolo de enrutamiento dinámico o una combinación de ambas opciones.

3. El router R2 pudo enviar el paquete hacia la red de destino de la PC3. Sin embargo, R2 descartó el paquete desde la PC2 a la PC1. Aunque R2 tiene información en su tabla de enrutamiento sobre la red de destino de la PC1, no sabemos si tiene la información para la ruta de regreso hacia la red de la PC1.

**Enrutamiento asimétrico**

Dado que los routers no necesariamente tienen la misma información en sus tablas de enrutamiento, los paquetes pueden recorrer la red en un sentido, utilizando una ruta, y regresar por otra ruta. Esto se denomina enrutamiento asimétrico. El enrutamiento asimétrico es más común en Internet, que usa el protocolo de enrutamiento BGP, que en la mayoría de las redes internas.

Este ejemplo implica que cuando se diseña una red y se resuelven problemas en ella, el administrador de red debe verificar la siguiente información de enrutamiento:
¿Existe una ruta de origen a destino que esté disponible en ambos sentidos?
¿Es la ruta que se tomó en ambos sentidos la misma ruta? (El enrutamiento asimétrico no es inusual, pero a veces puede causar otros problemas.)

## 1.4 DETERMINACION DE LA RUTA Y FUCIONES DE CONMUTACION.-

### 1.4.1 CAMPOS DE TRAMA Y PAQUETE.-

**Campos de trama y paquete**

Como se analizó anteriormente, los routers toman su principal decisión de envío al examinar la dirección IP de destino de un paquete. Antes de enviar un paquete desde la interfaz de salida correspondiente, el paquete IP debe ser encapsulado en una trama de enlace de datos de Capa 2. Más adelante en esta sección seguiremos un paquete IP de origen a destino, examinando el proceso de encapsulación y desencapsulación en cada router. Pero primero, revisaremos el formato de un paquete IP de Capa 3 y una trama de Ethernet de Capa 2.

**Formato de paquete de Internet Protocol (IP)**

El Internet Protocol especificado en RFC 791 define el formato de paquete IP. El encabezado del paquete IP tiene campos específicos que contienen información sobre el paquete y sobre los host emisores y receptores. La siguiente es una lista de los campos en el encabezado IP y una breve descripción de cada uno. Ya debe conocer de cerca los campos de dirección IP de destino, dirección IP de origen, versión y Período de vida (TTL). Los demás campos son importantes pero están fuera del ámbito de estudio de este curso.
Versión: número de versión (4 bits); la versión predominante es la IP versión 4 (IPv4)
Longitud del encabezado IP: longitud del encabezado en palabras de 32 bits (4 bits)
Prioridad y tipo de servicio: cómo debe administrarse el datagrama (8 bits); los primeros 3 bits son bits de prioridad (este uso ha sido reemplazado por el Punto de código de servicios diferenciados [Differentiated Services Code Point, DSCP], que usa los primeros 6 bits [se reservan los últimos 2])
Longitud del paquete: longitud total (encabezado + datos) (16 bits)
Identificación: valor único del datagrama IP (16 bits)
Señalizadores: controlan la fragmentación (3 bits)

Desplazamiento de fragmentos: admite la fragmentación de datagramas para permitir diferentes unidades máximas de transmisión (MTU) en Internet (13 bits)
Período de vida (TTL): identifica cuántos routers puede atravesar el datagrama antes de ser descartado (8 bits)
Protocolo: protocolo de capa superior que envía el datagrama (8 bits)
Checksum del encabezado: verificación de integridad del encabezado (16 bits)
Dirección IP de origen: dirección IP de origen de 32 bits (32 bits)
Dirección IP de destino: dirección IP de destino de 32 bits (32 bits)
Opciones de IP: pruebas de red, depuración, seguridad y otras (0 ó 32 bits, si corresponde)

Campos de paquetes IP

| Byte 1 | | Byte 2 | Byte 3 | Byte 4 |
|---|---|---|---|---|
| Versión | IHL | Tipo de servicio | Longitud del paquete | |
| Identificación | | | Señalizador | Desplazamiento de fragmentos |
| Período de vida | | Protocolo | Checksum del encabezado | |
| Dirección de origen | | | | |
| Dirección de destino | | | | |
| Opciones | | | | Relleno |

**Formato de trama de la Capa MAC**

La trama de enlace de datos de Capa 2 normalmente contiene información del encabezado con una dirección de origen y de destino del enlace de datos, información del tráiler y los datos reales transmitidos. La dirección de origen del enlace de datos es la dirección de Capa 2 de la interfaz que envió la trama de enlace de datos. La dirección de destino del enlace de datos es la dirección de Capa 2 de la interfaz del dispositivo de destino. Tanto la interfaz del enlace de datos de origen como la de destino se encuentran en la misma red. Cuando un paquete se envía de un router a otro, las direcciones IP de origen y destino de Capa 3 no cambiarán; sin embargo, sí lo harán las direcciones de enlace de datos de origen y destino de Capa 2. Este proceso se analizará con más profundidad más adelante en esta sección.

Nota: Cuando se usa NAT (Traducción de direcciones de red), la dirección IP de destino cambia, pero este proceso no tiene importancia para IP y es un proceso que se realiza dentro de la red de una empresa. El enrutamiento con NAT se analizará en otro curso.

El paquete IP de Capa 3 está encapsulado en la trama de enlace de datos de Capa 2 asociada con esa interfaz. En este ejemplo, mostraremos la trama de Ethernet de Capa 2. La figura muestra las dos versiones compatibles de Ethernet. La siguiente es una lista de los campos en una trama de Ethernet y una breve descripción de cada uno.
Preámbulo: siete bytes que alternan 1 y 0, utilizados para sincronizar señales
Delimitador de inicio de trama (SOF): 1 byte que señala el comienzo de la trama
Dirección de destino: dirección MAC de 6 bytes del dispositivo emisor en el segmento local
Dirección de origen: dirección MAC de 6 bytes del dispositivo receptor en el segmento local
Tipo/longitud: 2 bytes que especifican ya sea el tipo de protocolo de capa superior (formato de trama de Ethernet II) o la longitud del campo de datos (formato de trama IEEE 802.3)
Datos y Pad: de 46 a 1500 bytes de datos; ceros utilizados para completar cualquier paquete de datos de menos de 46 bytes
Secuencia de verificación de trama (FCS): 4 bytes utilizados para una comprobación de redundancia cíclica a fin de asegurar que no se dañó la trama

Campos de trama Ethernet

Ethernet

Longitud del campo en bytes

| 8 | 6 | 6 | 2 | 46-1500 | 4 |
|---|---|---|---|---|---|
| Preámbulo | Dirección de destino | Dirección de origen | Tipo | Datos | FCS |

IEEE 802.3

Longitud del campo en bytes

| 7 | 1 | 6 | 6 | 2 | 46-1500 | 4 |
|---|---|---|---|---|---|---|
| Preámbulo | SOF | Dirección de destino | Dirección de origen | Longitud | Encabezado y datos 802.2 | FCS |

### 1.4.2 LA MÉTRICA Y AL MEJOR RUTA.-

**La mejor ruta**

La identificación de la mejor ruta de un router implica la evaluación de múltiples rutas hacia la misma red de destino y la selección de la ruta óptima o "la más corta" para llegar a esa red. Cuando existen múltiples rutas para llegar a la misma red,

cada ruta usa una interfaz de salida diferente en el router para llegar a esa red. La mejor ruta es elegida por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Algunos protocolos de enrutamiento, como RIP, usan un conteo de saltos simple, que consiste en el número de routers entre un router y la red de destino. Otros protocolos de enrutamiento, como OSPF, determinan la ruta más corta al analizar el ancho de banda de los enlaces y al utilizar dichos enlaces con el ancho de banda más rápido desde un router hacia la red de destino.

Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. Una métrica es un valor cuantitativo que se usa para medir la distancia hacia una ruta determinada. La mejor ruta a una red es la ruta con la métrica más baja. Por ejemplo, un router preferirá una ruta que se encuentra a 5 saltos antes que una ruta que se encuentra a 10 saltos.

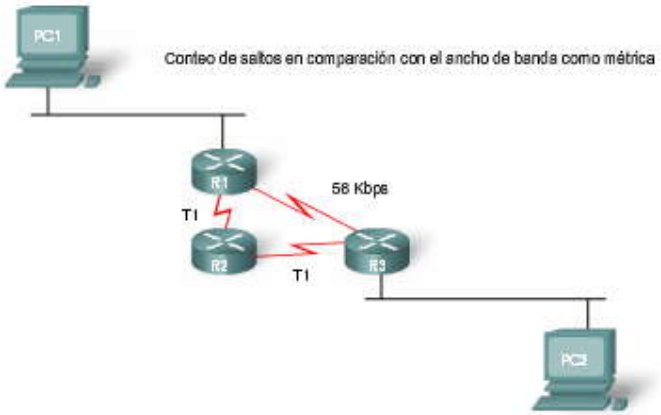
El objetivo principal del protocolo de enrutamiento es determinar las mejores trayectorias para cada ruta a fin de incluirlas en la tabla de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico. Cuanto menor es el valor de la métrica, mejor es la ruta.

**Comparación del conteo de saltos y la métrica del ancho de banda**

Dos de las métricas que usan algunos protocolos de enrutamiento dinámicos son:
Conteo de saltos: cantidad de routers que debe atravesar un paquete antes de llegar a su destino. Cada router es igual a un salto. Un conteo de saltos de cuatro indica que un paquete debe atravesar cuatro routers para llegar a su destino. Si hay múltiples rutas disponibles hacia un destino, el protocolo de enrutamiento (por ejemplo RIP) selecciona la ruta que tiene el menor número de saltos.
Ancho de banda: es la capacidad de datos de un enlace, a la cual se hace referencia a veces como la velocidad del enlace. Por ejemplo, la implementación del protocolo de enrutamiento OSPF de Cisco utiliza como métrica el ancho de banda. La mejor ruta hacia una red se determina según la ruta con una acumulación de enlaces que tienen los valores de ancho de banda más altos, o los enlaces más rápidos. El uso del ancho de banda en OSPF se explicará en el Capítulo 11.

Nota: Técnicamente, la velocidad no es una descripción precisa del ancho de banda porque todos los bits viajan a la misma velocidad a través del mismo medio físico. Más precisamente, el ancho de banda se define como la cantidad de bits que pueden transmitirse a través de un enlace por segundo.

Cuando se usa el conteo de saltos como métrica, la ruta resultante a veces puede ser subóptima. Por ejemplo, considere la red que se muestra en la figura. Si RIP es el protocolo de enrutamiento utilizado por los tres routers, entonces R1 utilizará la ruta subóptima hacia R3 para llegar a la PC2 porque esta ruta tiene menos saltos. No se tiene en cuenta el ancho de banda. Sin embargo, si se usa OSPF como protocolo de enrutamiento, entonces R1 elegirá la ruta basándose en el ancho de banda. Los paquetes podrán llegar a destino antes utilizando los dos enlaces T1 más rápidos, en comparación con el enlace único de 56 Kbps más lento.




### 1.4.3 BALANCEO DE CARGA DE MISMO COSTO.-

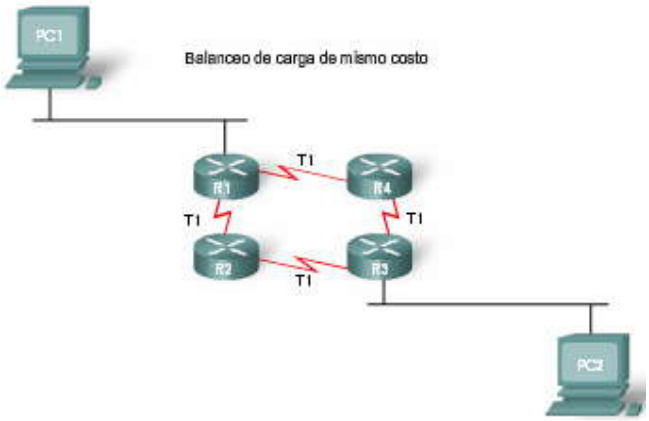
**Balanceo de carga de mismo costo**

Posiblemente se esté preguntando qué sucede si una tabla de enrutamiento tiene dos o más rutas con la misma métrica hacia la misma red de destino. Cuando un router tiene múltiples rutas hacia una red de destino y el valor de esa métrica (conteo de saltos, ancho de banda, etc.) es el mismo, esto se conoce como métrica de mismo costo, y el router realizará un balanceo de carga de mismo costo. La tabla de enrutamiento tendrá la única red de destino pero mostrará múltiples interfaces de salida, una para cada ruta del mismo costo. El router enviará los paquetes utilizando las múltiples interfaces de salida en la tabla de enrutamiento.

Si está configurado correctamente, el balanceo de carga puede aumentar la efectividad y el rendimiento de la red. El balanceo de carga de mismo costo puede configurarse para usar tanto protocolos de enrutamiento dinámico como rutas estáticas. El balanceo de carga de mismo costo se analizará con más profundidad en el Capítulo 8, "Tabla de enrutamiento: un estudio detallado".

**Rutas de mismo y diferente costo**

En caso de que se lo esté preguntando, un router puede enviar paquetes a través de múltiples redes aun cuando la métrica no sea igual, siempre que esté usando un protocolo de enrutamiento que tenga esta capacidad. A esto se lo conoce como balanceo de carga con distinto costo. Los EIGRP (además del IGRP) son los únicos protocolos de enrutamiento que pueden configurarse para el balanceo de carga con distinto costo. El balanceo de carga con distinto costo en EIGRP no es tema de estudio en este curso, pero se abarca en CCNP.




### 1.4.4 DETERMINACIONDE RUTA.-

**Determinación de ruta**

El envío de paquetes supone dos funciones:
Función de determinación de ruta
Función de conmutación

La función de determinación de ruta es el proceso según el cual el router determina qué ruta usar cuando envía un paquete. Para determinar la mejor ruta, el router busca en su tabla de enrutamiento una dirección de red que coincida con la dirección IP de destino del paquete.

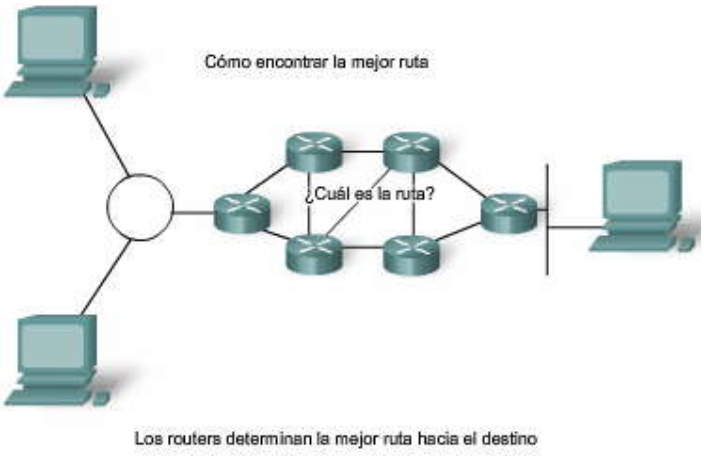
El resultado de esta búsqueda es una de tres determinaciones de ruta:

**Red conectada directamente:** si la dirección IP de destino del paquete pertenece a un dispositivo en una red que está directamente conectado a una de las interfaces del router, ese paquete se envía directamente a ese dispositivo. Esto significa que la dirección IP de destino del paquete es una dirección host en la misma red que la interfaz de este router.

**Red remota:** si la dirección IP de destino del paquete pertenece a una red remota, entonces el paquete se envía a otro router. Las redes remotas sólo se pueden alcanzar mediante el envío de paquetes a otro router.

**Sin determinación de ruta:** si la dirección IP de destino del paquete no pertenece ya sea a una red conectada o remota, y si el router no tiene una ruta por defecto, entonces el paquete se descarta. El router envía un mensaje ICMP de destino inalcanzable a la dirección IP de origen del paquete.

En los primeros dos resultados, el router vuelve a encapsular el paquete IP en el formato de la trama de enlace de datos de Capa 2 de la interfaz de salida. El tipo de interfaz determina el tipo de encapsulación de Capa 2. Por ejemplo, si la interfaz de salida es FastEthernet, el paquete se encapsula en una trama de Ethernet. Si la interfaz de salida es una interfaz serial configurada para PPP, el paquete IP se encapsula en una trama PPP.




### 1.4.5 FUNCION DE CONMUTACION.-

**Función de conmutación**

Después de que el router ha determinado la interfaz de salida utilizando la función de determinación de ruta, el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida.

La función de conmutación es el proceso utilizado por un router para aceptar un paquete en una interfaz y enviarlo desde otra interfaz. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida.

¿Qué hace un router cuando recibe un paquete desde una red y está destinado a otra red? El router ejecuta los tres siguientes pasos principales:

1. Desencapsula el paquete de Capa 3 al quitar el tráiler y el encabezado de trama de Capa 2.

2. Examina la dirección IP de destino del paquete IP para encontrar la mejor ruta en la tabla de enrutamiento.

3. Encapsula el paquete de Capa 3 en una nueva trama de Capa 2 y envía la trama desde la interfaz de salida.

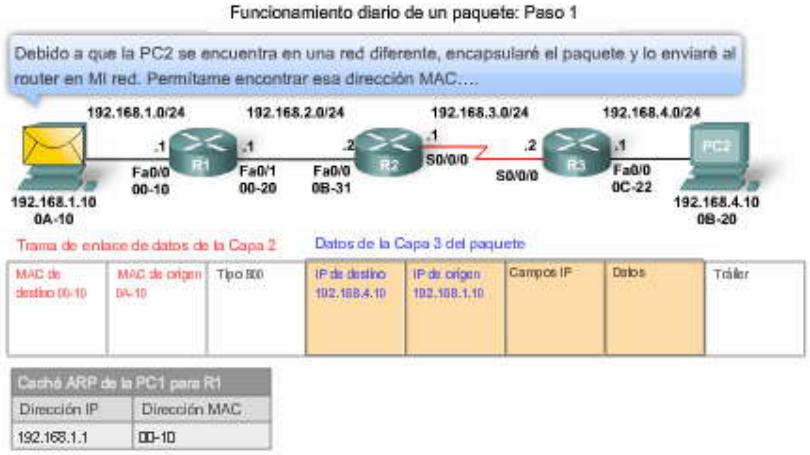
Haga clic en Reproducir para visualizar la animación.

Cuando se envía el paquete IP de Capa 3 de un router al siguiente, el paquete IP permanece sin cambios, salvo el campo Período de vida (TTL). Cuando un router recibe un paquete IP, disminuye el TTL en uno. Si el valor TTL resultante es cero, el router descarta el paquete. El TTL se usa para evitar que los paquetes IP viajen indefinidamente a través de las redes debido a un routing loop u otro desperfecto de la red. Los routing loops se analizan en un capítulo posterior.

Cuando el paquete IP se desencapsula de una trama de Capa 2 y se encapsula en una nueva trama de Capa 2, la dirección de destino del enlace de datos y la dirección de origen cambiarán al enviar el paquete de un router al siguiente. La dirección de origen del enlace de datos de Capa 2 representa la dirección de Capa 2 de la interfaz de salida. La dirección de destino de Capa 2 representa la dirección de Capa 2 del router del siguiente salto. Si el siguiente salto es el dispositivo de destino final, será la dirección de Capa 2 de ese dispositivo.

Es muy probable que el paquete se encapsule en un tipo de trama de Capa 2 diferente de la trama en la que se recibió. Por ejemplo, el router puede recibir el paquete en una interfaz FastEthernet, encapsularlo en una trama de Ethernet y enviarlo desde la interfaz serial encapsulado en una trama PPP.

Recuerde que cuando el paquete se dirige desde el dispositivo de origen al dispositivo de destino final, las direcciones IP de Capa 3 no cambian. Sin embargo, las direcciones de enlace de datos de Capa 2 cambian en cada salto cuando cada router desencapsula y vuelve a encapsular el paquete en una nueva trama.




**Detalles de la determinación de ruta y la función de conmutación**

¿Puede describir los detalles exactos de lo que le sucede a un paquete en la Capa 2 y la Capa 3 cuando viaja desde el origen hacia el destino? Si no puede hacerlo, estudie la animación y continúe con el análisis hasta que pueda describir el proceso sin ayuda.

Haga clic en Reproducir para visualizar la animación.

**Paso 1: La PC1 debe enviar un paquete a la PC2**

La PC1 encapsula el paquete IP en una trama de Ethernet con la dirección MAC de destino de la interfaz FastEthernet 0/0 de R1.

¿Cómo sabe la PC1 que debe enviar el paquete a R1 y no directamente a la PC2? La PC 1 ha determinado que las direcciones IP de origen y destino se encuentran en redes diferentes.

La PC1 conoce la red a la que pertenece al ejecutar una operación AND en su propia dirección IP y máscara de subred, lo cual da como resultado su dirección de red. La PC1 ejecuta esta misma operación AND utilizando la dirección IP de destino del paquete y la máscara de subred de la PC1. Si el resultado es el mismo que el de su propia red, la PC1 sabe que la dirección IP de destino se encuentra en su propia red y no necesita enviar el paquete al gateway por defecto, el router. Si el resultado de la operación AND es una dirección de red diferente, la PC1 sabe que la dirección IP de destino no se encuentra en su propia red y debe enviar el paquete al gateway por defecto, el router.

Nota: Si el resultado de la operación AND en la dirección IP de destino del paquete y la máscara de subred de la PC1 es una dirección de red diferente de la determinada por la PC1 como su propia dirección de red, esta dirección no necesariamente refleja la dirección de red remota real. La PC1 solamente sabe que si la dirección IP de destino se encuentra en su propia red, las máscaras serán las mismas y las direcciones de red también serán las mismas. La máscara de la red remota puede ser una máscara diferente. Si la dirección IP de destino da como resultado una dirección de red diferente, la PC1 no conocerá la dirección de red remota real, solamente sabe que no está en su propia red.

¿Cómo determina la PC1 la dirección MAC del gateway por defecto, el router R1? La PC1 busca en su tabla ARP la dirección IP del gateway por defecto y su dirección MAC asociada.

¿Qué sucede si esta entrada no existe en la tabla ARP? La PC1 envía una solicitud de ARP y el router R1 envía a cambio una respuesta ARP.

**Paso 2: El router R1 recibe la trama Ethernet**

1. El router R1 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, FastEthernet 0/0. Por lo tanto, R1 copiará la trama en su búfer.

2. R1 observa que el campo Tipo de Ethernet es 0x800, lo cual significa que la trama de Ethernet contiene un paquete IP en la porción de datos de la trama.

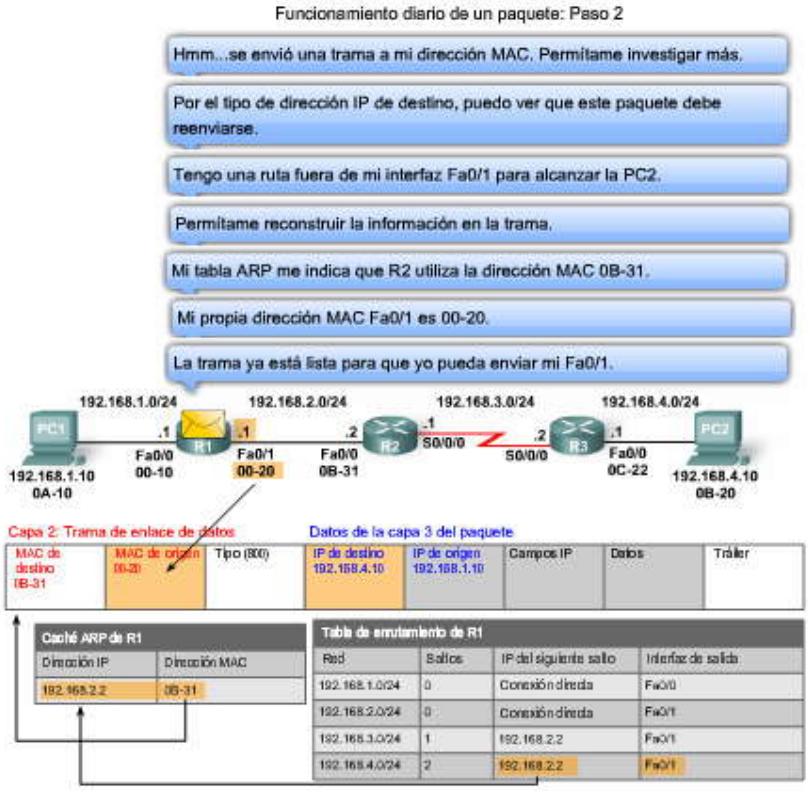
3. R1 desencapsula la trama de Ethernet.

4. Dado que la dirección IP de destino del paquete no coincide con ninguna de las redes de R1 conectadas directamente, el router consulta su tabla de enrutamiento para enrutar este paquete. R1 busca una dirección de red y una máscara de subred en la tabla de enrutamiento que incluya la dirección IP de destino de este paquete como una dirección host en esa red. En este ejemplo, la tabla de enrutamiento tiene una ruta para la red 192.168.4.0/24. La dirección IP de destino del paquete es 192.168.4.10, que es una dirección IP host en esa red.

La ruta de R1 hacia la red 192.168.4.0/24 tiene una dirección IP del siguiente salto de 192.168.2.2 y una interfaz de salida de FastEthernet 0/1. Esto significa que el paquete IP se encapsulará en una nueva trama de Ethernet con la dirección MAC de destino de la dirección IP del router del siguiente salto. Debido a que la interfaz de salida se encuentra en una red Ethernet, R1 debe resolver la dirección IP del siguiente salto con una dirección MAC de destino.

5. R1 busca la dirección IP del siguiente salto de 192.168.2.2 en su caché ARP para su interfaz FastEthernet 0/1. Si la entrada no se encuentra en el caché ARP, R1 envía una solicitud de ARP desde su interfaz FastEthernet 0/1. R2 envía a cambio una respuesta ARP. Luego, R1 actualiza su caché ARP con una entrada para 192.168.2.2 y la dirección MAC asociada.

6. El paquete IP ahora se encapsula en una nueva trama de Ethernet y se envía desde la interfaz FastEthernet 0/1 de R1.




**Paso 3: El paquete llega al router R2**

Haga clic en Reproducir para visualizar la animación.

1. El router R2 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, FastEthernet 0/0. Por lo tanto, R1 copiará la trama en su búfer.

2. R2 observa que el campo Tipo de Ethernet es 0x800, lo cual significa que la trama de Ethernet contiene un paquete IP en la porción de datos de la trama.

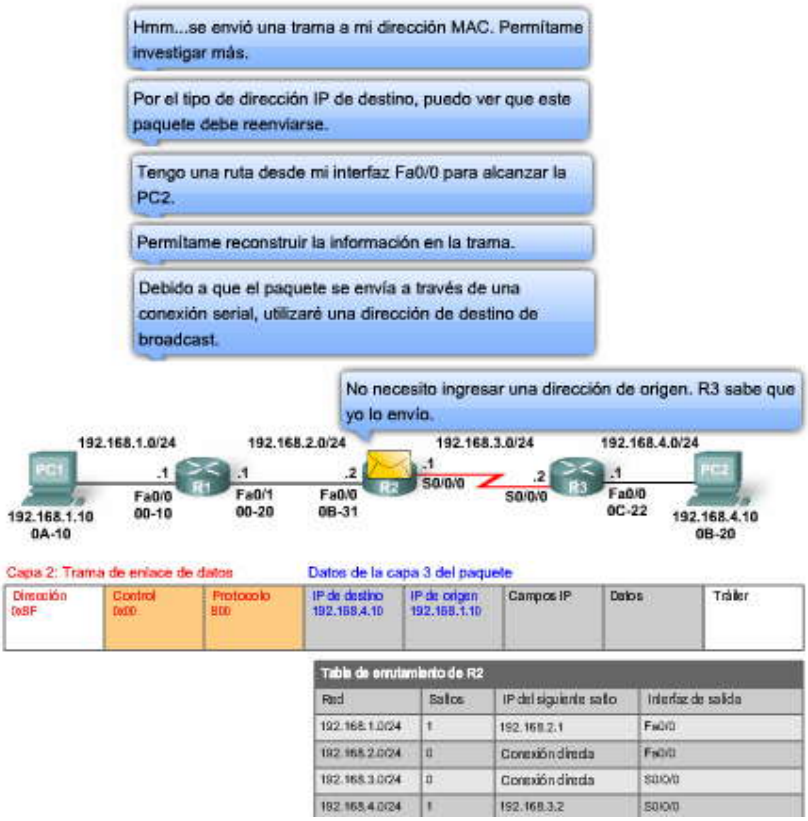
3. R2 desencapsula la trama de Ethernet.

4. Dado que la dirección IP de destino del paquete no coincide con ninguna de las direcciones de interfaz de R2, el router consulta su tabla de enrutamiento para enrutar este paquete. R2 busca la dirección IP de destino del paquete en la tabla de enrutamiento utilizando el mismo proceso que siguió R1.

La tabla de enrutamiento de R2 tiene una trayectoria hacia la ruta 192.168.4.0/24, con una dirección IP del siguiente salto de 192.168.3.2 y una interfaz de salida de Serial 0/0/0. Dado que la interfaz de salida no es una red Ethernet, R2 no tiene que resolver la dirección IP del siguiente salto con una dirección MAC de destino.

Cuando la interfaz es una conexión serial punto a punto, R2 encapsula el paquete IP en el formato de trama de enlace de datos adecuado utilizado por la interfaz de salida (HDLC, PPP, etc.). En este caso, la encapsulación de Capa 2 es PPP; por lo tanto, la dirección de destino del enlace de datos se configura en broadcast. Recuerde que no existen direcciones MAC en las interfaces seriales.

5. El paquete IP se encapsula ahora en una nueva trama de enlace de datos, PPP, y se envía desde la interfaz de salida serial 0/0/0.




**Paso 4: El paquete llega a R3.**

1. R3 recibe y copia la trama PPP de enlace de datos en su búfer.

2. R3 desencapsula la trama PPP de enlace de datos.

3. R3 busca la dirección IP de destino del paquete en la tabla de enrutamiento. El resultado de búsqueda en la tabla de enrutamiento es una de las redes de R3 conectadas directamente. Esto significa que el paquete puede enviarse directamente al dispositivo de destino y no es necesario enviarlo a otro router.

Dado que la interfaz de salida es una red Ethernet conectada directamente, R3 debe resolver la dirección IP de destino del paquete con una dirección MAC de destino.

4. R3 busca la dirección IP de destino del paquete de 192.168.4.10 en su caché ARP. Si la entrada no se encuentra en el caché ARP, R3 envía una solicitud de ARP desde su interfaz FastEthernet 0/0. La PC2 envía a cambio una respuesta ARP con su dirección MAC. R3 actualiza su caché ARP con una entrada para 192.168.4.10 y la dirección MAC recibida en la respuesta ARP.

5. El paquete IP se encapsula en una nueva trama de enlace de datos Ethernet y se envía desde la interfaz FastEthernet 0/0 de R3.

Paso 5: La trama de Ethernet llega a la PC2 con el paquete IP encapsulado.

1. La PC2 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, su NIC Ethernet. Por lo tanto, la PC2 copiará el resto de la trama en su búfer.

2. La PC2 observa que el campo Tipo de Ethernet es 0x800, lo cual significa que la trama de Ethernet contiene un paquete IP en la porción de datos de la trama.

3. La PC2 desencapsula la trama de Ethernet y envía el paquete IP al proceso IP de su sistema operativo.

Resumen

Hemos analizado el proceso de encapsulación y desencapsulación de un paquete al enviarlo de un router a otro, desde el dispositivo de origen hasta el dispositivo de destino final. También hemos analizado el proceso de búsqueda en la tabla de enrutamiento que se abordará con más profundidad en un capítulo posterior. Hemos visto que los routers no sólo tienen participación en las decisiones de enrutamiento de Capa 3, sino que además participan en procesos de Capa 2, entre ellos la encapsulación, y en redes Ethernet, ARP. Los routers también participan en la Capa 1 que se usa para transmitir y recibir los bits de datos a través del medio físico.

Las tablas de enrutamiento contienen tanto redes remotas como conectadas directamente. Los routers saben hacia dónde enviar los paquetes destinados a otras redes, entre ellas Internet, porque contienen direcciones para redes remotas en sus tablas de enrutamiento. En los próximos capítulos aprenderemos cómo los routers construyen y mantienen estas tablas de enrutamiento, ya sea mediante el uso de rutas estáticas ingresadas en forma manual o a través del uso de protocolos de enrutamiento dinámico.

## 1.5 PRACTICAS DE LABORATORIO.-

### 1.5.1 CABLEADO DE RED Y CONFIGURACION BÁSICA DEL ROUTER.-

### 1.5.2 CONFIGURACION BÁSICA DE ROUTER.-

### 1.5.3 DESAFIO DE CONFIGURACION DEL ROUTER.-

## 1.6 RESUMEN.-

### 1.6.1 RESUMEN Y REVISION.-

**Resumen**

Este capítulo fue una presentación del router. Los routers son computadoras e incluyen muchos de los componentes de hardware y software que se encuentran en una PC típica, como por ejemplo CPU, RAM, ROM y un sistema operativo.

El objetivo principal de un router es conectar múltiples redes y enviar paquetes desde una red a la siguiente. Esto significa que un router normalmente tiene múltiples interfaces. Cada interfaz es un miembro o host en una red IP diferente.

El router tiene una tabla de enrutamiento, que es una lista de redes conocidas por el router. La tabla de enrutamiento incluye direcciones de red para sus propias interfaces que son las redes conectadas directamente, además de direcciones de red para redes remotas. Una red remota es una red a la que se puede llegar únicamente mediante el envío del paquete a otro router.

Las redes remotas se incorporan a la tabla de enrutamiento de dos maneras: si el administrador de red configura las rutas estáticas en forma manual o al implementar un protocolo de enrutamiento dinámico. Las rutas estáticas no tienen tanta sobrecarga como los protocolos de enrutamiento dinámico; sin embargo, las rutas estáticas requieren más mantenimiento si la topología es inestable o está en constante cambio.

Los protocolos de enrutamiento dinámico automáticamente ajustan los cambios sin intervención alguna del administrador de red. Los protocolos de enrutamiento dinámico requieren más procesamiento de la CPU y además usan una cierta cantidad de capacidad de enlace para mensajes y actualizaciones de enrutamiento. En muchos casos, una tabla de enrutamiento tendrá tanto rutas estáticas como dinámicas.

Los routers toman su decisión principal de envío en la Capa 3, la capa de Red. Sin embargo, las interfaces del router participan en las Capas 1, 2 y 3. Los paquetes IP de Capa 3 se encapsulan en una trama de enlace de datos de Capa 2 y se codifican en bits en la Capa 1. Las interfaces del router participan en procesos de Capa 2 asociados con la encapsulación. Por ejemplo, una interfaz Ethernet en un router participa en el proceso ARP como otros hosts en esa LAN.

En el próximo capítulo, examinaremos la configuración de rutas estáticas e introduciremos la tabla de enrutamiento IP.

## 1.7 EXAMEN DE CAPITULO.-

### 1.7.1 EXAMEN DEL CAPITULO.-

# CAPITULO II – "ENRUTAMIENTO ESTATICO"

## 2.0 INTRODUCCION DEL CAPITULO.-

### 2.0.1 INTRODUCCION DEL CAPITULO.-

**Introducción del capítulo**

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de origen a destino. Los routers son dispositivos que se encargan de transferir paquetes de una red a la siguiente.

Como se enseñó en el capítulo anterior, los routers aprenden sobre redes remotas ya sea de manera dinámica, utilizando protocolos de enrutamiento, o de manera manual, utilizando rutas estáticas. En muchos casos, los routers utilizan una combinación de protocolos de enrutamiento dinámico y rutas estáticas. Este capítulo se enfoca en el enrutamiento estático. Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que, según veremos, requieren los protocolos de enrutamiento dinámico.
En este capítulo, seguiremos una topología de muestra a medida que configuremos rutas estáticas y aprendamos técnicas de resolución de problemas. En el proceso, examinaremos varios comandos IOS clave y los resultados que muestran. También presentaremos la tabla de enrutamiento utilizando redes conectadas directamente y rutas estáticas.
A medida que realiza las actividades del Packet Tracer relacionadas con estos comandos, tómese el tiempo necesario para probar dichos comandos y analizar los resultados. En poco tiempo podrá leer las tablas de enrutamiento de manera natural.

**En este capítulo, aprenderá a:**

- Definir la función general que tiene un router en las redes.
- Describir las redes conectadas directamente y las diferentes interfaces del router.
- Examinar las redes conectadas directamente en la tabla de enrutamiento y utilizar el protocolo CDP.
- Describir las rutas estáticas con las interfaces de salida.
- Describir las rutas de resumen y por defecto.
- Examinar de qué manera se reenvían los paquetes cuando se utilizan rutas estáticas.
- Identificar de qué manera se administran las rutas estáticas y se resuelven problemas en éstas.

## 2.1 ROUTER Y REDES.-

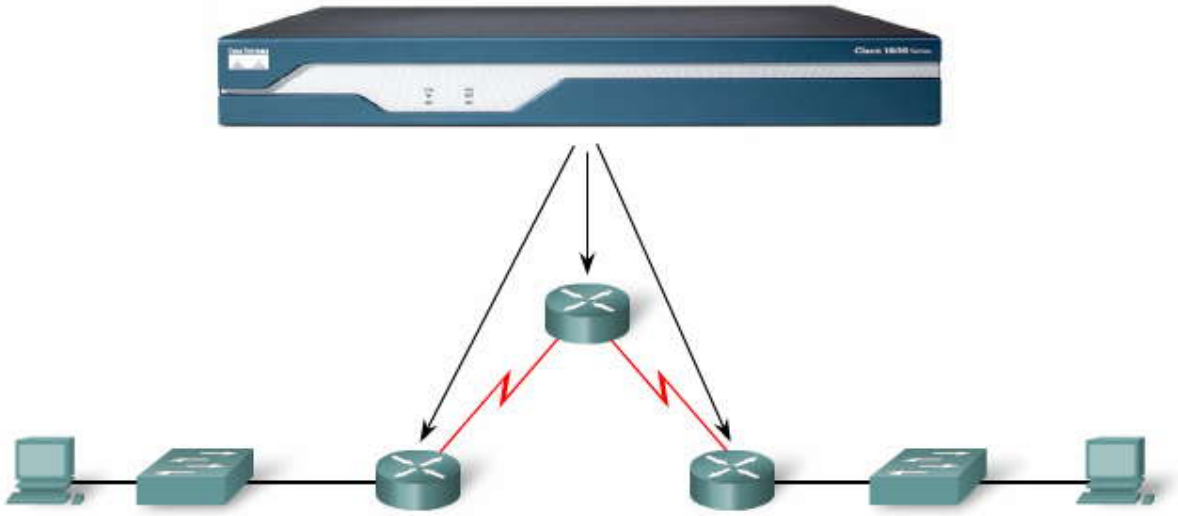
### 2.1.1 FUNCION DEL ROUTER.-

**Función del router**

El router es una computadora diseñada para fines especiales que desempeña una función clave en el funcionamiento de cualquier red de datos. Los routers son los principales responsables de la interconexión de redes por medio de:

- la determinación de la mejor ruta para enviar paquetes
- el envío de paquetes a su destino.

Los routers envían paquetes al aprender sobre redes remotas y al mantener la información de enrutamiento. El router es la unión o intersección que conecta múltiples redes IP. La principal decisión de envío de los routers se basa en la información de Capa 3, la dirección IP de destino.
La tabla de enrutamiento del router se utiliza para encontrar la mejor coincidencia entre la dirección IP de destino de un paquete y una dirección de red en la tabla de enrutamiento. La tabla de enrutamiento determinará finalmente la interfaz de salida para enviar el paquete y el router lo encapsulará en la trama de enlace de datos apropiada para dicha interfaz de salida.



### 2.1.2 INTRODUCCION DE LA TOPOLOGIA.-

**Introducción de la topología**

La figura muestra la topología utilizada en este capítulo. La topología está compuesta por tres routers, denominados R1, R2 y R3. Los routers R1 y R2 se conectan a través de un enlace WAN y los routers R2 y R3 se conectan a través de otro enl ace WAN. Cada router está conectado a una LAN Ethernet diferente, representada por un switch y una PC.

Cada router en este ejemplo es un Cisco 1841. Un router Cisco 1841 tiene las siguientes interfaces:

- Dos interfaces FastEthernet, FastEthernet 0/0 y FastEthernet 0/1
- Dos interfaces seriales, Serial 0/0/0 y Serial0/0/1

Si bien las interfaces de sus routers pueden variar en los de tipo 1841, deberá poder seguir las instrucciones de este capítulo con algunas pequeñas modificaciones y completar las prácticas de laboratorio. Las actividades del Packet Tracer también están disponibles durante todo el análisis del enrutamiento estático para que pueda practicar las aptitudes a medida que se presentan. La Práctica de laboratorio 2.8.1, "Configuración básica de la ruta estática", refleja la topología, las configuraciones y los comandos que se analizan en este capítulo.

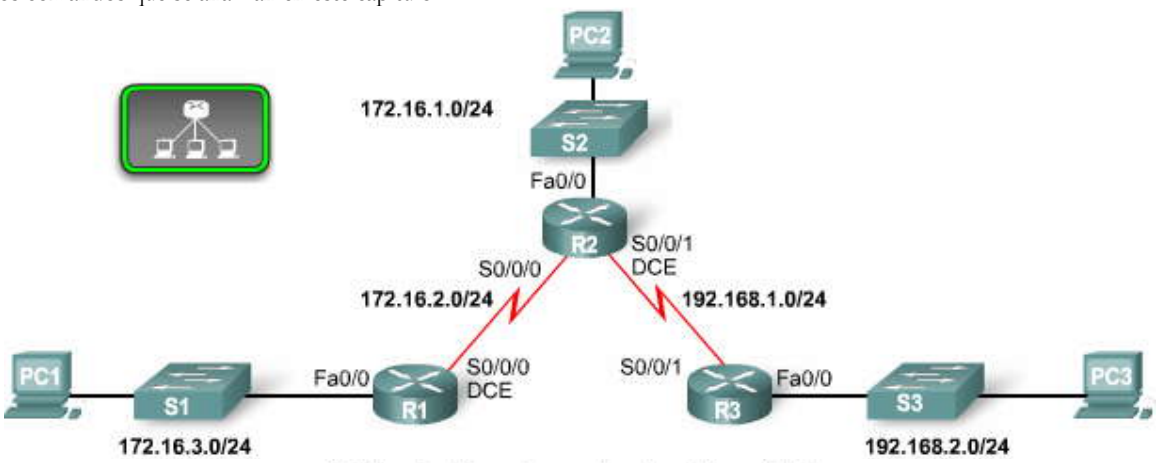



Tabla de direccionamiento del capítulo

| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway por defecto |
|---|---|---|---|---|
| R1 | Fa0/0 | 172.16.3.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 172.16.2.1 | 255.255.255.0 | N/A |
| R2 | Fa0/0 | 172.16.1.1 | 255.255.255.0 | N/A |
| | S0/0/0 | 172.16.2.2 | 255.255.255.0 | N/A |
| | S0/0/1 | 192.168.1.2 | 255.255.255.0 | N/A |
| R3 | Fa0/0 | 192.168.2.1 | 255.255.255.0 | N/A |
| | S0/0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
| PC1 | NIC | 172.16.3.10 | 255.255.255.0 | 172.16.3.1 |
| PC2 | NIC | 172.16.1.10 | 255.255.255.0 | 172.16.1.1 |
| PC3 | NIC | 192.168.2.10 | 255.255.255.0 | 192.168.2.1 |

### 2.1.3 EXAMEN DE CONEXIONES DE ROUTER.-

**Conexiones del router**

La conexión de un router a una red requiere que un conector de interfaz de router esté ac oplado a un conector de cable. Como puede verse en la figura, los routers Cisco admiten diversos tipos de conectores.

**Conectores seriales**

**Haga clic en 1 en la figura.**

Para las conexiones WAN, los routers Cisco admiten los estándares EIA/TIA-232, EIA/TIA-449, V.35, X.21 y EIA/TIA-530 para conectores seriales, como se muestra. No es importante memorizar estos tipos de conexiones. Sólo debe saber que un router tiene un puerto DB-60 que puede admitir cinco estándares de cableado diferentes. Debido a que admite cinco tipos de cableado diferentes, este puerto a veces se denomina puerto serial cinco en uno. El otro extremo del cable serial cuenta con un conector adecuado para uno de los cinco estándares posibles.

**Nota:** La documentación para el dispositivo al que desee conectarse debe indicar el estándar para dicho dispositivo.

**Haga clic en 2 y 3 en la figura.**

Los routers más nuevos admiten la interfaz serial inteligente que permite enviar una mayor cantidad de datos a través de una menor cantidad de pins de cable. El extremo serial del cable serial inteligente es un conector de 26 pins. Es mucho más pequeño que el conector DB-60 que se utiliza para conectarse a un puerto serial cinco en uno. Estos cables de transición admiten los cinco estándares seriales y están disponibles en configuraciones DTE o DCE.

**Nota:** Para obtener una explicación más detallada acerca de DTE y DCE, consulte la Práctica de laboratorio 1.5.1, "Cableado de red y configuración básica de router".

Estas designaciones de cables sólo serán de su interés cuando configure su equipo de laboratorio para simular un entorno "real". En un entorno de producción, usted determina el tipo de cable según el servicio WAN que utilice.

**Conectores Ethernet**

**Haga clic en 4 en la figura.**

Se utiliza un conector diferente en un entorno LAN basado en Ethernet. El conector RJ-45 para el cable de par trenzado no blindado (UTP) es el conector que se utiliza con mayor frecuencia para conectar interfaces LAN. En cada extremo de un cable RJ-45 debe haber ocho tiras de colores o pins. El cable Ethernet utiliza los pins 1, 2, 3 y 6 para transmitir y recibir datos.

Pueden utilizarse dos tipos de cables con interfaces LAN Ethernet:

- un cable de conexión directa con el mismo orden de pins de colores en cada extremo del cable
- un cable de conexión cruzada con el pin 1 conectado al pin 3 y el pin 2 conectado al pin 6

Los cables de conexión directa se utilizan para conectar lo siguiente:

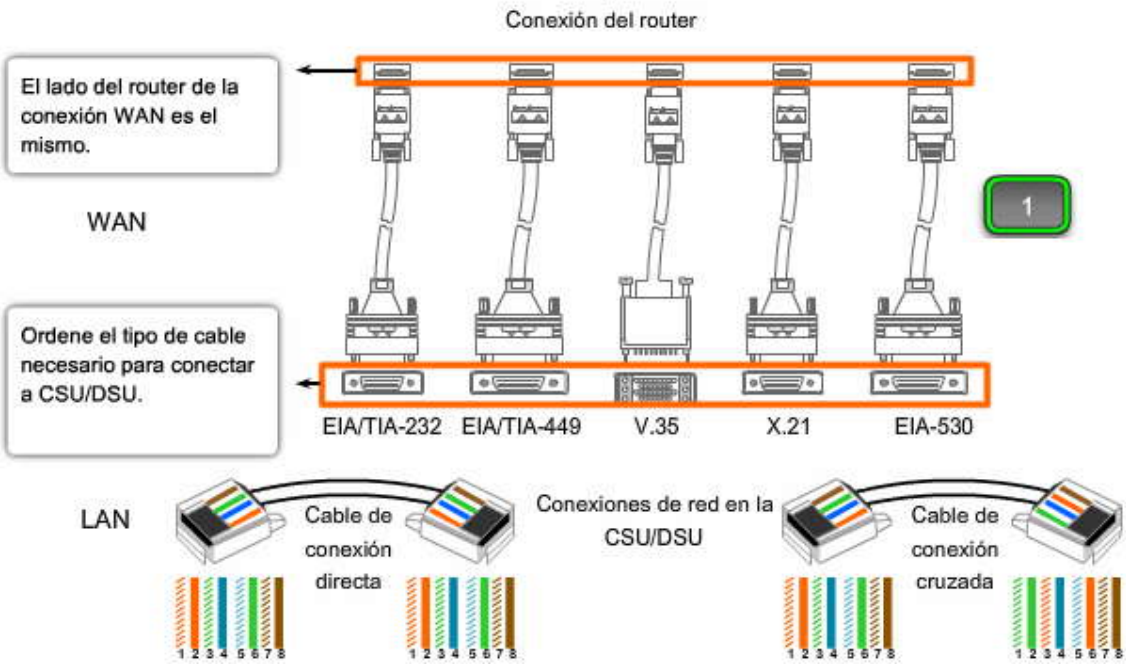
- switch a router,
- switch a PC,
- hub a PC
- hub a servidor

Los cables de conexión cruzada se utilizan para conectar lo siguiente:

- switch a switch,
- PC a PC,
- switch a hub,
- hub a hub,
- router a router
- router a servidor

**Nota:** La conectividad inalámbrica se analizará en otro curso.

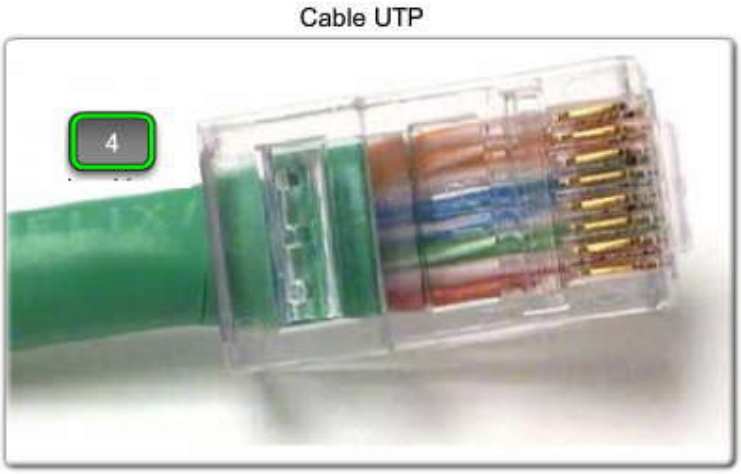
## Conexiones y conectores




Cable serial DTE DB60


Cable serial inteligente DTE DB60


Lado DTE de un cable serial utilizado con las series de router más recientes (1700, 1800, 2600, 2800, etc.)




Cable Ethernet TIA/EIA 568B UTP.

## 2.2 REPASO DE LA CONFIGURACION DEL ROUTER.-

### 2.2.1 EXAMEN DE INTERFACES DEL ROUTER.-

**Examen de interfaces del router**

Como hemos aprendido en el Capítulo 1, el comando show ip route se utiliza para mostrar la tabla de enrutamiento. En principio, la tabla de enrutamiento estará vacía si no se configuró ninguna interfaz.

Como se puede ver en la tabla de enrutamiento para R1, no se configuró ninguna interfaz con una dirección IP y máscara de subred.

**Nota:** Las rutas estáticas y dinámicas no se agregarán a la tabla de enrutamiento hasta que las interfaces locales adecuadas, también conocidas como interfaces de salida, se hayan configurado en el router. Este procedimiento se analizará con más profundidad en los siguientes capítulos.

**Interfaces y su estado**

Puede examinarse el estado de cada interfaz utilizando diversos comandos.

**Haga clic en show interfaces en la figura.**

El comando **show interfaces** muestra el estado y proporciona una descripción detallada de todas las interfaces del router. Como puede ver, los resultados del comando pueden ser un tanto extensos. Para ver la mis ma información pero para una interfaz específica, como por ejemplo, FastEthernet 0/0, utilice el comando **show interfaces** con un parámetro que especifique la interfaz. Por ejemplo:

R1**#show interfaces fastethernet 0/0**
FastEthernet0/0 is administratively down, line protocol is down

Observe que la interfaz **está administrativamente inactiva** y que **el protocolo de línea está desactivado**. "Administratively down" significa que la interfaz se encuentra actualmente en modo inactivo o apagada. "Line protocol is down" significa en este caso que la interfaz no recibe una señal portadora de un switch o del hub. Esta condición también puede deberse al hecho de que la interfaz se encuentra en modo inactivo.

Observará que el comando **show interfaces** no muestra ninguna dirección IP de las interfaces de R1. Esto se debe a que todavía no hemos configurado las direcciones IP de ninguna de las interfaces.

**Comandos adicionales para examen de estado de interfaz**

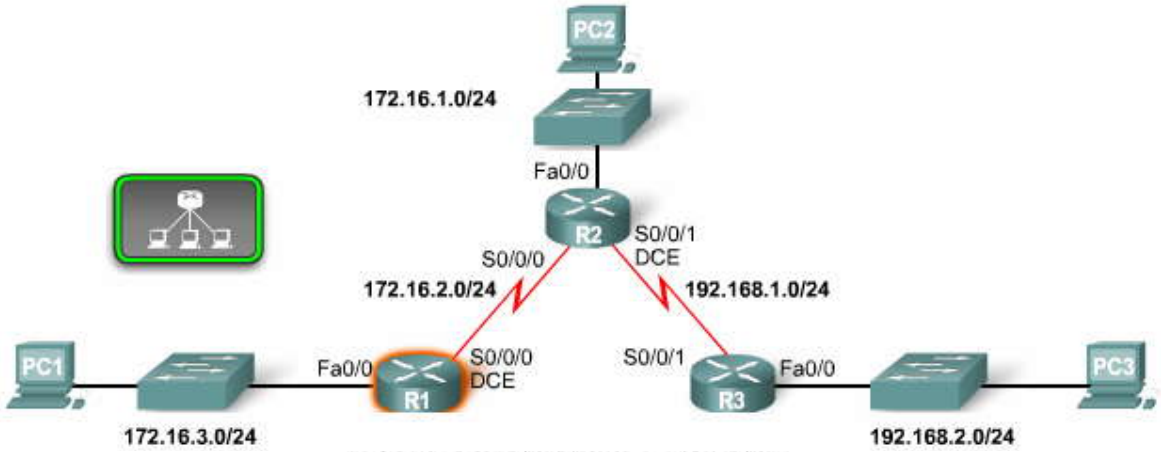
**Haga clic en show interface brief en la figura.**
El comando **show interface brief** puede utilizarse para ver una parte de la información de la interfaz en formato condensado.

**Haga clic en show running-config en la figura.**

El comando **show running-config** muestra el archivo de configuración actual que utiliza el router. Los comandos de configuración se almacenan temporalmente en el archivo de configuración en ejecución y el router los implementa de inmediato. El uso de este comando es otra manera de verificar el estado de una interfaz, como FastEthernet 0/0.

R1#**show running-config**
<some output omitted>
interface FastEthernet0/0
no ip address
shutdown
<some output omitted>

Sin embargo, la utilización de **show running-config** no es necesariamente la mejor manera de verificar las configuraciones de las interfaces. Utilice el **comando show ip interface brief** para verificar rápidamente que las interfaces estén **up** y **up** (es decir, que estén **activadas** por el administrador y que el protocolo de línea esté **activado**).




La tabla de enrutamiento no tiene rutas

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R1#
```

show ip route

Con **show interfaces** se puede acceder a información detallada sobre la interfaz

```
R1#show interfaces
FastEthernet0/0 is administratively down, line protocol is down
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

show interfaces

Con **show ip interface brief** se puede acceder al resumen del estado de la interfaz

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            unassigned      YES manual administratively down down
Serial0/0/0                unassigned      YES unset  administratively down down
FastEthernet0/1            unassigned      YES unset  administratively down down
Serial0/0/1                unassigned      YES unset  administratively down down
```

show ip interface brief

```
R1#show running-config
!
version 12.3
!
hostname R1
!
!
enable secret 5 $1$.3RO$VLUOdBF2OqNBn0EjQBvR./
!
!
interface FastEthernet0/0
 mac-address 000c.3010.9260
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
```

show running-config

### 2.2.2 CONFIGURACION DE U INTERFAZ ETHERNET.-

**Configuración de una interfaz Ethernet**

Como se mostró anteriormente, R1 todavía no tiene ninguna ruta. Agreguemos una ruta configurando una interfaz y explorando exactamente qué sucede cuando se activa la interfaz. Por defecto, todas las interfaces del router están **desactivadas** o apagadas. Para activar esta interfaz, utilice el comando **no shutdown**, que cambia el estado de la interfaz de **administrativamente inactiva** a **conectada**.

R1(config)#**interface fastethernet 0/0**
R1(config-if)#**ip address 172.16.3.1 255.255.255.0**
R1(config-if)#**no shutdown**

El IOS muestra el siguiente mensaje:

*Mar 1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Estos dos mensajes son importantes. El primer mensaje **changed state to up** indica que la conexión es físicamente buena. Si no obtiene este primer mensaje, asegúrese de que la interfaz esté conectada correctamente a un switch o hub.

**Nota:** Si bien está habilitada con **no shutdown**, la interfaz Ethernet no estará activa o **up** a menos que reciba una señal portadora de otro dispositivo (switch, hub, PC u otro router).

El segundo mensaje changed state to **up** indica que la capa de Enlace de datos funciona. En interfaces LAN, no rmalmente no cambiamos los parámetros de la capa de Enlace de datos. Sin embargo, las interfaces WAN en un entrono de laboratorio requieren temporización de un lado del enlace, como se analizó en la Práctica de laboratorio 1.5.1, "Cableado de red y configuración básica de router". También se abordará más adelante en la sección "Configuración de una interfaz serial". Si configura correctamente la frecuencia del reloj, el protocolo de línea (la capa de Enlace de datos) no cambiará a up.

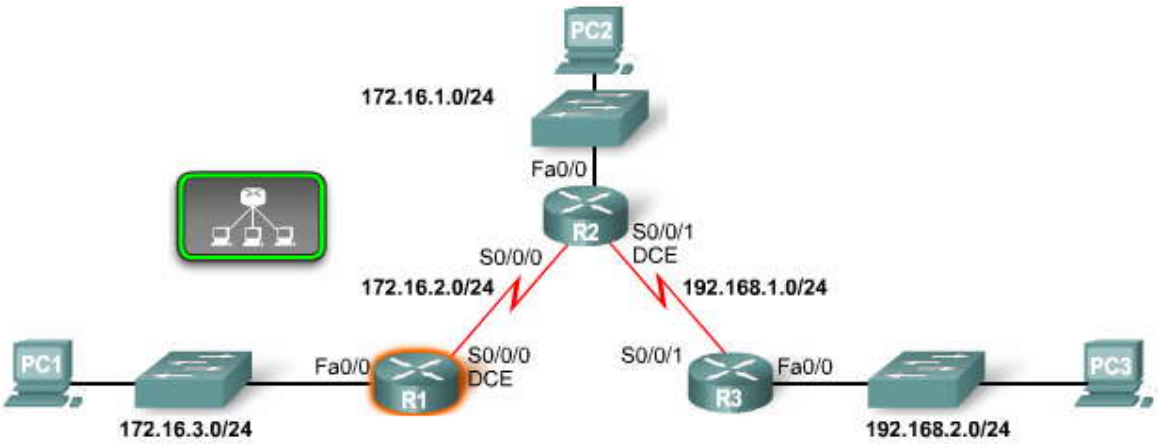
**Mensajes no solicitados de IOS**

**Haga clic en Mensajes no solicitados de IOS en la figura.**

El IOS a menudo envía mensajes no solicitados similares a los mensajes **changed state to up** que acabamos de analizar. Como se puede ver en la figura, a veces estos mensajes se mostrarán cuando esté escribiendo un comando, como por ejemplo, cuando configura una descripción para la interfaz. El mensaje de IOS no afecta el comando, pero puede llegar a perder su ubicación cuando escribe.

**Haga clic en Conexión en modo síncrono en la figura.**

Para mantener los resultados no solicitados separados de sus entradas, ingrese al modo de configuración de línea para el puerto de consola y agregue el comando **logging synchronous**, como se muestra. Verá que los mensajes de IOS ya no interfieren con su escritura.




La tabla de enrutamiento no tiene rutas

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R1#
```

show ip route

Entrada de comando interrumpida por IOS

```
R1(config)#int fa0/0
R1(config-if)#ip address 172.16.3.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#descri
*Mar  1 01:16:08.212: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 01:16:09.214: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to upption
R1(config-if)#
```

Mensaje no solicitado de IOS

El comando `description` se interrumpió por mensajes no solicitados del IOS.


**Lectura de la tabla de enrutamiento**

Vea la tabla de enrutamiento que se muestra en la figura. Observe que R1 ahora tiene una interfaz FastEthernet 0/0 "conectada directamente" como una red nueva. La interfaz se configuró con la dirección IP 172.16.3.1/24, lo que hace que sea miembro de la red 172.16.3.0/24.

Examine la siguiente línea de resultados de la tabla:

C 172.16.3.0 is directly connected, FastEthernet0/0

La **C** al comienzo de la ruta indica que es una red conectada directamente. En otras palabras, R1 tiene una interfaz que pertenece a esta red. El significado de C se define en la lista de códigos de la parte superior de la tabla de enrutamiento.

La máscara de subred /**24** para esta ruta se muestra en la línea que se encuentra sobre la ruta real.

172.16.0.0/24 is subnetted, 1 subnets
C 172.16.3.0 is directly connected, FastEthernet0/0

**Los routers generalmente almacenan direcciones de red**

Salvo por muy pocas excepciones, las tablas de enrutamiento tienen rutas para direcciones de red en lugar de direcciones host individuales. La ruta 172.16.3.0/24 de la tabla de enrutamiento significa que esta ruta coincide con todos los paquetes con una dirección de destino perteneciente a esta red. El hecho de que una sola ruta represente toda una red de direcciones IP host hace que la tabla de enrutamiento sea más pequeña y tenga menos rutas, logrando una mayor rapidez al buscar en la tabla de enrutamiento. La tabla de enrutamiento puede contener las 254 direcciones IP host individuales para la red 172.16.3.0/24, pero es una manera ineficiente de almacenar direcciones.

Un directorio telefónico es una buena analogía para la estructura de una tabla de enrutamiento. El directorio telefónico es una lista de nombres y números de teléfono ordenados por orden alfabético según el apellido. Cuando buscamos un número, podemos asumir que cuanto menos nombres haya en el directorio, más rápido será encontrar un determinado nombre. Será mucho más fácil buscar en un directorio telefónico de 20 páginas con aproximadamente 2000 entradas que en uno de 200 páginas con 20 000 entradas.

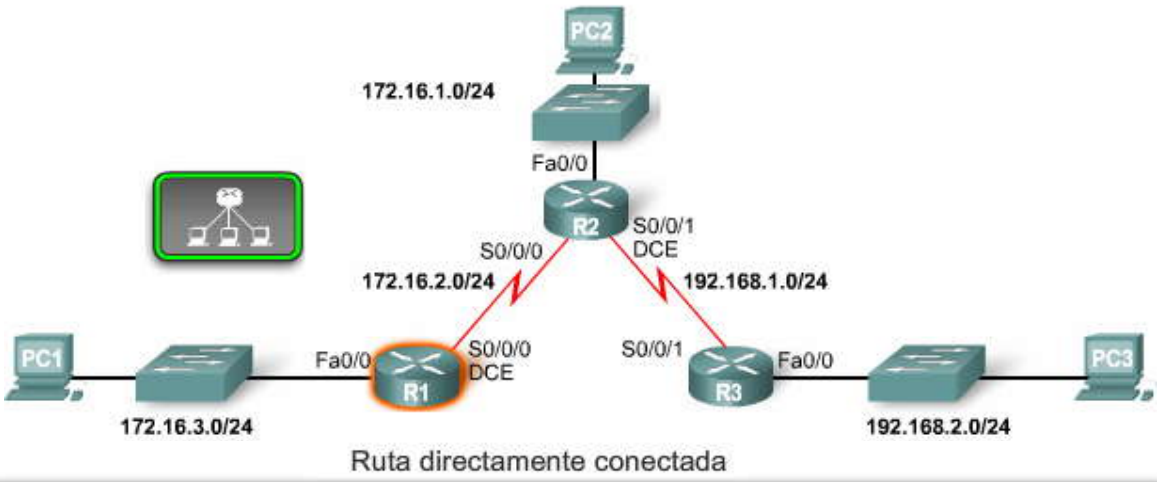
El directorio telefónico sólo contiene una entrada para cada número de teléfono. Por ejemplo, la familia Stanford puede encontrarse como:

**Stanford, Harold, 742 Evergreen Terrace, 555-1234**

Ésta es la única entrada para todos los que vivan en este domicilio y tengan el mismo número de teléfono. El directorio telefónico podría contener una entrada para cada persona, pero esto aumentaría el tamaño del directorio. Por ejemplo, podría haber entradas separadas para Harold Stanford, Margaret Stanford, Brad Stanford, Leslie Stanford y Maggie Stanford, todos con la misma dirección y el mismo número de teléfono. Si se hiciera esto para cada familia, el directorio sería más grande y tardaríamos más en buscar un número.

Las tablas de enrutamiento funcionan de la misma manera: una entrada en la tabla representa una "familia" de dispositivos que comparten la misma red o espacio de dirección (la diferencia entre una red y un espacio de dirección será más clara a medida que avance en el curso). Cuanto menos entradas tenga la tabla de enrutamiento, más rápido será el proceso de búsqueda. Para que las tablas de enrutamiento sigan siendo pequeñas, se enumeran las direcciones de red con máscaras de subred en lugar de las direcciones IP host individuales.

**Nota:** A veces se ingresa una "ruta host" en la tabla de enrutamiento que representa una dirección IP host individual. Se enumera con la dirección IP host del dispositivo y una máscara de subred /32 (255.25 5.255.255). El tema de las rutas host se analizará en otro curso.




```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, FastEthernet0/0
R1#
```

Ahora R1 tiene una red conectada.

### 2.2.3 VERIFICACION DE UNA INTERFAZ ETHERNET.-

**Comandos para verificar la configuración de la interfaz**

El comando **show interfaces fastethernet 0/0** en la figura muestra ahora que la interfaz está **up** y el protocolo de línea está **up**. El comando **no shutdown** cambió la interfaz de **administratively down** a **up**. Observe que ahora aparece la dirección IP.

Haga clic en **show ip interface brief** en la figura.

El comando **show ip interface brief** también verifica esta información. Debajo del estado y el protocolo, debería ver "up". El comando **show running-config** muestra la configuración actual de esta interfaz. Cuando la interfaz está desactivada, el comando **running-config** muestra **shutdown**. Sin embargo, cuando la interfaz está activada, no se muestra **no shutdown**.

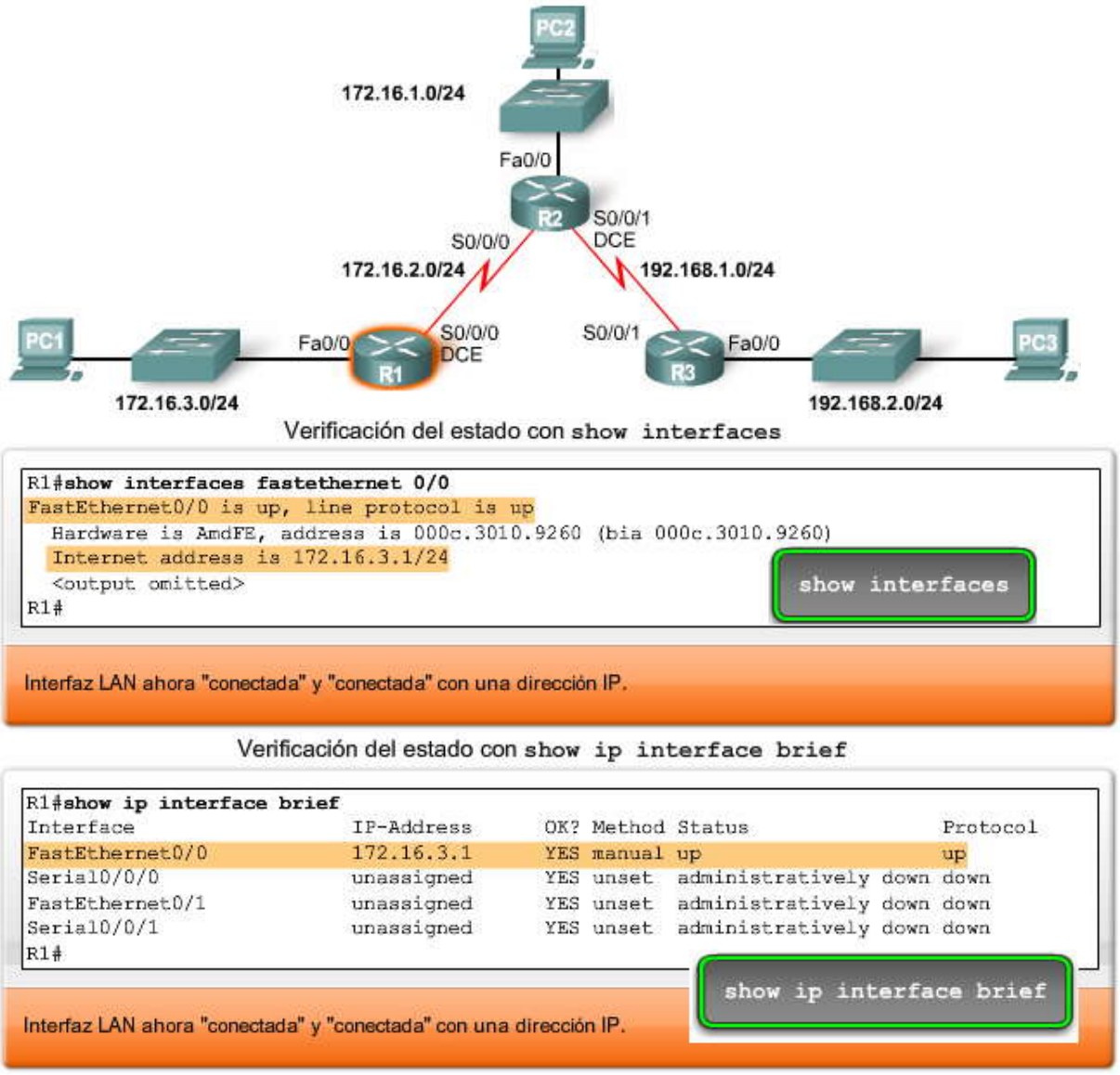
R1#**show running-config**
<output omitted>
interface FastEthernet0/0
ip address 172.16.3.1 255.255.255.0
<output omitted>

Como se explicó en el Capítulo 1, un router no puede tener múltiples interfaces que pertenezcan a la misma subred IP. Cada interfaz debe pertenecer a una subred separada. Por ejemplo, un router no puede tener su interfaz FastEthernet 0/0 configurada como máscara y dirección 172.16.3.1/24 y su interfaz FastEthernet 0/1 configurada como 172.16.3.2/24.

El IOS mostrará el siguiente mensaje de error si intenta configurar la segunda interfaz con la misma subred IP que la primera interfaz:

R1(config-if)**#int fa0/1**
R1(config-if)**#ip address 172.16.3.2 255.255.255.0**
172.16.3.0 overlaps with FastEthernet0/0
R1(config-if)#

Generalmente, la interfaz Ethernet o FastEthernet del router será la dirección IP del gateway por defecto para cualquier dispositivo de esa LAN. Por ejemplo, la PC1 podría configurarse con una dirección IP host que pertenezca a la red 172.16.3.0/24 con la dirección IP del gateway por defecto 172.16.3.1. 172.16.3.1 es la dirección IP FastEthernet del router R1. Recuerde que la interfaz Ethernet o FastEthernet de un router también participará en el proceso ARP como miembro de esa red Ethernet.



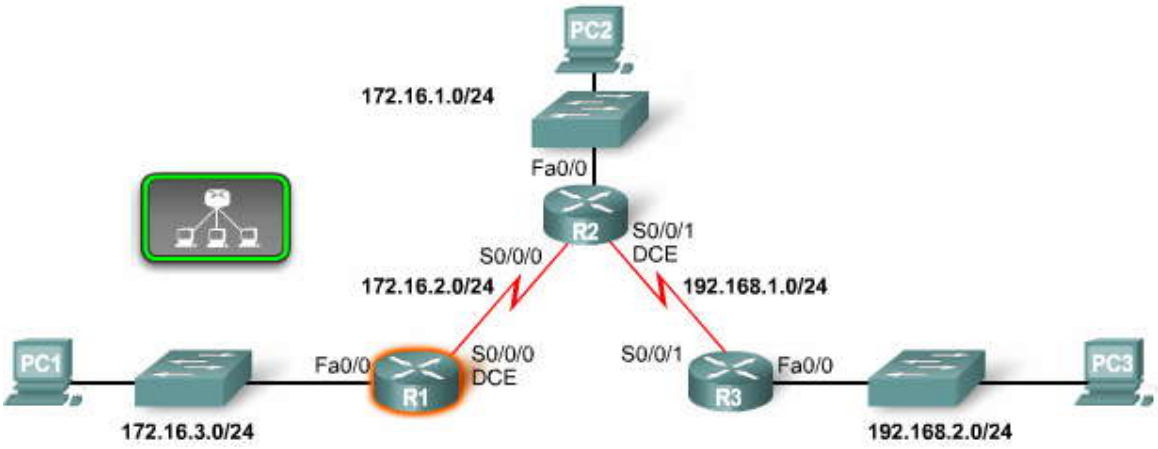

**Las interfaces Ethernet participan en el ARP**

La interfaz Ethernet de un router participa en una red LAN al igual que cualquier otro dispositivo de esa red. Esto significa que estas interfaces tienen una dirección MAC de Capa 2, como se muestra en la figura. El comando **show interfaces** muestra la dirección MAC para las interfaces Ethernet.

R1#**show interfaces fastethernet 0/0**

Como se demostró en el Capítulo 1, una interfaz Ethernet participa en las solicitudes y respuestas de ARP y man tiene una tabla ARP. Si un router tiene un paquete destinado a un dispositivo en una red Ethernet conectada directamente, éste busca en la tabla ARP una entrada con esa dirección IP de destino para poder asignarla a la dirección MAC. Si la tabla ARP no contiene esta dirección IP, la interfaz Ethernet envía una solicitud de ARP. El dispositivo con la dirección IP de destino

envía a cambio una respuesta de ARP que contiene su dirección MAC. La información de la dirección IP y de la dirección MAC se agrega entonces a la tabla ARP para esa interfaz Ethernet. Ahora el router puede encapsular el paquete IP en una trama de Ethernet con la dirección MAC de destino de su tabla ARP. La trama de Ethernet, con el paquete encapsulado, se envía entonces a través de la interfaz Ethernet.




Verificando las direcciones MAC en interfaces Ethernet

```
R1#show interfaces fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3010.9260 (bia 000c.3010.9260)
  Internet address is 172.16.3.1/24
  <output omitted>
R1#
```

Las interfaces Ethernet tienen direcciones MAC.

### 2.2.4 CONFIGURACION DE UN INTERFAZ SERIAL.-

**Configuración de una interfaz serial**

A continuación configuraremos la interfaz Serial 0/0/0 en el router R1. Esta interfaz se encuentra en la red 172.16.2.0/24 y se le asigna la dirección IP y la máscara de subred de 172.16.2.1/24. El proceso que utilizamos para la configuración de la interfaz serial 0/0/0 es similar al proceso que utilizamos para configurar la interfaz FastEthernet 0/0.

R1(config)#**interface serial 0/0/0**
R1(config-if)#**ip address 172.16.2.1 255.255.255.0**
R1(config-if)#**no shutdown**

Después de haber ingresado estos comandos, el estado de la interfaz serial puede variar según el tipo de conexión WAN. Este tema se analizará luego con más profundidad en otro curso. En este curso, utilizaremos conexiones punto a punto seriales y dedicadas entre dos routers. La interfaz serial se encontrará en estado **up** sólo después de que el otro extremo del enlace serial también haya sido configurado correctamente. Podemos mostrar el estado actual de la interfaz serial 0/0/0 utilizando el comando **show interfaces serial 0/0/0**, como se muestra en la figura.

Como puede verse, el enlace todavía está desactivado. El enlace está desactivado porque todavía no hemos configurado y activado el otro extremo del enlace serial.

R1#**show interfaces serial 0/0/0**
Serial0/0/0 is administratively down, line protocol is down

Ahora configuraremos el otro extremo de este enlace, el Serial 0/0/0 para el router R2.

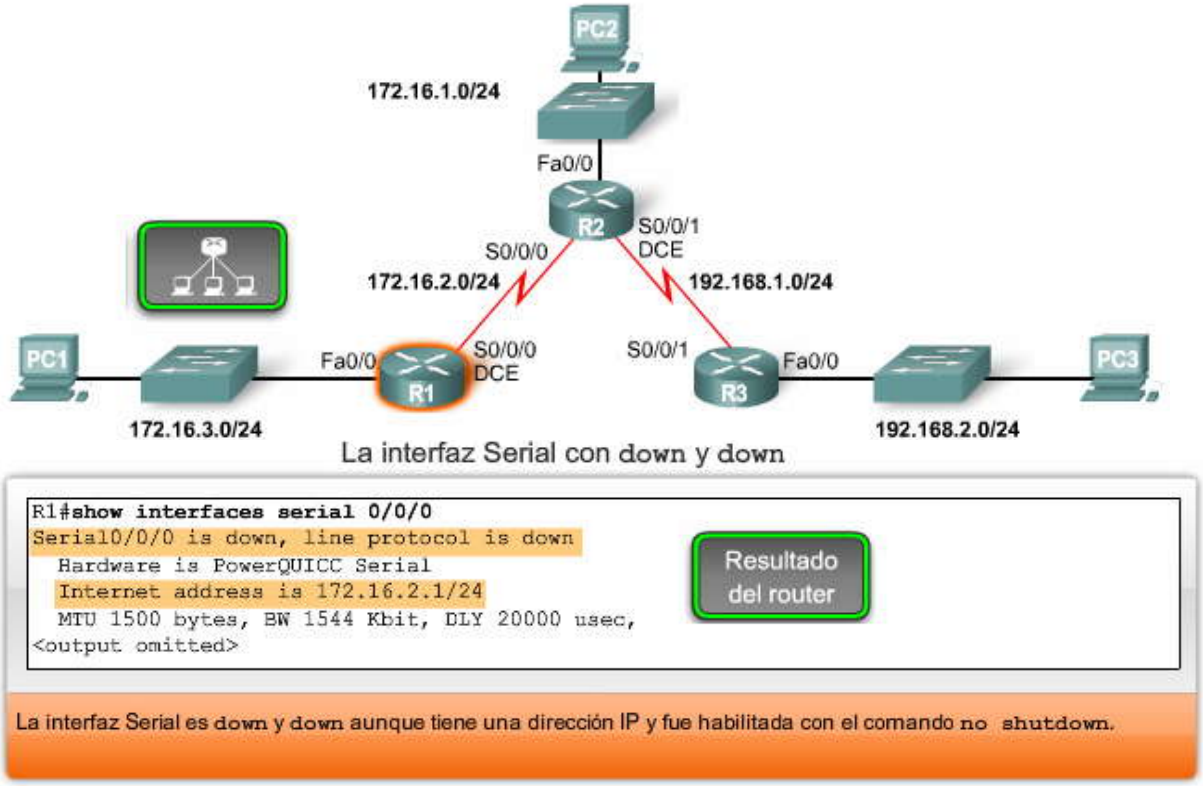
**Nota:** No es necesario que ambos extremos del enlace serial utilicen la misma interfaz, en este caso, Serial 0/0/0. Sin embargo, dado que las dos interfaces son miembros de la misma red, ambas deben tener direcciones IP que pertenezcan a la red 172.16.2.0/24. (Los términos red y subred pueden intercambiarse en este caso). La interfaz Serial 0/0/0 de R2 está configurada con la dirección IP y máscara de subred 172.16.2.2/24.

R2(config)#**interface serial 0/0/0**
R2(config-if)#**ip address 172.16.2.2 255.255.255.0**
R2(config-if)#**no shutdown**

Si ahora ejecutamos el comando **show interfaces serial 0/0/0** en cualquiera de los routers, todavía veremos que el enlace se encuentra up/down.

R2#**show interfaces serial 0/0/0**
Serial0/0/0 is up, line protocol is down
<output omitted>

El enlace físico entre R1 y R2 está up porque ambos extremos del enlace serial se han configurado correctamente con una máscara/dirección IP y activado con el comando **no shutdown**. Sin embargo, el protocolo de línea todavía está **down**. Esto sucede porque la interfaz no recibe una señal de temporización. Existe un comando más que debemos ingresar, el comando **clock rate**, en el router con el cable DCE. El comando **clock rate** configurará la señal de temporización para el enlace. La configuración de la señal de temporización se analizará en la próxima sección.




### 2.2.5 EXAMEN DE INTERFACES DEL ROUTER.-

**Conexión física de una interfaz WAN**

La capa Física WAN describe la interfaz entre el equipo terminal de datos (DTE) y el equipo de terminación de circuitos de datos (DCE). Normalmente el DCE es el proveedor del servicio, mientras que el DTE es el dispositivo conectado. En este modelo, los servicios brindados al DTE se ofrecen a través de un módem o de una CSU/DSU.

Generalmente, el router es el dispositivo DTE y está conectado a una CSU/DSU, que es el dispositivo DCE. La CSU/DSU (dispositivo DCE) se usa para convertir los datos del router (dispositivo DTE) en una forma aceptable para el proveedor de servicio WAN. La CSU/DSU (dispositivo DCE) también es responsable de convertir los datos del proveedor de servicio WAN en una forma aceptable por el router (dispositivo DTE). Generalmente, el router se conecta a la CSU/DSU utilizando un cable DTE serial, como se muestra.

**Las interfaces seriales necesitan una señal de temporización para controlar los tiempos de la comunicación.** En la mayoría de los entornos, el proveedor de servicio (un dispositivo DCE, como por ejemplo una CSU/DSU) proporcionará la temporización. Por defecto, los routers Cisco son dispositivos DTE. Sin embargo, en un entorno de laboratorio, no utilizamos ninguna CSU/DSU y evidentemente no tenemos un proveedor de servicio WAN.

**Coloque el cursor del mouse sobre los cables y los dispositivos para ver cuáles son.**

Conexión CSU/DSU utilizando un cable DTE


Coloque el cursor del mouse sobre los cables y los dispositivos para ver cuáles son.

**Configuración de enlaces seriales en un entorno de laboratorio**

Para los enlaces seriales que están interconectados directamente, al igual que en un entorno de laboratorio, un lado de la conexión debe considerarse como un DCE y proporcionar una señal de temporización. Si bien las interfaces seriales Cisco son dispositivos DTE por defecto, pueden configurarse como dispositivos DCE.

Para configurar un router para que actúe como dispositivo DCE:

1. Conecte el extremo DCE del cable a la interfaz serial.

2. Configure la señal de temporización de la interfaz serial utilizando el comando **clock rate**.

Los cables seriales que se utilizan en el laboratorio son generalmente uno de estos dos tipos:

- un cable de conexión cruzada DTE/DCE, en el que un extremo es DTE y el otro extremo es DCE
- un cable DTE conectado a un cable DCE

En nuestra topología de laboratorio, la interfaz Serial 0/0/0 de R1 está conectada al extremo DCE del cable y la interfaz serial 0/0/0 de R2 está conectada al extremo DTE del cable. Se debe colocar una etiqueta DTE o DCE en el cable.

También puede distinguir el DTE del DCE mirando el conector entre los dos cables. El cable DTE tiene un conector macho, mientras que el cable DCE tiene un conector hembra.

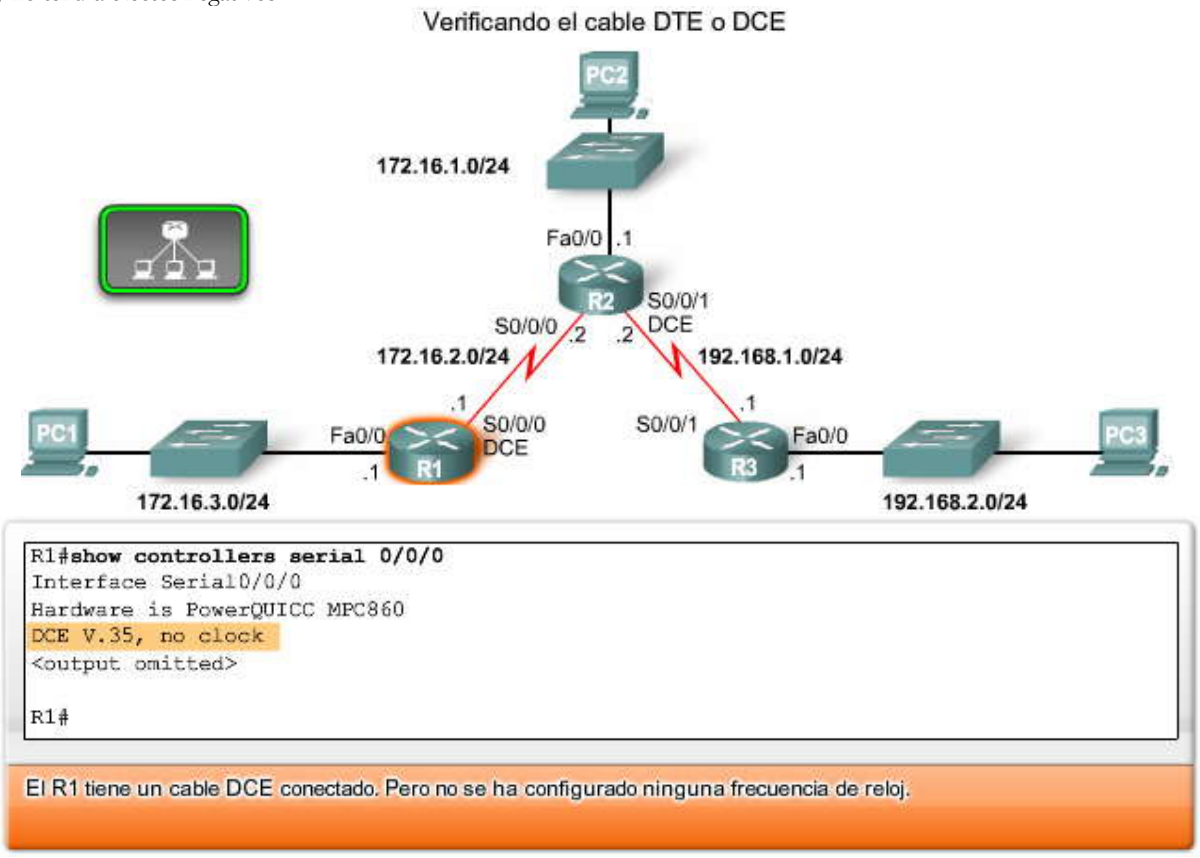
Si se conecta un cable entre los dos routers, puede utilizar el comando **show controllers** para determinar qué extremo del cable está conectado a esa interfaz. En los resultados del comando, observe que R1 tiene el cable DCE conectado a su interfaz serial 0/0 y que la frecuencia de reloj no está configurada.

R1#**show controllers serial 0/0/0**
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, no clock
<output omitted>

Una vez que se conecta el cable, el reloj puede configurarse con el comando **clock rate**. Las frecuencias de reloj disponibles, en bits por segundo, son 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000 y 4000000. Es posible que algunas de estas frecuencias de bit no estén disponibles en algunas interfaces seriales. Debido a que la interfaz Serial 0/0/0 de R1 tiene el cable DCE conectado, configuraremos esa interfaz co n una frecuencia de reloj.

R1(config)#**interface serial 0/0**
R1(config-if)#**clock rate 64000**
01:10:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

**Nota:** Si la interfaz de un router con un cable DTE está configurada con el comando clock rate, el IOS ignorará el comando y no tendrá efectos negativos.




**Verificación de la configuración de la interfaz serial**

Como puede verse en la figura, podemos determinar que el protocolo de línea ahora está activado y verificar esto en ambos extremos del enlace serial utilizando los comandos **show interfaces** y **show ip interface brief**. Recuerde que la interfaz serial sólo estará activada si ambos extremos del enlace están configurados correctamente. En nuestro entorno de laboratorio, hemos configurado la frecuencia de reloj en el extremo con el cable DCE.

También podemos verificar que el enlace esté up/up haciendo ping en la interfaz remota.

R1#**ping 172.16.2.2**

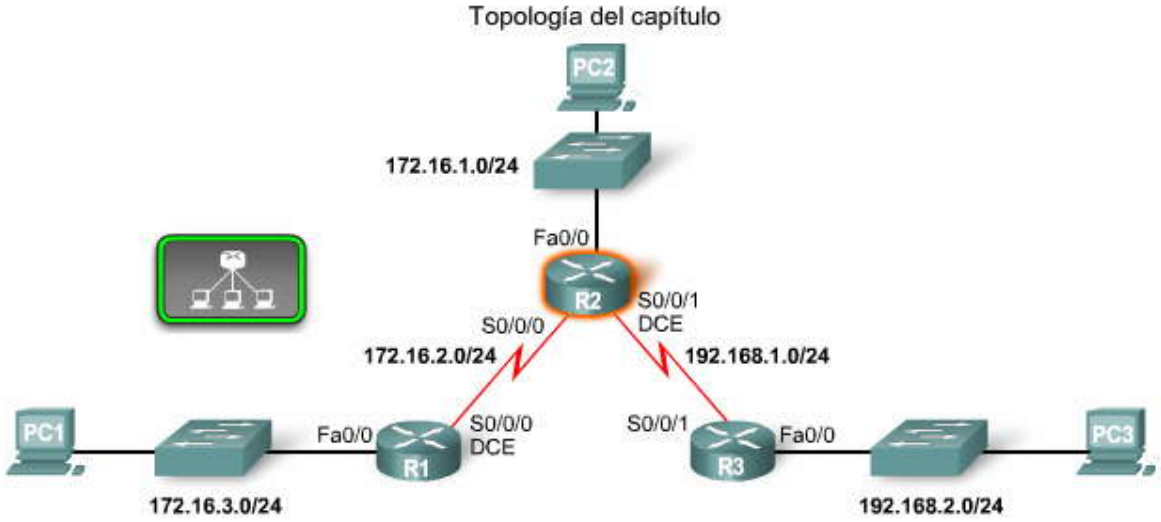
Finalmente, podemos ver la red serial 172.16.2.0/24 en las tablas de enrutamie nto de ambos routers. Si ejecutamos el comando **show ip route** en R1, veremos la ruta conectada directamente para la red 172.16.2.0/24.

R1#**show ip route**

Ahora observe la configuración en ejecución del router R1 utilizando el comando show running -config.

R1#**show running-config**

**Nota:** Si bien el comando **clock rate** contiene dos palabras, el IOS escribe **clockrate** como una sola palabra en los archivos de configuración en ejecución y de configuración de inicio.




```
R1#show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.16.2.1/24
<output omitted>

R1#show ip interface brief
Interface                  IP-Address      OK? Method Status         Protocol
FastEthernet0/0            172.16.3.1      YES manual up                    up
Serial0/0/0                172.16.2.1      YES manual up                    up
<output omitted>
```

Interfaces de R1

```
R1#ping 172.16.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1#
```

R1 hace ping a R2

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
R1#
```

show ip route

```
R1#show run
Building configuration...

Current configuration : 1130 bytes
!
hostname R1
!
<output omitted>
!
interface FastEthernet0/0
 description R1 LAN
 ip address 172.16.3.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R2
 ip address 172.16.2.1 255.255.255.0
 clockrate 64000
```

show run

## 2.3 EXPLORACION DE REDES CONECTADAS DIRECTAMENTE.-

### 2.3.1 VERIFICACION DE LOS CAMBIOS EN LA TABLA DE ENRUTAMIENTO.-

**Conceptos de la tabla de enrutamiento**

Como puede verse en la figura, el comando **show ip route** muestra el contenido de la tabla de enrutamiento. Revisemos el objetivo de una tabla de enrutamiento. Una tabla de enrutamiento es una estructura de datos que almacena información de enrutamiento obtenida de diferentes orígenes. El objetivo principal de una tabla de enrutamiento es proporcionarle al router rutas para llegar a diferentes redes de destino.

La tabla de enrutamiento consiste en una lista de direcciones de red "conocidas", es decir, aquellas direcciones que están conectadas directamente, configuradas estáticamente y que se aprenden dinámicamente. R1 y R2 sólo tienen rutas para redes conectadas directamente.

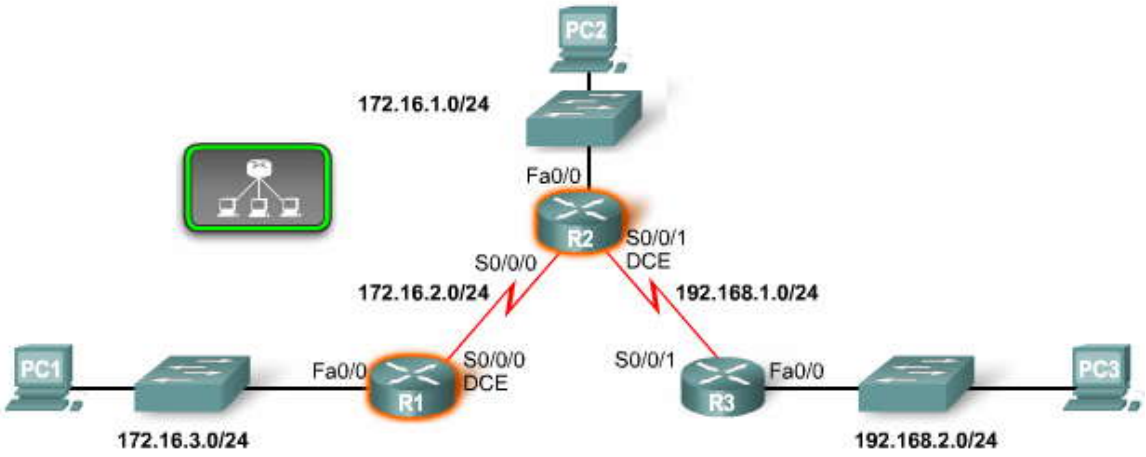



Tabla de enrutamiento actual de R1

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
R1#
```

Tabla de enrutamiento de R1

Tabla de enrutamiento actual de R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Serial0/0/0

R2#
```

Tabla de enrutamiento de R2

**Observación de la incorporación de una ruta a la tabla de enrutamiento**

Ahora estudiaremos detalladamente cómo se agregan y eliminan de la tabla de enrutamiento las rutas conectadas directamente. A diferencia de los comandos **show**, los comandos **debug** pueden utilizarse para controlar las operaciones de routers en tiempo real. El comando **debug ip routing** nos permitirá ver cualquier cambio que realice el router al agregar o eliminar rutas. Configuraremos las interfaces del router R2 y examinaremos este proceso.

Primero, activaremos la depuración con el comando **debug ip routing** para que podamos ver las redes conectadas directamente a medida que se las agrega a la tabla de enrutamiento.

R2#**debug ip routing**
IP routing debugging is on

**Configuración de la dirección IP y la máscara de subred**

A continuación, configuraremos la dirección IP y máscara de subred para la interfaz FastEthernet 0/0 de R2 y utilizaremos el comando no shutdown. Debido que la interfaz FastEthernet se conecta a la red 172.16.1.0/24, debe configurarse con una dirección IP host para esa red.

R2(config)#**interface fastethernet 0/0**
R2(config-if)#**ip address 172.16.1.1 255.255.255.0**
R2(config-if)#**no shutdown**

El IOS mostrará el siguiente mensaje:

02:35:30: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
02:35:31: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Después de ingresar el comando **no shutdown** y que el router determine que la interfaz y el protocolo de línea están en estado **up** y **up**, los resultados de debug muestran que R2 agrega esta red conectada directamente a la tabla de enrutamiento.

02:35:30: RT: add 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
02:35:30: RT: interface FastEthernet0/0 added to routing table

**Haga clic en la Tabla 1 en la figura.**

La tabla de enrutamiento muestra ahora la ruta para la red conectada directamente 172.16.1.0/24, como se ve en la figura.

El comando **debug ip routing** muestra los procesos de la tabla de enrutamiento para cualquier ruta, ya sea que dicha ruta sea un red conectada directamente, una ruta estática o una ruta dinámica.

Haga clic en Desactivar depuración en la figura.

Desactive **debug ip routing** utilizando el comando **undebug ip routing** o el comando **undebug all.**

**Cambio de una dirección IP**

Para cambiar una dirección IP o máscara de subred para una interfaz, reconfigure la dirección IP y máscara de subred para dicha interfaz. Este cambio sobreescribirá la entrada anterior. Existen maneras de configurar una sola interfaz con múltiples direcciones IP, siempre y cuando cada dirección se encuentre en una subred diferente. Este tema se analizará posteriormente en otro curso.

Para eliminar una red conectada directamente de un router, utilice estos dos comandos: **shutdown** y no **ip address**.

El comando **shutdown** se utiliza para desactivar interfaces. Este comando puede utilizarse por sí solo si desea conservar la configuración de dirección IP/máscara de subred de la interfaz pero desea desactivarla temporalmente. En nuestro ejemplo , este comando desactivará la interfaz FastEthernet de R2. Sin embargo, la dirección IP aún estará en el archivo de configuración, running-config.

Después de utilizar el comando shutdown, puede eliminar la dirección IP y máscara de subred de la interfaz. No es importante el orden en el que se ejecuten estos dos comandos.

**Haga clic en Depuración 2 en la figura.**

Si utilizamos debug ip routing, podemos ver el proceso de la tabla de enrutamiento y eliminaremos la configuración de la interfaz FastEthernet 0/0 de R2.

R2(config)#**interface fastethernet 0/0**
R2(config-if)#**shutdown**

Podemos ver el proceso de la tabla de enrutamiento mediante el cual se elimina la ruta conectada directamente.

02:53:58: RT: interface FastEthernet0/0 removed from routing table
02:53:58: RT: del 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
02:53:58: RT: delete subnet route to 172.16.1.0/24

El IOS también indica que la interfaz y el protocolo de línea están ahora **down:**

02:54:00: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state to administratively down
02:54:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to down
Ahora eliminaremos la dirección IP de la interfaz.

R2(config-if)#**no ip address**

Disable debugging:

R2#**undebug all**
All possible debugging has been turned off

Haga clic en la Tabla de enrutamiento 2 en la figura.

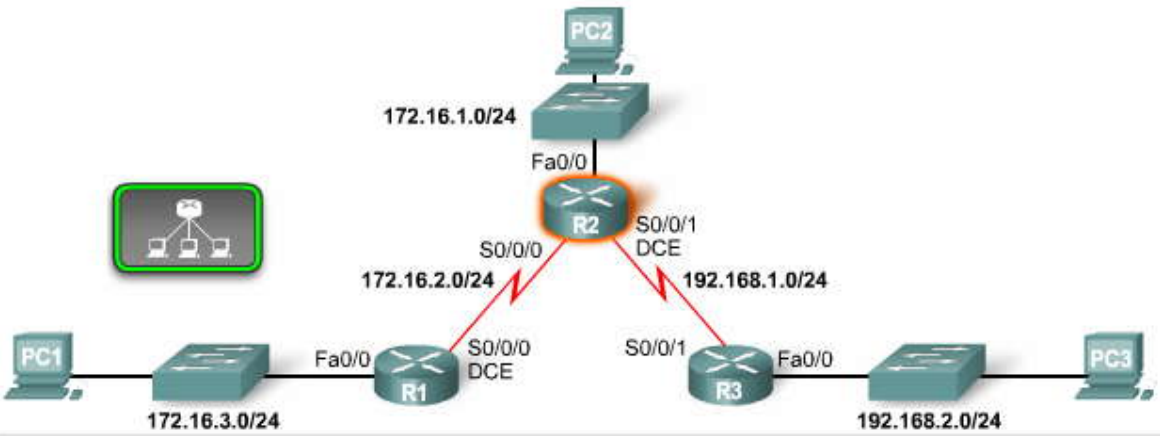
Para verificar que la ruta se haya eliminado de la tabla de enrutamiento, utilizamos el comando **show ip route**. Observe que la ruta hacia 172.16.1.0/24 ha sido eliminada.

Reconfiguración de la interfaz para continuar con el capítulo.

Durante el resto del capítulo asumiremos que no se eliminó el direccionamiento para FastEthernet 0/0. Para reconfigurar la interfaz, simplemente ingrese nuevamente los comandos:

R2(config)#**interface fastethernet 0/0**
R2(config-if)#**ip address 172.16.1.1 255.255.255.0**
R2(config-if)#**no shutdown**

**ADVERTENCIA:** Los comandos debug, especialmente el comando **debug all,** deben utilizarse moderadamente. Estos comandos pueden interferir en las operaciones del router. Los comandos debug son útiles para configurar o solucionar problemas relacionados con una red. Sin embargo, pueden hacer un uso intensivo de la CPU y de los recursos de la memoria. Se recomienda que ejecute la menor cantidad necesaria de procesos debug y que los desactive inmediatamente cuando ya no los necesite. Los comandos debug deben utilizarse con precaución en redes de producción porque pueden afectar el rendimiento del dispositivo.




```
R2#debug ip routing
IP routing debugging is on

R2(config)#int fa0/0
R2(config-if)#ip address 172.16.1.1 255.255.255.0
R2(config-if)#no shutdown

%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

RT: add 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: interface FastEthernet0/0 added to routing table
```

Debug 1

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
R2#
```

Tabla de enrutamiento 1

```
R2#undebug all
All possible debugging has been turned off
!
or
!
R2#undebug ip routing
IP routing debugging is off
R2#
```

Desactivar debug

```
R2#debug ip routing
IP routing debugging is on
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int fa0/0
R2(config-if)#shutdown

is_up: 0 state: 6 sub state: 1 line: 1
RT: interface FastEthernet0/0 removed from routing table
RT: del 172.16.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: delete subnet route to 172.16.1.0/24

<some ouput omitted>

R2(config-if)#no ip address
R2(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R2#undebug all
All possible debugging has been turned off
R2#
```

Debug 2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
R2#
```

Tabla de enrutamiento 2

### 2.3.2 DISPOSITIVOS EN REDES CONECTADAS DORECTAMENTE.-

**Acceso a dispositivos en redes conectadas directamente**

Para regresar a nuestra configuración en la topología de muestra, asumiremos que todas las redes conectadas directamente están configuradas para los tres routers. La figura muestra el resto de las configuraciones para los routers R2 y R3.

**Haga clic en show ip interface brief en la figura.**

Los resultados en esta figura verifican que todas las interfaces configuradas están "**up**" y "**up**".

**Haga clic en show ip route en la figura.**

Si revisamos las tablas de enrutamiento en la figura, podemos verificar que todas las redes conectadas directamente estén instaladas para el enrutamiento.

El paso crucial en la configuración de su red es verificar que todas las interfaces estén "up" y "up" y que las tabla s de enrutamiento estén completas. Independientemente de qué esquema de enrutamiento configure al final (estático, dinámico o una combinación de ambos), verifique sus configuraciones de red inicial con el comando **show ip interface brief** y el comando **show ip route** antes de proceder con configuraciones más complejas.

Cuando un router sólo tiene configuradas sus interfaces y la tabla de enrutamiento contiene las redes conectadas directamente pero no otras rutas, sólo podrán alcanzarse los dispositivos en dich as redes conectadas.

- R1 puede comunicarse con cualquier dispositivo en las redes 172.16.3.0/24 y 172.16.2.0/24.
- R2 puede comunicarse con cualquier dispositivo en las redes 172.16.1.0/24, 172.16.2.0/24 y 192.168.1.0/24.
- R3 puede comunicarse con cualquier dispositivo en las redes 192.168.1.0/24 y 192.168.2.0/24.

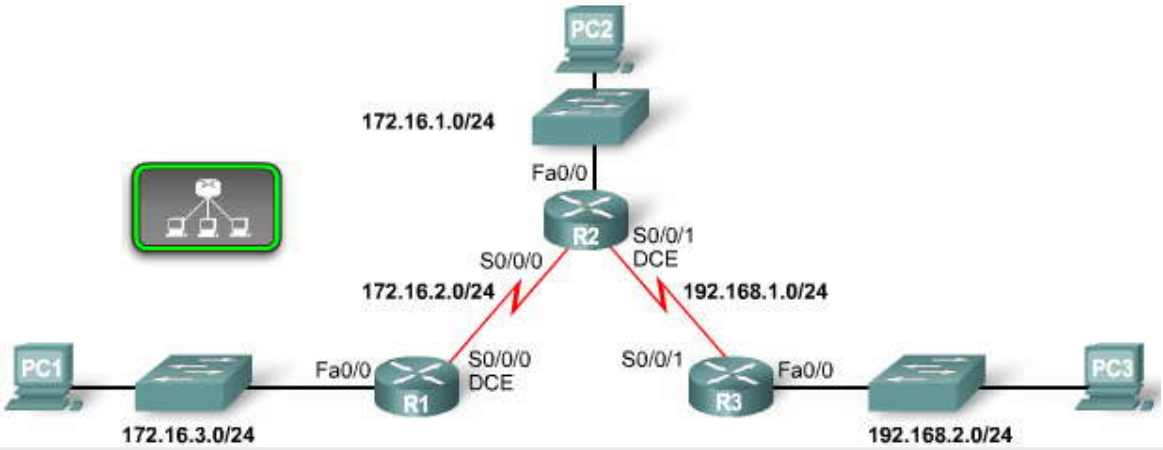
Debido a que estos routers sólo tienen información acerca de sus redes conectadas directamente, los routers sólo pueden comunicarse con aquellos dispositivos en sus propias redes seriales y LAN conectadas directamente.

Por ejemplo, la PC1 en la topología ha sido configurada con la dirección IP 172.16.3.10 y la máscara de subred 255.255.255.0. La PC1 también ha sido configurada con la dirección IP de gateway por defecto 172.16.3.1, que es la dirección IP de la interfaz FastEthernet 0/0 del router. Debido a que R1 sólo tiene información acerca de redes conectadas directamente, éste puede enviar paquetes desde la PC1 a los dispositivos en la red 172.16.2.0/24, como 172.16.2.1 y 172.16.2.2. R1 descartará los paquetes de la PC1 con cualquier otra dirección IP de destino, como la PC2 en 172.16.1.10.

Observemos la tabla de enrutamiento de R2 en la figura. R2 sólo tiene información acerca de tres redes conectadas directamente. Intente predecir qué sucederá si hacemos ping en una de las interfaces FastEthernet de uno de los otros routers.

**Haga clic en ping en la figura.**

Observe que los pings fallaron como se indica en las series de cinco períodos. El proceso falló porque R2 no tiene una ruta en su tabla de enrutamiento que coincida con 172.16.3.1 ó 192.168.2.1, que es la dirección IP de destino del paquete de ping. Para tener una coincidencia entre la dirección IP de destino de 172.16.3.1 del paquete y una ruta de la tabla de enrutamiento, la dirección debe coincidir con el número de bits que se encuentran más a la izquierda de la dirección de red, como se indica en el prefijo de la ruta. Para R2, todos las rutas tiene un prefijo /24. Por lo tanto, los 24 bits que se encuentran más a la izquierda se verifican para cada ruta.




```
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 192.168.1.2 255.255.255.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
```

Resultado del router

```
R3(config)#interface fastethernet 0/0
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip address 192.168.1.1 255.255.255.0
R3(config-if)#no shutdown
```

show ip interface brief

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            172.16.3.1      YES manual up                    up
Serial0/0/0                172.16.2.1      YES manual up                    up
FastEthernet0/1            unassigned      YES manual administratively down down
Serial0/0/1                unassigned      YES manual administratively down down
R1#
```


**Verificación de una ruta por vez**

La primera ruta de la tabla de R1 es 172.16.1.0/24.

172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, FastEthernet0/0

El proceso de la tabla de enrutamiento del IOS verifica si los 24 bits que se encuentran más a la izquierda de la dirección IP de destino del paquete, 172.16.3.1, coinciden con la red 172.16.1.0/24.

**Reproduzca la primera animación en la figura.**

Si convierte estas direcciones en binarias y las compara, como se muestra en la animación, verá que los primeros 24 bits de esta ruta no coinciden porque el bit número 23 no coincide. Por lo tanto, se rechaza esta ruta.

172.16.0.0/24 is subnetted, 2 subnets
C 172.16.2.0 is directly connected, Serial0/0/0

En la animación, vemos que no hay coincidencia en los primeros 24 bits de la segunda ruta porque el bit número 24 no coincide. Por lo tanto, también se rechaza esta ruta y el proceso continúa con la próxima ruta en la tabla de enrutamiento.

C 192.168.1.0/24 is directly connected, Serial0/0/1

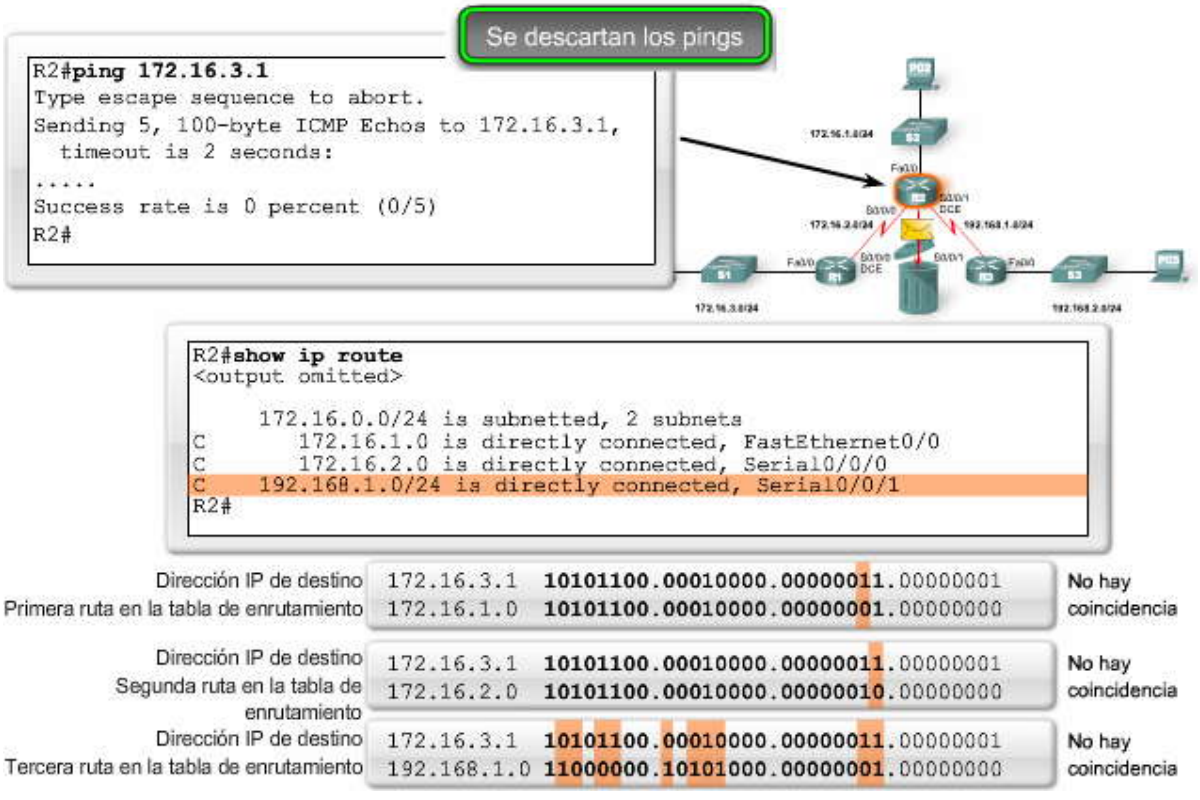
La tercera ruta tampoco es una coincidencia. Como se muestra, 10 de los primeros 24 bits no coinciden. Por lo tanto, se rechaza esta ruta. Debido a que no existen más rutas en la tabla de enrutamiento, se descartan los pin gs. El router toma su decisión de envío en Capa 3, realiza el "mejor intento" para enviar un paquete, pero no ofrece ninguna garantía.

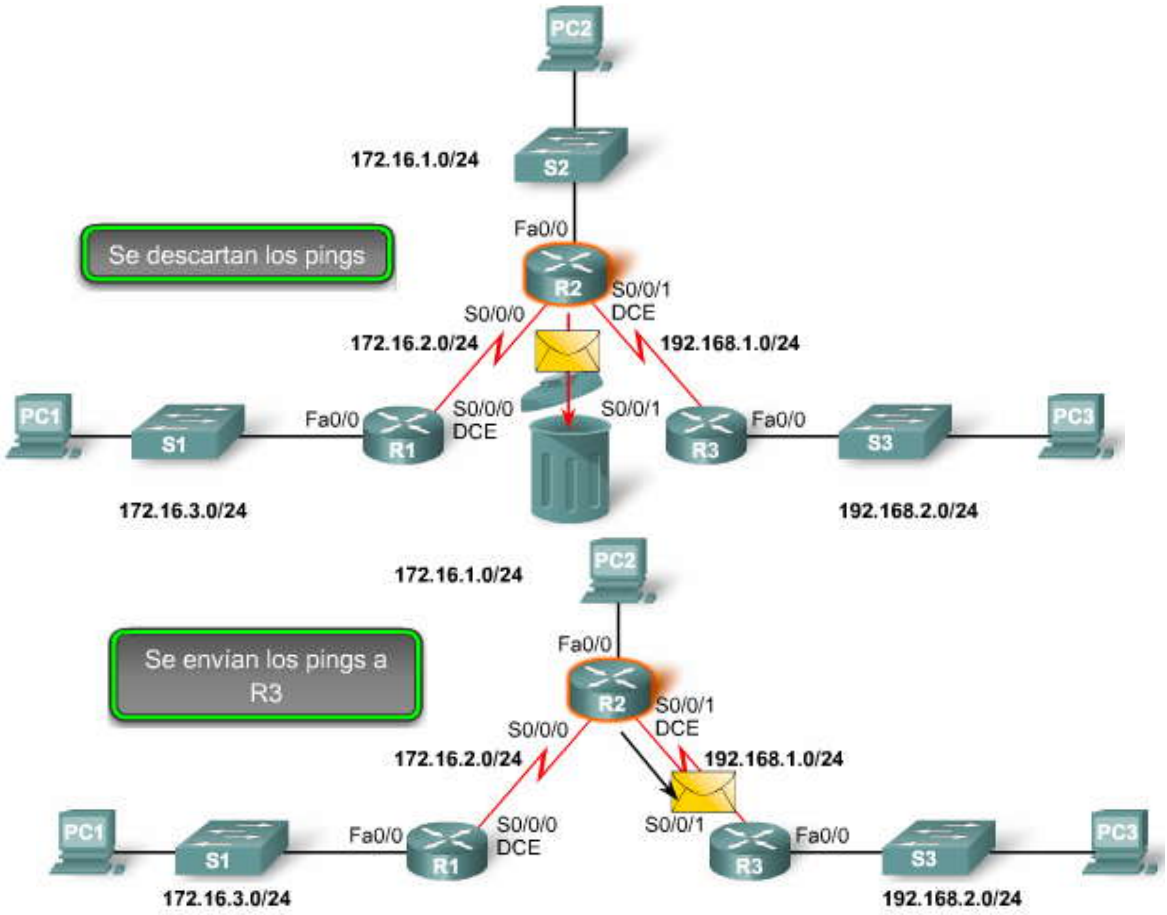
**Haga clic en Pings se envían a R3 en la figura y reproduzca la animación.**

Observemos la segunda animación para ver qué sucede si el router R2 hace ping en la interfaz 192.168.1.1 del router R3.

¡Esta vez el ping es exitoso! Fue exitoso porque R2 tiene una ruta en su tabla de enrutamiento que coincide con 192.168.1.1, que es la dirección IP de destino del paquete de ping. Se rechazan las primeras dos rutas, 172.16.1.0/24 y 172.16.2.0/24. Sin embargo, la última ruta, 192.168.1.0/24, coincide con los primeros 24 bits de la dirección IP de destino. El paquete de ping se encapsula en el protocolo HDLC de Capa 2 de Serial0/0/1, la interfaz de salida, y se envía a través de la interfaz Serial0/0/1. R2 ahora se realiza tomando las decisiones de envío para este paquete. Las decisiones que tomen otros routers con respecto a este paquete no son de su interés.

**Nota**: El proceso de búsqueda en la tabla de enrutamiento se analizará en mayor detalle en el Capítulo 8, "La tabla de enrutamiento: Un estudio detallado".






### 2.3.3 CISCO DISCOVERY PROTOCOL (CDP).-

**Descubrimiento de red con CDP**

El Cisco Discovery Protocol (CDP) es una poderosa herramienta de control y resolución de problemas de redes. El CDP es una herramienta de recopilación de información utilizada por administradores de red para obtener información acerca de los dispositivos Cisco conectados directamente. El CDP es una herramienta patentada que le permite acceder a un resumen de información de protocolo y dirección sobre los dispositivos Cisco conectados directamente. Por defecto, cada dispositivo Cisco envía mensajes periódicos, conocidos como publicaciones CDP, a dispositivos Cisco conectados directamente. Estas publicaciones contienen información acerca de los tipos de dispositivos que están conectados, las interfaces del router a las que están conectados, las interfaces utilizadas para realizar las conexiones y los números de modelo de los dispositivos.

Por naturaleza, la mayoría de los dispositivos de red no funcionan de manera aislada. Un dispositivo Cisco a menudo tiene como vecinos a otros dispositivos Cisco en la red. La información obtenida de otros dispositivos puede ayudarlo a tomar decisiones relacionadas con el diseño de la red, solucionar problemas y realizar cambios en el equipo. El CDP puede utilizarse como una herramienta de descubrimiento de redes que le permite crear una topología lógica de una red cuando falta dicha documentación o cuando no tiene información suficiente.

La familiaridad con el concepto general de vecinos es importante para comprender el CDP y los análisis futuros acerca de los protocolos de enrutamiento dinámico.

**Vecinos de Capa 3**

En este punto de nuestra configuración de topología, sólo tenemos vecinos conectados directamente. En la Capa 3, los protocolos de enrutamiento consideran que los vecinos son dispositivos que comparten el mismo espacio de dirección de red.

Por ejemplo, R1 y R2 son vecinos. Ambos son miembros de la red 172.16.1.0/24. R2 y R3 también son vecinos porque ambos comparten la red 192.168.1.0/24. Sin embargo, R1 y R3 no son vecinos porque no comparten ningún espacio de dirección de red. Si R1 y R3 se conectaran con un cable y cada uno de ellos se configurara con una dirección IP de la misma red, entonces serían vecinos.

**Vecinos de Capa 2**

El CDP funciona sólo en la Capa 2. Por lo tanto, los vecinos del CDP son dispositivos Cisco que están conectados físicamente en forma directa y comparten el mismo enlace de datos. En la figura del protocolo CDP, el administrador de red se conecta al S3. El S3 recibirá las publicaciones del CDP de S1, S2 y R2 solamente.

Si asumimos que todos los routers y switches de la figura son dispositivos Cisco que ejecutan el CDP, ¿cuántos vecinos tendría R1? ¿Puede determinar los vecinos de CDP para cada dispositivo?

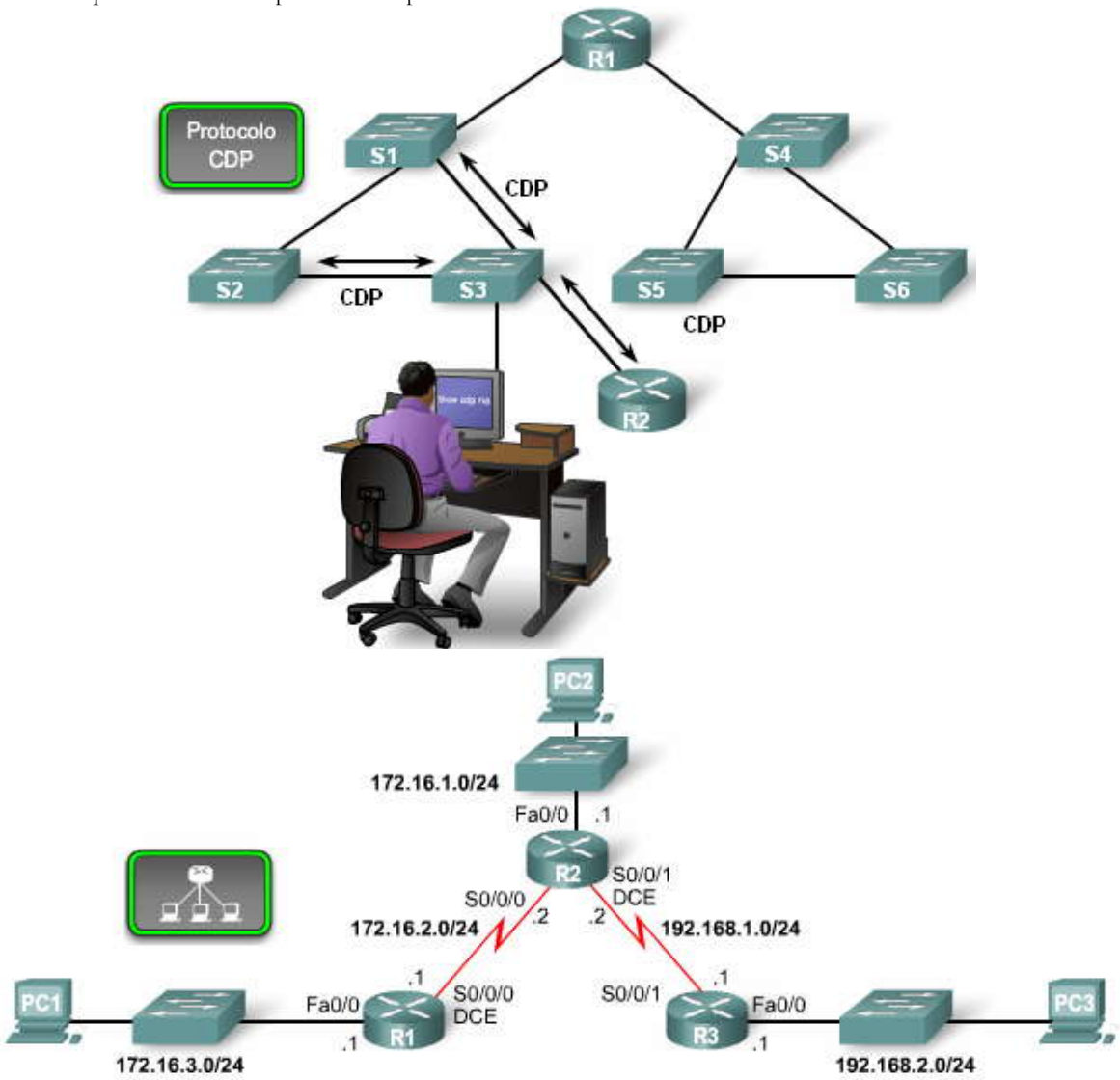
**Haga clic en el botón Topología en la figura.**

En nuestra topología del capítulo, podemos ver las siguientes relaciones de vecinos de CDP:

- R1 y S1 son vecinos de CDP.
- R1 y R2 son vecinos de CDP.
- R2 y S2 son vecinos de CDP.
- R2 y R3 son vecinos de CDP.
- R3 y S3 son vecinos de CDP.

Observe la diferencia entre los vecinos de Capa 2 y Capa 3. Los switches no son vecinos de los routers de Capa 3 porque los switches funcionan sólo en la Capa 2. Sin embargo, los switches son vecinos de Capa 2 de sus routers conectados directamente.

Veamos de qué manera el CDP puede ser útil para un administrador de red.



**Funcionamiento del CDP**

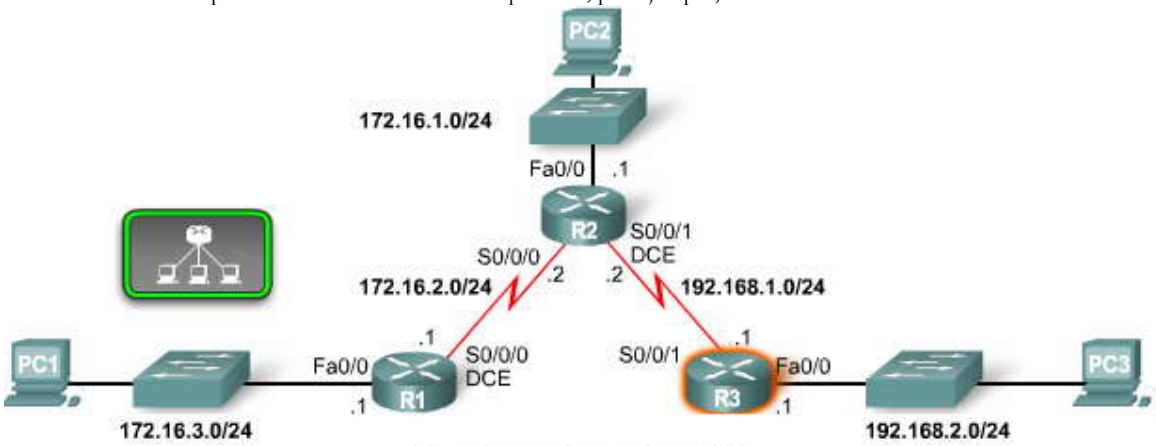
Examine los resultados de los comandos **show cdp neighbors y show cdp neighbors detail** en la figura. Observe que R3 ha recopilado información detallada acerca de R2 y el switch conectado a la interfaz Fast Ethernet de R3.

El CDP se ejecuta en la capa de Enlace de datos que conecta los medios físicos a los protocolos de capa superior (ULP). Dos o más dispositivos de red Cisco, como por ejemplo los routers que admiten diferentes protocolos de capa de Red (por ejemplo, IP y Novell IPX) pueden aprender uno del otro debido a que el CDP funciona en la capa de Enlace de datos.

Cuando un dispositivo Cisco se inicia, el CDP se inicia por defecto. El CDP descubre automáticamente los dispositivos Cisco que ejecutan el CDP, independientemente de qué protocolo o conjunto de aplicaciones se ejecute. El CDP intercambia información del hardware y software del dispositivo con sus vecinos CDP conectados directamente.

El CDP brinda la siguiente información acerca de cada dispositivo vecino de CDP:

- Identificadores de dispositivos: por ejemplo, el nombre host configurado de un switch
- Lista de direcciones: hasta una dirección de capa de Red para cada protocolo admitido
- Identificador de puerto: el nombre del puerto local y remoto en forma de una cadena de carácter ASCII, como por ejemplo, ethernet0
- Lista de capacidades: por ejemplo, si el dispositivo es un router o un switch
- Plataforma: la plataforma de hardware del dispositivo; por ejemplo, un router Cisco serie 7200




Examinando los vecinos CDP

```
R3#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Fas 0/0            151         S I       WS-C2950  Fas 0/6
R2               Ser 0/0/1          125          R        1841      Ser 0/0/1

R3#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
```

Resultado del router

### 2.3.4 UTILIZACION DEL CDP PARA DESCUBRIR UNA RED.-

**Comandos show del CDP**

La información obtenida por el protocolo CDP puede analizarse con el comando show cdp neighbors. Para cada vecino de CDP se muestra la siguiente información:

- ID de dispositivo vecino,
- Interfaz local,

- Valor de tiempo de espera, en segundos,
- Código de capacidad del dispositivo vecino,
- Plataforma de hardware del vecino e
- ID del puerto remoto del vecino.

**Haga clic en show cdp neighbors detail en la figura.**

El comando **show cdp neighbors detail** también muestra la dirección IP de un dispositivo vecino. El CDP revelará la dirección IP del vecino, independientemente de si puede hacer ping en el vecino o no. Este comando es muy útil cuando dos routers Cisco no pueden enrutarse a través de su enlace de datos compartido. El comando **show cdp neighbors detail** lo ayudará a determinar si uno de los vecinos de CDP tiene un error de configuración IP.

Para situaciones de descubrimiento de redes, la dirección IP del vecino de CDP es generalmente la única información necesaria para hacer telnet en ese dispositivo. Con una sesión de Telnet establecida, puede obtenerse información acerca de los dispositivos Cisco conectados directamente de un vecino. De esta manera, puede hacer telnet en una red y crear una topología lógica. En la próxima actividad del Packet Tracer, hará precisamente eso.

**Desactivación del CDP**

¿Es posible que el CDP implique un riesgo de seguridad? Sí, es posible. Probablemente, ya haya visto los paquetes CDP en las prácticas de laboratorio de captura de paquetes de un curso anterior. Debido a que algunas versiones de IOS envían publicaciones CDP por defecto, es importante que sepa cómo desactivar el CDP.

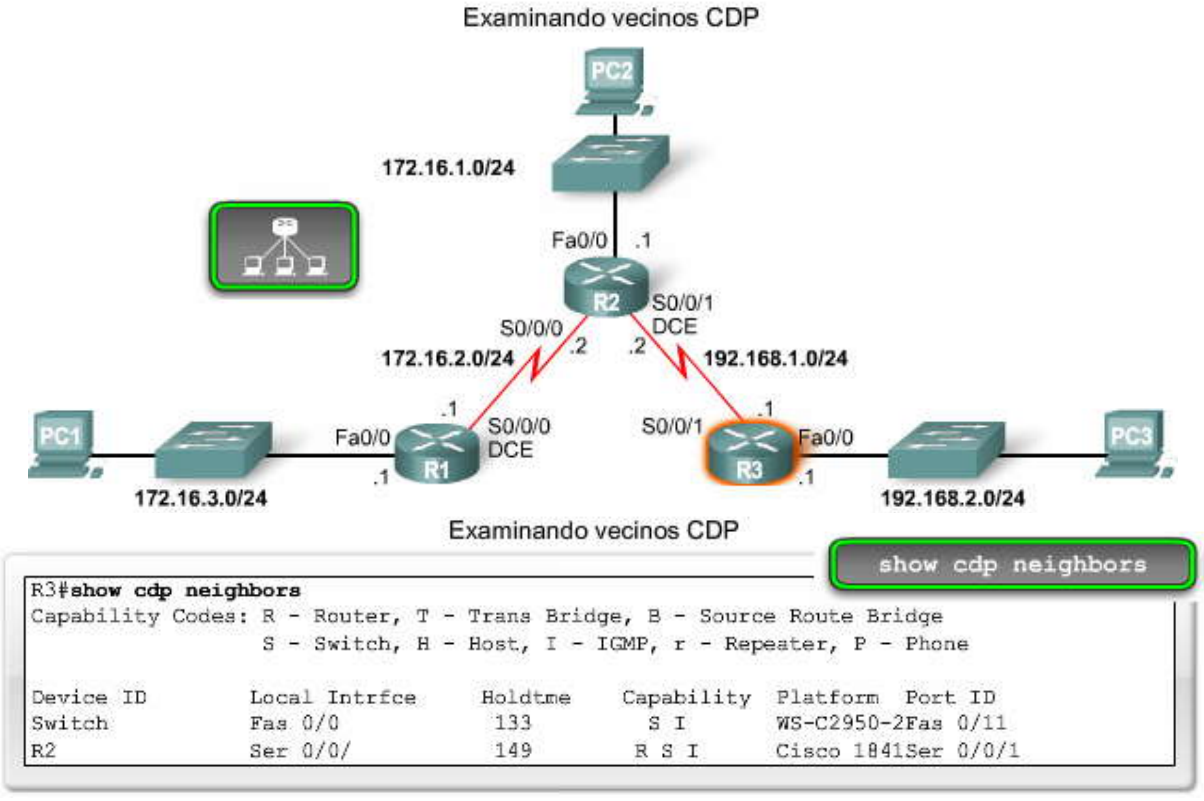
**Haga clic en Desactivar CDP en la figura.**

Si necesita desactivar el CDP globalmente, para todo el dispositivo, utilice este comando:

Router(config)#**no cdp run**

Si desea utilizar el CDP pero necesita interrumpir las publicaciones CDP en una interfaz determinada, utilice este comando:

Router(config-if)#**no cdp enable**



Examinando detalle de los vecinos CDP

```
R3#show cdp neighbors detail
-------------------------
Device ID: R2
Entry address(es):
  IP address: 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version 12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
```

show cdp neighbors detail

Desactivando CDP

```
!To disable CDP globally use...
R3(config)#no cdp run
!
!or, to disable CDP on only an interface...
R3(config-if)#no cdp enable
```

Desactivando CDP

Los comandos show del CDP pueden utilizarse para descubrir información acerca de dispositivos desconocidos en una red. Los comandos show del CDP muestran información acerca de dispositivos Cisco conectados directamente, incluyendo una dirección IP que puede utilizarse para alcanzar el dispositivo. A continuación, puede hacer telnet al dispositivo y repetir el proceso hasta que se haya asignado toda la red.

## 2.4 RUTAS ESTÁTICAS CON DIRECCIONES DEL "SIGUIENTE SALTO"

### 2.4.1 PROPÓSITO Y SINTAXIS DE COMANDO DE IP ROUTE.-

**Propósito y sintaxis de comando de ip route**

Como se analizó anteriormente, un router puede aprender sobre redes remotas de dos maneras:

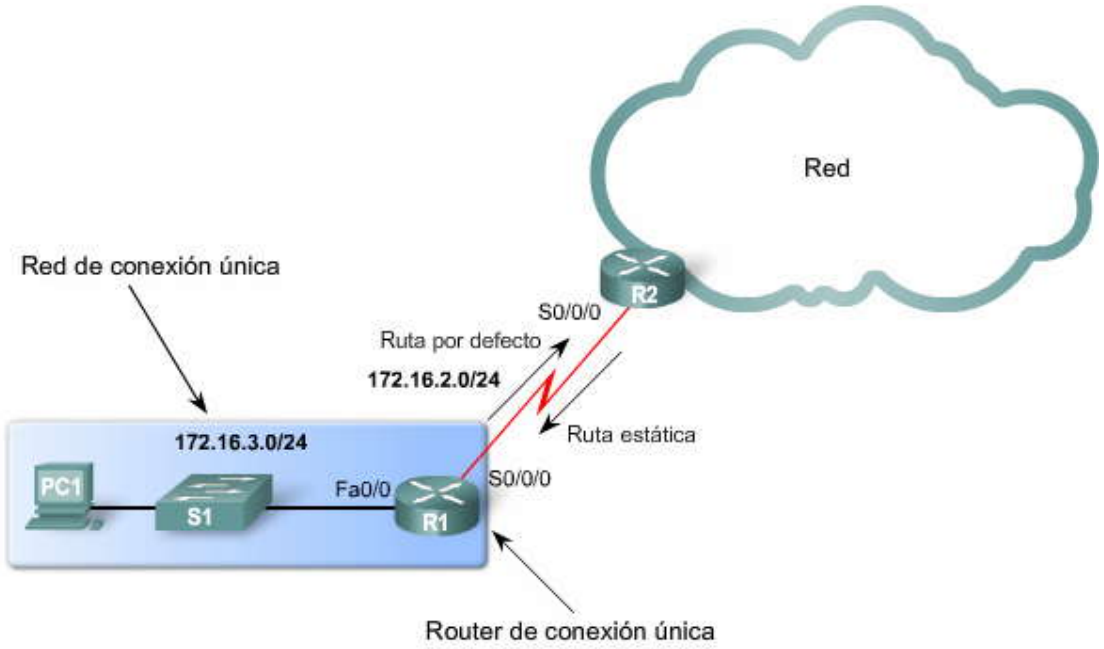
- Manualmente, a partir de las rutas estáticas configuradas
- Automáticamente, a partir de un protocolo de enrutamiento dinámico

El resto de este capítulo se enfoca en la configuración de rutas estáticas. Los protocolos de enrutamiento dinámico se presentarán en el próximo capítulo.

**Rutas estáticas**

Las rutas estáticas se utilizan generalmente cuando se enruta desde una red a una red de conexión única. **Una red de conexión única es una red a la que se accede por una sola ruta.** Por ejemplo, observe la figura. Vemos que cualquier red conectada a R1 sólo tendrá una manera de alcanzar otros destinos, ya sean redes conectadas a R2 o destinos más allá de R2. Por lo tanto, la red 172.16.3.0 es una red de conexión única y R1 es el router de conexión única.

La ejecución de un protocolo de enrutamiento entre R1 y R2 es un desperdicio de recursos porque R1 sólo tiene una manera de enviar tráfico que no sea local. Por lo tanto, las rutas estáticas se configuran para obtener conectividad a redes remotas que no están conectadas directamente al router. Nuevamente, y con referencia a la figura, deberíamos configurar una ruta estática en R2 a la LAN conectada a R1. Además, veremos cómo configurar una ruta estática por defecto de R1 a R2 posteriormente en el capítulo para que R1 pueda enviar tráfico a cualquier destino más allá de R2.




**El comando ip route**

El comando para configurar una ruta estática es **ip route**. La sintaxis completa para configurar una ruta estática es:

Router(config)#**ip route prefix mask** {ip-address | interface-type interface-number [ip-address]} [distance] [name] [**permanent**] [**tag** tag]

La mayoría de estos parámetros no son relevantes para este capítulo o para sus estudios de CCNA. Como se muestra en la figura, utilizaremos una versión más simple de la sintaxis:

Router(config)#**ip route** network-address subnet-mask {ip-address | exit-interface }

Se utilizan los siguientes parámetros:

- network-address: dirección de red de destino de la red remota que se agregará a la tabla de enrutamiento
- subnet-mask: máscara de subred de la red remota que se agregará a la tabla de enrutamiento. La máscara de subred puede modificarse para resumir un grupo de redes.

Además, deberá utilizarse uno de los siguientes parámetros, o ambos:

- ip-address: generalmente se denomina dirección IP del router del "siguiente salto"
- exit-interface: interfaz de salida que se utilizaría para enviar paquetes a la red de destino

**Nota:** El parámetro ip-address generalmente se denomina dirección IP del router del "siguiente salto". La dirección IP del router del siguiente salto se utiliza generalmente para este parámetro. Sin embargo, el parámetro ip-address podría ser cualquier dirección IP, siempre que sea determinable en la tabla de enrutamiento. Esto excede el alcance de este curso, pero agregamos este punto para mantener la precisión técnica.

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-interface }
```

| Parámetro | Descripción |
|---|---|
| **network-address** | Dirección de la red de destino de la red remota que será agregada a la tabla de enrutamiento. |
| **subnet-mask** | Máscara de subred de la red remota que será agregada a la tabla de enrutamiento. La máscara de subred puede ser modificada para resumir un grupo de redes. |
| **ip-address** | Se la denomina comúnmente como dirección IP del router del siguiente salto. |
| **exit-interface** | Interfaz de salida utilizada para enviar paquetes a la red de destino. |

## 2.4.2 CONFIGURACION DE RUTAS ESTÁTICAS.-

**Instalación de una ruta estática en la tabla de enrutamiento**

Recuerde que R1 tiene información acerca de sus redes conectadas directamente. Éstas son las rutas que actualmente se encuentran en su tabla de enrutamiento. Las redes remotas sobre las cuales R1 **no** tiene información son:

- 172.16.1.0/124: LAN de R2
- 192.168.1.0/24: red serial entre R2 y R3
- 192.168.2.0/24: LAN de R3

**Haga clic en Ruta estática en la figura.**

Primero, active debug ip routing para que el IOS muestre un mensaje cuando la nueva ruta se agregue a la tabla de enrutamiento. A continuación, utilice el comando ip route para configurar rutas estáticas de R1 para cada una de estas redes. La figura muestra la primera ruta configurada.

R1#**debug ip routing**
R1#**conf t**
R1(config)#**ip route 172.16.1.0 255.255.255.0 172.16.2.2**

Analicemos cada elemento de este resultado:

- **ip route:** comando de ruta estática
- **172.16.1.0:** dirección de red de la red remota
- **255.255.255.0:** máscara de subred de la red remota
- **172.16.2.2:** dirección IP de la interfaz Serial 0/0/0 de R2, que es el "siguiente salto" para esta red

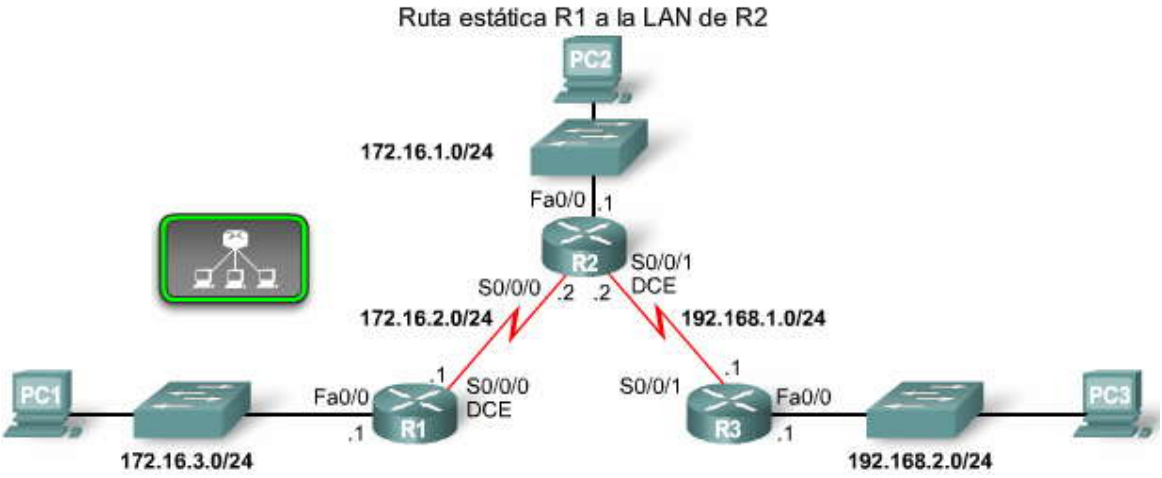
Cuando la dirección IP es la dirección IP real del router del siguiente salto, ésta es alcanzable desde una de las redes del router conectadas directamente. En otras palabras, la dirección IP **172.16.2.2** del siguiente salto está en la red **172.16.2.0/24** Serial 0/0/0 conectada directamente del router R1.

**Verificación de la ruta estática**

El resultado de **debug ip routing** muestra que esta ruta ha sido agregada a la tabla de enrutamiento.
00:20:15: RT: add 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
Observe en la figura que al ingresar **show ip route** en R1 se muestra la nueva tabla de enrutamiento. La entrada de la ruta estática está resaltada.
Analicemos este resultado:

- **S:** código de la tabla de enrutamiento para la ruta estática
- **172.16.1.0.** dirección de red para la ruta
- **/24:** máscara de subred para esta ruta; se muestra en la línea de arriba, conocida como la ruta primaria, como se analiza en el Capítulo 8
- **[1/0]:** distancia administrativa y métrica para la ruta estática (que se explicará posteriormente en otro capítulo)
- **via 172.16.2.2:** dirección IP del router del siguiente salto, la dirección IP de la interfaz Serial 0/0/0 de R2

Todos los paquetes de dirección IP de destino con 24 bits que se encuentran más a la izquierda y que coincidan con **172.16.1.0** utilizarán esta ruta.



Ruta estática R1 a la LAN de R2

```
R1#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
```

Rutas directamente conectadas

```
R2#show ip route
172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
```

```
R3#show ip route
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Ruta estática R1 a la LAN de R2

```
R1#debug ip routing
<some debug output omitted>
R1#conf t
R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2

00:20:15: RT: add 172.16.1.0/24 via 172.16.2.2, static metric [1/0]

R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
R1#
```

Ruta estática

**Configuración de rutas a otras dos redes remotas**

En la figura aparecen los comandos para configurar las rutas de otras dos redes remotas. Observe que las tres rutas estáticas configuradas de R1 tienen la misma dirección IP del siguiente salto: 172.16.2.2. Utilizando el diagrama de topología como referencia, podemos ver que esto ocurre porque los paquetes para todas las redes remotas deben enviarse al router R2, el router del siguiente salto.

Utilice el comando **show ip route** nuevamente para analizar las nuevas rutas estáticas de la tabla de enrutamiento, como se muestra.

S 192.168.1.0/24 [1/0] via 172.16.2.2
S 192.168.2.0/24 [1/0] via 172.16.2.2

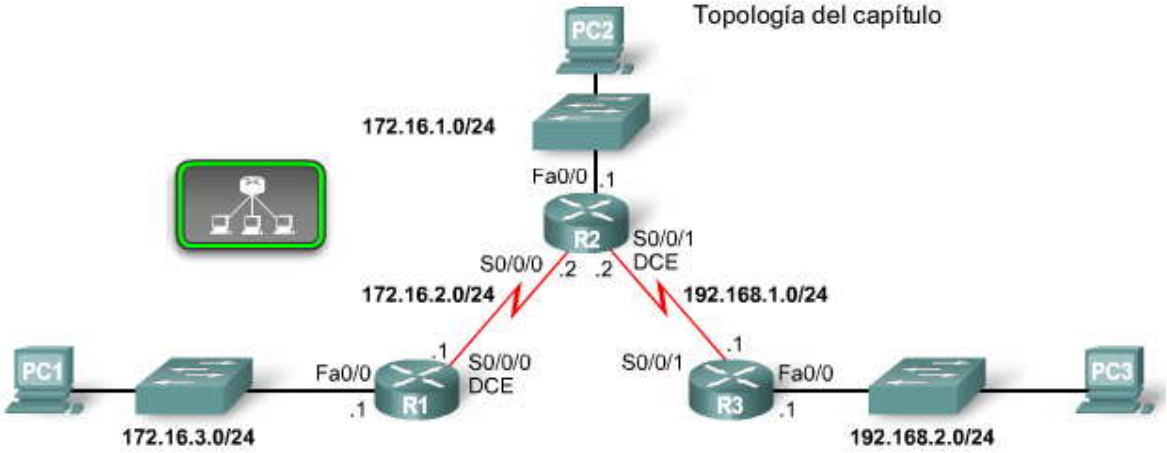
Las máscaras de subred /24 se encuentran en la misma línea que la dirección de red. Por ahora, esta diferencia no es importante. Esto se explicará en mayor detalle en el Capítulo 8, "La tabla de enrutamiento: Un estudio detallado".

**Haga clic en Verificar configuración de ruta estática en la figura.**

Las rutas estáticas que se configuraron también pueden verificarse analizando la configuración en ejecución con el comando **show running-config**.

Éste es un buen momento para guardar la configuración en NVRAM:

R1#**copy running-config startup-config**




Configurando las rutas estáticas R1 restantes

```
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
```

Rutas estáticas R1

Verificando los comandos de las rutas estáticas

```
R1#show running-config
Building configuration...

Current configuration : 849 bytes
!
hostname R1
!
<output omitted>
!
ip classless
ip route 172.16.1.0 255.255.255.0 172.16.2.2
ip route 192.168.1.0 255.255.255.0 172.16.2.2
ip route 192.168.2.0 255.255.255.0 172.16.2.2
!
<output omitted>
!
end

R1#
```

Verificar la configuración de las rutas estáticas

### 2.4.3 PRINCIPIOS DE LA TABLA DE ENRUTAMIENTO Y RUTAS ESTÁTICAS.-

**Principios de la tabla de enrutamiento**

Ahora que las tres rutas estáticas están configuradas, ¿puede predecir si los paquetes destinados para estas redes alcanzarán sus destinos? ¿Llegarán al destino los paquetes de todas estas redes destinados a la red 172.16.3.0/24?

Presentaremos tres principios de la tabla de enrutamiento, como los describe Alex Zinin en su libro Cisco IP Routing.

**Principio 1: "Cada router toma su decisión por sí solo según la información que tenga en su propia tabla de enrutamiento".**

R1 tiene tres rutas estáticas en su tabla de enrutamiento y toma decisiones de envío solamente basado en la información de la tabla de enrutamiento. R1 no consulta las tablas de enrutamiento de ningún otro router. Tampoco tiene información acerca de si esos routers tienen rutas hacia otras redes o no. Es responsabilidad del administrador de red que cada router tenga información acerca de las redes remotas.

**Principio 2: "El hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los demás routers tengan la misma información".**

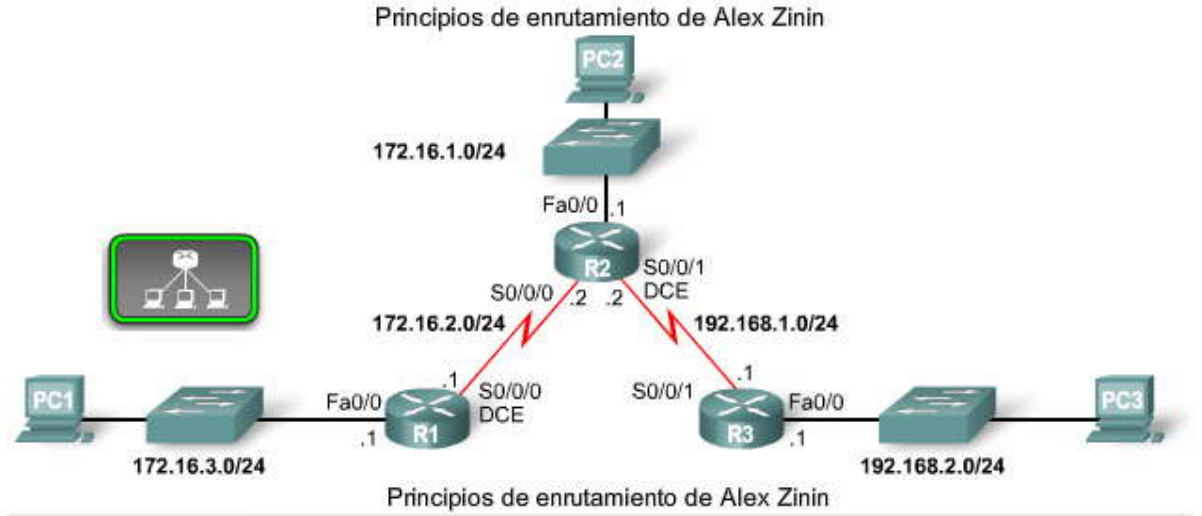
R1 no sabe qué información tienen los demás routers en su tabla de enrutamiento. Por ejemplo, R1 tiene una ruta hacia la red 192.168.2.0/24 a través del router R2. Todos los paquetes que coincidan con esta ruta pertenecen a la red 192.168.2.0/24 y se enviarán al router R2. R1 no tiene información acerca de si R2 tiene una ruta a la red 192.168.2.0/24 o no. Una vez más, el administrador de red será responsable de garantizar que el router del siguiente salto también tenga una ruta hacia esta red.

Utilizando el Principio 2, todavía necesitamos configurar el enrutamiento apropiado en los demás routers (R2 y R3) para asegurarnos de que tengan rutas hacia estas tres redes.

**Principio 3: "La información de enrutamiento sobre una ruta desde una red hacia otra no brinda información de enrutamiento sobre la ruta inversa o de regreso".**

La mayor parte de la comunicación entre las redes es bidireccional. Esto significa que los paquetes deben trasladarse en ambas direcciones entre los dispositivos finales involucrados. Un paquete de la PC1 puede alcanzar a la PC3 porque todas los routers involucrados tienen rutas hacia la red de destino 192.168.2.0/24. Sin embargo, el éxito de cualquier paquete que regrese desde la PC3 a la PC1 depende de si los routers involucrados tienen o no una ruta hacia la ruta de regreso, la red 172.16.3.0/24 de la PC1.

Utilizando el Principio 3 como guía, configuraremos rutas estáticas adecuadas en los demás routers para asegurarnos de que tengan rutas de regreso a la red 172.16.3.0/24.




Principio 1:

"Cada router toma sus decisiones individualmente basándose en la información que posee en su propia tabla de enrutamiento."

Principio 2:

"El hecho de que un router posea determinada información en su tabla de enrutamiento no significa que otros routers posean la misma información."

Principio 3:

"La información de enrutamiento acerca de una ruta desde una red a otra no brinda información de enrutamiento acerca de la ruta inversa o de la ruta de regreso."

**Aplicación de los principios**

Con estos principios en mente, ¿cómo respondería las preguntas que formulamos con respecto a los paquetes que se originan desde la PC1?

1. ¿Llegarán los paquetes de la PC1 a su destino?

En este caso, los paquetes destinados para las redes 172.16.1.0/24 y 192.168.1.0/24 llegarían a su destino. Esto sucede porque el router R1 tiene una ruta hacia estas redes a través de R2. Cuando los paquetes alcanzan el router R2, estas redes están conectadas directamente en R2 y se enrutan utilizando su tabla de enrutamiento.

Los paquetes destinados para la red 192.168.2.8/24 no llegarían a su destino. R1 tiene una ruta estática hacia esta red a través de R2. Sin embargo, cuando R2 recibe un paquete, lo descartará porque R2 no tiene todavía una ruta hacia esta red en su tabla de enrutamiento.

2. ¿Esto significa que cualquier paquete proveniente de estas redes destinado a la red 172.16.3.0/24 llegará a su destino?

Si R2 o R3 recibe un paquete destinado a 172.16.3.0/24, el paquete no llegará a su destino porque ningún router tiene una ruta hacia la red 172.16.3.0/24.

**Haga clic en Rutas estáticas R2 y R3 en la figura.**

Con los comandos que se muestran en la figura, ahora todos los routers tienen rutas hacia todas las redes remotas.

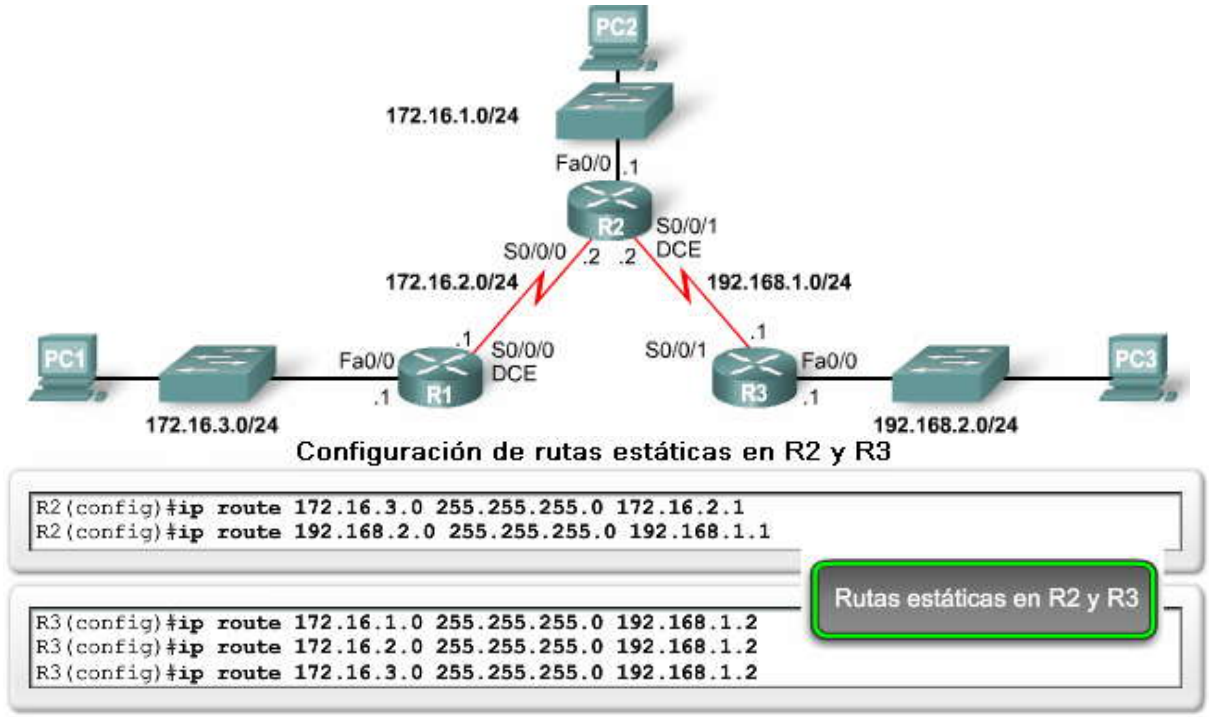
**Haga clic en show ip route en la figura.**

Analice las tablas de enrutamiento en la figura para verificar que todos los routers tengan ahora rutas hacia todas las redes remotas.

**Haga clic en ping en la figura.**

La conectividad también puede verificarse haciendo ping en las interfaces remotas desde el router R1, como se muestra en la figura.

Ahora se logra la conectividad completa para los dispositivos de nuestra topología. Cualquier PC o LAN puede ahora acceder a las PC de todas las demás LAN.



**Verificación de que las rutas estáticas se encuentran en las tablas de enrutamiento**

```
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 [1/0] via 172.16.2.2
```

show ip route

```
R2#show ip route
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 [1/0] via 172.16.2.1
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1
```

```
R3#show ip route
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 192.168.1.2
S       172.16.2.0 [1/0] via 192.168.1.2
S       172.16.3.0 [1/0] via 192.168.1.2
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
R1#ping 192.168.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R1#ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#
```

ping

### 2.4.4 RESOLUCION PARA UNA INTERFAZ DE SALIDA.-

**Búsqueda de ruta recurrente**

Antes de que un router envíe un paquete, el proceso de la tabla de enrutamiento debe determinar qué interfaz de salida utilizará para enviar el paquete. A esto se lo conoce como resolución de rutas. Analicemos este proceso observando la tabla de enrutamiento para R1 en la figura. R1 tiene una ruta estática para la red remota 192.168.2.0/24 que envía todos los paquetes a la dirección IP del siguiente salto 172.16.2.2.

**S 192.168.2.0/24 [1/0] via 172.16.2.2**

Encontrar una ruta es sólo el primer paso del proceso de búsqueda. R1 debe determinar cómo llegar a la dirección IP del siguiente salto 172.16.2.2. Realizará una segunda búsqueda para encontrar una coincidencia para 172.16.2.2. En este caso, la dirección IP 172.16.2.2 coincide con la ruta para la red conectada directamente 172.16.2.0/24.

**C 172.16.2.0 is directly connected, Serial0/0/0**

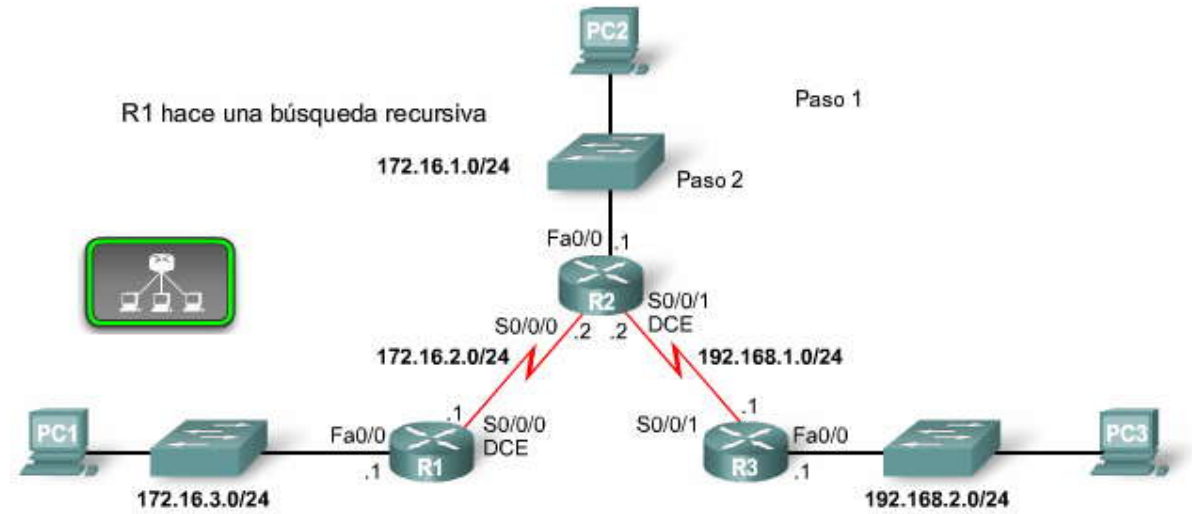
La ruta 172.16.2.0 es una red conectada directamente con la interfaz Serial 0/0/0 de salida. Esta búsqueda le indica al proceso de la tabla de enrutamiento que este paquete será enviado desde esa interfaz. Por lo tanto, en realidad se requieren dos procesos de búsqueda en la tabla de enrutamiento para enviar cualquier paquete a la red 192.168.2.0/24. Cuando el router tiene que realizar múltiples búsquedas en la tabla de enrutamiento antes de enviar un paquete, éste realiza un proceso que se conoce como búsqueda recurrente. En este ejemplo:

1. La dirección IP de destino del paquete se hace coincidir con la ruta estática 192.168.2.0/24 con la dirección IP del siguiente salto 172.16.2.2.

2. La dirección IP del siguiente salto de la ruta estática, 172.16.2.2, se hace coincidir con la red conectada directamente 172.16.2.0/24 con la interfaz Serial 0/0/0 de salida.

Todas las rutas que hacen referencia sólo a la dirección IP del siguiente salto y que no hacen referencia a una interfaz de salida, deben tener la dirección IP del siguiente salto resuelta utilizando otra ruta de la tabla de enrutamiento que tenga una interfaz de salida.

Generalmente, estas rutas se resuelven para las rutas de la tabla de enrutamiento que son redes conectadas directamente porque estas entradas siempre tendrán una interfaz de salida. En la próxima sección, observaremos que las rutas estáticas pueden configurarse con una interfaz de salida. Esto significa que no necesitan resolverse utilizando otra entrada de ruta.

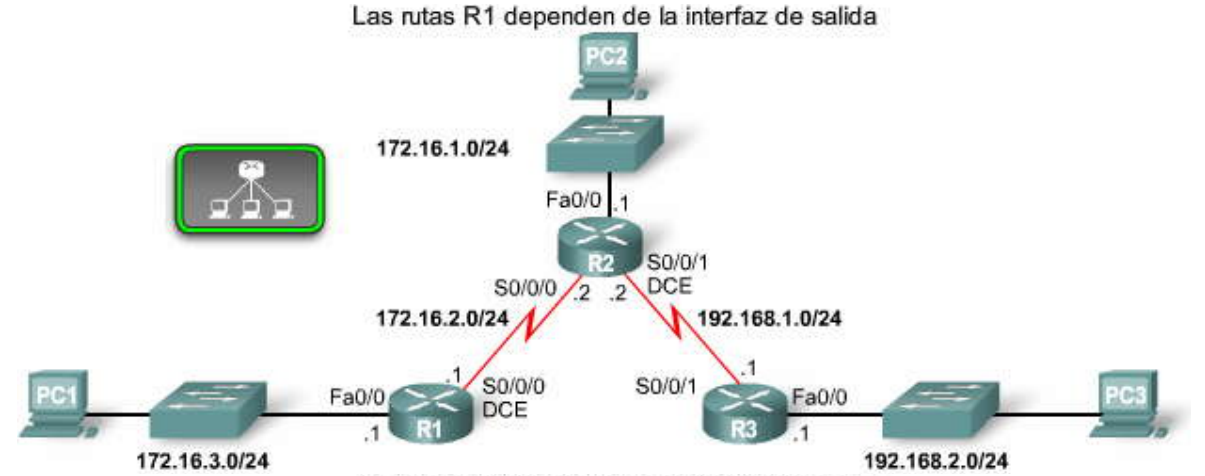



**La interfaz de salida está desactivada**

Consideremos qué sucedería si una interfaz de salida deja de funcionar. Por ejemplo, ¿qué le sucedería a la ruta estática de R1 hacia 192.16.2.0/24 si su interfaz Serial 0/0/0 estuviera desactivada? Si la ruta estática no puede resolverse para una interfaz de salida, en este caso, Serial 0/0/0, la ruta estática se elimina de la tabla de enrutamiento.

Analice este proceso con **debug ip routing** en R1 y a continuación configure la Serial 0/0/0 en **shutdown**, como se muestra.

Observe que en los resultados de la depuración, las tres rutas estáticas se eliminaron cuando la interfaz Serial 0/0/0 se apagó. Se eliminaron porque las tres rutas estáticas se resolvieron para la Serial 0/0/0. Sin embargo, las rutas estáticas aún se encuentran en la configuración en ejecución de R1. Si la interfaz vuelve al estado up (si se habilita nuevamente con **no shutdown**), el proceso de la tabla de enrutamiento del IOS volverá a instalar estas rutas estáticas en la tabla de enrutamiento.




```
R1#debug ip routing
IP routing debugging is on
R1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#shutdown
R1(config-if)#end

is_up: 0 state: 6 sub state: 1 line: 0
RT: interface Serial0/0/0 removed from routing table
RT: del 172.16.2.0/24 via 0.0.0.0, connected metric [0/0]
RT: delete subnet route to 172.16.2.0/24
RT: del 192.168.1.0 via 172.16.2.2, static metric [1/0]
RT: delete network route to 192.168.1.0
RT: del 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
RT: delete subnet route to 172.16.1.0/24

R1#show ip route
<output omitted>
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.3.0 is directly connected, FastEthernet0/0
```

Se eliminan cuatro rutas.
Sólo queda una ruta en la tabla.

## 2.5 RUTAS ESTÁTICAS CON INTERFACES DE SALIDA.-

### 2.5.1 CONFIGURACIÓN DE UNA RUTA ESTÁTICA CON INTERFAZ DE SALIDA.-

**Configuración de una ruta estática con interfaz de salida**

Investiguemos otra manera de configurar las mismas rutas estáticas. Actualmente, la ruta estática de R1 para la red 192.168.2.0/24 está configurada con la dirección IP del siguiente salto de 172.16.2.2. Observe la siguiente línea en la configuración en ejecución:

**ip route 192.168.2.0 255.255.255.0 172.16.2.2**

Como recordará de la sección anterior, esta ruta estática requiere una segunda búsqueda en la tabla de enrutamiento para resolver la dirección IP del siguiente salto 172.16.2.2 para una interfaz de salida. Sin embargo, la mayoría de las rutas estáticas pueden configurarse con una interfaz de salida, lo que permite a la tabla de enrutamiento resolver la interfaz de salida en una sola búsqueda, en lugar de en dos.

```
Router(config)#ip route network-address subnet-mask
  {ip-address | exit-interface }
```

| Parámetro | Descripción |
|---|---|
| *network-address* | Dirección de la red de destino de la red remota que será agregada a la tabla de enrutamiento. |
| *subnet-mask* | Máscara de subred de la red remota que será agregada a la tabla de enrutamiento. La máscara de subred puede ser modificada para resumir un grupo de redes. |
| *ip-address* | Se la denomina comúnmente como dirección IP del router del siguiente salto. |
| *exit-interface* | Interfaz de salida utilizada para enviar paquetes a la red de destino. |

**Ruta estática con una interfaz de salida**

Volvamos a configurar esta ruta estática para utilizar una interfaz de salida en lugar de una dirección IP del siguiente salto. Lo primero que debemos hacer es eliminar la ruta estática actual. Esto se logra utilizando el comando **no ip route**, como se muestra en la figura.

A continuación, configure la ruta estática de R1 hacia **192.168.2.0/24** utilizando la interfaz Serial 0/0/0 de salida. Después, utilice el comando **show ip route** para analizar el cambio en la tabla de enrutamiento. Observe que la entrada en la tabla de enrutamiento ya no hace referencia a la dirección IP del siguiente salto sino que se refiere directamente a la interfaz de salida. Esta interfaz de salida es la misma en la que se resolvió la ruta estática cuando utilizó la dirección IP del siguiente salto.

**S 192.168.2.0/24 is directly connected, Serial0/0/0**

Ahora, cuando el proceso de la tabla de enrutamiento tenga una coincidencia para un paquete y para esta ruta estática, podrá resolver la ruta para una interfaz de salida en una sola búsqueda. Como puede observar en la figura, las otras dos rutas estáticas todavía deben procesarse en dos pasos y resolverse para la misma interfaz Serial 0/0/0.

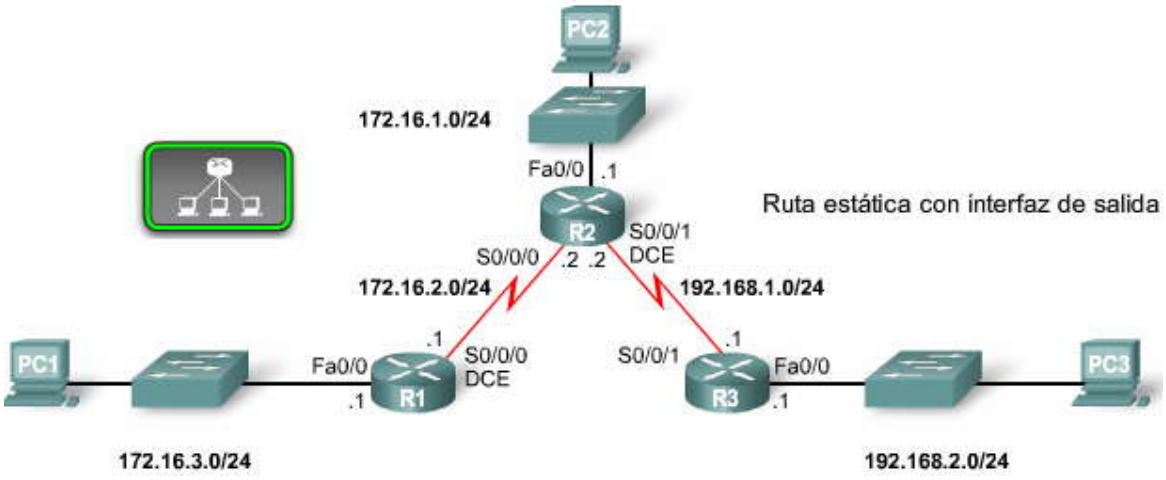
**Nota:** La ruta estática muestra la ruta como **directly connected**. Es importante comprender que esto no significa que esta ruta sea una red conectada directamente o una ruta conectada directamente. Esta ruta todavía es una ruta estática. Analizaremos la importancia de esto al abordar las Distancias administrativas en el siguiente capítulo. Aprenderemos que este tipo de ruta estática aún tiene una distancia administrativa de "1". Por ahora, sólo observe que esta ruta todavía es una ruta estática con una distancia administrativa de "1" y que no es una red conectada directamente.

**Rutas estáticas y redes punto a punto**

Las rutas estáticas que están configuradas con interfaces de salida en vez de direcciones IP del siguiente salto son ideales para la mayoría de las redes seriales punto a punto. Las redes punto a punto que utilizan protocolos tales como HDLC y PPP no utilizan la dirección IP del siguiente salto en el proceso de envío de paquetes. El paquete IP enrutado está encapsulado en una trama HDLC de Capa 2 con una dirección de destino broadcast de Capa 2.

Estos tipos de enlaces seriales punto a punto son como tuberías. Un tubo tiene dos extremos. Lo que ingresa por un extremo sólo puede tener un destino: el otro extremo del tubo. Todo paquete que se envíe a través de la interfaz Serial 0/0/0 de R1 sólo puede tener un destino: la interfaz Serial 0/0/0 de R2. En este caso la interfaz serial de R2 es la dirección IP 172.16.2.2.

**Nota:** En determinadas condiciones, el administrador de red no deseará configurar la ruta estática con una interfaz de salida sino con la dirección IP del siguiente salto. Este tipo de situación excede el alcance de este curso pero es importante mencionarla.



Ruta estática con interfaz de salida

```
R1(config)#no ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/0
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 [1/0] via 172.16.2.2
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 [1/0] via 172.16.2.2
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

Interfaz de salida ahora especificada en la ruta estática. No se necesita una búsqueda recurrente.

### 2.5.2 MODIFICACIÓN DE RUTAS ESTÁTICAS.-

**Modificación de rutas estáticas**

Algunas veces, es necesario modificar una ruta estática configurada previamente:

- la red de destino ya no existe y, por lo tanto, la ruta estática debe eliminarse.
- Se produce un cambio en la topología y debe cambiarse la dirección intermedia o la interfaz de salida.

No existe manera de modificar una ruta estática existente. La ruta estática debe eliminarse y debe configurarse una nueva.

Para eliminar una ruta estática, agregue **no** en frente del comando **ip route,** seguido del resto de la ruta estática que se eliminará.

En la sección anterior, teníamos una ruta estática:

**ip route 192.168.2.0 255.255.255.0 172.16.2.2**

Podemos eliminar dicha ruta estática con el comando no **ip route:**

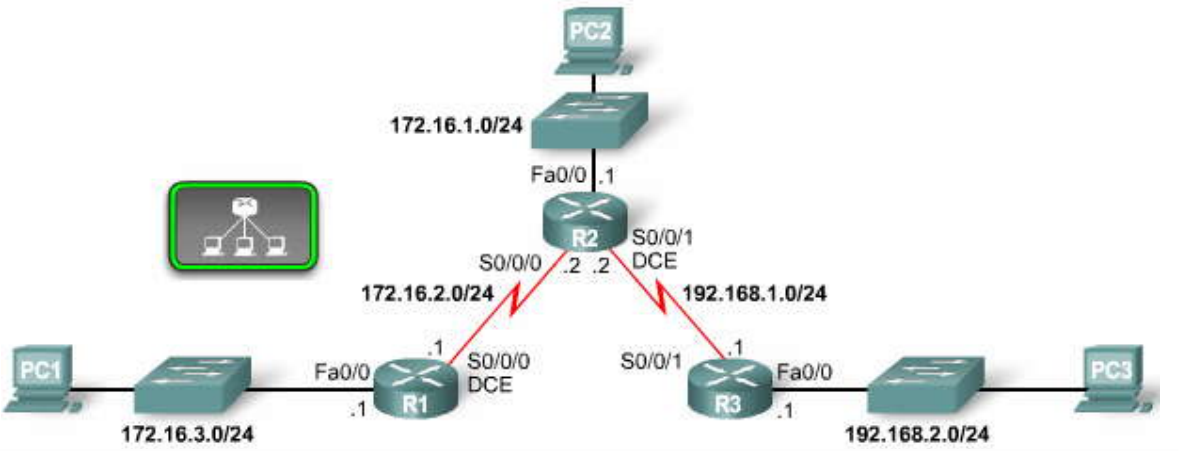
**no ip route 192.168.2.0 255.255.255.0 172.16.2.2**

Como recordará, eliminamos la ruta estática porque queríamos modificarla para utilizar una interfaz de salida en lugar de una dirección IP del siguiente salto. Configuramos una nueva ruta estática utilizando la interfaz de salida:

R1(config)#**ip route 192.168.2.0 255.255.255.0 serial 0/0/0**

Es más eficiente para el proceso de búsqueda en la tabla de enrutamiento tener rutas estáticas con interfaces de salida (al menos para redes seriales punto a punto de salida). Configuremos el resto de las rutas estáticas de R1, R2 y R3 para utilizar interfaces de salida.

Como puede verse en la figura, a medida que eliminamos cada ruta, configuraremos una nueva ruta hacia la misma red utilizando una interfaz de salida.




```
R1(config)#no ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/0
R1(config)#no ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

```
R2(config)#no ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/0
R2(config)#no ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2(config)#ip route 192.168.2.0 255.255.255.0 serial 0/0/1
```

```
R3(config)#no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.1.0 255.255.255.0 serial 0/0/1
R3(config)#no ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.2.0 255.255.255.0 serial 0/0/1
R3(config)#no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)#ip route 172.16.3.0 255.255.255.0 serial 0/0/1
```

### 2.5.3 VERIFICACIÓN DE LA CONFIGURACION DE RUTAS ESTATICAS.-

**Verificación de la configuración de rutas estáticas**

Cada vez que se realice un cambio a las rutas estáticas (o a otros aspectos de la red), verifique que los cambios se hayan implementado y que produzcan los resultados deseados.

**Verificación de cambios a las rutas estáticas**

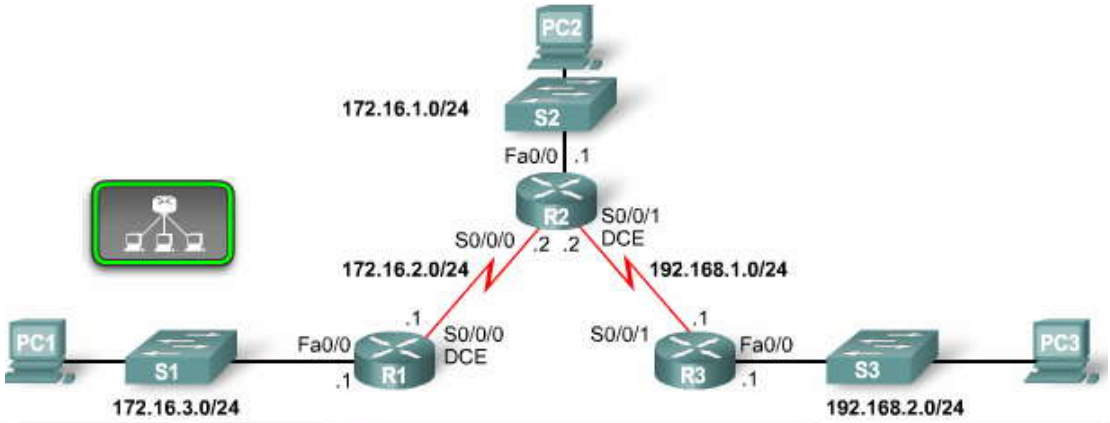
En la sección anterior, eliminamos y reconfiguramos las rutas estáticas de los tres routers. Recuerde que la configuración en ejecución contiene la configuración actual del router (los comandos y parámetros que el router utiliza actualmente). Verifique sus cambios analizando la configuración en ejecución. La figura muestra las partes de la configuración en ejecución de cada router que indican la ruta estática actual.

**Haga clic en show ip route en la figura.**

Esta figura muestra la tabla de enrutamiento para los tres routers. Observe que las rutas estáticas con interfaces de salida se agregaron a la tabla de enrutamiento y que se eliminaron las rutas estáticas anteriores con direcciones del siguiente salto.

**Haga clic en ping en la figura.**

La prueba final es enrutar paquetes desde el origen al destino. Utilizando el comando **ping**, podemos probar si los paquetes de cada router alcanzan su destino y si la ruta de regreso también funciona adecuadamente. Esta figura muestra los resultados exitosos del ping.




show running-config

```
R1#show running-config
<output omitted>
ip route 172.16.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.1.0 255.255.255.0 Serial0/0/0
ip route 192.168.2.0 255.255.255.0 Serial0/0/0
```

```
R2#show running-config
<output omitted>
ip route 172.16.3.0 255.255.255.0 Serial0/0/0
ip route 192.168.2.0 255.255.255.0 Serial0/0/1
<output omitted>
```

```
R3#show running-config
<output omitted>
ip route 172.16.1.0 255.255.255.0 Serial0/0/1
ip route 172.16.2.0 255.255.255.0 Serial0/0/1
ip route 172.16.3.0 255.255.255.0 Serial0/0/1
```

show ip route

```
R1#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
S    192.168.1.0/24 is directly connected, Serial0/0/0
S    192.168.2.0/24 is directly connected, Serial0/0/0
```

```
R2#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 is directly connected, Serial0/0/1
```

```
R3#show ip route
<output omitted>
     172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

```
R1#ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

ping

```
R2#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
```

```
R3#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
```

### 2.5.4 RUTAS ESTÁTICAS CON INTERFACES ETHERNET.-

**Interfaces Ethernet y ARP**

A veces, la interfaz de salida es una red Ethernet.

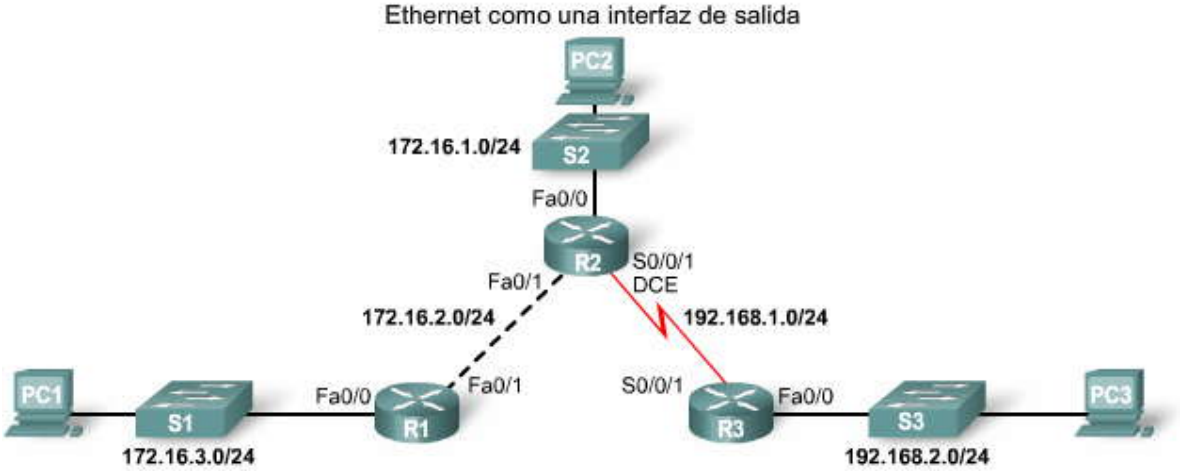
Supongamos que el enlace de red entre R1 y R2 es un enlace Ethernet y que la interfaz FastEthernet 0/1 de R1 está conectada a dicha red, como se muestra en la figura. Se puede configurar una red estática que utiliza la dirección IP del siguiente salto para la red 192.168.2.0/24 mediante este comando:
R1(config)#**ip route 192.168.2.0 255.255.255.0 172.16.2.2**

Como se analizó en la sección anterior, "Configuración de una interfaz Ethernet", el paquete IP debe encapsularse en una trama de Ethernet con una dirección MAC de destino Ethernet. Si el paquete fuera a enviarse a un router del siguiente salto, la dirección MAC de destino será la dirección de la interfaz Ethernet del router del siguiente salto. En este caso, la dirección MAC de destino Ethernet coincidirá con la dirección IP del siguiente salto 172.16.2.2. R1 busca en la tabla ARP de FastEthernet 0/1 una entrada con 172.16.2.2 y una dirección MAC correspondiente.

**Envío de una solicitud de ARP**

Si dicha entrada no se encuentra en la tabla ARP, R1 envía una solicitud de ARP a través de la interfaz FastEthernet 0/1. El broadcast de Capa 2 solicita la respuesta de un dispositivo con su dirección MAC si tiene una dirección IP 172.16.2.2. Debido a que tiene la dirección IP 172.16.2.2, la interfaz FastEthernet 0/1 de R2 envía una respuesta de ARP con la dirección MAC para dicha interfaz.

R1 recibe la respuesta de ARP y agrega la dirección IP 172.16.2.2 y la dirección MAC asociada a su tabla ARP. El paquete IP ahora se encapsula en una trama de Ethernet con la dirección MAC de destino que se encuentra en la tabla ARP. La trama de Ethernet con el paquete encapsulado se envía desde la interfaz FastEthernet 0/1 al router R2.



**Rutas estáticas e interfaces de salida Ethernet**

Configuremos una ruta estática con una interfaz de salida Ethernet en lugar de una dirección IP del siguiente salto. Cambie la ruta estática por 192.168.2.0/24 para utilizar una interfaz de salida con este comando:

R1(config)#**ip route 192.168.2.0 255.255.255.0 fastethernet 0/1**

La diferencia entre una red Ethernet y una red serial punto a punto es que una red punto a punto sólo tiene un dispositivo más en esa red (el router que se encuentra en el otro extremo del enlace). Con las redes Ethernet, es posible que existan muchos dispositivos diferentes que comparten la misma red de accesos múltiples, incluyendo hosts y hasta routers múltiples. La designación de la interfaz de salida Ethernet en la ruta estática por sí sola no provee al router información suficiente para determinar cuál es el dispositivo del siguiente salto.

R1 tiene información sobre qué paquete debe encapsularse en una trama de Ethernet y enviarse desde de la interfaz FastEthernet 0/1. Sin embargo, R1 no tiene información sobre la dirección IP del siguiente salto. Por lo tanto, no puede determinar la dirección MAC de destino para la trama de Ethernet.

Según la topología y las configuraciones de otros routers, esta ruta estática puede funcionar o no. No entraremos en detalles ahora, pero se recomienda no utilizar sólo la interfaz de salida en la ruta estática cuando la interfaz de salida sea una red Ethernet.

Uno podría preguntarse: ¿Existe una manera de configurar una ruta estática en una red Ethernet de modo que no tenga que utilizar la búsqueda recurrente de la dirección IP del siguiente salto? Sí, puede realizarse configurando la ruta estática para que incluya la interfaz de salida y la dirección IP del siguiente salto.

Como puede verse en la figura, la interfaz de salida sería FastEthernet 0/1 y la dirección IP del siguiente salto sería 172.16.2.2.

R1(config)#**ip route 192.168.2.0 255.255.255.0 fastethernet 0/1 172.16.2.2**

La entrada de la tabla de enrutamiento para esta ruta sería:

**S 192.168.2.0/24 [1/0] via 172.16.2.2 FastEthernet0/1**

El proceso de la tabla de enrutamiento sólo deberá realizar una sola búsqueda para obtener la interfaz de salida y la dirección IP del siguiente salto.

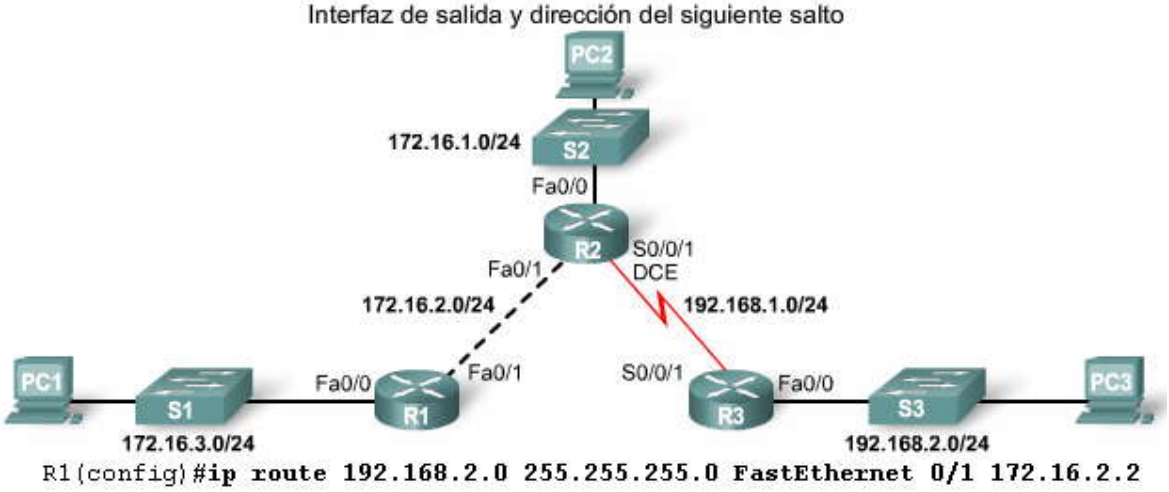
**Ventajas de utilizar una interfaz de salida con rutas estáticas**

Existe una ventaja en la utilización de interfaces de salida en rutas estáticas tanto para redes seriales punto a punto como para redes de salida Ethernet. El proceso de la tabla de enrutamiento sólo tiene que realizar una sola búsqueda para encontrar la interfaz de salida en lugar de una segunda búsqueda para resolver una dirección del siguiente salto.

Para las rutas estáticas con redes seriales punto a punto de salida, es mejor configurar las rutas estáticas sólo con la interfaz de salida. Para interfaces seriales punto a punto, el proceso de entrega de paquetes nunca utiliza la dirección del siguiente salto en la tabla de enrutamiento, por lo que no se necesita.

Para rutas estáticas con redes de salida Ethernet, es mejor configurar las rutas estáticas tanto con la dirección del siguiente salto como con la interfaz de salida.

**Nota:** Para obtener más información acerca de los problemas que pueden presentarse con las rutas estáticas que sólo utilizan una interfaz de salida Ethernet o FastEthernet, consulte el libro Cisco IP Routing, de Alex Zinin.



## 2.6 RUTAS ESTÁTICAS POR DEFECTO Y DE RESUMEN.-

### 2.6.1 RUTAS ESTÁTICAS DE RESUMEN.-

**Resumen de rutas para reducir el tamaño de la tabla de enrutamiento**

La creación de tablas de enrutamiento más pequeñas hace que el proceso de búsqueda en la tabla de enrutamiento sea más eficiente ya que existen menos rutas para buscar. Si se puede utilizar una ruta estática en lugar de múltiples rutas estáticas, el tamaño de la tabla de enrutamiento se reducirá. En muchos casos, una sola ruta estática puede utilizarse para representar docenas, cientos o incluso miles de rutas.

Podemos utilizar una sola dirección de red para representar múltiples subredes. Por ejemplo, las redes 10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, 10.4.0.0/16, 10.5.0.0/16, hasta 10.255.0.0/16, pueden representarse con una sola dirección de red: 10.0.0.0/8.

**Resumen de rutas**

Las múltiples rutas estáticas pueden resumirse en una sola ruta estática si:

- las redes de destino pueden resumirse en una sola dirección de red, y
- todas las múltiples rutas estáticas utilizan la misma interfaz de salida o dirección IP del siguiente salto.

Esto se denomina resumen de rutas.

En nuestro ejemplo, R3 tiene tres rutas estáticas. Las tres rutas envían tráfico desde la misma interfaz Serial0/0/1. Las tres rutas estáticas de R3 son:

**ip route 172.16.1.0 255.255.255.0 Serial0/0/1**
**ip route 172.16.2.0 255.255.255.0 Serial0/0/1**
**ip route 172.16.3.0 255.255.255.0 Serial0/0/1**

De ser posible, nos gustaría resumir todas estas rutas en una sola ruta estática. 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24 pueden resumirse en la red 172.16.0.0/22. Debido a que las tres rutas utilizan la misma interfaz de salida, éstas pueden resumirse en la red única 172.16.0.0 255.255.252.0 y podemos crear una sola ruta de resumen.

**Cálculo de una ruta de resumen**

Éste es el proceso para crear la ruta de resumen 172.16.1.0/22, como se muestra en la figura:

1. Escriba las redes que desea resumir en sistema binario.

2. Si desea encontrar la máscara de subred para el resumen, comience con el bit que se encuentra más a la izquierda.

3. Avance hacia la derecha a medida que encuentra todos los bits que coinciden consecutivamente.

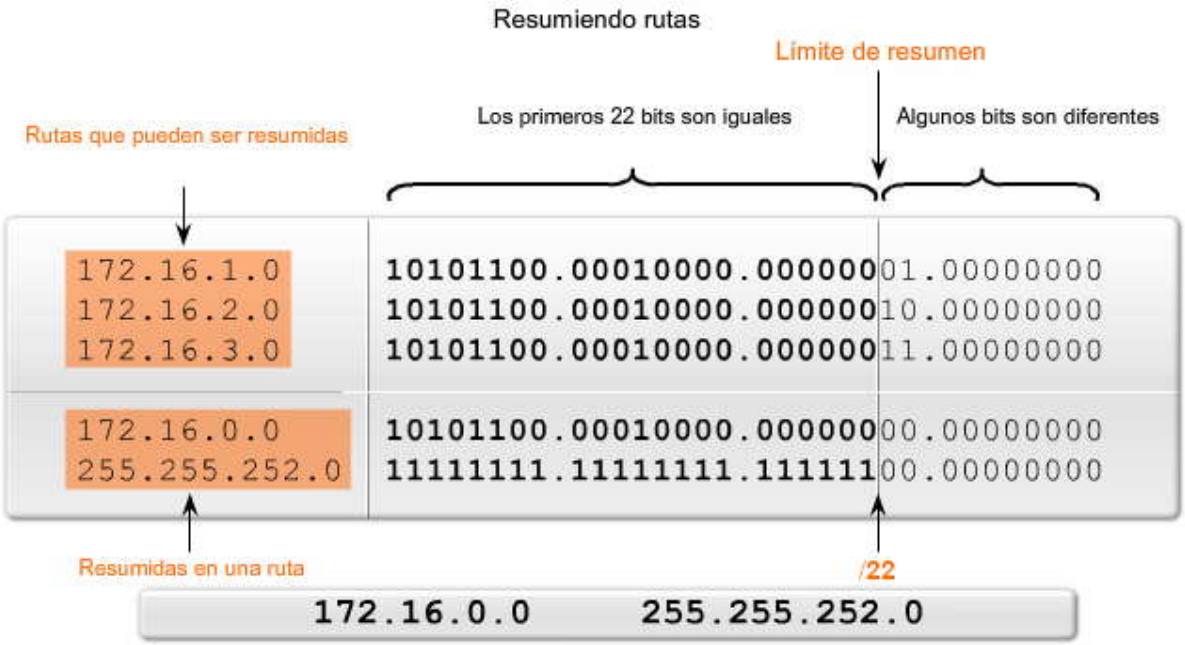
4. Cuando encuentre una columna de bits que no coincidan, deténgase. Se encuentra en el límite de resumen.

5. Ahora, cuente la cantidad de bits que coinciden y que se encuentran más a la izquierda. En nuestro ejemplo es 22. Este número se convierte en su máscara de subred para la ruta de resumen, /22 ó 255.255.252.0

6. Si desea encontrar la dirección de red para el resumen, copie los 22 bits que coinciden y agregue al final todos los bits 0 necesarios hasta obtener 32 bits.

Si seguimos estos pasos, podemos descubrir que las tres rutas estáticas de R3 pueden resumirse en una sola ruta estática utilizando la dirección de red de resumen 172.16.0.0 255.255.252.0:

**ip route 172.16.0.0 255.255.252.0 Serial0/0/1**




**Configuración de una ruta de resumen**
Para implementar la ruta de resumen, primero debemos eliminar las tres rutas estáticas actuales:

R3(config)#**no ip route 172.16.1.0 255.255.255.0 serial0/0/1**
R3(config)#**no ip route 172.16.2.0 255.255.255.0 serial0/0/1**
R3(config)#**no ip route 172.16.3.0 255.255.255.0 serial0/0/1**
A continuación, configuraremos la ruta estática de resumen:
R3(config)#**ip route 172.16.0.0 255.255.252.0 serial0/0/1**
**Haga clic en Efecto de la ruta de resumen en la figura.**
Para verificar la ruta estática nueva, analice la tabla de enrutamiento de R3 con el comando show ip route, como se muestra:
172.16.0.0/22 is subnetted, 1 subnets
S 172.16.0.0 is directly connected, Serial0/0/1

Con esta ruta de resumen, la dirección IP de destino de un paquete sólo debe coincidir con los 22 bits que se encuentran más a la izquierda de la dirección de red 172.16.0.0. Cualquier paquete con una dirección IP de destino que pertenezca a la red 172.16.1.0/24, 172.16.2.0/24 ó 172.16.3.0/24 coincide con esta ruta de resumen.

**Haga clic en Verificar ruta de resumen en la figura.**

Como puede verse en la figura, podemos probar la reconfiguración utilizando el comando ping. Verificamos que tod avía tenemos la conectividad adecuada en toda la red.

**Nota:** A partir de marzo de 2007, existen más de 200 000 rutas en los routers centrales de Internet. La mayoría de estas rutas son rutas de resumen.

Verificando la ruta resumida con **ping**

```
R3#show ip route
<output omitted>

Gateway of last resort is not set

 172.16.0.0/24 is subnetted, 3 subnets
S       172.16.1.0 is directly connected, Serial0/0/1
S       172.16.2.0 is directly connected, Serial0/0/1
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Efecto de la ruta resumida

```
R3#show ip route
<output omitted>

Gateway of last resort is not set

     172.16.0.0/22 is subnetted, 1 subnets
S       172.16.0.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/1
C    192.168.2.0/24 is directly connected, FastEthernet0/0
```

Verificando la ruta resumida con **ping**

```
R3#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms
R3#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3#ping 172.16.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms
R3#
```

### 2.6.2 RUTA ESTÁTICA POR DEFECTO.-

**Coincidencia más específica**

Es posible que la dirección IP de destino de un paquete coincida con múltiples rutas en la tabla de enrutamiento. Por ejemplo, ¿qué sucedería si tuviéramos las siguientes dos rutas estáticas en la tabla de enrutamiento?:

172.16.0.0/24 is subnetted, 3 subnets
S 172.16.1.0 is directly connected, Serial0/0/0 and
S 172.16.0.0/16 is directly connected, Serial0/0/1

Considere un paquete cuya dirección IP de destino sea 172.16.1.10. Esta dirección IP coincide con ambas rutas. El proceso de búsqueda en la tabla de enrutamiento utilizará la coincidencia más específica. Debido a que los 24 bits coinciden con la ruta 172.16.1.0/24 y que sólo coinciden 16 bits de la ruta 172.16.0.0/16, se utilizará la ruta estática con una coincidencia de 24 bits. Ésta es la mayor coincidencia. El paquete se encapsulará entonces en una trama de Capa 2 y se enviará a través de la interfaz Serial 0/0/0. Recuerde que la máscara de subred de la entrada de ruta es la que determina cuántos bits deben coincidir con la dirección IP de destino del paquete para que esta ruta coincida.

**Nota:** Este proceso se aplica para todas las rutas de la tabla de enrutamiento, incluso las rutas estáticas, las rutas aprendidas desde un protocolo de enrutamiento y las redes conectadas directamente. El proceso de búsqueda en la tabla de enrutamiento se explicará en mayor detalle en otro capítulo.

La ruta estática por defecto coincide con todos los paquetes.

Una ruta estática por defecto es una ruta que coincidirá con todos los paquetes. Las rutas estáti cas por defecto se utilizan en los siguientes casos:

- Cuando ninguna otra ruta de la tabla de enrutamiento coincide con la dirección IP de destino del paquete. En otras palabras, cuando no existe una coincidencia más específica. Se utilizan comúnmente cuand o se conecta el router extremo de una empresa a la red ISP.
- Cuando un router sólo tiene otro router más al que está conectado. Esta condición se conoce como router de conexión única.

**Configuración de una ruta estática por defecto**

La sintaxis para una ruta estática por defecto es similar a cualquier otra ruta estática, excepto que la dirección de red es 0.0.0.0 y la máscara de subred es 0.0.0.0:

Router(config)#**ip route 0.0.0.0 0.0.0.0 [exit-interface | ip-address ]**

La máscara y dirección de red 0.0.0.0 0.0.0.0 se denomina ruta "quad-zero".

R1 es un router de conexión única. Sólo está conectado a R2. Actualmente, R1 tiene tres rutas estáticas que se utilizan para alcanzar todas las redes remotas de nuestra topología. Las tres rutas estáticas tienen la i nterfaz Serial 0/0/0 de salida que envía paquetes al router R2 del siguiente salto.

Las tres rutas estáticas de R1 son:

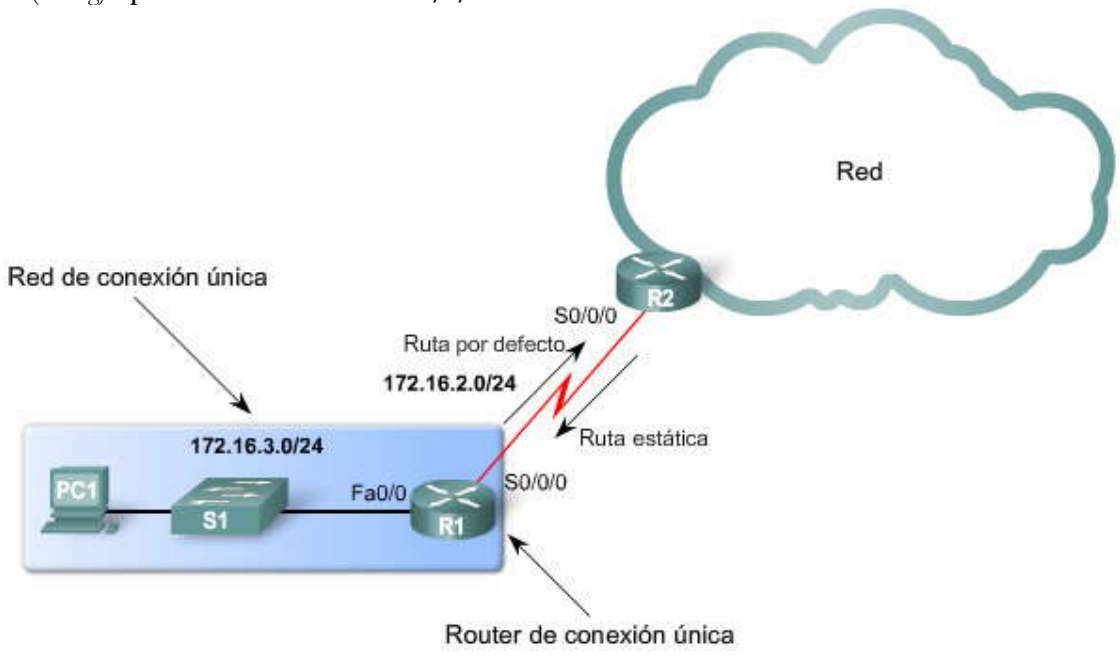
**ip route 172.16.1.0 255.255.255.0 serial 0/0/0**
**ip route 192.168.1.0 255.255.255.0 serial 0/0/0**
**ip route 192.168.2.0 255.255.255.0 serial 0/0/0**

R1 es un candidato ideal para que todas sus rutas estáticas se reemplacen con una sola ruta por defecto. Primero, elimine las tres rutas estáticas:

R1(config)#**no ip route 172.16.1.0 255.255.255.0 serial 0/0/0**
R1(config)#**no ip route 192.168.1.0 255.255.255.0 serial 0/0/0**
R1(config)#**no ip route 192.168.2.0 255.255.255.0 serial 0/0/0**

A continuación, configure la única ruta estática por defecto utilizando la misma interfaz Serial 0/0/0 de salida de las tres rutas estáticas anteriores:

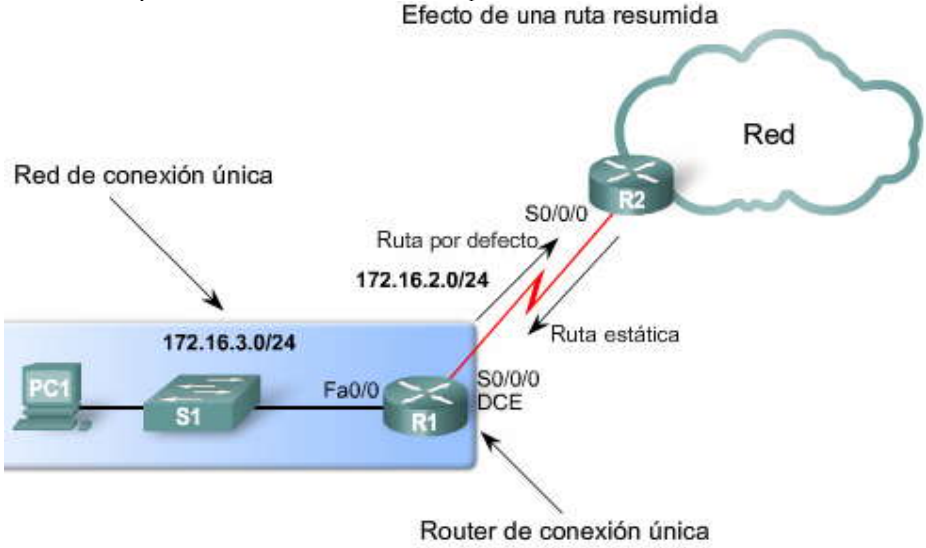
R1(config)#**ip route 0.0.0.0 0.0.0.0 serial 0/0/0**

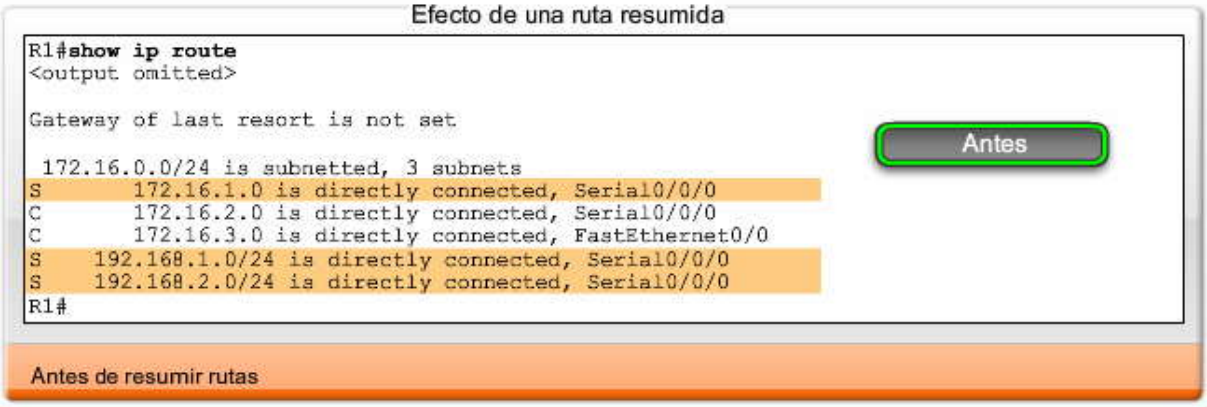


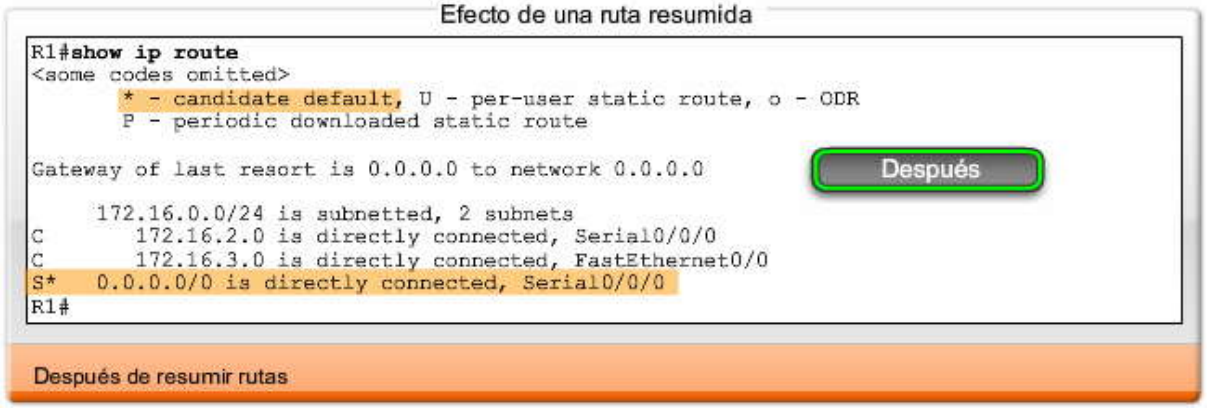
**Verificación de una ruta estática por defecto**

Verifique el cambio en la tabla de enrutamiento con el comando show ip route, como se muestra en la Figura:

**S* 0.0.0.0/0 is directly connected, Serial0/0/0**
Observe el * o asterisco junto a la **S**. Como puede verse en la tabla de **Códigos** en la figura, el asterisco indica que esta ruta estática es una ruta **candidata por defecto.** Es por esto que se denomina ruta "estática por defecto". En los siguientes capítulos veremos que una ruta "por defecto" no siempre tiene que ser una ruta "estática".
La clave para esta configuración es la máscara **/0.** Anteriormente, dijimos que la máscara de subred de la tabla de enrutamiento es la que determina cuántos bits deben coincidir entre la dirección IP de destino del paquete y la ruta de la tabla de enrutamiento. Una máscara /0 indica que no debe coincidir ningún bit. Siempre y cuando no exista una coincidencia más específica, la ruta estática por defecto coincidirá con todos los paquetes.
**Las rutas por defecto son muy comunes en los routers.** En lugar de almacenar rutas para todas las redes en Internet, los routers pueden almacenar una sola ruta por defecto que represente a cualquier red que no esté en la tabla de enrutamiento. Este tema se analizará en mayor detalle cuando analicemos los protocolos de enrutamiento dinámico.



## 2.7 ADMINISTRACION Y RESOLUCION DE PROBLEMAS DE RUTAS ESTÁTICAS.-

### 2.7.1 RUTAS ESTÁTICAS Y ENVIO DE PAQUETES.-

**Rutas estáticas y envío de paquetes**

El siguiente es un ejemplo del proceso de envío de paquetes con rutas estáticas. Como puede verse en la animación, la PC1 envía un paquete a la PC3:

1. El paquete llega a la interfaz FastEthernet 0/0 de R1.

2. R1 no tiene una ruta específica hacia la red de destino, 192.168.2.0/24. Por lo tanto, R1 utiliza la ruta estática por defecto.

3. R1 encapsula el paquete en una nueva trama. Debido a que el enlace a R2 es un enlace punto a punto, R1 agrega una dirección de "sólo unos" para la dirección de destino de Capa 2.

4. La trama se envía desde la interfaz serial 0/0/0. El paquete llega a la interfaz Serial 0/0/0 de R2.

5. R2 desencapsula la trama y busca una ruta hacia el destino. R2 tiene una ruta estática hacia 192.168.2.0/24 desde Serial0/0/1.

6. R2 encapsula el paquete en una trama nueva. Debido a que el enlace a R3 es un enlace punto a punto, R2 agrega una dirección de "sólo unos" para la dirección de destino de Capa 2.

7. La trama se envía desde la interfaz Serial0/0/1. El paquete llega a la interfaz Serial0/0/1 de R3.

8. R3 desencapsula la trama y busca una ruta hacia el destino. R3 tiene una ruta conectada hacia 192.168.2.0/24 desde FastEthernet 0/1.

9. R3 busca la entrada en la tabla ARP para 192.168.2.10 para encontrar la dirección MAC de Capa 2 para la PC3.

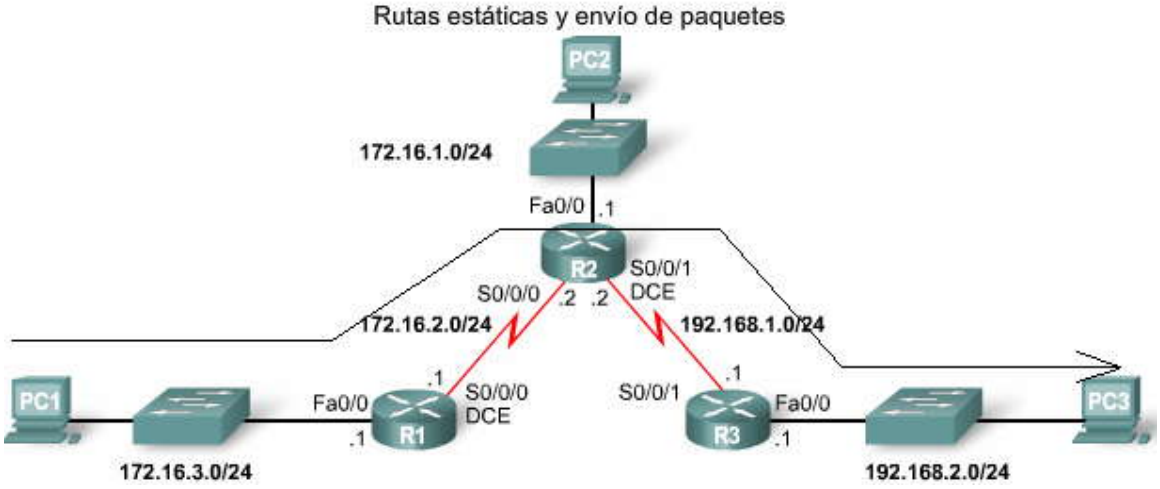
a. Si no existe ninguna entrada, R3 envía una solicitud de ARP desde FastEthernet 0/0.

b. La PC3 responde con una respuesta de ARP que incluye la dirección MAC de la PC3.

10. R3 encapsula el paquete en una trama nueva con la dirección MAC de la interfaz FastEthernet 0/0 como dirección de Capa 2 de origen y la dirección MAC de la PC3 como dirección MAC de destino.

11. La trama se envía desde la interfaz FastEthernet 0/0. El paquete llega a la interfaz NIC de la PC3.

Este proceso es igual al proceso que se demostró en el Capítulo 1. Como se explicó en el Capítulo 1, debería poder describir este proceso en detalle. Es fundamental para todos los análisis de enrutamiento saber de qué manera un router realiza sus dos funciones básicas (determinación de ruta y envío de paquetes). En la práctica de laboratorio 2.8.1, "Configuración básica de la ruta estática", tendrá la oportunidad de demostrar su conocimiento sobre el proceso de determinación de ruta y envío de paquetes.



## 2.7.2 RESOLUCION DE PROBLEMAS PARA UNA RUTA QUE FALTA.-

**Resolución de problemas para una ruta que falta**

Las redes están sujetas a diferentes situaciones que pueden provocar un cambio en su estado con bastante frecuencia:

- falla una interfaz,
- un proveedor de servicios desactiva una conexión,
- se produce una sobresaturación de enlaces o
- un administrador ingresa una configuración incorrecta.

Cuando se produce un cambio en la red, es posible que se pierda la conectividad. Como administrador de red, usted es responsable de identificar y resolver el problema.

¿Qué pasos puede seguir?

En este punto ya debe estar muy familiarizado con algunas herramientas que pueden ayudarlo a aislar problemas de enrutamiento. Entre estas herramientas enumeradas en la figura se incluyen las siguientes:

**ping**
**traceroute**
**show ip route**

Si bien aún no hemos utilizado traceroute en este curso, debería estar familiarizado con sus capacidades teniendo en cuenta los estudios anteriores. Recuerde que los comandos traceroute encontrarán una interrupción en la ruta desde el origen hacia el destino.
A medida que avancemos en este curso podrá descubrir más herramientas. Por ejemplo, **show ip interface brief** le proporciona un resumen rápido del estado de la interfaz. El CDP puede ayudarlo a recopilar información sobre la configuración IP de un dispositivo Cisco conectado directamente utilizando el comando **show cdp neigbors detail.**

Herramientas para la resolución de problemas de conectividad

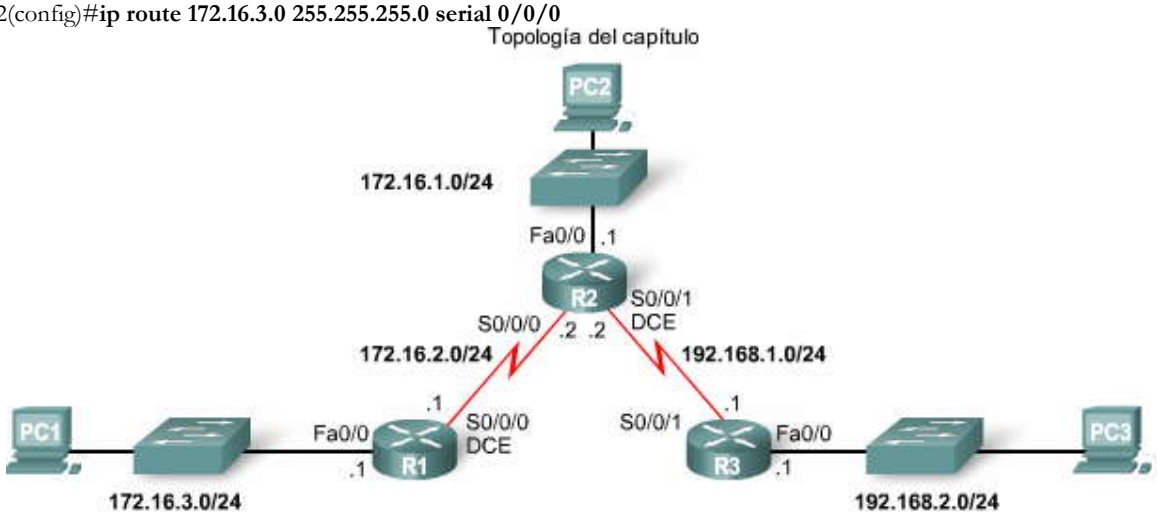
- ping
- traceroute
- show ip route
- show ip interface brief
- show cdp neighbors detail

## 2.7.3 RESOLUCION DE LA RUTA QUE FALTA.-

**Resolución de la ruta que falta**

Encontrar una ruta que falta (o mal configurada) es relativamente simple si utiliza metódicamente las h erramientas adecuadas.
Considere este problema: la PC1 no puede hacer ping en la PC3. Un traceroute muestra que R2 responde pero que no hay respuesta de R3. La tabla de enrutamiento de R2 muestra que la red 172.16.3.0/24 está configurada incorrectamente. La interfaz de salida está configurada para enviar paquetes a R3. Obviamente, desde la topología, podemos ver que R1 tiene la red 172.16.3.0/24. Por lo tanto, R2 debe utilizar Serial 0/0/0 como la interfaz de salida y no Serial0/0/1.
Para resolver esta situación, elimine la ruta incorrecta y agregue la ruta hacia la red 172.16.3.0/24 con la Serial 0/0/0 especificada como interfaz de salida.
R2(config)#**no ip route 172.16.3.0 255.255.255.0 serial0/0/1**
R2(config)#**ip route 172.16.3.0 255.255.255.0 serial 0/0/0**

Topología del capítulo



Ruta estática mal configurada

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Ruta mal configurada a 172.16.3.0/24

**2.8 PRÁCTICA DE LABORATORIO DE COFIGURACIÓN DE RUTAS ESTÁTICAS.-**
**2.8.1 CONFIGURACION BÁSICA DE LA RUTA ESTÁTICA.-**
**2.8.2 DESAFÍO DE CONFIGURACIÓN DE RUTAS ESTÁTICAS.-**
**2.8.3 RESOLUCIÓN DE PROBLEMAS DE RUTAS ESTÁTICAS.-**
**2.9 RESUMEN DEL CAPITULO.-**
**2.9.1 RESUMEN Y REVISION.-**
**Resumen**

En este capítulo, usted aprendió cómo pueden utilizarse las rutas estáticas para alcanzar redes remotas. Las redes remotas son redes a las que se puede llegar únicamente mediante el envío del paquete a otro router. Las rutas estáticas son fáciles de configurar. Sin embargo, en grandes redes, esta operación manual puede resultar complicada. Como veremos en los siguientes capítulos, las rutas estáticas aún siguen siendo utilizadas, incluso cuando se implementa un protocolo de enrutamiento dinámico.

Las rutas estáticas pueden configurarse con una dirección IP del siguiente salto que generalmente es la dirección IP del router del siguiente salto. Cuando se utiliza una dirección IP del siguiente salto, el proceso de la tabla de enrutamiento debe resolver esta dirección para una interfaz de salida. En enlaces seriales punto a punto, generalmente resulta más eficaz configurar la ruta estática con un interfaz de salida. En redes de accesos múltiples como Ethernet, deben configurarse tanto una dirección IP del siguiente salto como una interfaz de salida en la ruta estática.

Las rutas estáticas tienen una distancia administrativa por defecto de "1". Esta distancia administrativa también se aplica a las rutas estáticas configuradas con una dirección del siguiente salto y una interfaz de salida.

Sólo se ingresará una ruta estática en la tabla de enrutamiento si la dirección IP del siguiente salto puede resolverse a través de una interfaz de salida. Ya sea si la ruta estática está configurada con una dirección IP del siguiente salto o una interfaz de salida, la ruta estática no se incluirá en la tabla de enrutamiento si la interfaz de salida que se utiliza para enviar dicho paquete no se encuentra en la tabla de enrutamiento.

En muchos casos, pueden configurarse varias rutas estáticas como una sola ruta de resumen. Esto significa que habrá menos entradas en la tabla de enrutamiento y que el proceso de búsqueda en la tabla de enrutamiento será más rápido. La ruta de resumen final es una ruta por defecto configurada con una dirección de red 0.0.0.0 y una máscara de subred 0.0.0.0. Si no existe una coincidencia más específica en la tabla de enrutamiento, dicha tabla utilizará la ruta por defecto para enviar el paquete a otro router.
**Nota:** El proceso de búsqueda en la tabla de enrutamiento se analizará en mayor detalle en el Capítulo 8, "La tabla de enrutamiento: Un estudio detallado".

**En este capítulo, aprendió a:**

- Definir la función general que tiene un router en las redes.
- Describir las redes que se encuentran conectadas directamente y las diferentes interfaces del router.
- Examinar las redes conectadas directamente en la tabla de enrutamiento y utilizar el protocolo CDP.
- Describir las rutas estáticas con las interfaces de salida.
- Describir las rutas de resumen y por defecto.
- Examinar de qué manera se reenvían los paquetes cuando se utilizan rutas estáticas.
- Identificar de qué manera se administran las rutas estáticas y se resuelven problemas en éstas.

# CAPITULO III – "INTRODUCCION A LOS PROTOCOLOS DE ENRUTAMIENTO DINÁMICO"

## 3.0 INTRODUCCIÓN DEL CAPITULO.-

### 3.0.1 INTRODUCCIÓN DEL CAPITULO.-

Las redes de datos que usamos en nuestras vidas cotidianas para aprender, jugar y trabajar varían desde pequeñas redes locales hasta grandes internetworks globales. En su casa, posiblemente tenga un router y dos o más computadoras. En el trabajo, su organización probablemente tenga varios routers y switches que atienden a las necesidades de comunicación de datos de cientos o hasta miles de PC.

En los capítulos anteriores conocimos cómo se usan los routers en el envío de paquetes y que los routers aprenden sobre las redes remotas mediante el uso de rutas estáticas y protocolos de enrutamiento dinámico. También conoce la manera en q ue las rutas hacia redes remotas pueden configurarse en forma manual usando rutas estáticas.

Este capítulo introduce los protocolos de enrutamiento dinámico, incluso cómo se clasifican los diferentes protocolos de enrutamiento, qué métricas usan para determinar la mejor ruta y los beneficios de utilizar un protocolo de enrutamiento dinámico.

Los protocolos de enrutamiento dinámico generalmente se usan en redes de mayor tamaño para facilitar la sobrecarga administrativa y operativa que implica el uso de rutas estáticas únicamente. Normalmente, una red usa una combinación de un protocolo de enrutamiento dinámico y rutas estáticas. En la mayoría de las redes, se usa un único protocolo de enrutamiento dinámico. Sin embargo, hay casos en que las distintas parte s de la red pueden usar diferentes protocolos de enrutamiento.

Desde principios de la década del ochenta, han surgido varios protocolos de enrutamiento dinámico diferentes. En este capítulo, comenzaremos a analizar algunas de las características y diferen cias entre estos protocolos de enrutamiento; sin embargo, se verá con más claridad en capítulos posteriores cuando analicemos en detalle varios de estos protocolos de enrutamiento.

Aunque muchas redes usarán únicamente un solo protocolo de enrutamiento o usarán solamente rutas estáticas, es importante que un profesional de redes comprenda los conceptos y las operaciones de todos los diferentes protocolos de enrutamiento. Un profesional de redes debe estar capacitado para tomar decisiones fundadas respecto de cuándo usar un protocolo de enrutamiento dinámico y qué protocolo de enrutamiento es la mejor opción para un entorno en particular.


**En este capítulo, aprenderá a:**

- Describir el rol de los protocolos de enrutamiento dinámico y ubicar estos protocolos en el contexto del diseño de redes modernas.
- Identificar varias formas de clasificar los protocolos de enrutamiento.
- Describir cómo usan las métricas los protocolos de enrutamiento e identificar las clases de métrica que usan los protocolos de enrutamiento dinámico.
- Determinar la distancia administrativa de una ruta y describir su importancia en el proceso de enrutamiento.
- Identificar los distintos elementos presentes en la tabla de enrutamiento.
- Dadas las limitaciones existentes, elaborar y aplicar esquemas de división de redes.

## 3.1 INTRODUCCIÓN Y VENTAJAS.-

### 3.1.1 PERSPECTIVA E INFORMACIÓN BÁSICA.-

**Evolución de los protocolos de enrutamiento dinámico**

Los protocolos de enrutamiento dinámico se han usado en redes desde comienzos de la década de los ochenta. La primera versión de RIP se lanzó en 1982, pero algunos de los algoritmos básicos dentro del protocolo ya se usaban en ARPANET en 1969.

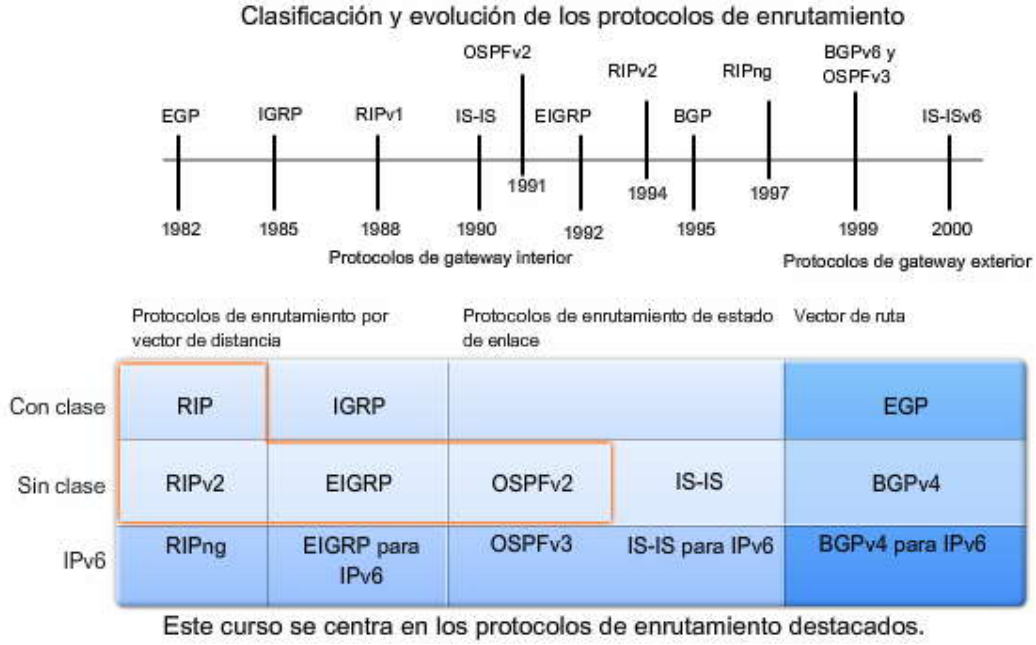
Debido a la evolución de las redes y a su complejidad cada vez mayor, han surgido nuevos protocolos de enrutamiento. La figura muestra la clasificación de los protocolos de enrutamiento.

Uno de los primeros protocolos de enrutamiento fue el Routing Information Proto col (RIP). RIP ha evolucionado a una nueva versión, el RIPv2. Sin embargo, la versión más nueva de RIP aún no escala a implementaciones de red más extensas. Para abordar las necesidades de redes más amplias, se desarrollaron dos protocolos de enrutamiento avanzados: Open Shortest Path First (OSPF) e Intermediate System-to-Intermediate System (IS-IS). Cisco desarrolló el Interior Gateway Routing Protocol (IGRP) y el Enhanced IGRP (EIGRP), que también escala bien en implementaciones de redes más grandes.

Asimismo, surgió la necesidad de interconectar diferentes internetworks y proveer el enrutamiento entre ellas. El protocolo Border Gateway Routing (BGP) ahora se usa entre ISP y entre ISP y sus clientes privados más grandes para intercambiar información de enrutamiento.

Con la llegada de numerosos dispositivos para consumidores que usan IP, el espacio de direccionamiento IPv4 está prácticamente agotado. Por tal motivo, ha surgido el IPv6. A fin de sostener la comunicación basada en IPv6, se han desarrollado versiones más nuevas de los protocolos de enrutamiento IP (consulte la fila IPv6 en la tabla).

**Nota:** Este capítulo presenta una descripción general de los diferentes protocolos de enrutamiento dinámico. Los protocolos de enrutamiento RIP, EIGRP y OSPF se analizarán en mayor detalle en los siguientes capítulos. Los protocolos de enrutamiento IS-IS y BGP se explican en el programa de estudio de CCNP. El IGRP es el antecesor de EIGRP y ahora ha caído en desuso.

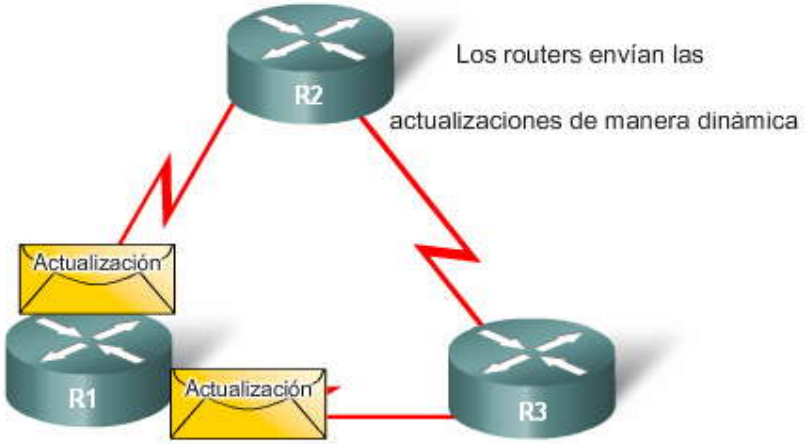



**Función de los protocolos de enrutamiento dinámico**

¿Qué son exactamente los protocolos de enrutamiento dinámico? Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento. Esto se muestra en la animación.

Los protocolos de enrutamiento determinan la mejor ruta a cada red que luego se agrega a la tabla de enrutam iento. Uno de los principales beneficios de usar un protocolo de enrutamiento dinámico es que los routers intercambian información de enrutamiento cuando se produce un cambio de topología. Este intercambio permite a los routers aprender automáticamente sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual.

En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, el costo de usar protocolos de enrutamiento dinámico es dedicar parte de los recursos de un router para la operación del protocolo, incluso el tiempo de la CPU y el ancho de banda del enlace de red. Pese a los beneficios del enrutamiento dinámico, el enrutamiento estático aún ocupa su lugar. En algunas ocasiones el enrutamiento estático es más apropiado, mientras que en otras, el enrutamiento dinámico es la mejor opción. Muy a menudo, se encontrará una combinación de los dos tipos de enrutamiento en una red que tiene un nivel de complejidad moderado. Analizaremos las ventajas y desventajas del enrutamiento estático y dinámico más adelante en este capítulo.




### 3.1.2 DESCUBRIMIENTO DE REDES Y MANTENIMIENTO DE LA TABLA DE ENRUTAMIENTO.-

**Propósito de los protocolos de enrutamiento dinámico**

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la selección de las mejores rutas del protocolo de enrutamiento. El propósito de un protocolo de enrutamiento incluye:

- descubrimiento de redes remotas,
- mantenimiento de información de enrutamiento actualizada,
- selección de la mejor ruta hacia las redes de destino y
- capacidad de encontrar una mejor nueva ruta si la ruta actual deja de estar disponible.

¿Cuáles son los componentes de un protocolo de enrutamiento?

- **Estructuras de datos:** algunos protocolos de enrutamiento usan tablas y/o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- **Algoritmo**: un algoritmo es una lista limitada de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar la mejor ruta.
- **Mensajes del protocolo de enrutamiento:** los protocolos de enrutamiento usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de enrutamiento y otras tareas para aprender y conservar información precisa sobre la red.

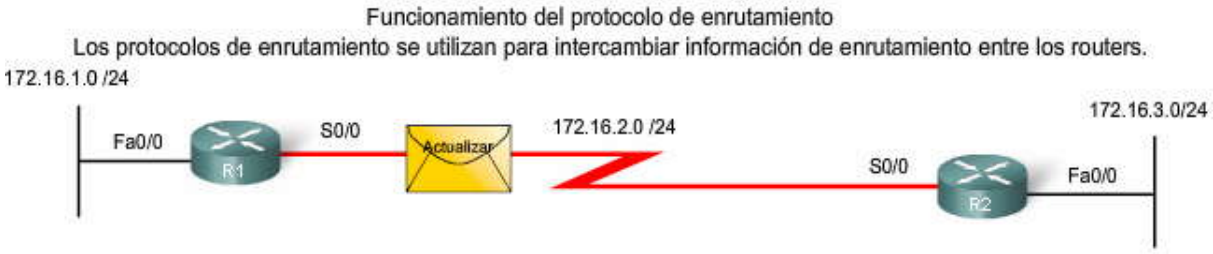
**Operación del protocolo de enrutamiento dinámico**

Todos los protocolos de enrutamiento tienen el mismo propósito: conocer sobre redes remotas y adaptarse rápidamente cuando ocurre un cambio en la topología. El método que usa un protocolo de enrutamiento para lograr su propósito depende del algoritmo que use y de las características operativas de ese protocolo. Las operaciones de un protocolo de enrutamiento dinámico varían según el tipo de protocolo de enrutamiento y el protocolo de enrutamiento en sí. En general, las operaciones de un protocolo de enrutamiento dinámico pueden describirse de la siguiente manera:

- El router envía y recibe mensajes de enrutamiento en sus interfaces.
- El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.
- Los routers intercambian información de enrutamiento para aprender sobre redes remotas.
- Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.

**Reproduzca la animación para ver protocolos de enrutamiento dinámico en funcionamiento.**

**Nota:** La comprensión de los conceptos y la operación del protocolo de enrutamiento dinámico y su uso en redes reales requiere de un sólido conocimiento de la división en subredes y el direccionamiento IP. Al final de este capítulo se ofrecen como práctica tres situaciones de división en subredes.




### 3.1.3 VENYAJAS.-

**Uso del enrutamiento estático**

Antes de identificar los beneficios de los protocolos de enrutamiento dinámico, debemos considerar los motivos por los que usaríamos el enrutamiento estático. El enrutamiento dinámico ciertamente tiene múltiples ventajas en comparación con el enrutamiento estático. Sin embargo, el enrutamiento estático aún se usa en las redes de la actualidad. De hecho, las redes generalmente usan una combinación de enrutamiento estático y dinámico.

**El enrutamiento estático tiene varios usos principales , entre ellos:**

- Facilita el mantenimiento de la tabla de enrutamiento en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
- Enrutamiento desde y hacia redes de conexión única (ver Capítulo 2).
- Uso de una única ruta por defecto que se usa para representar una ruta hacia cualquier red que no tiene una coincidencia más específica con otra ruta en la tabla de enrutamiento.

**Ventajas y desventajas del enrutamiento estático**

En la tabla se comparan directamente las ventajas y desventajas del enrutamiento dinámico y estático. A partir de esta comparación, podemos enumerar las ventajas de cada método de enrutamiento. Las ventajas de un método son las desventajas del otro.

**Ventajas del enrutamiento estático:**

- El procesamiento de la CPU es mínimo.
- Es más fácil de comprender para el administrador.
- Es fácil de configurar.

**Desventajas del enrutamiento estático:**

- La configuración y el mantenimiento son prolongados.
- La configuración es propensa a errores, especialmente en redes extensas.
- Se requiere la intervención del administrador para mantener la información cambiante de la ruta.
- No se adapta bien con las redes en crecimiento; el mantenimiento se torna cada vez más complicado.
- Requiere un conocimiento completo de toda la red para una correcta implementación.

**Ventajas y desventajas del enrutamiento dinámico**

**Ventajas del enrutamiento dinámico:**

- El administrador tiene menos trabajo en el mantenimiento de la configuración cuando agrega o quita redes.
- Los protocolos reaccionan automáticamente a los cambios de topología.
- La configuración es menos propensa a errores.
- Es más escalable, el crecimiento de la red normalmente no representa un problema.

**Desventajas del enrutamiento dinámico:**

- Se utilizan recursos del router (ciclos de CPU, memoria y ancho de banda del enlace).
- El administrador requiere más conocimientos para la configuración, verificación y resolución de problemas.

Enrutamiento dinámico versus enrutamiento estático

| | Enrutamiento dinámico | Enrutamiento estático |
|---|---|---|
| **Complejidad de la configuración** | Por lo general es independiente del tamaño de la red | Se incrementa con el tamaño de la red |
| **Conocimientos requeridos del administrador** | Se requiere de un conocimiento avanzado | No se requieren conocimientos adicionales |
| **Cambios de topología** | Se adapta automáticamente a los cambios de topología | Se requiere la intervención del administrador |
| **Escalamiento** | Adecuado para las topologías simples y complejas | Adecuada para topologías simples |
| **Seguridad** | Es menos seguro | Más segura |
| **Uso de recursos** | Utiliza CPU, memoria y ancho de banda de enlace | No se requieren recursos adicionales |
| **Capacidad de predicción** | La ruta depende de la topología actual | La ruta hacia el destino es siempre la misma |

## 3.2 CLASIFICACION DE PROTOCOLOS DE ENRUTAMIENTO DINÁMICO.-

### 3.2.1 DESCRIPCIÓN GENERAL.-

**Clasificación de los protocolos de enrutamiento dinámico**

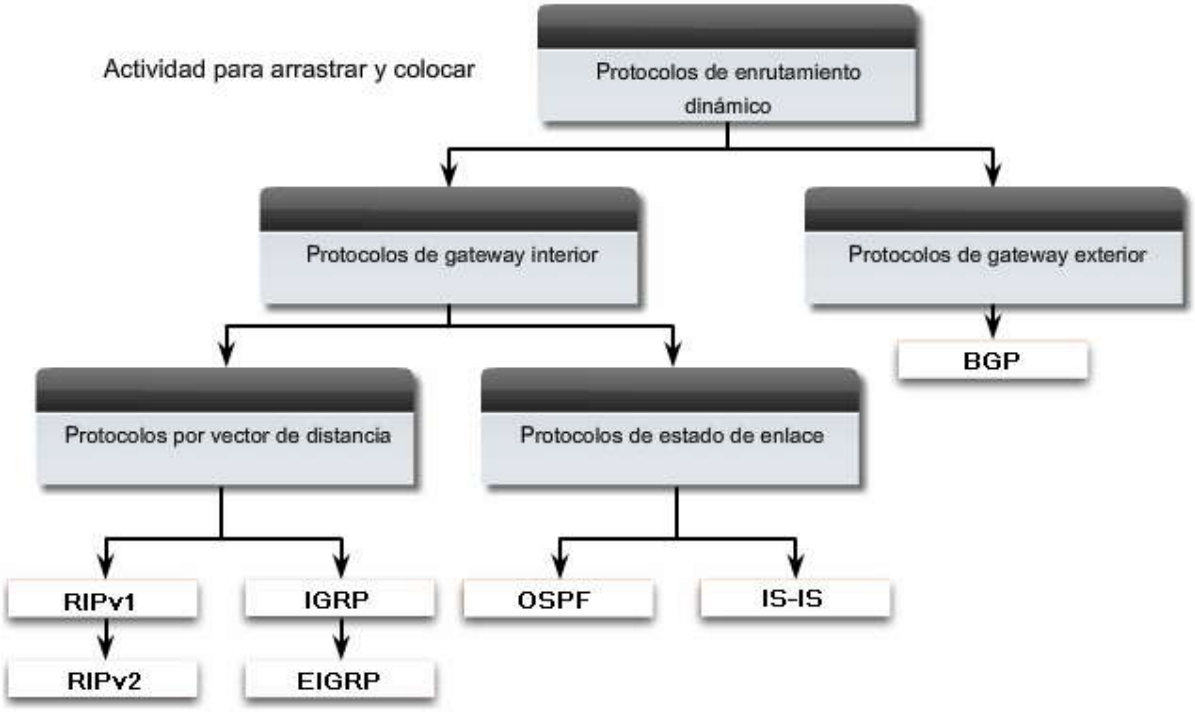
Los protocolos de enrutamiento pueden clasificarse en diferentes grupos según sus características. Los proto colos de enrutamiento que se usan con más frecuencia son:

- **RIP**: un protocolo de enrutamiento interior por vector de distancia
- **IGRP**: el enrutamiento interior por vector de distancia desarrollado por Cisco (en desuso desde 12.2 IOS y versiones posteriores)
- **OSPF**: un protocolo de enrutamiento interior de estado de enlace
- **IS-IS**: un protocolo de enrutamiento interior de estado de enlace
- **EIGRP**: el protocolo avanzado de enrutamiento interior por vector de distancia desarrollado por Cisco
- **BGP**: un protocolo de enrutamiento exterior de vector de ruta

**Nota**: IS-IS y BGP exceden el alcance de este curso y se abordan en el programa de estudio de CCNP.

Los criterios de clasificación se explican más adelante en este capítulo.

- Es posible que sobren algunas respuestas.
- Algunas respuestas se usan más de una vez.



### 3.2.2 IGP Y EGP.-

Un sistema autónomo (AS), conocido también como dominio de enrutamiento, es un conjunto de routers que se encuentran bajo una administración en común. Algunos ejemplos típicos son la red interna de una empresa y la red de un proveedor de servicios de Internet. Debido a que Internet se basa en el concepto de sistema autónomo, se requieren dos tipos de protocolos de enrutamiento: protocolos de enrutamiento interior y exterior. Estos protocolos son:

- **Interior Gateway Protocols (IGP):** se usan para el enrutamiento de sistemas intrautónomos (el enrutamiento dentro de un sistema autónomo)
- **Exterior Gateway Protocols (EGP):** se usan para el enrutamiento de sistemas interautónomos (el enrutamiento entre sistemas autónomos)

La figura es una vista simplificada de la diferencia entre IGP y EGP. El concepto de sistema autónomo se explicará con mayor detalle más adelante en el capítulo.

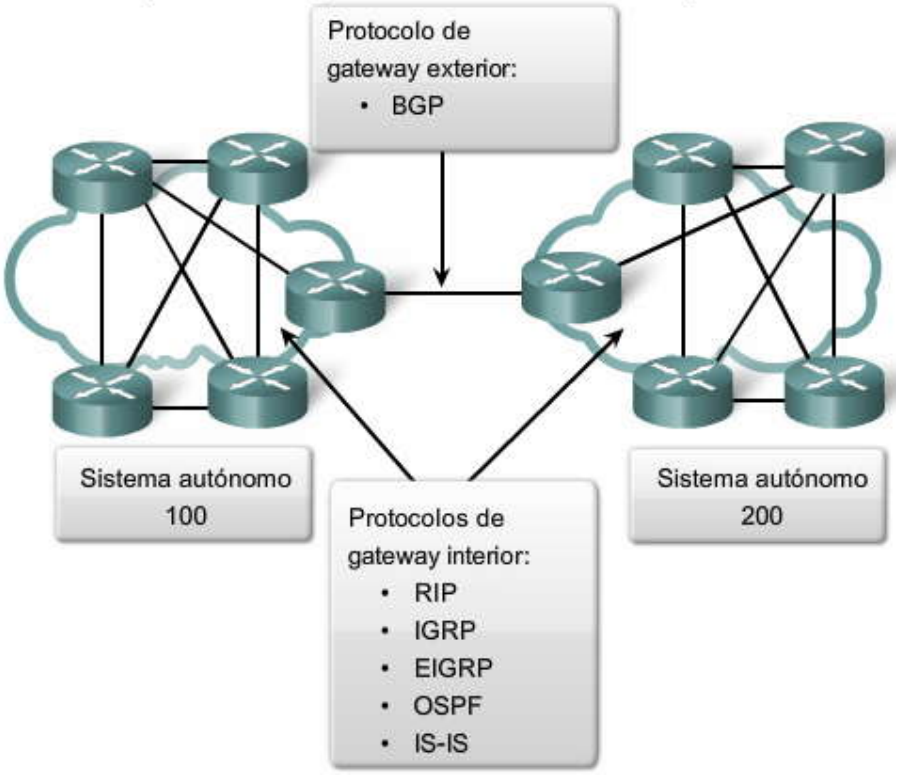
**Características de los protocolos de enrutamiento IGP y EGP**

Los IGP se usan para el enrutamiento dentro de un dominio de enrutamiento, aquellas redes bajo el control de una única organización. Un sistema autónomo está comúnmente compuesto por muchas redes individuales que pertenecen a empresas, escuelas y otras instituciones. Un IGP se usa para enrutar dentro de un sistema autónomo, y también se usa para enrutar dentro de las propias redes individuales. Por ejemplo, CENIC opera un sistema autónomo integrado por escuelas, colegios y universidades de California. CENIC usa un IGP para enrutar dentro de su sistema autónomo a fin de interconectar a todas estas instituciones. Cada una de las instituciones educativas también usa un IGP de su propia elección para enrutar dentro de su propia red individual. El IGP utilizado por cada entidad provee la determinación de la mejor ruta dentro de sus propios dominios de enrutamiento, del mismo modo que el IGP utilizado por CENIC provee las mejores rutas dentro del sistema autónomo en sí. Los IGP para IP incluyen RIP, IGRP, EIGRP, OSPF e IS-IS.

Los protocolos de enrutamiento, y más específicamente el algoritmo utilizado por ese protocolo de enrutamiento, utilizan una métrica para determinar la mejor ruta hacia una red. La métrica utilizada por el protocolo de enrutamiento RIP es el conteo de saltos, que es el número de routers que un paquete debe atravesar para llegar a otra red. OSPF usa el ancho de banda para determinar la ruta más corta.

Por otro lado, los EGP están diseñados para su uso entre diferentes sistemas autónomos que están controlados por distintas administraciones. El BGP es el único EGP actualmente viable y es el protocolo de enrutamiento que usa Internet. El BGP es un protocolo de vector de ruta que puede usar muchos atributos diferentes para medir las rutas. En el ámbito del ISP, con frecuencia hay cuestiones más importantes que la simple elección de la ruta más rápida. En general, el BGP se utiliza entre ISP y a veces entre una compañía y un ISP. El BGP no forma parte de este curso o CCNA; se aborda en CCNP.

Comparación entre protocolos de enrutamiento IGP y EGP



### 3.2.3 VECTOR DE DISTANCIA Y ESTADO DE ENLACE.-

Los protocolos de gateway interiores (IGP) pueden clasificarse en dos tipos:

- Protocolos de enrutamiento por vector de distancia
- Protocolos de enrutamiento de estado de enlace

**Operación del protocolo de enrutamiento por vector de distancia**

El vector de distancia significa que las rutas son publicadas como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es simplemente el router del siguiente salto o la interfaz de salida. Los protocolos por vector de distancia generalmente usan el algoritmo Bellman-Ford para la determinación de la mejor ruta.

Algunos protocolos por vector de distancia envían en forma periódica tablas de enrutamiento completas a todos los vecinos conectados. En las redes extensas, estas actualizaciones de enrutamiento pueden llegar a ser enormes y provocar un tráfico importante en los enlaces.

**Reproduzca la animación para observar la operación de los protocolos de enrutamiento por vector de distancia.**

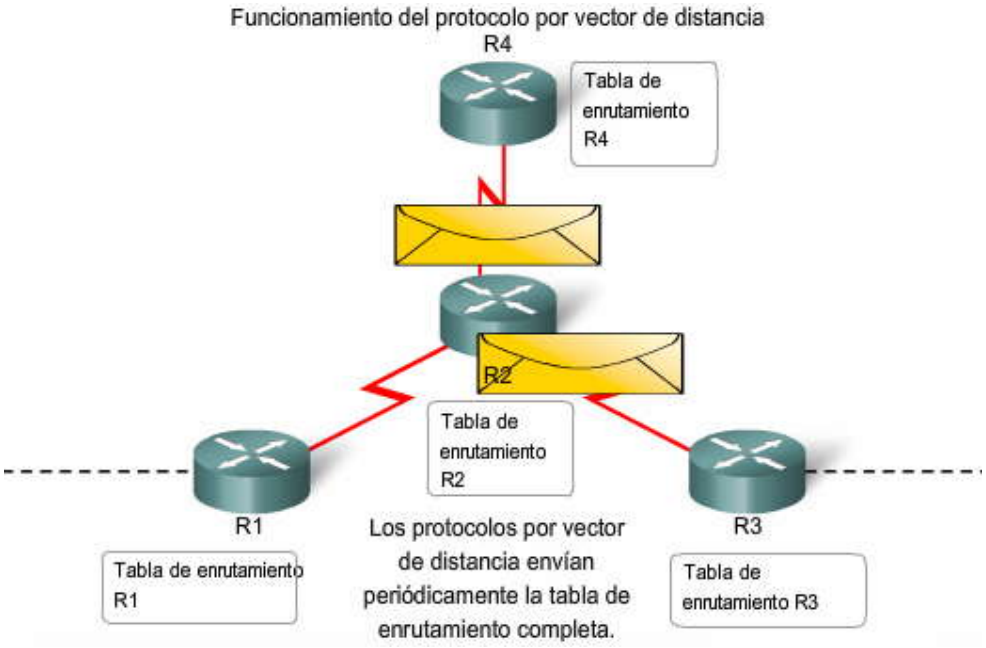
Aunque el algoritmo Bellman-Ford eventualmente acumula suficiente conocimiento como para mantener una base de datos de las redes alcanzables, el algoritmo no permite que un router conozca la topología exacta de una internetwork. El router solamente conoce la información de enrutamiento que recibió de sus vecinos.

Los protocolos por vector de distancia utilizan routers como letreros a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento por vector de distancia no tienen un mapa en sí de la topología de la red.

Los protocolos por vector de distancia funcionan mejor en situaciones donde:

- la red es simple y plana y no requiere de un diseño jerárquico especial,
- los administradores no tiene suficientes conocimientos como para configurar protocolos de estado de enlace y resolver problemas en ellos,
- se están implementando tipos de redes específicos, como las redes hub-and-spoke y
- Los peores tiempos de convergencia en una red no son motivo de preocupación.

Las funciones y operaciones del protocolo de enrutamiento por vector de distancia se explicarán en el próximo capítulo. También se aprenderá sobre las operaciones y la configuración de los protocolos de enrutamiento por vector de distancia RIP y EIGRP.




**Operación del protocolo de estado de enlace**

A diferencia de la operación del protocolo de enrutamiento por vector de distancia, un router configurado con un protocolo de enrutamiento de estado de enlace puede crear una "vista completa" o topología de la red al reunir información

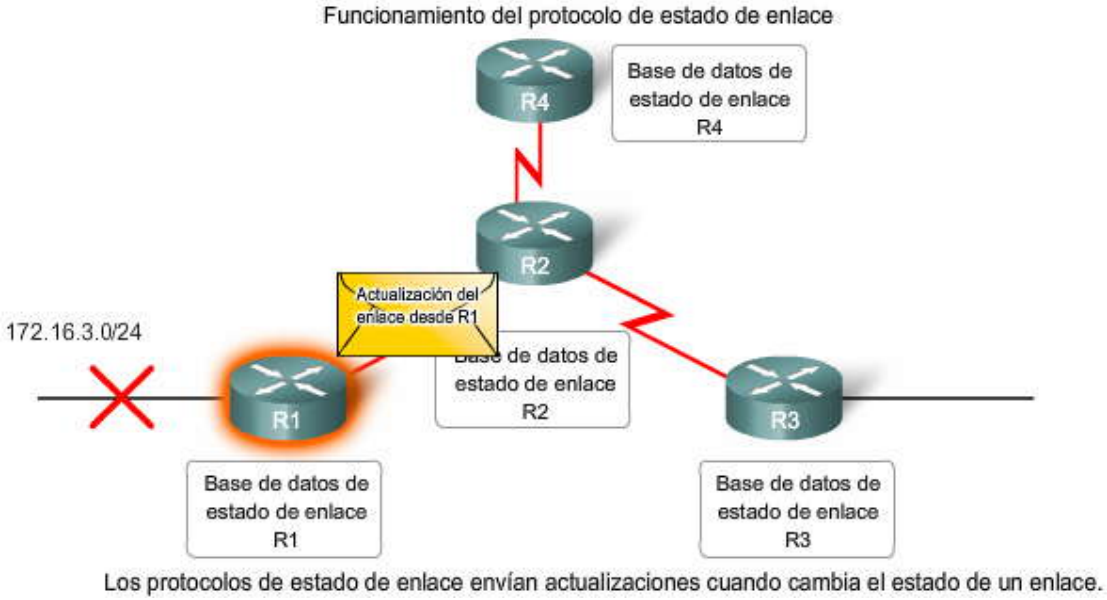
proveniente de todos los demás routers. Para continuar con nuestra analogía de letreros, el uso de un pro tocolo de enrutamiento de estado de enlace es como tener un mapa completo de la topología de la red. Los letreros a lo largo de la ruta desde el origen al destino no son necesarios, porque todos los routers de estado de enlace usan un "mapa" idéntico de la red. Un router de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar la mejor ruta hacia todas las redes de destino en la topología.

**Reproduzca la animación.**
Con algunos protocolos de enrutamiento por vector de distancia, los routers envían actualizaciones periódicas de su información de enrutamiento a sus vecinos. Los protocolos de enrutamiento de estado de enlace no usan actualizaciones periódicas. Luego de que la red ha convergido, la actualización del estado de enlace sólo se envía cuando se produce un cambio en la topología. Por ejemplo, la actualización del estado de enlace en la animación no se envía hasta que la red 172.16.3.0 se desactiva.

Los protocolos de estado de enlace funcionan mejor en situaciones donde:

- El diseño de red es jerárquico, y por lo general ocurre en redes extensas.
- Los administradores conocen a fondo el protocolo de enrutamiento de estado de enlace implementado.
- Es crucial la rápida convergencia de la red.

Las funciones y operaciones del protocolo de enrutamiento de estado de enlace se explicarán en capítulos posteriores. También se aprenderán las operaciones y la configuración del protocolo de enrutamiento de estado de enlace OSPF.




### 3.2.4 CON CLASE Y SIN CLASE.-

**Protocolos de enrutamiento con clase**

**Los protocolos de enrutamiento con clase no envían información de la máscara de subred en las actualizaciones de enrutamiento.** Los primeros protocolos de enrutamiento tales como el RIP, fueron con clase. En aquel momento, las direcciones de red se asignaban en función de las clases; clase A, B o C. No era necesario que un protocolo de enrutamiento incluyera una máscara de subred en la actualización de enrutamiento porque la máscara de red podía determinarse en función del primer octeto de la dirección de red.

Los protocolos de enrutamiento con clase aún pueden usarse en algunas de las redes actuales, pero dado que no incluyen la máscara de subred, no pueden usarse en todas las situaciones. Los protocolos de enrutamiento con clase no pueden usarse cuando una red se divide en subredes utilizando más de una máscara de subred; en otras palabras, los protocolos de enrutamiento con clase no admiten máscaras de subred de longitud variable (VLSM).

Existen otras limitaciones de los protocolos de enrutamiento con clase, entre ellas la imposibilidad de admitir redes no contiguas. Los protocolos de enrutamiento con clase, las redes no contiguas y VLSM se analizarán en capítulos posteriores.

Los protocolos de enrutamiento con clase incluyen RIPv1 e IGRP.

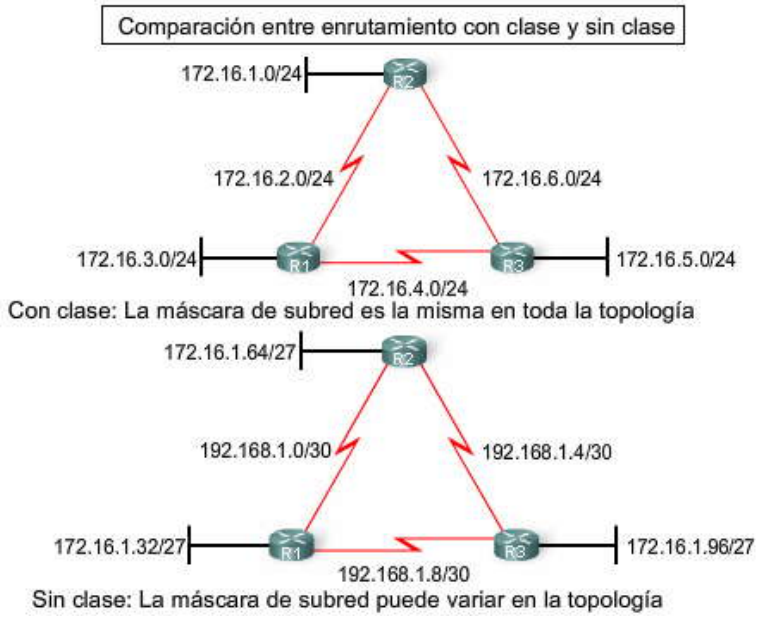
**Protocolos de enrutamiento sin clase**

Los protocolos de enrutamiento sin clase incluyen la máscara de subred con la dirección de red en las actualizaciones de enrutamiento. Las redes de la actualidad ya no se asignan en función de las clases y la máscara de subred no puede

determinarse según el valor del primer octeto. La mayoría de las redes de la actualidad requieren protocolos de enrutamiento sin clase porque admiten VLSM, redes no contiguas y otras funciones que se analizarán en capítulos posteriores.

En la figura, observe que la versión sin clase de la red está usando máscaras de subred /30 y /27 en la misma topología. Además, observe que esta topología está usando un diseño no contiguo.

Los protocolos de enrutamiento sin clase son RIPv2, EIGRP, OSPF, IS-IS y BGP.



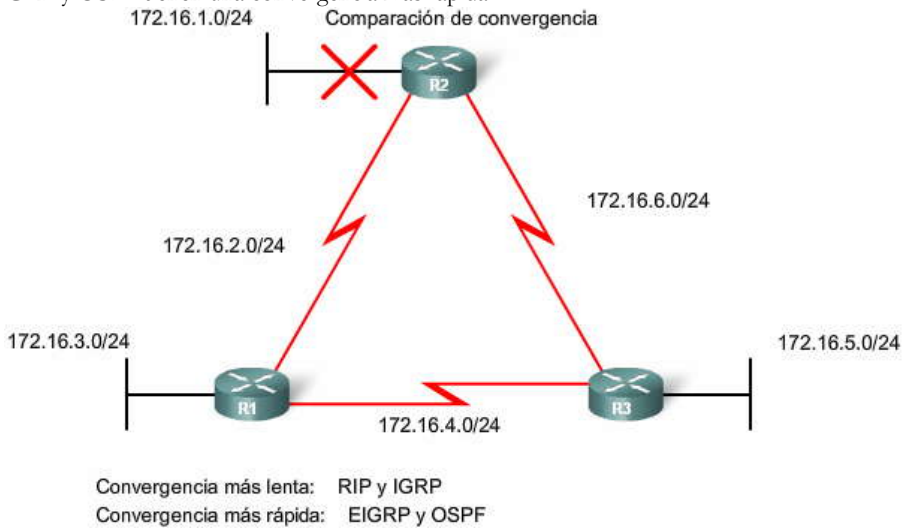

### 3.2.5 CONVERGENCIA.-

**¿Qué es la convergencia?**

La convergencia ocurre cuando todas las tablas de enrutamiento de los routers se encuentran en un estado de uniformidad. La red ha convergido cuando todos los routers tienen información completa y precisa sobre la red. El tiempo de convergencia es el tiempo que los routers tardan en compartir información, calcular las mejores rutas y actualizar sus tablas de enrutamiento. Una red no es completamente operativa hasta que la red haya convergido; por lo tanto, la mayoría de las redes requieren tiempos de convergencia cortos.

La convergencia es cooperativa e independiente. Los routers comparten información entre sí pero deben calcular en forma independiente los impactos del cambio de topología en sus propias rutas. Dado que establecen un acuerdo con la nueva topología en forma independiente, se dice que convergen sobre este consenso.

Las propiedades de convergencia incluyen la velocidad de propagación de la información de enrutamiento y el cálculo de rutas óptimas. Los protocolos de enrutamiento pueden clasificarse en base a la velocidad de convergencia; cuanto más rápida sea la convergencia, mejor será el protocolo de enrutamiento. Por lo general, RIP e IGRP tienen convergencia lenta, mientras que EIGRP y OSPF tienen una convergencia más rápida.



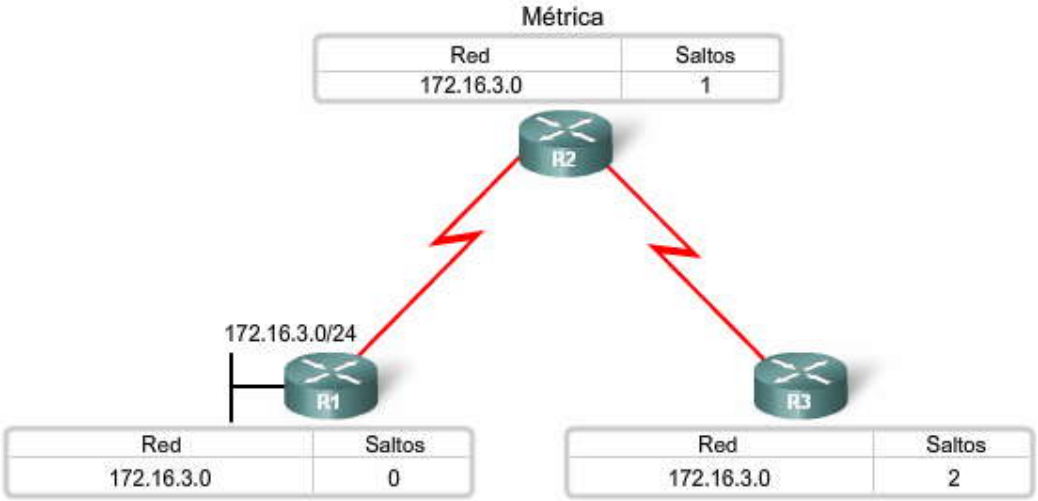
## 3.3 MÉTRICAS.-

### 3.3.1 PROPÓSITO DE UNA MÉTRICA.-

En algunos casos, un protocolo de enrutamiento aprende sobre más de una ruta hacia el mismo destino. Para seleccionar la mejor ruta, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Para tal fin, se usa una **métrica**. Una métrica es un valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar las redes remotas. La métrica se utiliza para determinar qué ruta es más preferible cuando existen múltiples rutas hacia la misma red remota.

Cada protocolo de enrutamiento usa su propia métrica. Por ejemplo, RIP usa el conteo de saltos, EIGRP usa una combinación de ancho de banda y retardo, y la implementación de OSPF de Cisco usa el ancho de banda. El conteo de saltos es la métrica más sencilla para hacer previsiones. El conteo de saltos se refiere a la cantidad de routers que debe atravesar un paquete para llegar a la red de destino. Para R3 en la figura, la red 172.16.3.0 se encuentra a dos saltos o dos routers de distancia.

**Nota**: Las métricas para un protocolo de enrutamiento particular y su forma de calcularlas se analizarán en el capítulo dedicado a ese protocolo de enrutamiento específico.




### 3.3.2 MÉTRICAS Y PROTOCOLOS DE ENRUTAMIENTO.-

**Parámetros de las métricas**

Diferentes protocolos de enrutamiento usan diferentes métricas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de enrutamiento diferentes pueden elegir diferentes rutas hacia el mismo destino debido al uso de diferentes métricas.

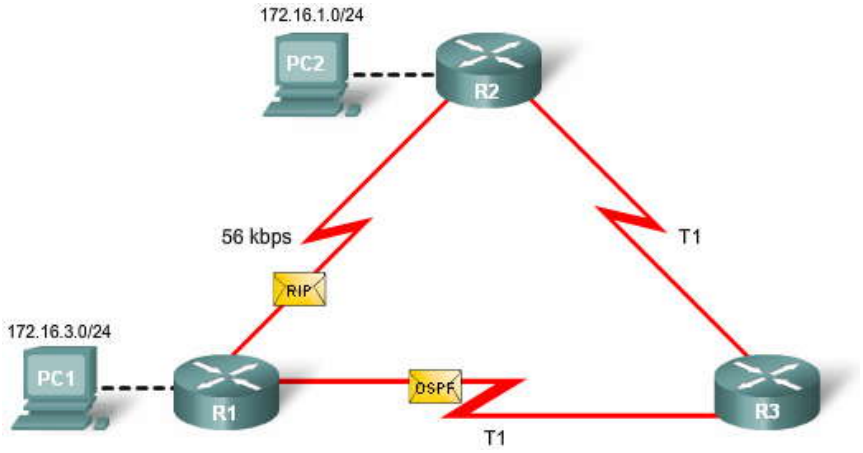
**Reproduzca la animación.**

El RIP elegirá la ruta con la menor cantidad de saltos, mientras que OSPF elegirá la ruta con el ancho de banda más alto.

Las métricas utilizadas en los protocolos de enrutamiento IP incluyen:

- **Conteo de saltos:** una métrica simple que cuenta la cantidad de routers que un paquete tiene que atravesar
- **Ancho de banda:** influye en la selección de rutas al preferir la ruta con el ancho de banda más alto
- Carga: considera la utilización de tráfico de un enlace determinado
- **Retardo:** considera el tiempo que tarda un paquete en atravesar una ruta
- **Confiabilidad:** evalúa la probabilidad de una falla de enlace calculada a partir del conteo de errores de la interfaz o las fallas de enlace previas
- **Costo:** un valor determinado ya sea por el IOS o por el administrador de red para indicar la preferencia hacia una ruta. El costo puede representar una métrica, una combinación de las mismas o una política.

Nota: En este punto, no es importante comprender completamente estas métricas ya que se explicarán en capítulos posteriores.

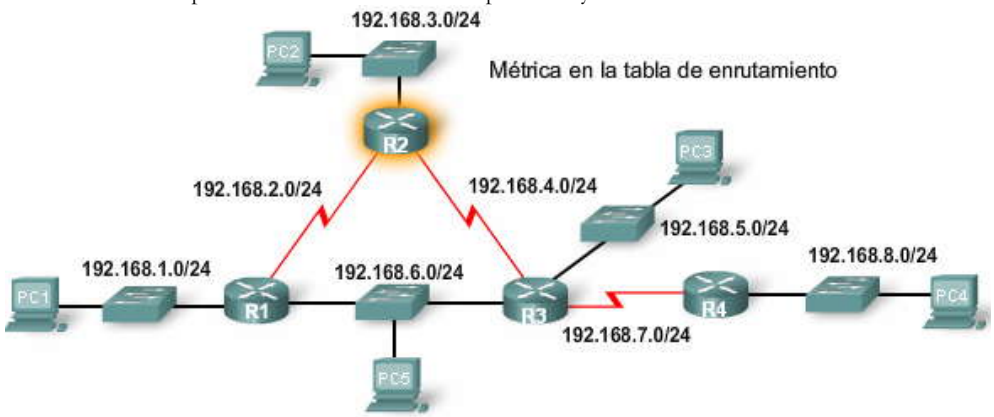



**El campo Métrica en la tabla de enrutamiento**

La métrica para cada protocolo de enrutamiento es:

- **RIP**: conteo de saltos: la mejor ruta se elige según la ruta con el menor conteo de saltos.
- **IGRP e EIGRP:** ancho de banda, retardo, confiabilidad y carga; la mejor ruta se elige según la ruta con el valor de métrica compuesto más bajo calculado a partir de estos múltiples parámetros. Por defecto, sólo se usan el ancho de banda y el retardo.
- **IS-IS y OSPF:** costo; la mejor ruta se elige según la ruta con el costo más bajo. . La implementación de OSPF de Cisco usa el ancho de banda. IS-IS es desarrollado en CCNP.

Los protocolos de enrutamiento determinan la mejor ruta en base a la ruta con la métrica más baja.
Consulte el ejemplo en la figura. Los routers están usando el protocolo de enrutamiento RIP. La métrica asociada con una ruta determinada puede visualizarse mejor utilizando el comando **show ip route**. El valor de métrica es el segundo valor en los corchetes para una entrada de la tabla de enrutamiento. En la figura, R2 tiene una ruta hacia la red 192.168.8.0/24 que se encuentra a 2 saltos de distancia.
**R 192.168.8.0/24 [120/2] mediante 192.168.4.1, 00:00:26, Serial0/0/1**
**Nota:** En capítulos posteriores que describen a los protocolos de enrutamiento individuales, se ofrecerá información más detallada sobre las métricas de protocolos de enrutamiento específicos y cómo calcularlas.




```
R2#show ip route
<output omitted>

Gateway of last resort is not set

R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
C    192.168.2.0/24 is directly connected, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.6.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0
                            [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:26, Serial0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:26, Serial0/1
```

Son 2 saltos desde R2 a 192.168.8.0/24

### 3.3.3 BALANCEO DE CARGA.-

Hemos visto que los protocolos de enrutamiento individuales utilizan métricas para determinar la mejor ruta para llegar a redes remotas. Pero, ¿qué sucede cuando dos o más rutas hacia el mismo destino tienen valores de métrica idénticos? ¿Cómo decidirá el router qué ruta usar para el envío de paquetes? En este caso, el router no elige sólo una ruta. **En cambio, el router realiza un "balanceo de carga" entre estas dos rutas del mismo costo.** Los paquetes se envían utilizando todas las rutas del mismo costo.

Para comprobar si el balanceo de carga está en uso, verifique la tabla de enrutamiento. **El balanceo de carga está en uso si dos o más rutas se asocian con el mismo destino.**

Nota: El balanceo de carga puede realizarse ya sea por paquete o por destino. El modo en que un router realiza realmente el balanceo de carga de los paquetes entre rutas del mismo costo depende del proceso de conmutación. El proceso de conmutación se analizará con más profundidad en otro capítulo.

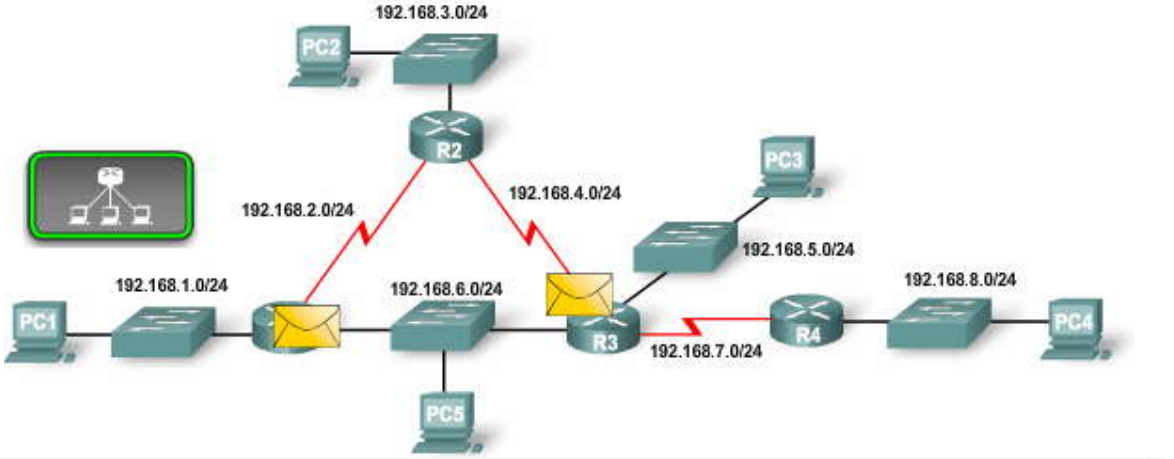
**Reproduzca la animación.**

R2 realiza el balanceo de carga del tráfico hacia la PC5 a través de dos rutas del mismo

El comando **show ip route** revela que la red de destino 192.168.6.0 está disponible a través de 192.168.2.1 (Serial 0/0/0) y 192.168.4.1 (Serial 0/0/1).

R 192.168.6.0/24 [120/1] a través de 192.168.2.1, 00:00:24, Serial0/0/0
[120/1] a través de 192.168.4.1, 00:00:26, Serial0/0/1

Por defecto, todos los protocolos de enrutamiento analizados en este curso son capaces de realizar un balanceo de carga del tráfico en forma automática para un máximo de cuatro rutas del mismo costo por defecto. El EIGRP también admite el balanceo de carga a través de rutas de distinto costo. Esta función de EIGRP se analiza en CCNP.




## 3.4 DISTANCIAS ADMINISTRATIVAS.-

### 3.4.1 PROPÓSITO DE LA DISTANCIA ADMINISTRATIVA.-

**Múltiples orígenes de enrutamiento**

Sabemos que los routers aprenden sobre redes adyacentes que están conectadas directamente y sobre redes remotas mediante el uso de rutas estáticas y protocolos de enrutamiento dinámico. En realidad, un router puede aprender sobre una ruta hacia la misma red a través de más de un origen. Por ejemplo, una ruta estática puede haber sido configurada para la misma red/máscara de subred que se aprendió en forma dinámica mediante un protocolo de enrutamiento dinámico, como RIP. El router debe elegir qué ruta instalar.

**Nota:** Posiblemente se esté preguntando sobre las rutas del mismo costo. Sólo pueden instalarse múltiples rutas hacia la misma red cuando provienen del mismo origen de enrutamiento. Por ejemplo, para que se instalen rutas del mismo costo, ambas rutas deben ser estáticas o deben ser rutas RIP.

Aunque es menos común, puede implementarse más de un protocolo de enrutamiento dinámico en la misma red. En algunas situaciones, posiblemente sea necesario enrutar la misma dirección de red utilizando múltiples protocolos de enrutamiento como RIP y OSPF. Debido a que diferentes protocolos de enrutamiento usan diferentes métricas, RIP usa el conteo de saltos y OSPF usa el ancho de banda, no es posible comparar las métricas para determinar la mejor ruta.

Entonces, ¿cómo determina un router qué ruta instalar en la tabla de enrutamiento cuando se ha aprendido sobre una misma red desde más de un origen de enrutamiento?

**El propósito de la distancia administrativa**

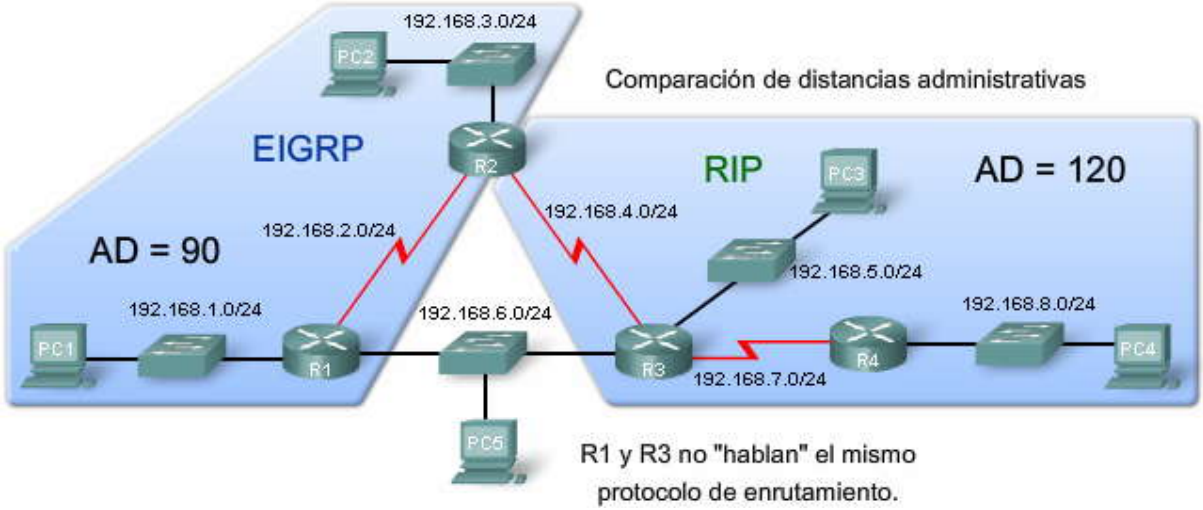
La distancia administrativa (AD) define la preferencia de un origen de enrutamiento. A cada origen de enrutamiento, entre ellas protocolos de enrutamiento específicos, rutas estáticas e incluso redes conectadas directamente , se le asigna un orden de preferencia de la más preferible a la menos preferible utilizando el valor de distancia administrativa. Los routers Cisco usan la función de AD para seleccionar la mejor ruta cuando aprende sobre la misma red de destino desde dos o más orígenes de enrutamiento diferentes.

La distancia administrativa es un valor entero entre 0 y 255. Cuanto menor es el valor, mayor es la preferencia del origen de ruta. Una distancia administrativa de 0 es la más preferida. Solamente una red conectada directamente tiene una distancia administrativa igual a 0 que no puede cambiarse.

Es posible modificar la distancia administrativa para las rutas estáticas y los protocolos de enrutamiento dinámico. Este tema se trata en CCNP.

Una distancia administrativa de 255 indica que el router no creerá en el origen de esa ruta y no se instalará en la tabla de enrutamiento.

**Nota:** Comúnmente se usa el término confiabilidad cuando se define la distancia administrativa. Cuanto menor es el valor de la distancia administrativa, mayor será la confiabilidad de la ruta.




**Haga clic en show ip route en la figura.**

El valor de AD es el primer valor en los corchetes para una entrada de la tabla de enrutamiento. Observe que R2 tiene una ruta hacia la red 192.168.6.0/24 con un valor de AD de 90.

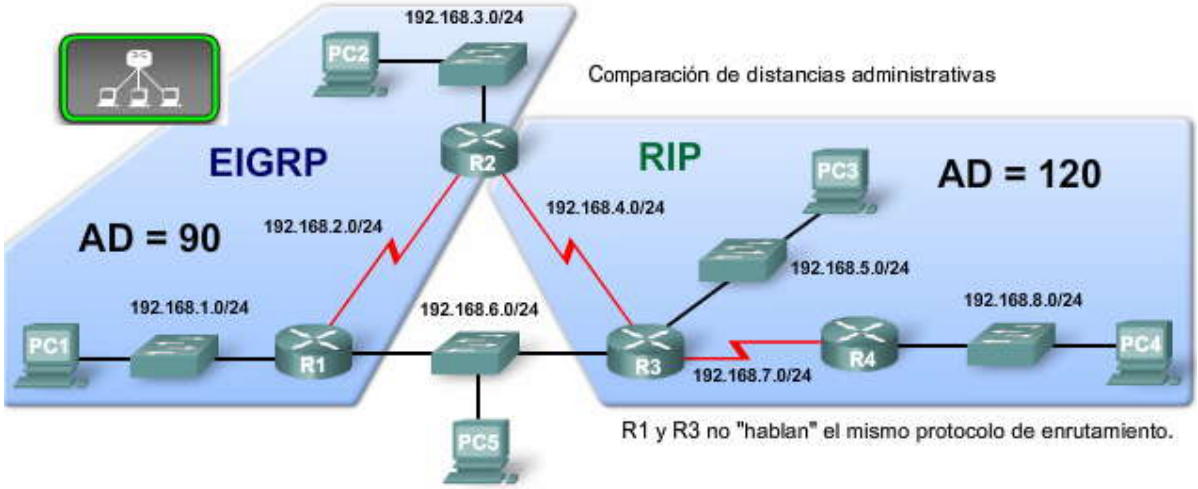
D 192.168.6.0/24 [90/2172416] a través de 192.168.2.1, 00:00:24, Serial0/0/0

R2 está ejecutando los protocolos de enrutamiento RIP y EIGRP. (Recuerde: No es común que los routers ejecuten múltiples protocolos de enrutamiento dinámico, pero se usan aquí para demostrar cómo funciona la distancia administrativa). R2 ha aprendido sobre la ruta 192.168.6.0/24 por R1 a través de actualizaciones de EIGRP y desde R3 a través de actualizaciones de RIP. RIP tiene una distancia administrativa de 120, pero EIGRP tiene una distancia administrativa más baja, igual a 90. Por lo tanto, R2 agrega la ruta que aprendió utilizando el EIGRP en la tabla de enrutamiento y envía todos los paquetes para la red 192.168.6.0/24 al router R1.

**Haga clic en show ip rip database en la figura.**

¿Qué sucede si el enlace hacia R1 deja de estar disponible? Entonces, R2 no tendrá una ruta hacia 192.168.6.0. En realidad, R2 aún tiene almacenada en la base de datos del RIP la información de ruta del RIP para 192.168.6.0. Esto puede verificarse

con el comando **show ip rip database**. Este comando muestra todas las rutas RIP aprendidas por R2, independientemente de si la ruta RIP se instala en la tabla de enrutamiento.




Comparación de distancias administrativas

```
R2#show ip route
<output omitted>
Gateway of last resort is not set
D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

show ip route

```
R2#show ip rip database
192.168.3.0/24    directly connected, FastEthernet0/0
192.168.4.0/24    directly connected, Serial0/0/1
192.168.5.0/24
    [1] via 192.168.4.1, Serial0/0/1
192.168.6.0/24
    [1] via 192.168.4.1, Serial0/0/1
192.168.7.0/24
    [1] via 192.168.4.1, Serial0/0/1
192.168.8.0/24
    [2] via 192.168.4.1, Serial0/0/1
```

show ip rip database

### 3.4.2 PROTOLOCO DE ENRUTAMIENTO DINÁMICO.-

**Haga clic en show ip route en la figura.**

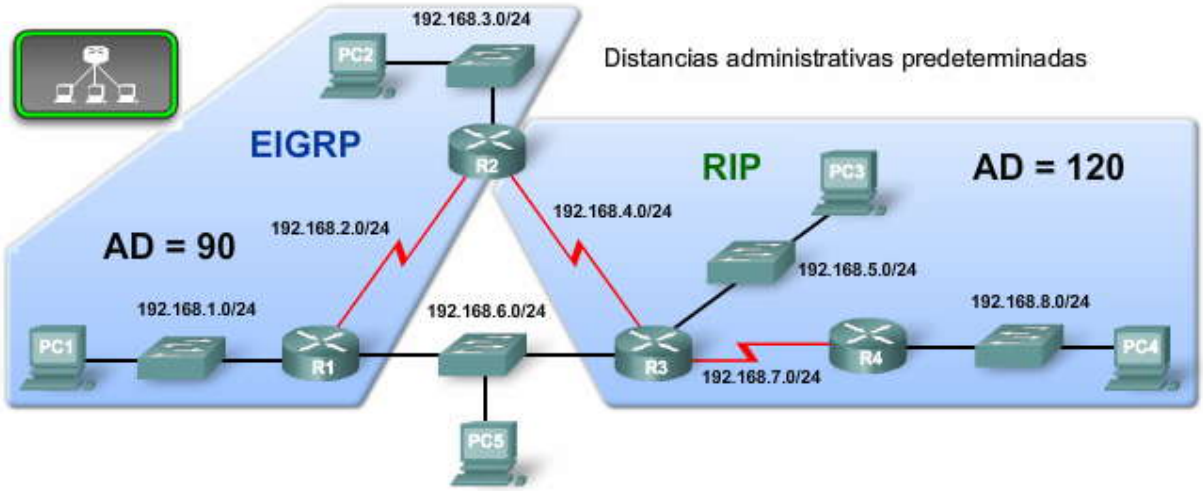
Usted ya sabe que puede verificar estos valores de AD con el comando **show ip route.**

**Haga clic en show ip protocols en la figura.**

El valor de AD también puede verificarse con el comando **show ip protocols**. Este comando muestra toda la información pertinente sobre los protocolos de enrutamiento que funcionan en el router. Analizaremos el comando show ip protocols en detalle en reiteradas oportunidades durante el resto de este curso. Sin embargo, por ahora observe el resultado resa ltado: R2 tiene dos protocolos de enrutamiento indicados y el valor de AD se denomina **Distancia.**

**Haga clic en la Tabla de AD en la figura.**

Observe los diferentes valores de distancia administrativa para los diversos protocolos de enrutamiento.




R1 y R3 no "hablan" el mismo protocolo de enrutamiento.

Distancias administrativas predeterminadas

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
D    192.168.6.0/24 [90/2172416] via 192.168.2.1, 00:00:24, Serial0/0/0
R    192.168.7.0/24 [120/1] via 192.168.4.1, 00:00:08, Serial0/0/1
R    192.168.8.0/24 [120/2] via 192.168.4.1, 00:00:08, Serial0/0/1
```

show ip route

## Distancias administrativas predeterminadas

```
R2#show ip protocols

Routing Protocol is "eigrp  100 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  Automatic network summarization is in effect
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     192.168.2.0
     192.168.3.0
     192.168.4.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1     90            2366569
  Distance: internal 90 external 170

Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 12 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 1, receive any version
  Interface                Send    Recv    Triggered   RIP   Key-chain
  Serial0/0/1                1     2 1
  FastEthernet0/0            1     2 1
Automatic network summarization is in effect
Maximum path: 4
Routing for Networks:
   192.168.3.0
   192.168.4.0
Passive Interface(s):
Routing Information Sources:
   Gateway            Distance         Last Update
   192.168.4.1        120
```

show ip protocols

## Distancias administrativas predeterminadas

| Origen de la ruta | Distancia administrativa |
|---|---|
| Conectado | 0 |
| Estática | 1 |
| Ruta sumarizada EIGRP | 5 |
| BGP externo | 20 |
| EIGRP interno | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EIGRP externo | 170 |
| BGP interno | 200 |

Tabla AD

### 3.4.3 RUTAS ESTÁTICAS.-

Como se analizó en el Capítulo 2, las rutas estáticas son ingresadas por un administrador que desea configurar en forma manual la mejor ruta hacia el destino. Por ese motivo, las rutas estáticas tienen un valor de AD por defecto igual a 1. Esto significa que después de las redes conectadas directamente, que tienen un valor de AD por defecto igual a 0, las rutas estáticas son el origen de ruta de mayor preferencia.

Existen situaciones en las que un administrador configurará una ruta estática al mismo destino que se aprendió utilizando un protocolo de enrutamiento dinámico pero utilizando una ruta diferente. La ruta estática se configurará con una AD mayor que la del protocolo de enrutamiento. Si ocurre una falla de enlace en la ruta utilizada por el protocolo de enrutamiento dinámico, la ruta ingresada por el protocolo de enrutamiento se elimina de la tabla de enrutamiento. La ruta estática se convertirá entonces en el único origen y se agregará automáticamente a la tabla de enrutamiento. Esto se conoce como ruta estática flotante y se analiza en CCNP.

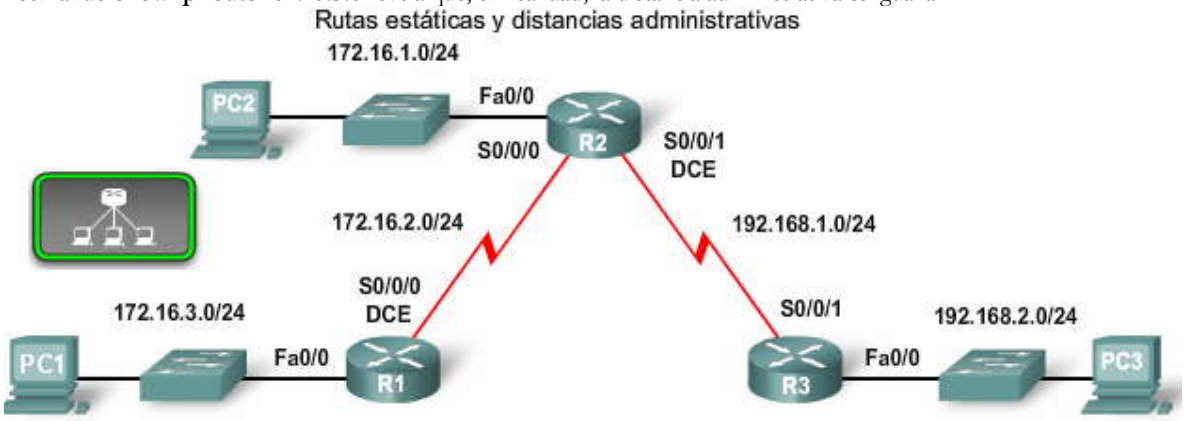
Una ruta estática que usa una dirección IP del siguiente salto o una interfaz de salida, tiene un valor de AD por defecto igual a 1. Sin embargo, el valor de AD no figura en show ip route cuando se configura una ruta estática con la interfaz de salida especificada. Cuando se configura una ruta estática con una interfaz de salida, el resultado muestra a la red como conectada directamente a través de esa interfaz.

**Haga clic en show ip route en la figura.**

La ruta estática a 172.16.3.0 aparece como **conectada directamente**. Sin embargo, no hay información sobre cuál es el valor de AD. Comúnmente se interpreta erróneamente que el valor de AD de esta ruta debe ser igual a 0 porque la indicación es "conectada directamente". Sin embargo, esta suposición es falsa. El valor de AD por defecto de cualquier ruta estática es 1, incluso de aquellas configuradas con una interfaz de salida. Recuerde que solamente una red conectada directamente puede tener una AD igual a 0. Esto puede verificarse extendiendo el comando **show ip route** con la opción[**route**]. Al especificar [**route**] se revela información detallada sobre la ruta, incluso su distancia o valor de AD.

**Haga clic en show ip route 172.16.3.0 en la figura.**

El comando **show ip route 172.16.3.0** revela que, en realidad, la distancia administrativa es igual a 1.




Rutas estáticas y distancias administrativas

```
R2#show ip route
<output omitted>
Gateway of last resort is not set
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1
```

show ip route

Rutas estáticas y distancias administrativas

```
R2#show ip route 172.16.3.0
Routing entry for 172.16.3.0/24
Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Serial0/0/0
      Route metric is 0, traffic share count is 1
```

show ip route 172.16.3.0

### 3.4.4 REDES CONECTADAS DIRECTAMENTE.-

Las redes conectadas directamente se muestran en la tabla de enrutamiento en cuanto se configura la dirección IP en la interfaz y ésta se encuentra habilitada y operativa. El valor de AD de las redes conectadas directamente es igual a 0, lo cual significa que éste es el origen de enrutamiento de mayor preferencia. No existe una ruta mejor para un router que tener una de sus interfaces conectadas directamente a esa red. Por tal motivo, la distancia administrativa de una red conectada directamente no puede cambiarse y ningún otro origen de ruta puede tener una distancia administrativa igual a 0.

**Haga clic en show ip route en la figura.**

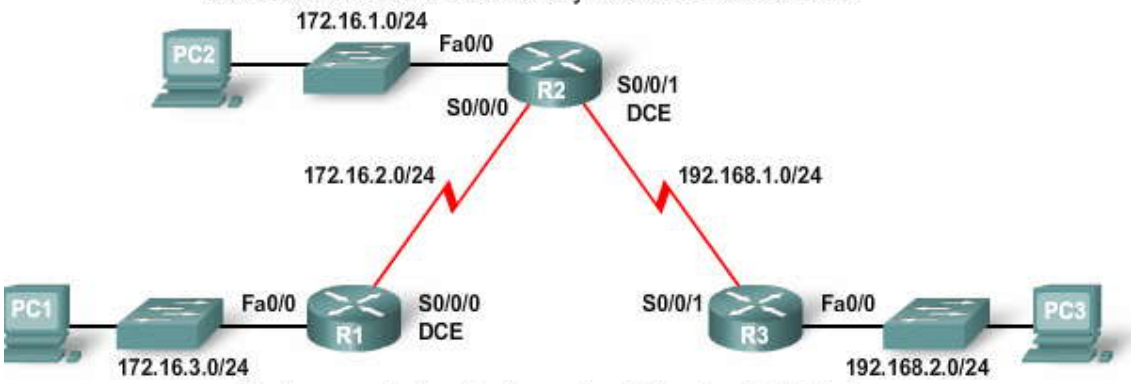
El resultado del comando **show ip route** muestra las redes conectadas directamente sin información sobre el valor de AD. El resultado es similar al de las rutas estáticas que señalan a una interfaz de salida. La única diferencia es la letra C al comienzo de la entrada, lo cual indica que ésta es una red conectada directamente.

Para visualizar el valor de AD de una red conectada directamente, use la opción [**route**].

**Haga clic en show ip route 172.16.1.0 en la figura.**

El comando **show ip route 172.16.1.0** revela que la distancia es igual a 0 para esa ruta conectada directamente.

Redes conectadas directamente y distancia administrativa




Redes conectadas directamente y distancia administrativa

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
S       172.16.3.0 is directly connected, Serial0/0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.2.0/24 [1/0] via 192.168.1.1
```

show ip route

Redes conectadas directamente y distancia administrativa

```
R2#show ip route 172.16.1.0
Routing entry for 172.16.1.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via FastEthernet0/0
      Route metric is 0, traffic share count is 1
```

show ip route 172.16.1.0

## 3.5 PROTOCOLOS DE ENRUTAMIENTO Y ACTIVIDADES DE DIVISION EN SUBREDES

### 3.5.1 IDENTIFICACIÓN DE ELEMENTOS DE LA TABLA DE ENRUTAMIENTO.-

El propósito de este ejercicio es practicar cómo identificar correctamente el origen de ruta, la distancia administrativa y la métrica para una ruta determinada en función del resultado del comando **show ip route**.

El resultado no es común en la mayoría de las tablas de enrutamiento. La ejecución de más de un protocolo de enrutamiento en el mismo router es poco frecuente. La ejecución de tres protocolos, como se muestra aquí, es más que nada un ejercicio académico cuyo valor es ayudar a aprender a interpretar el resultado de la tabla de enrutamiento.

Arrastre y coloque las respuestas correctas en el espacio correspondiente de la tabla.
Utilice como referencia la información de Show IP Route.
No se usan todas las respuestas.
Algunas respuestas se usan más de una vez.

Actividad para arrastrar y colocar

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
     10.0.0.0/16 is subnetted, 1 subnets
S       10.4.0.0 is directly connected, Serial0/0
     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0
D       172.16.3.0 [90/2172416] via 172.16.2.1, 00:00:18, Serial0/0
C    192.168.1.0/24 is directly connected, Serial0/1
O    192.168.100.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0
O    192.168.110.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0
R    192.168.120.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0
```

| Router | Origen del router | AD | Métrica |
|---|---|---|---|
| 10.4.0.0/16 | Estática | 1 | 0 |
| 172.16.2.0/24 | Conectado | 0 | 0 |
| 172.16.1.0/24 | Conectado | 0 | 0 |
| 172.16.3.0/24 | EIGRP | 90 | 2172416 |
| 192.168.1.0/24 | Conectado | 0 | 0 |
| 192.168.100.0/24 | OSPF | 110 | 65 |
| 192.168.110.0/24 | OSPF | 110 | 65 |
| 192.168.120.0/24 | RIP | 120 | 1 |

**3.5.2 SITUACIÓN 1 DE DIVISIÓN EN SUBREDES.-**
**3.5.3 SITUACIÓN 2 DE DIVISIÓN EN SUBREDES.-**
**3.5.4 SITUACIÓN 3 DE DIVISIÓN EN SUBREDES.-**
**3.6 RESUMEN.-**
**3.6.1 RESUMEN Y REVISIÓN.-**
**Resumen**

Los routers utilizan protocolos de enrutamiento dinámico para aprender automáticamente las redes remotas de otros routers. En este capítulo se presentaron varios protocolos de enrutamiento dinámico diferentes.

Se aprendió que los protocolos de enrutamiento pueden clasificarse ya sea como con clase o sin clase, por vector de distancia o estado de enlace, o vector de ruta, y si un protocolo de enrutamiento es un protocolo de gateway interior o un protocolo de gateway exterior. Las diferencias entre estas clasificaciones se comprenderán mejor cuando conozca más a fondo estos conceptos y protocolos de enrutamiento en capítulos posteriores.

Los protocolos de enrutamiento no sólo descubren redes remotas sino que también tienen un procedimiento para mantener información de red precisa. Cuando ocurre un cambio en la topología, es tarea del protocolo de enrutamiento informar a los otros routers sobre este cambio.

Cuando ocurre un cambio en la topología de la red, algunos protocolos de enrutamiento pueden propagar esa información a través del dominio de enrutamiento con más rapidez que otros protocolos de enrutamiento. El proceso de colo car a todas las tablas de enrutamiento en un estado de uniformidad se denomina convergencia. La convergencia ocurre cuando todos los routers en el mismo dominio o área de enrutamiento tienen información completa y precisa sobre la red.

Los protocolos de enrutamiento usan métricas para determinar la mejor ruta o la ruta más corta para llegar a una red de destino. Diferentes protocolos de enrutamiento pueden usar diferentes métricas. Por lo general, una métrica inferior indica una mejor ruta. Cinco saltos para llegar a una red es mejor que 10 saltos.

Los routers a veces aprenden sobre múltiples rutas hacia la misma red a partir de rutas estáticas y protocolos de enrutamiento dinámico. Cuando un router aprende sobre una red de destino desde más de un origen de enrutamiento, los routers Cisco usan el valor de distancia administrativa para determinar qué origen usar. Cada protocolo de enrutamiento dinámico tiene un valor administrativo único junto con las rutas estáticas y las redes conectadas directamente. Cua nto menor es el valor administrativo, mayor es la preferencia del origen de ruta. Una red conectada directamente es siempre el origen preferido, seguido de las rutas estáticas y luego los diversos protocolos de enrutamiento dinámico.

Todas las clasificaciones y los conceptos de este capítulo se analizarán con más profundidad en el resto de los capítulos de este curso. Al finalizar este curso, quizás sea conveniente repasar este capítulo para obtener una revisión y una descripción general de esta información.

**Escalas de enrutamiento dinámico a redes más grandes**

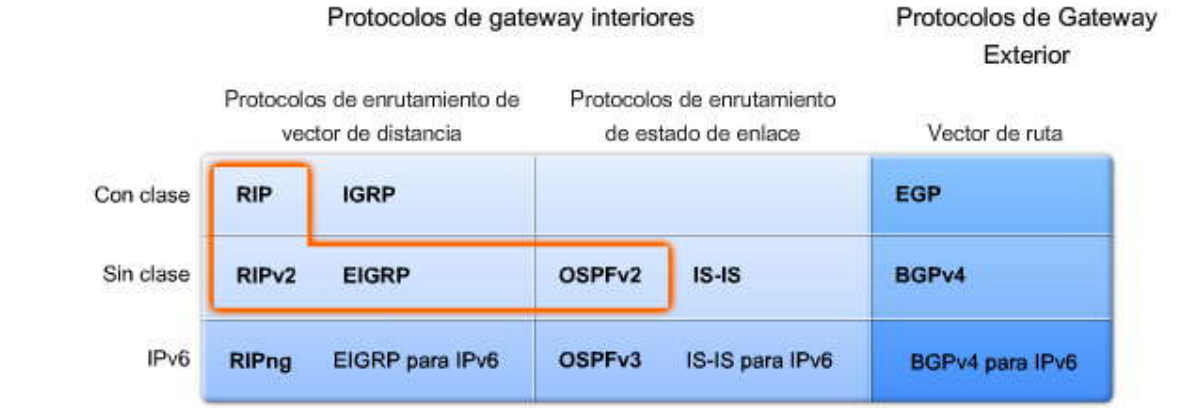

**En este capítulo, aprendió a:**

- Describir el rol de los protocolos de enrutamiento dinámico y ubicar estos protocolos en el contexto del diseño de redes modernas.
- Identificar varias formas de clasificar los protocolos de enrutamiento.
- Describir cómo usan las métricas los protocolos de enrutamiento e identificar las clases de métrica que usan los protocolos de enrutamiento dinámico.
- Determinar la distancia administrativa de una ruta y describir su importancia en el proceso de enrutamiento.
- Identificar los distintos elementos presentes en la tabla de enrutamiento.
- Dadas las limitaciones existentes, elaborar y aplicar esquemas de división de redes.

# CAPITULO IV – "PROTOCOLOS DE ENRUTAMIENTO POR VECTOR DISTANCIA"

## 4.0 INTRODUCCIÓN DEL CAPITULO.-
### 4.0.1 INTRODUCCIÓN DEL CAPITULO.-

**Introducción**
Los capítulos sobre enrutamiento dinámico de este curso se enfocan en los Interior Gateway Protocols (IGP). Como se analizó en el Capítulo 3, los IGP se clasifican en protocolos de enrutamiento por vector de distancia o de estado de enlace. Este capítulo describe las características, operaciones y funcionalidad de los protocolos de enrutamiento por vector de distancia. Existen ventajas y desventajas en cuanto al uso de cualquier tipo de protocolo de enrutamiento. Por lo tanto, se describen las condiciones que afectan el funcionamiento de los protocolos por vector de distancia, las dificultades del funcionamiento de dichos protocolos y las soluciones para dichas dificultades. Es esencial comprender cómo funciona el enrutamiento por vector de distancia a fin de habilitar, verificar y resolver problemas relacionados con estos protocolos.




En este capítulo, aprenderá a:
- Identificar las características de los protocolos de enrutamiento de vector de distancia.
- Describir el proceso de descubrimiento de redes de los protocolos de enrutamiento de vector de distancia utilizando el Routing Information Protocol (RIP).
- Describir los procesos para mantener tablas de enrutamiento precisas utilizadas por los protocolos de enrutamiento de vector de distancia.
- Identificar las condiciones que provocan un routing loop y explicar las consecuencias para el rendimiento del router.
- Identificar los tipos de protocolos de enrutamiento de vector de distancia que se utilizan actualmente.

## 4.1 INTRODUCCIÓN A LOS PROTOCOLOS DE ENRUTAMIENTO POR VECTOR DISTANCIA.-
### 4.1.1 PROTOCOLOS DE ENRUTAMIENTO POR VECTOR DISTANCIA.-
Los protocolos de enrutamiento dinámico ayudan al administrador de red a superar el proceso exigente y prolongado que implica configurar y mantener rutas estáticas. Por ejemplo, ¿puede imaginarse cómo sería mantener las configuraciones de enrutamiento estático de los 28 routers que se muestran en la figura? ¿Qué sucede cuando un enlace deja de funcionar? ¿Cómo garantiza que las rutas redundantes estén disponibles? El enrutamiento dinámico es la opción más común para grandes redes como la que se muestra.

Los protocolos de enrutamiento por vector de distancia incluyen el RIP, el IGRP y el EIGRP.

**RIP**

El Routing Information Protocol (RIP) se especificó originalmente en el RFC 1058. Sus características principales son las siguientes:
Utiliza el conteo de saltos como métrica para la selección de rutas.
Si el conteo de saltos de una red es mayor de 15, el RIP no puede suministrar una ruta para esa red.
Por defecto, se envía un broadcast o multicast de las actualizaciones de enrutamiento cada 30 segundos.

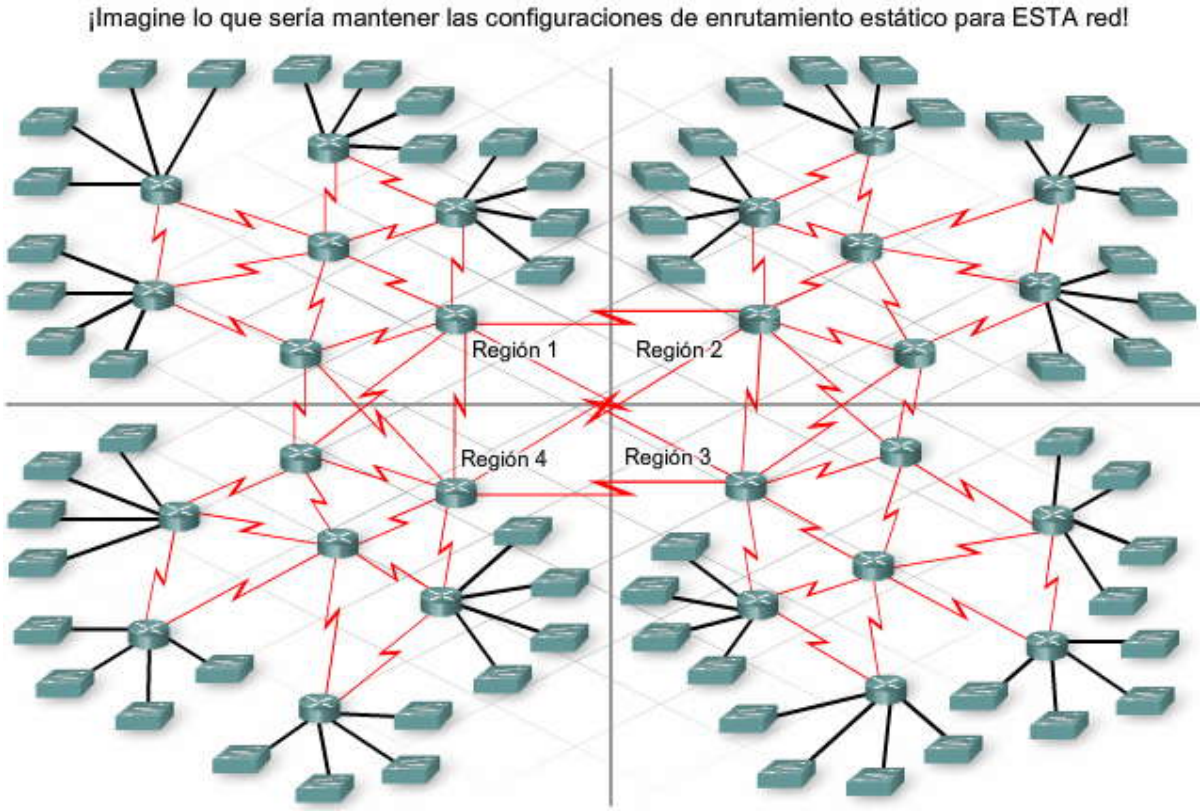
**IGRP**

El Interior Gateway Routing Protocol (IGRP) es un protocolo patentado desarrollado por Cisco. Las características principales de diseño del IGRP son las siguientes:
Se considera el ancho de banda, el retardo, la carga y la confiabilidad para crear una métrica compuesta.
Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

El IGRP es el antecesor de EIGRP y actualmente se considera obsoleto.

**EIGRP**

Enhanced IGRP (IGRP mejorado) es un protocolo de enrutamiento por vector de distancia, patentado por Cisco. Las características principales del EIGRP son las siguientes:
Puede realizar un balanceo de carga con distinto costo.
Utiliza el Algoritmo de actualización por difusión (DUAL) para calcular la ruta más corta.
No existen actualizaciones periódicas, como sucede con el RIP y el IGRP. Las actualizaciones de enrutamiento sólo se envían cuando se produce un cambio en la topología..



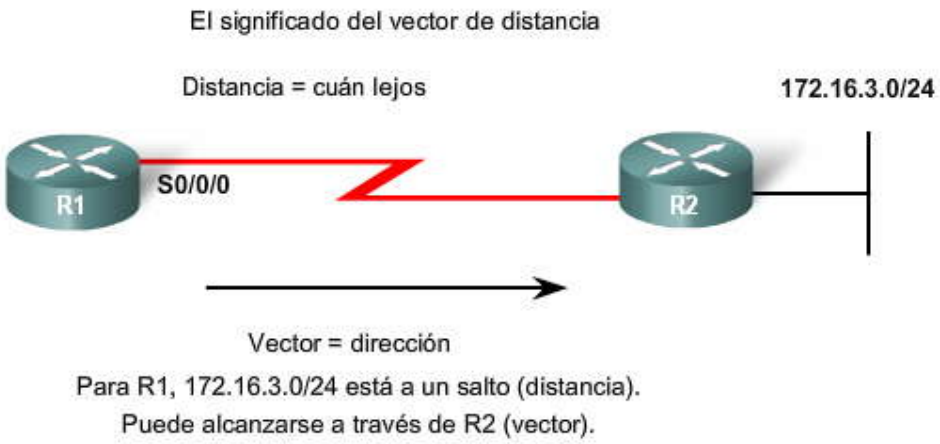

### 4.1.2 TECNNOLOGIA DEL VECTOR DISTANCIA.-

**Significado del vector de distancia**

Como su nombre lo indica, el vector de distancia significa que las rutas son publicadas como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es simplemente el router del siguiente salto o la interfaz de salida.

Un router que utiliza un protocolo de enrutamiento por vector de distancia no conoce toda la ruta hasta la red de destino. En cambio, el router sólo conoce:
la dirección o interfaz en la que deben enviarse los paquetes y
la distancia o qué tan lejos está de la red de destino.

Por ejemplo, en la figura, R1 sabe que la distancia para alcanzar la red 172.16.3.0/24 es de un salto y que la dirección sale desde la interfaz S0/0/0 hacia R2.




**Funcionamiento de los protocolos de enrutamiento por vector de distancia**

Algunos protocolos de enrutamiento por vector de distancia solicitan al router que envíe periódicamente un broadcast de toda la tabla de enrutamiento para cada uno de los vecinos. Este método no es eficiente porque las actualizaciones no sólo consumen ancho de banda sino también los recursos de la CPU del router para procesar las actualizaciones.

Los protocolos de enrutamiento por vector de distancia comparten ciertas características.

Las **actualizaciones periódicas** se envían a intervalos regulares (30 segundos para RIP y 90 segundos para IGRP). Incluso si la topología no ha cambiado en varios días, las actualizaciones periódicas continúan enviándose a todos los vecinos.

Los **vecinos** son routers que comparten un enlace y que están configurados para utilizar el mismo protocolo de enrutamiento. El router sólo conoce las direcciones de red de sus propias interfaces y las direcciones de red remota que puede alcanzar a través de sus vecinos. No tiene un conocimiento más amplio de la topología de la red**. Los routers que utilizan el enrutamiento por vector de distancia no tienen conocimiento de la topología de la red.**

Las **actualizaciones de broadcast** se envían a 255.255.255.255. Los routers vecinos que están configurados con el mismo protocolo de enrutamiento procesarán las actualizaciones. Todos los demás dispositivos también procesarán la actualización hasta la Capa 3 antes de descartarla. Algunos protocolos de enrutamiento por vector de distancia utilizan direcciones de multicast en vez de direcciones de broadcast.

Las **actualizaciones de toda la tabla de enrutamiento** se envían periódicamente a todos los vecinos, salvo algunas excepciones que analizaremos más adelante. Los vecinos que reciban estas actualizaciones deben procesar toda la actualización para encontrar información pertinente y descartar el resto. Algunos protocolos de enrutamiento por vector de distancia, como por ejemplo, el EIGRP, no envían actualizaciones periódicas de la tabla de enrutamiento.

### 4.1.3 ALGORITMOS DE LOS PROTOCOLOS DE ENRUTAMIENTO.-

Objetivo del algoritmo

El algoritmo se encuentra en el centro del protocolo por vector de distancia. El algoritmo se utiliza para calcular las mejores rutas y después enviar dicha información a los vecinos.

Un algoritmo es un procedimiento para realizar una determinada tarea, comenzando por un estado inicial dado y terminando en un estado final definido. Diferentes protocolos de enrutamiento utilizan diferentes algoritmos para instalar rutas en la tabla de enrutamiento, enviar actualizaciones a los vecinos y tomar decisiones de determinación de rutas.

El algoritmo utilizado para los protocolos de enrutamiento define los siguientes procesos:

- mecanismo para enviar y recibir información de enrutamiento,
- mecanismo para calcular las mejores rutas e instalar rutas en la tabla de enrutamiento y
- mecanismo para detectar y reaccionar ante cambios en la topología.

En la animación, R1 y R2 están configurados con un protocolo de enrutamiento. El algoritmo envía y recibe actualizaciones. Tanto R1 como R2 obtienen información nueva de la actualización. En este caso, cada router obtiene información acerca de una red nueva. El algoritmo de cada router realiza los cálculos de manera independiente y actualiza la tabla de enrutamiento con la información nueva. Cuando la LAN de R2 deja de funcionar, el algoritmo construye un update "disparado" y la envía a R1. Luego, R1 elimina la red de la tabla de enrutamiento. Los updates disparados se analizarán más adelante en este capítulo.

- Envío y recepción de actualizaciones
- Calcular la mejor ruta e instalarla
- Detectar cambios en la topología y reaccionar a ellos


| Red | Interfaz | Salto |
|---|---|---|
| 172.16.1.0/24 | Fa0/0 | 0 |
| 172.16.2.0/24 | S0/0/0 | 0 |
| 172.16.3.0/24 | S0/0/0 | 1 |

| Red | Interfaz | Salto |
|---|---|---|
| 172.16.2.0/24 | S0/0/0 | 0 |
| 172.16.3.0/24 | Fa0/0 | 0 |
| 172.16.1.0/24 | S0/0/0 | 1 |

### 4.1.4 CARACTERISTICAS DE LOS PROTOCOLOS DE ENRUTAMIENTO.-

Características de los protocolos de enrutamiento

Los protocolos de enrutamiento pueden compararse según las siguientes características:

**Tiempo de convergencia:** El tiempo de convergencia define con qué rapidez los routers de la topología de la red comparten información de enrutamiento y alcanzan un estado de conocimiento constante. Cuanto más rápida sea la convergencia, más preferible será el protocolo. Los routing loops pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios.

**Escalabilidad:** La escalabilidad define cuán grande puede ser una red según el protocolo de enrutamiento que se implementa. Cuanto más grande sea la red, más escalable debe ser el protocolo de enrutamiento.

**Sin clase (uso de VLSM) o con clase:** Los protocolos de enrutamiento sin clase incluyen la máscara de subred en las actualizaciones. Esta función admite la utilización de la Máscara de subred de longitud variable (VSLM) y un mejor resumen de ruta. Los protocolos de enrutamiento sin clase no incluyen la máscara de subred y no pueden admitir VLSM.

**Uso de recursos:** El uso de recursos incluye los requisitos de un protocolo de enrutamiento, como por ejemplo, el espacio de memoria y la utilización de la CPU y el ancho de banda del enlace. Un mayor número de requisitos de recursos exige hardware más potente para admitir el funcionamiento del protocolo de enrutamiento además de los procesos de envío de paquetes.

**Implementación y mantenimiento:** La implementación y el mantenimiento describen el nivel de conocimiento requerido para que un administrador de red implemente y mantenga la red según el protocolo de enrutamiento aplicado.

Las ventajas y desventajas de los protocolos de enrutamiento por vector de distancia se muestran en la tabla.

Ventajas y desventajas de los protocolos de enrutamiento por vector de distancia

| Ventajas: | Desventajas: |
|---|---|
| **Implementación y mantenimiento simples.** No se requiere de mucho conocimiento para implementar y posteriormente mantener una red con protocolo por vector de distancia. | **Convergencia lenta.** La utilización de actualizaciones periódicas puede hacer que la convergencia sea más lenta. Incluso si se utilizan técnicas avanzadas, como por ejemplo, los updates disparados (que se analizarán más adelante), la convergencia general aún sigue siendo más lenta en comparación con los protocolos de enrutamiento de estado de enlace. |
| **Pocos requisitos de recursos.** Los protocolos por vector de distancia generalmente no requieren una gran cantidad de memoria para almacenar información. Tampoco requieren de una CPU muy potente. Dependiendo del tamaño de la red y del direccionamiento IP implementado, generalmente tampoco requieren de un alto nivel de ancho de banda de enlace para enviar actualizaciones de enrutamiento. Sin embargo, esto puede representar un problema si se implementa un protocolo por vector de distancia en una gran red. | **Escalabilidad limitada.** La convergencia lenta puede limitar el tamaño de la red porque las redes más grandes requieren más tiempo para propagar la información de enrutamiento. |
| | **Routing loops.** Los routing loops pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios. |

**Verificación de aprendizaje sobre los protocolos de enrutamiento**

En la figura, todos los protocolos de enrutamiento analizados en el curso se comparan según estas características. Si bien el IGPR no es más admitido por el IOS, éste se muestra aquí para compararlo con la versión mejorada (Enhanced). Además, el protocolo de enrutamiento IS-IS se analiza en los cursos CCNP pero se muestra aquí porque es un protocolo de gateway interior comúnmente utilizado.

Estudie la figura y después haga clic en el botón Restablecer para vaciar la tabla. Arrastre y coloque las características adecuadas para cada protocolo de enrutamiento. Teniendo en cuenta la información que se analizó anteriormente, debería poder identificar las ventajas y desventajas de los protocolos de enrutamiento por vector de distancia.

| | Vector de distancia | | | | Estado de enlace | |
|---|---|---|---|---|---|---|
| | RIPv1 | RIPv2 | IGRP | EIGRP | OSPF | IS-IS |
| Velocidad de convergencia | Lento | Lento | Lento | Rápido | Rápido | Rápido |
| Escalabilidad: tamaño de la red | Pequeño | Pequeño | Pequeño | Grande | Grande | Grande |
| Uso de VLSM | No | Sí | No | Sí | Sí | Sí |
| Uso de recursos | Bajo | Bajo | Bajo | Medio | Alto | Alto |
| Implementación y mantenimiento | Simple | Simple | Simple | Complejo | Complejo | Complejo |

## 4.2 DESCUBRIMIENTOS DE LA RED.-

### 4.2.1 ARRANQUE EN FRIO.-

Cuando un router arranca en frío o se enciende, no tiene conocimiento alguno de la topología de la red. Ni siquiera tiene conocimiento de que existen dispositivos en el otro extremo de sus enlaces. La única información que tiene un router proviene de su propio archivo de configuración almacenado en la NVRAM. Una vez que se inicia exitosamente, dicho router aplica la configuración guardada. Como se describió en el Capítulo 1 y 2, si el direccionamiento IP se configura correctamente, el router descubrirá inicialmente sus propias redes conectadas directamente.

**Descubrimiento inicial de la red**

En el ejemplo de la figura, después de un arranque en frío y antes del intercambio de la información de enrutamiento, los routers descubren inicialmente sus propias redes conectadas directamente y máscaras de subred. Esta información se agrega a sus tablas de enrutamiento:

**R1**

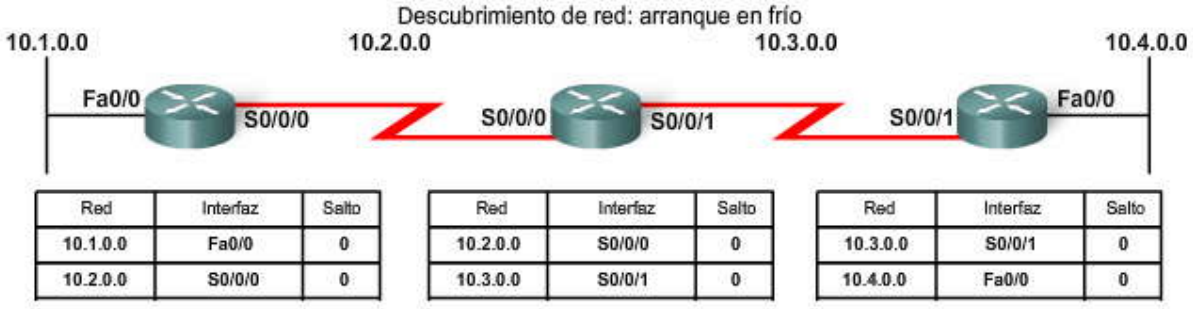
- 10.1.0.0 disponible a través de la interfaz FastEthernet 0/0
- 10.2.0.0 disponible a través de la interfaz Serial 0/0/0

**R2**

- 10.2.0.0 disponible a través de la interfaz Serial 0/0/0
- 10.3.0.0 disponible a través de la interfaz Serial 0/0/1

**R3**

- 10.3.0.0 disponible a través de la interfaz Serial 0/0/0
- 10.4.0.0 disponible a través de la interfaz FastEthernet 0/0




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | Fa0/0 | 0 |

### 4.2.2 INTERCAMBIO INICIAL DE INFORMACIÓN DE ENRUTAMIENTO.-

Si se configura un protocolo de enrutamiento, los routers comienzan a intercambiar actualizaciones de enrutamiento. Inicialmente, estas actualizaciones sólo incluyen información acerca de sus redes conectadas directamente. Una vez recibida la actualización, el router verifica si contiene información nueva. Se agregará cualquier ruta que no esté actualmente en su tabla de enrutamiento.

**Intercambio inicial**

Reproduzca la animación para ver cómo R1, R2 y R3 comienzan el intercambio inicial. Los tres routers envían sus tablas de enrutamiento a sus vecinos que sólo contienen en este momento redes conectadas directamente. Cada router procesa las actualizaciones de la siguiente manera:

**R1**

- Envía una actualización acerca de la red 10.1.0.0 desde la interfaz Serial0/0/0.
- Envía una actualización acerca de la red 10.2.0.0 desde la interfaz FastEthernet0/0.
- Recibe una actualización de R2 acerca de la red 10.3.0.0 con una métrica de 1.
- Almacena la red 10.3.0.0 en la tabla de enrutamiento con una métrica de 1.

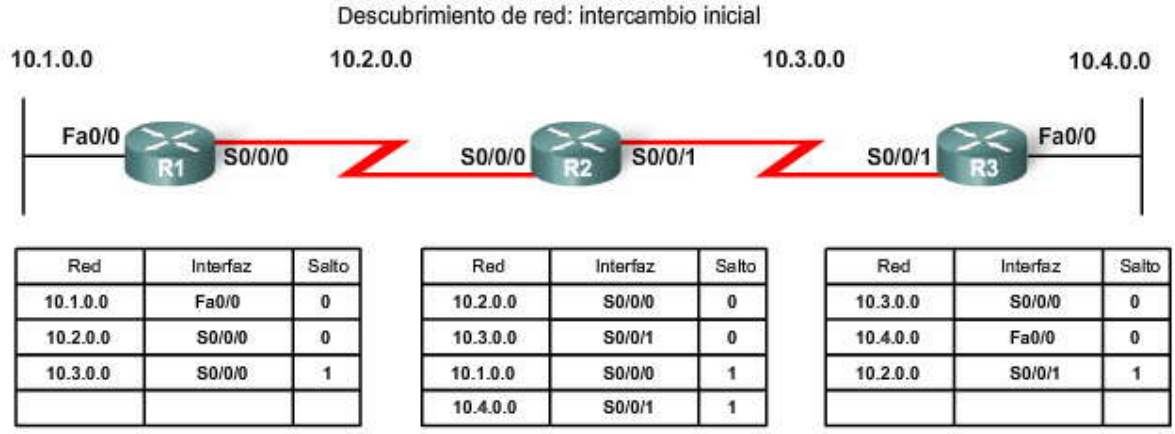
**R2**

- Envía una actualización acerca de la red 10.3.0.0 desde la interfaz Serial 0/0/0.
- Envía una actualización acerca de la red 10.2.0.0 desde la interfaz Serial 0/0/1.
- Recibe una actualización de R1 acerca de la red 10.1.0.0 con una métrica de 1.
- Almacena la red 10.1.0.0 en la tabla de enrutamiento con una métrica de 1.
- Recibe una actualización de R3 acerca de la red 10.4.0.0 con una métrica de 1.
- Almacena la red 10.4.0.0 en la tabla de enrutamiento con una métrica de 1.

**R3**

- Envía una actualización acerca de la red 10.4.0.0 desde la interfaz Serial 0/0/0.
- Envía una actualización acerca de la red 10.3.0.0 desde la FastEthernet0/0.
- Recibe una actualización de R2 acerca de la red 10.2.0.0 con una métrica de 1.
- Almacena la red 10.2.0.0 en la tabla de enrutamiento con una métrica de 1.

Después de esta primera ronda de intercambios de actualizaciones, cada router tiene información acerca de las redes conectadas de sus vecinos conectados directamente. Sin embargo, ¿observó que R1 todavía no tiene información acerca de 10.4.0.0 al igual que R3 acerca de 10.1.0.0? Se obtendrá información completa y se convergerá la red cuando se produzca otro intercambio de información de enrutamiento.




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| | | |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 1 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/0 | 0 |
| 10.4.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/1 | 1 |
| | | |

### 4.2.3 INETRCAMBIO DE INFORMACIÓN DE ENRRUTAMIENTO.-

En este punto, los routers tienen información sobre sus propias redes conectadas directamente y las de sus vecinos más cercanos. Siguiendo el camino hacia la convergencia, los routers intercambian la siguiente ronda de actualizaciones periódicas. Cada router verifica las actualizaciones otra vez para ver si hay información nueva.

**Siguiente actualización**

Reproduzca la animación para ver cómo R1, R2 y R3 envían la tabla de enrutamiento más reciente a sus vecinos. Cada router procesa las actualizaciones de la siguiente manera:

**R1**

Envía una actualización acerca de la red 10.1.0.0 desde la interfaz Serial 0/0/0.
Envía una actualización acerca de las redes 10.2.0.0 y 10.3.0.0 desde la interfaz FastEthernet0/0.
Recibe una actualización de R2 sobre la red 10.4.0.0 con una métrica de 2.
Almacena la red 10.4.0.0 en la tabla de enrutamiento con una métrica de 2.

La misma actualización de R2 contiene información acerca de la red 10.3.0.0 con una métrica de 1. No se produce ningún cambio; por lo tanto, la información de enrutamiento sigue siendo la misma.

**R2**
Envía una actualización acerca de las redes 10.3.0.0 y 10.4.0.0 desde la interfaz Serial 0/0/0.
Envía una actualización acerca de las redes 10.1.0.0 y 10.2.0.0 desde la interfaz Serial 0/0/1.
Recibe una actualización de R1 acerca de la red 10.1.0.0. No se produce ningún cambio; por lo tanto, la información de enrutamiento sigue siendo la misma.
Recibe una actualización de R3 acerca de la red 10.4.0.0. No se produce ningún cambio; por lo tanto, la información de enrutamiento sigue siendo la misma.

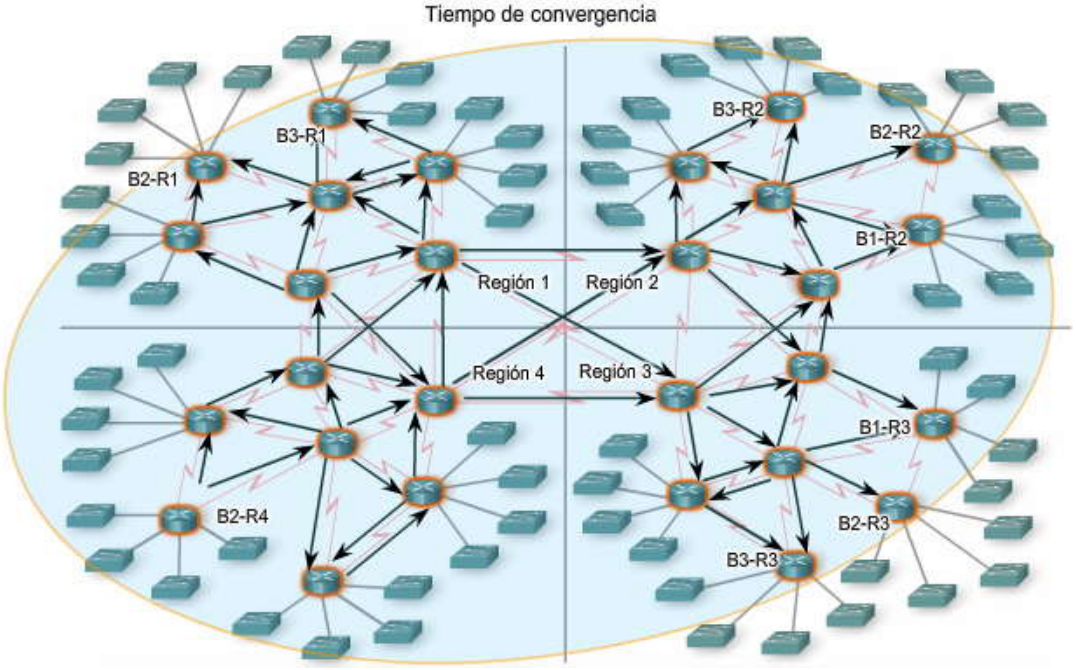
**R3**
Envía una actualización acerca de la red 10.4.0.0 desde la interfaz Serial 0/0/0.
Envía una actualización acerca de las redes 10.2.0.0 y 10.3.0.0 desde la interfaz FastEthernet0/0.
Recibe una actualización de R2 sobre la red 10.1.0.0 con una métrica de 2.
Almacena la red 10.1.0.0 en la tabla de enrutamiento con una métrica de 2.
La misma actualización de R2 contiene información acerca de la red 10.2.0.0 con una métrica de 1. No se produce ningún cambio; por lo tanto, la información de enrutamiento sigue siendo la misma.

**Nota:** Generalmente, los protocolos de enrutamiento por vector de distancia implementan una técnica conocida como horizonte dividido. El horizonte dividido evita que la información se envíe desde la misma interfaz en la que se recibió dicha información. Por ejemplo, R2 no enviaría una actualización desde Serial 0/0/0 que contenga la red 10.1.0.0 porque R2 ya aprendió sobre esa red a través de Serial 0/0/0. Este mecanismo se explicará en mayor detalle más adelante en este capítulo.

### 4.2.4 COVERGENCIA.-
La cantidad de tiempo necesario para que una red sea convergente es directamente proporcional al tamaño de dicha red. En la animación, un router de una sucursal en la Región 4 (B2-R4) está arrancando en frío. La animación muestra la propagación de la nueva información de enrutamiento a medida que se envían las actualizaciones entre los routers vecinos. Se necesitan cinco rondas de intervalos de actualizaciones periódicas antes de que la mayoría de los routers de sucursales de las Regiones 1, 2 y 3 aprendan sobre las nuevas rutas publicadas por B2-R4. Los protocolos de enrutamiento se comparan según la rapidez con la que pueden propagar esta información (su velocidad para converger).

La velocidad para alcanzar la convergencia consiste en:
- La velocidad en que los routers propagan un cambio de topología en una actualización de enrutamiento a sus vecinos.
- La velocidad para calcular las mejores rutas utilizando la nueva información de enrutamiento obtenida.

Una red no está completamente operativa hasta que haya convergido; por lo tanto, los administradores de red prefieren protocolos de enrutamiento con tiempos de convergencia más cortos.



## 4.3 PROTOCOLO DE MANTENIMIENTO DE LAS TABLAS DE ENRUTAMIENTO.-

### 4.3.1 ACTUALIZACIONES PERIODICAS: RIPv1 e IGRP.-

**Mantenimiento de las tablas de enrutamiento**

Muchos protocolos por vector de distancia utilizan actualizaciones periódicas para intercambiar información de enrutamiento con sus vecinos y mantenerla actualizada en la tabla de enrutamiento. El RIP y el IGRP son ejemplos de dichos protocolos.

En la animación, los routers envían periódicamente la tabla de enrutamiento a los vecinos. El término actualizaciones periódicas se refiere al hecho de que un router envía la tabla de enrutamiento completa a sus vecinos a intervalos predefinidos. Para el RIP, estas actualizaciones se envían cada 30 segundos como un broadcast (255.255.255.255), ya sea que se haya producido un cambio en la topología o no. Este intervalo de 30 segundos es un temporizador de actualización de ruta que también ayuda a realizar un seguimiento de la antigüedad de la información en la tabla de enrutamiento.

La antigüedad de la información de una tabla de enrutamiento se renueva cada vez que se recibe una actualización. De esta manera, se puede mantener la información de la tabla de enrutamiento cuando se produce un cambio en la topología. Los cambios pueden producirse por diversas razones entre las que se incluyen:
falla de un enlace,
introducción de un enlace nuevo,
falla de un router y
cambio en los parámetros del enlace.


```
R1#show ip route
<output omitted>

Gateway of last resort is not set

     10.0.0.0/16 is subnetted, 4 subnets
C       10.2.0.0 is directly connected, Serial0/0/0
R       10.3.0.0 [120/1] via 10.2.0.2, 00:00:04, Serial0/0/0
C       10.1.0.0 is directly connected, FastEthernet0/0
R       10.4.0.0 [120/2] via 10.2.0.2, 00:00:04, Serial0/0/0
```

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 13 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  <output omitted>
  Routing for Networks:
    10.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.3.0.1              120      00:00:27
  Distance: (default is 120)
```

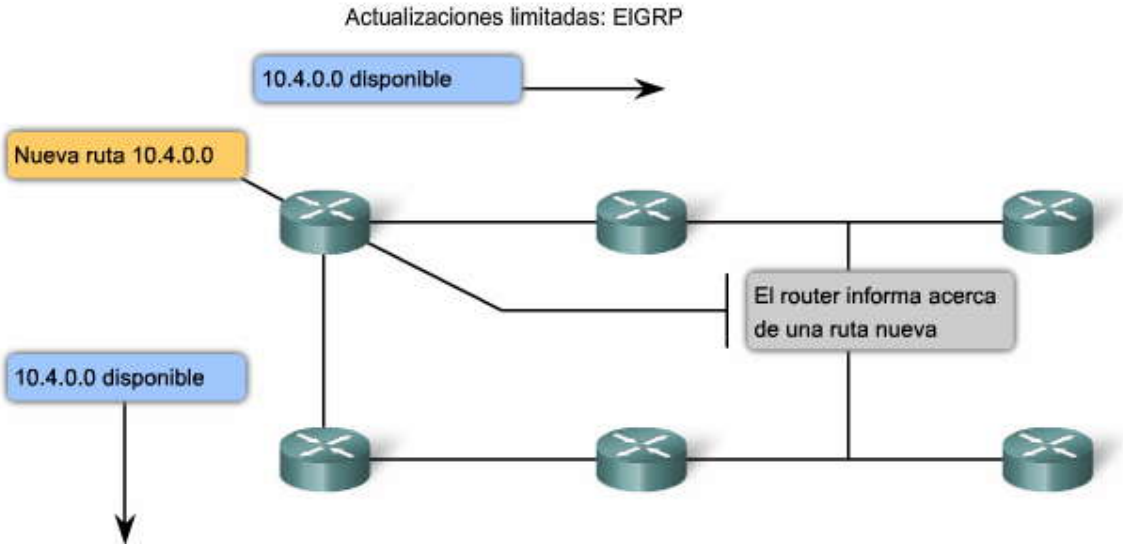
### 4.3.2 ACTUALIZACIONES LIMITADAS: EIGRP.-

A diferencia de los protocolos de enrutamiento por vector de distancia, los EIGRP no envían actualizaciones periódicas. En cambio, el EIGRP envía actualizaciones limitadas acerca de una ruta cuando cambia una ruta o su métrica. Cuando una nueva ruta se vuelve disponible o cuando debe eliminarse una ruta, el EIGRP envía una actualización solamente acerca de dicha red en lugar de toda la tabla. Esta información se envía sólo a aquellos routers que la necesitan.

El EIGRP utiliza actualizaciones que son:

- actualizaciones no periódicas porque no se envían de manera regular,
- actualizaciones parciales que se envían sólo cuando se produce un cambio en la topología que afecta la información de enrutamiento y
- actualizaciones limitadas, es decir, la propagación de las actualizaciones parciales se limita automáticamente, de modo que sólo se actualizan aquellos routers que necesitan la información.

**Nota:** Se presentará más información sobre cómo funciona el EIGRP en el Capítulo 9.




### 4.3.3 UPDATES DISPARADOS.-

Para acelerar la convergencia cuando se produce un cambio en la topología, el RIP utiliza updates disparados. Un update disparado es una actualización de la tabla de enrutamiento que se envía de manera inmediata en respuesta a un cambio en el enrutamiento. Los updates disparados no esperan a que venzan los temporizadores de actualización. El router detector envía de manera inmediata un mensaje de actualización a los routers adyacentes. A su vez, los routers receptores generan updates disparados que notifican a sus vecinos acerca del cambio.

Los updates disparados se envían cuando se produce cualquiera de las siguientes situaciones:

- Una interfaz cambia de estado (up o down).
- Una ruta ingresa (o sale) al estado "inalcanzable".
- Se instala una ruta en la tabla de enrutamiento.

Sólo la utilización de updates disparados debería ser suficiente si se pudiera garantizar que la ola de actualizaciones alcanza de inmediato a todos los routers correspondientes. Sin embargo, existen dos problemas con los upd ates disparados:

- Los paquetes que contienen un mensaje de actualización pueden descartarse o corromperse debido a algún enlace de la red.
- Los updates disparados no se producen instantáneamente. Puede suceder que un router ejecute una actualización regular en el momento equivocado cuando todavía no ha recibido el update disparado. Como resultado, la ruta no válida vuelve a insertarse en un vecino que ya había recibido el update disparado.

**Reproduzca la animación para observar cómo se propaga un cambio en la topología de la red a través de toda la red.** Cuando la red 10.4.0.0 deja de estar disponible y el router C obtiene información al respecto, se envía la información a sus vecinos. Por lo tanto, la información se propaga a través de la red.


### 4.3.4 FLUCTUACIONES DE LA FASE ALEATORIA.-

**Problemas con actualizaciones sincronizadas**

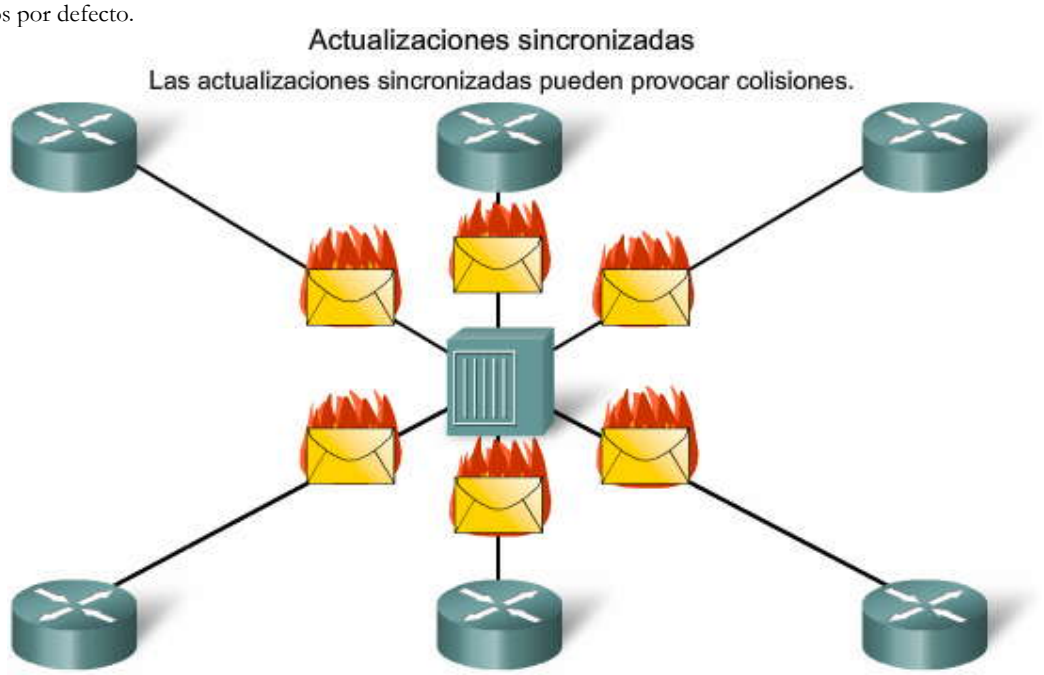
Cuando varios routers transmiten actualizaciones de enrutamiento al mismo tiempo en segmentos LAN multiacceso (como se muestra en la animación), los paquetes de actualización pueden colisionar y producir retardos o consumir demasiado ancho de banda.

**Nota:** Las colisiones sólo son un problema con los hubs y no con los switches.

El envío de actualizaciones al mismo tiempo se conoce como sincronización de actualizaciones. La sincronización puede representar un problema para los protocolos de enrutamiento por vector de distancia debido a que utilizan actualizaciones periódicas. A medida que aumenta la sincronización de temporizadores de routers, se produce una mayor cantidad de colisiones de actualizaciones y retardos en la red. Al comienzo, las actualizaciones de los routers no se sincronizarán. Pero con el tiempo, los temporizadores a lo largo de toda una red se volverán globalmente sincronizados.

**La solución**

Para evitar la sincronización de actualizaciones entre routers, el IOS de Cisco utiliza una variable aleatoria denominada RIP_JITTER que resta una cantidad de tiempo variable al intervalo de actualización de cada router de la red. Esta fluctuación de fase aleatoria, o cantidad de tiempo variable, varía del 0% al 15% del intervalo de actualización especificado. De este modo, el intervalo de actualización varía aleatoriamente en un rango de 25 a 30 segundos para el intervalo de 30 segundos por defecto.




### 4.4 ROUTING LOOPS.-
### 4.4.1 DIFINICION Y CONSECUENCIAS.-

¿Qué es un routing loop?

Un routing loop es una condición en la que un paquete se transmite continuamente dentro de una serie de routers sin que nunca alcance la red de destino deseada. Un routing loop puede producirse cuando dos o más routers tienen información de enrutamiento que indica erróneamente que existe una ruta válida a un destino inalcanzable.

El loop puede ser el resultado de lo siguiente:

- rutas estáticas configuradas incorrectamente,
- redistribución de ruta configurada incorrectamente (la redistribución es un proceso de envío de la información de enrutamiento desde un protocolo de enrutamiento a otro y se analizará en los cursos de nivel CCNP),
- tablas de enrutamiento incongruentes que no se actualizan debido a una convergencia lenta en una red cambiante y
- rutas de descarte configuradas o instaladas incorrectamente.

Los protocolos de enrutamiento por vector de distancia tienen un funcionamiento simple. Su simplicidad origina algunas desventajas, como por ejemplo, los routing loops. Los routing loops no son tan problemáticos con los protocolos de enrutamiento de estado de enlace, pero pueden producirse en determinadas circunstancias.

**Nota:** El protocolo IP tiene su propio mecanismo para evitar la posibilidad de que un paquete atravies e la red indefinidamente. El IP tiene un campo Período de vida (TTL) y su valor disminuye en 1 en cada router. Si el TTL es cero, el router descarta el paquete.

**¿Qué consecuencias tienen los routing loops?**

Un routing loop puede tener un efecto devastador en una red y producir un menor rendimiento o incluso un tiempo de inactividad de dicha red.

Un routing loop puede producir las siguientes condiciones:

- El ancho de banda del enlace se utilizará para el tráfico que se transmita de un sitio a otro entre los routers de un loop.
- La CPU de un router estará exigida debido a los paquetes con loops.
- La CPU de un router se cargará con el envío inútil de paquetes, lo que afectará negativamente la convergencia de la red.
- Las actualizaciones de enrutamiento pueden perderse o no ser procesadas de manera oportuna. Estas condiciones podrían originar routing loops adicionales, lo que empeoraría aún más la situación.
- Los paquetes pueden perderse en "agujeros negros".

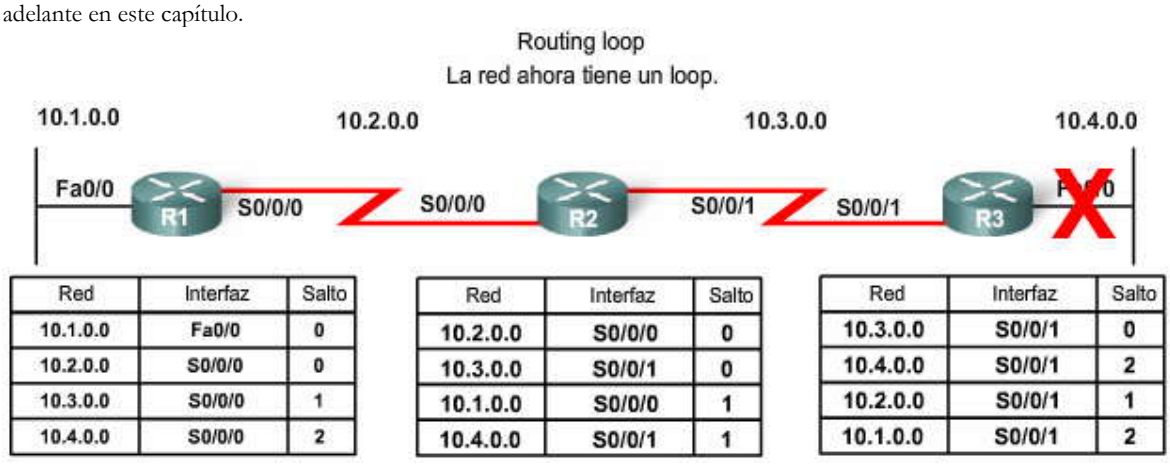
Reproduzca la animación para observar una posible situación de routing loop en el que no existen mecanismos para evitar dichos loops.

Como puede observar, los routing loops consumen mucho ancho de banda y los recursos del router. Como resultado, la red funciona más lenta o incluso no responde.

Existen varios mecanismos disponibles para eliminar los routing loops, principalmente con los protocolos de enrutamiento por vector de distancia. Estos mecanismos incluyen:

- definición de una métrica máxima para evitar una cuenta a infinito,
- temporizadores de espera,
- horizonte dividido,
- envenenamiento de ruta o envenenamiento en reversa y
- updates disparados.

Los updates disparados se analizaron en la sección anterior. Los demás mecanismos para evitar loops se analizarán más adelante en este capítulo.




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 2 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 1 |

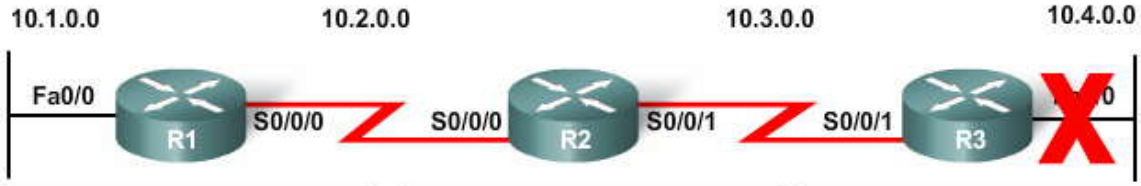
| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | S0/0/1 | 2 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

### 4.4.2 PROBLEMA: CUENTA A INFINITO.-

La cuenta a infinito es una condición que se produce cuando las actualizaciones de enrutamiento inexactas aumentan el valor de la métrica a "infinito" para una red que ya no se puede alcanzar. La animación muestra qué sucede con las tabl as de enrutamiento cuando los tres routers continúan enviando actualizaciones inexactas entre sí.

Cuenta a infinito

La red 10.4.0.0 deja de funcionar.
Antes de que R3 pueda enviar una actualización, R2 envía una actualización.
R3 instala una ruta "no válida" hacia la red 10.4.0.0 con un conteo de saltos de 2.
R3 envía una actualización a R2 con un conteo de saltos de 3 hacia la red 10.4.0.0.
R2 aumenta el conteo de saltos hasta 3 para la red 10.4.0.0.
R2 envía una actualización a R1 con un conteo de saltos de 4 hacia la red 10.4.0.0.
R1 aumenta el conteo de saltos hasta 4 para la red 10.4.0.0.
R2 envía la siguiente actualización periódica con un conteo de saltos de 4 hacia la red 10.4.0.0.
R3 aumenta el conteo de saltos hasta 4 para la red 10.4.0.0.
R3 envía una actualización a R2 con un conteo de saltos de 5 hacia la red 10.4.0.0.
R2 aumenta el conteo de saltos desde 3 hasta 5 para la red 10.4.0.0.
R2 envía una actualización a R1 con un conteo de saltos de 6 hacia la red 10.4.0.0.
R1 aumenta el conteo de saltos hasta 6 para la red 10.4.0.0.
R2 envía la siguiente actualización periódica con un conteo de saltos de 6 hacia la red 10.4.0.0.
R3 aumenta el conteo de saltos hasta 6 para la red 10.4.0.0.
R3 envía una actualización a R2 con un conteo de saltos de 7 hacia la red 10.4.0.0.
R2 aumenta el conteo de saltos desde 5 hasta 7 para la red 10.4.0.0.
R2 envía una actualización a R1 con un conteo de saltos de 8 hacia la red 10.4.0.0.
R1 aumenta el conteo de saltos hasta 8 para la red 10.4.0.0.
Cada ronda de actualizaciones continúa aumentando el conteo de saltos.




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 16 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 16 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | S0/0/1 | 16 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

### 4.4.3 CONFIGURACION DE UN VALOR MÁXIMO.-

Para detener eventualmente el aumento de la métrica, **"infinito" se define configurando un valor máximo de métrica.** Por ejemplo, el RIP define lo que es infinito con un valor de 16 saltos (una métrica "inalcanzable"). Una vez realizada la "cuenta a infinito", los routers marcan la ruta como inalcanzable.

10.4.0.0 es inalcanzable. El conteo de saltos es de 16.


| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 16 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 16 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | S0/0/1 | 16 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

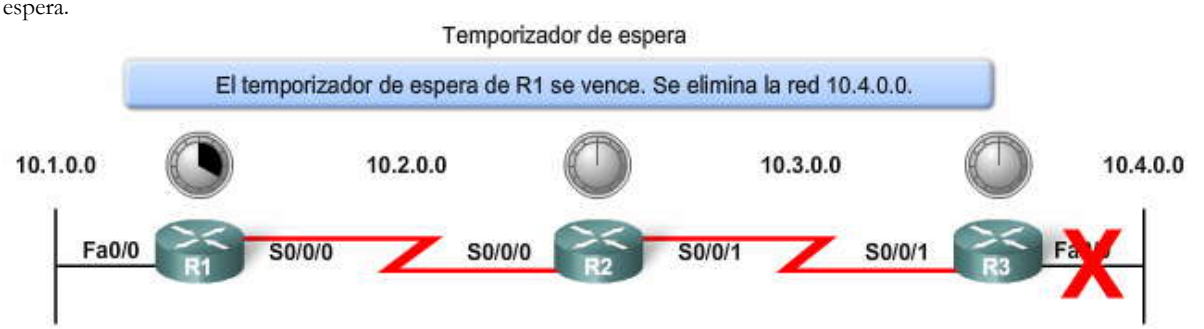
### 4.4.4 PREVENCION DE ROUTING LOOP CON TEMPORIZADORES DE ESPERA.-

Anteriormente, aprendió que los protocolos por vector de distancia utilizan updates disparados para acelerar el proceso de convergencia. Recuerde que además de los updates disparados, los routers que utilizan protocolos de enrutamiento por vector de distancia también envían actualizaciones periódicas. Supongamos que una determinada red es inestable. La interfaz se reestablece como up, después como down y luego nuevamente como up, en una sucesión rápida. La ruta se está "sacudiendo". Mediante la utilización de updates disparados, los routers pueden reaccionar demasiado rápido y crear, sin saberlo, un routing loop. Un routing loop también puede producirse por una actualización periódica que los routers envían

durante la inestabilidad. Los temporizadores de espera evitan que los routing loops se produzcan por estas condiciones. También previenen la condición de cuenta a infinito.

**Los temporizadores de espera se utilizan para evitar que los mensajes de actualización regulares reinstauren de manera inadecuada una ruta que puede no ser válida**. Estos temporizadores le indican al router que se mantenga en espera ante los cambios que pueden afectar las rutas durante un período determinado. Si se identifica una ruta como down o possibly down, cualquier otra información para dicha ruta que contenga el mismo estado, u otro peor, se ignorará durante un período predeterminado (el período de espera). Esto significa que los routers dejarán una ruta marcada como inalcanzable en ese estado durante un período que sea lo suficientemente prolongado como para que las actualizaciones propaguen las tablas de enrutamiento con la información más actual.

**Los temporizadores de espera funcionan de la siguiente manera:**
1. Un router recibe una actualización de un vecino que indica que una red que anteriormente era accesible ahora no lo es más.
2. El router marca la red como possibly down e inicia el temporizador de espera.
3. Si se recibe una actualización con una métrica mejor para esa red desde cualquier router vecino durante el período de espera, la red se reinstala y se elimina el temporizador de espera.
4. Si se recibe una actualización desde cualquier otro vecino durante el período de espera con la misma métrica o una métrica peor para esa red, se ignorará dicha actualización. De este modo, se dispone de más tiempo para que la información acerca del cambio pueda propagarse.
5. Los routers continúan enviando paquetes a las redes de destino que están marcadas como possibly down. Esto permite que el router supere cualquier dificultad relacionada con la conectividad intermitente. Si realmente la red de destino no está disponible y los paquetes se envían, se crea un enrutamiento de agujero negro y dura hasta que venza el temporizador de espera.




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 2 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 1 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | S0/0/1 | 0 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

### 4.4.5 REGLA DE HORIZONTE DIVIDIDO.-

Otro método que se utiliza para evitar routing loops producidos por la convergencia lenta de un protocolo de enrutamiento por vector de distancia es el horizonte dividido. **La regla de horizonte dividido establece que un router no debería publicar una red a través de la interfaz por la cual provino la actualización**.
La aplicación del horizonte dividido en el ejemplo anterior de la ruta 10.4.0.0 produce las siguientes acciones:

- R3 publica la red 10.4.0.0 a R2.
- R2 recibe la información y actualiza su tabla de enrutamiento.
- A continuación, R2 publica la red 10.4.0.0 a R1 desde S0/0/0. R2 no publica la red 10.4.0.0 a R3 desde S0/0/1 porque la ruta se originó desde dicha interfaz.
- R1 recibe la información y actualiza su tabla de enrutamiento.
- Debido al horizonte dividido, R1 tampoco publica la información acerca de la red 10.4.0.0 a R2.

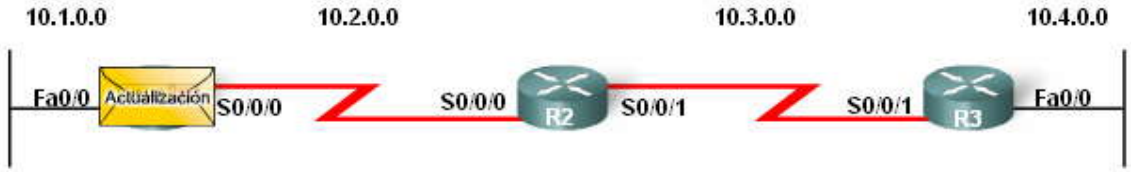
Se intercambian las actualizaciones de enrutamiento completas, con la excepción de las rutas que violan la regla del horizonte dividido. Los resultados serán similares a los siguientes:

- R2 publica las redes 10.3.0.0 y 10.4.0.0 a R1.
- R2 publica las redes 10.1.0.0 y 10.2.0.0 a R3.
- R1 publica la red 10.1.0.0 a R2.
- R3 publica la red 10.4.0.0 a R2.

Reproduzca la animación para observar el proceso.
Observe que R2 envía actualizaciones de enrutamiento diferentes a R1 y a R3.

Nota: Un administrador puede desactivar el horizonte dividido. En determinadas condiciones, es necesario realizar esto para lograr el enrutamiento adecuado. Estas condiciones se analizarán en otros cursos.

Regla de horizonte dividido para la red 10.4.0.0
R1 sólo publica la red 10.1.0.0 a R2.




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 2 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 1 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

### 4.4.6 HORIZONTE DIVIDIDO CON ENVENAMIENTO EN REVERSA O ENVENENAMIENTO DE RUTA.-

Envenenamiento de ruta

El envenenamiento de ruta es otro método más que utilizan los protocolos de enrutamiento por vector de distancia para evitar los routing loops. **El envenenamiento de ruta se utiliza para marcar la ruta como inalcanzable en una actualización de enrutamiento que se envía a otros routers**. Se interpreta a lo inalcanzable como una métrica que está configurada en un valor máximo. Para el RIP, una ruta envenenada tiene una métrica de 16.

Se llevan a cabo los siguientes procesos:
La red 10.4.0.0 se vuelve no disponible debido a una falla de enlace.

- R3 envenena la métrica con un valor de 16 y después envía un update disparado donde establece que la red 10.4.0.0 no está disponible.
- R2 procesa dicha actualización. Debido a que la métrica es de 16, R2 invalida la entrada de enrutamiento en su tabla de enrutamiento.
- R2 envía luego una actualización de envenenamiento a R1 indicando que la ruta no está disponible, nuevamente mediante la configuración del valor de la métrica en 16.
- R1 procesa dicha actualización e invalida la entrada de enrutamiento para la red 10.4.0.0 en su tabla de enrutamiento.

El envenenamiento de ruta acelera el proceso de convergencia ya que la información acerca de la red 10.4.0.0 se pro paga a través de la misma más rápido que al esperar a que el conteo de saltos alcance "infinito".

Envenenamiento de ruta
La red ahora es convergente en una ruta "envenenada".


| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 16 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 16 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | Fa0/0 | 16 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

**Horizonte dividido con envenenamiento en reversa**

El envenenamiento en reversa puede combinarse con la técnica del horizonte dividido. Este método se denom ina horizonte dividido con envenenamiento en reversa**. La regla de horizonte dividido con envenenamiento en reversa establece que, al enviar actualizaciones desde una determinada interfaz, se debe designar como inalcanzable a cualquier red sobre la cual se obtuvo información mediante dicha interfaz.**

El concepto de horizonte dividido con envenenamiento en reversa se basa en el hecho de que es mejor comunicar explícitamente a un router que ignore una ruta en lugar de no informarle nada al respeto en primer lugar.

Se llevan a cabo los siguientes procesos:

- La red 10.4.0.0 se vuelve no disponible debido a una falla de enlace.
- R3 envenena la métrica con un valor de 16 y después envía un update disparado donde establece que la red 10.4.0.0 no está disponible.
- R2 procesa dicha actualización, invalida la entrada de enrutamiento en su tabla de enrutamiento e inmediatamente envía un envenenamiento en reversa a R3.

El envenenamiento en reversa es una circunstancia específica que supera al horizonte dividido. Se produce para garantizar que R3 no sea susceptible a las actualizaciones inapropiadas sobre la red 10.4.0.0.

**Nota:** El horizonte dividido está activado por defecto. Sin embargo, el horizonte dividido con envenenamiento en reversa puede no ser la opción por defecto en todas las implementaciones de IOS.

Envenenamiento en reversa

R2 envía un "envenenamiento en reversa" a R3.


| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/0 | 2 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.1.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 16 |

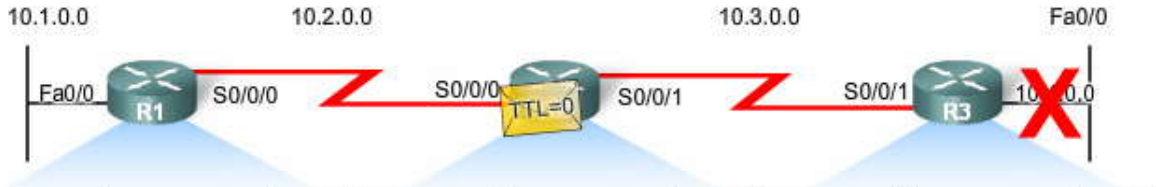
| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | Fa0/0 | 16 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

### 4.4.7 IP Y TTL.-

**El Período de vida (TTL) es un campo de 8 bits en el encabezado IP que limita la cantidad de saltos que un paquete puede atravesar por la red antes de descartarlo.** El propósito del campo TTL es evitar que un paquete que no puede entregarse continúe circulando en la red indefinidamente. Con el TTL, el campo de 8 bits se configura con un valor mediante el dispositivo de origen del paquete. El TTL disminuye en uno por cada router en la ruta a su destino. Si el campo TTL alcanza un valor de cero antes de que el paquete llegue a destino, dicho paquete se descarta y el router envía un mensaje de error de Internet Control Message Protocol (ICMP) al origen del paquete IP.

La animación muestra que incluso en caso de que ocurra un routing loop, los paquetes no entrarán en un loop interminable en la red. Eventualmente, el valor de TTL disminuirá hasta alcanzar 0 y el router descartará el paquete.

TTL en vigencia




| Red | Interfaz | Salto |
|---|---|---|
| 10.1.0.0 | Fa0/0 | 0 |
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/0 | 1 |
| 10.2.0.0 | S0/0/0 | 4 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.2.0.0 | S0/0/0 | 0 |
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | S0/0/0 | 1 |
| 10.4.0.0 | S0/0/1 | 3 |

| Red | Interfaz | Salto |
|---|---|---|
| 10.3.0.0 | S0/0/1 | 0 |
| 10.4.0.0 | S0/0/1 | 2 |
| 10.2.0.0 | S0/0/1 | 1 |
| 10.1.0.0 | S0/0/1 | 2 |

## 4.5 PROTOCOLOS DE ENRUTAMIENTO POR VECTOR DISTANCIA EN AL ACTUALIDAD

### 4.5.1 RIP Y EIGRP

Para los protocolos de enrutamiento por vector de distancia, sólo existen realmente dos opciones: RIP o EIGRP. La decisión acerca de qué protocolo de enrutamiento se utilizará en una situación determinada depende de varios factores, entre los que se incluyen:

- el tamaño de la red,
- la compatibilidad entre los modelos de routers y
- el requisito de conocimientos administrativos.

**RIP**

Con el tiempo, el RIP ha pasado de ser un protocolo de enrutamiento con clase (RIPv1) a un protocolo de enrutamie nto sin clase (RIPv2). El RIPv2 es un protocolo de enrutamiento estandarizado que funciona en un entorno de router de fabricante mixto. Los routers fabricados por empresas diferentes pueden comunicarse utilizando el RIP. Éste es uno de los protocolos de enrutamiento más fáciles de configurar, lo que lo convierte en una buena opción para las redes pequeñas. Sin embargo, el RIPv2 todavía tiene limitaciones. Tanto el RIPv1 como el RIPv2 tienen una métrica de ruta que se basa sólo en el conteo de saltos y que se limita a 15 saltos.

Características del RIP:

- Admite el horizonte dividido y el horizonte dividido con envenenamiento en reversa para evitar loops.
- Es capaz de admitir un balanceo de carga de hasta seis rutas del mismo costo. El valor por defecto es de c uatro rutas del mismo costo.

El RIPv2 introdujo las siguientes mejoras al RIPv1:

- Incluye una máscara de subred en las actualizaciones de enrutamiento, lo que lo convierte en un protocolo de enrutamiento sin clase.
- Tiene un mecanismo de autenticación para la seguridad de las actualizaciones de las tablas.
- Admite una máscara de subred de longitud variable (VLSM).
- Utiliza direcciones multicast en vez de broadcast.
- Admite el resumen manual de ruta.

**EIGRP**

El Enhanced IGRP (EIGRP) se desarrolló a partir del IG RP, otro protocolo por vector de distancia. El EIGRP es un protocolo de enrutamiento por vector de distancia sin clase que tiene características propias de los protocolos de enrutamiento de estado de enlace. Sin embargo, y a diferencia del RIP o el OSPF, e1 EIGRP es un protocolo patentado desarrollado por Cisco y sólo se ejecuta en los routers Cisco.

Las características del EIGRP incluyen:

- Updates disparados (el EIGRP no tiene actualizaciones periódicas).
- Utilización de una tabla de topología para mantener todas las rutas recibidas de los vecinos (no sólo las mejores rutas).
- Establecimiento de adyacencia con los routers vecinos utilizando el protocolo de saludo EIGRP.
- Admite VLSM y el resumen manual de ruta. Esta característica le permite al EIGRP crear gra ndes redes estructuradas jerárquicamente.

Ventajas del EIGRP:

- Si bien las rutas se propagan como un vector de distancia, la métrica se basa en el ancho de banda mínimo y en el retardo acumulado de la ruta en lugar del conteo de saltos.
- Rápida convergencia debida al cálculo de ruta del Algoritmo de actualización por difusión (DUAL). El DUAL permite la inserción de rutas de respaldo en la tabla de topología de EIGRP. Éstas se utilizan en caso de falla de la ruta principal. Debido a que se trata de un procedi miento local, el cambio a la ruta de respaldo es inmediato y no implica ninguna acción en ningún otro router.
- Las actualizaciones limitadas significan que el EIGRP utiliza menos ancho de banda, especialmente en grandes redes con muchas rutas.
- El EIGRP admite múltiples protocolos de capa de red a través de los Módulos dependientes de protocolos, que incluyen la admisión de IP, IPX y AppleTalk.

Comparación de los protocolos de enrutamiento por vector de distancia

| | Ripv1 | Ripv2 | IGRP | EIGRP |
|---|---|---|---|---|
| Velocidad de convergencia | Lento | Lento | Lento | Rápido |
| Escalabilidad: tamaño de la red | Pequeño | Pequeño | Pequeño | Grande |
| Uso de VLSM | No | Sí | No | Sí |
| Uso de recursos | Bajo | Bajo | Bajo | Medio |
| Implementación y mantenimiento | Simple | Simple | Simple | Complejo |





**4.6 ACTIVIDADES DE LABORATORIO.-**
**4.6.1 ACTIVIDADES DE LABORATORIO.-**
**4.7 RESUMEN.-**
**4.7.1 RESUMEN.-**
**Resumen**

Una manera de clasificar los protocolos de enrutamiento es teniendo en cuenta el tipo de algoritmo que utilizan para determinar la mejor ruta hacia la red de destino. Los protocolos de enrutamiento pueden clasificarse en vector de distancia, estado de enlace o vector de ruta. El vector de distancia significa que las rutas se publican como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es simplemente el router del siguiente salto o la interfaz de salida.

Los protocolos de enrutamiento por vector de distancia incluyen:

- RIPv1,
- RIPv2,
- IGRP y
- EIGRP.

Los routers que utilizan este tipo de protocolo determinan la mejor ruta para redes remotas según la información que aprenden de sus vecinos. Si el router X aprende dos rutas hacia la misma red, una a través del router Y en 7 saltos y la otra a través del router Z en 10 saltos, el router elegirá la ruta más corta utilizando el router Y como el router del siguiente salto. El router X no conoce cómo es la red más allá de los routers Y y Z, y sólo puede tomar la decisión acerca de cuál es la mejor ruta según la información que le envían estos dos routers. Los protocolos de enrutamiento por vector de distancia no tienen un mapa de la topología como en el caso de los protocolos de enrutamiento de estado de enlace.

El descubrimiento de la red es un proceso importante para cualquier protocolo de enrutamiento. Algunos protocolos de enrutamiento por vector de distancia, como por ejemplo el RIP, deben realizar un proceso paso a paso para aprender y compartir información de enrutamiento con sus vecinos. A medida que se aprende sobre las rutas desde los vecinos, dicha información se transfiere a los otros vecinos con un aumento en la métrica de enrutamiento.

Los protocolos de enrutamiento también deben mantener sus tablas de enrutamiento para que estén actualizadas y precisas. El RIP intercambia información de la tabla de enrutamiento con sus vecinos cada 30 segundos. El EIGRP, otro protocolo de enrutamiento por vector de distancia, no envía estas actualizaciones periódicas. Solamente envía una actualización "limitada" cuando se produce un cambio en la topología y sólo a los routers que necesitan dicha información. Este protocolo se analizará en otro capítulo.

El RIP también utiliza temporizadores para determinar cuándo un router vecino ya no se encuentra disponible o cuándo algunos de los routers pueden no tener información de enrutamiento actualizada. Esto sucede generalmente porque la red todavía no es convergente debido a un cambio reciente en la topología. Los protocolos de enrutamiento por vector de distancia también utilizan updates disparados para ayudar a acelerar el tiempo de convergencia.

Una de las desventajas de estos protocolos es la posibilidad de que se produzcan routing loops. Los routing loops pueden producirse cuando la red no se encuentra en estado convergente. Este tipo de protocolo utiliza temporizadores de espera para evitar que el router utilice otra ruta a una red marcada como recently down hasta que todos los routers tengan el tiempo suficiente para aprender sobre este cambio en la topología.

Los routers también utilizan el horizonte dividido y el horizonte dividido con envenenamiento en reversa para evitar que se produzcan routing loops. La regla de horizonte dividido establece que un router nunca debe publicar una ruta a través de la interfaz por medio de la cual aprendió dicha ruta. El horizonte dividido con envenenamiento en reversa significa que es mejor establecer explícitamente que este router no tiene una ruta para esa red al envenenarla con una métrica que establece que la ruta es inalcanzable.

Un protocolo de enrutamiento por vector de distancia se denomina a veces "enrutamiento por rumor", aunque éste puede ser un nombre poco apropiado. Estos protocolos son muy populares entre los diferentes administradores de red ya que generalmente son fáciles de entender y su implementación es simple. Esto no significa necesariamente que los protocolos de enrutamiento de estado de enlace sean más complicados o difíciles de configurar. Desafortunadamente, los protocolos de enrutamiento de estado de enlace tienen esta reputación injustificada. En los siguientes capítulos aprenderemos que los protocolos de enrutamiento de estado de enlace son tan fáciles de entender y configurar como los protocolos de enrutamiento por vector de distancia.

| | Protocolos de gateway interiores | | | | Protocolos de Gateway exterior |
|---|---|---|---|---|---|
| | Protocolos de enrutamiento de vector de distancia | | Protocolos de enrutamiento de estado de enlace | | Vector de ruta |
| Con clase | RIP | IGRP | | | EGP |
| Sin clase | RIPv2 | EIGRP | OSPFv2 | IS-IS | BGPv4 |
| IPv6 | RIPng | EIGRP para IPv6 | OSPFv3 | IS-IS para IPv6 | BGPv4 para IPv6 |

**En este capítulo, aprendió a:**

- Identificar las características de los protocolos de enrutamiento de vector de distancia.
- Describir el proceso de descubrimiento de redes de los protocolos de enrutamiento de vector de distancia utilizando el Routing Information Protocol (RIP).
- Describir los procesos para mantener tablas de enrutamiento precisas utilizadas por los protocolos de enrutamiento de vector de distancia.
- Identificar las condiciones que provocan un routing loop y explicar las consecuencias para el rendimiento del router.
- Identificar los tipos de protocolos de enrutamiento de vector de distancia que se utilizan actualmente.

# CAPITULO V – "RIP VERSION 1"

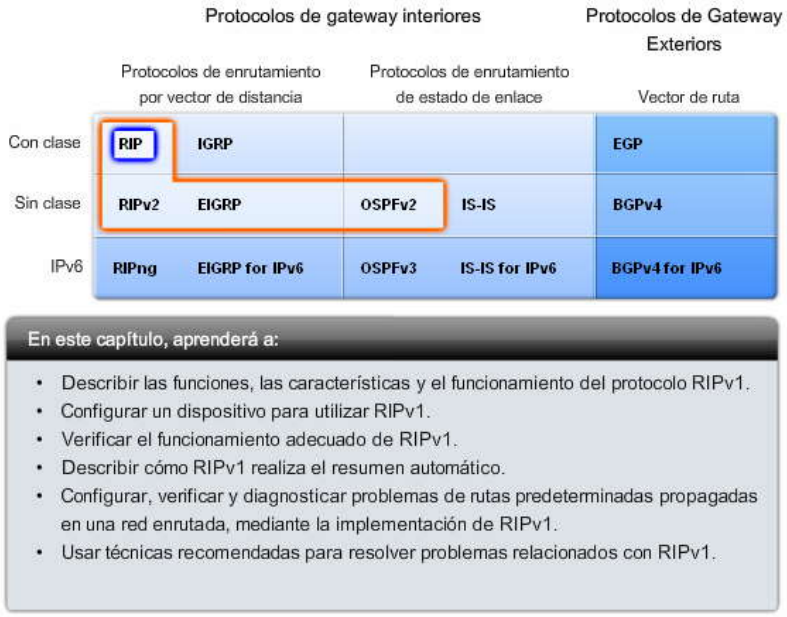
## 5.0 PROTOCOLO DE INFORMACION DE ENRRUTAMIENTO.-

### 5.0.1 INTRODUCCIÓN DEL CAPITULO.-

Con el transcurso del tiempo, los protocolos de enrutamiento han evolucionado para cumplir con las crecientes demandas de las redes complejas. El primer protocolo utilizado fue el Protocolo de información de enrutamiento (RIP). RIP aún es popular debido a su simplicidad y amplia compatibilidad.

Comprender el RIP es importante para sus estudios de networking debido a dos motivos. Primero, RIP aún está en u so. Puede enfrentarse a la implementación de una red lo suficientemente amplia para necesitar un protocolo de enrutamiento y aun lo suficientemente simple para utilizar el RIP en forma efectiva. Además, la familiaridad con muchos de los conceptos fundamentales de RIP lo ayudarán a comparar RIP con otros protocolos. Comprender el funcionamiento y la implementación de RIP facilitará su aprendizaje de otros protocolos de enrutamiento.

Este capítulo abarca los detalles de la primera versión de RIP, que incluy e un poco de historia, las características, el funcionamiento, la configuración, la verificación y resolución de problemas de RIPv1. A lo largo del capítulo, puede utilizar las actividades del Packet Tracer para practicar lo que aprende. Al finalizar el capítulo, se ofrecen tres actividades prácticas de laboratorio y una actividad de Desafío de integración de aptitudes del Packet Tracer para ayudarlo a integrar RIPv1 a su creciente conjunto de conocimientos y habilidades sobre networking.




## 5.1 RIPv1: PROTOCOLO DE ENRUTAMIENTO CON CLASE DE VECTOR DISTANCIA.-

### 5.1.1 INFORMACION BÁSICA Y PERSPECTIVA.-

**Influencia histórica de RIP**

RIP es el protocolo de enrutamiento por vector de distancia más antiguo. Si bien RIP carece de la sofisticación de los protocolos de enrutamiento más avanzados, su simplicidad y amplia utilización en forma continua representan el testimonio de su longevidad. RIP no es un protocolo "en extinción". De hecho, se cuenta ahora con un tipo de RIP de IPv6 llamado RIPng (próxima generación).

**Haga clic en las fechas de la figura para comparar el desarrollo del protocolo de red y RIP a lo largo del tiempo.**

RIP evolucionó de un protocolo anterior desarrollado en Xerox, llamado Protocolo de información de gateway (GWINFO). Con el desarrollo de Xerox Netwo rk System (XNS), GWINFO evolucionó a RIP. Luego, adquirió popularidad ya que se implementó en la Distribución del Software Berkeley (BSD) como un daemon denominado routed (se pronuncia "routi -dí" y no "routid"). Algunos fabricantes realizaron sus propias y ligeramente diferentes implementaciones de RIP. En reconocimiento de la necesidad de estandarización del protocolo, Charles Hedrick escribió RFC 1058 en 1988, donde documentó el protocolo existente y especificó ciertas mejoras. Desde entonces, se mejoró el RIP con RIPv2 en 1994 y con RIPng en 1997.

**Nota:** A la primera versión de RIP se la denomina generalmente RIPv1 para distinguirla de RIPv2. Sin embargo, ambas versiones comparten muchas funciones similares. Al discutir las funciones comunes de ambas ver siones, nos referiremos a RIP. Al discutir funciones propias de cada versión, utilizaremos RIPv1 y RIPv2. RIPv2 se discutirá en un capítulo posterior.

Descripción general del impacto histórico de RIP


Haga clic en las fechas para comparar el desarrollo de protocolos de red y RIP con el tiempo.

### 5.1.2 CARACTERISTICA Y FORMATO DE MENSAJES DE RIPv1.-

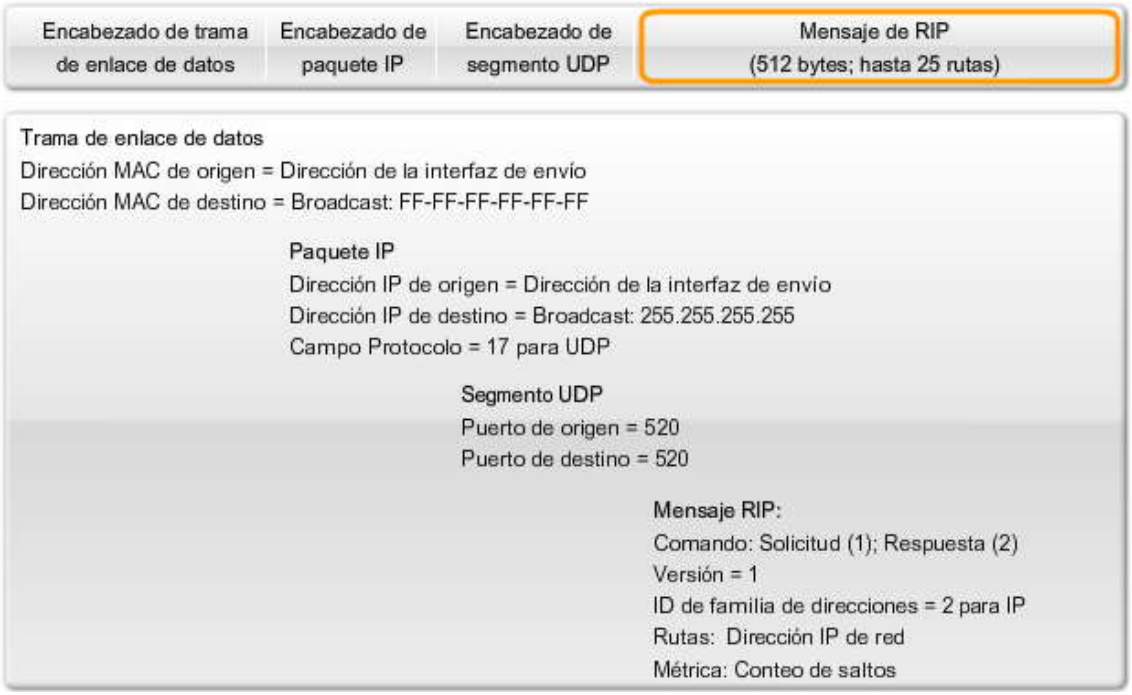
**Características de RIP**

Según lo discutido en el Capítulo 4, "Protocolos de enrutamiento por vector de distancia", RIP posee las siguientes características clave:

- RIP es un protocolo de enrutamiento por vector de distancia.
- RIP utiliza el conteo de saltos como su única métrica para la selección de rutas.
- Las rutas publicadas con conteo de saltos mayores que 15 son inalcanzables.
- Se transmiten mensajes cada 30 segundos.

**Coloque el cursor sobre los campos en el Mensaje de RIPv1 encapsulado para ver el proceso de encapsulación.**
La porción de datos de un mensaje de RIP se encapsula en un segmento UDP, con los números de puerto de origen y destino establecidos en 520. El encabezado IP y los encabezados de enlace de datos agregan direcciones de destino de broadcast antes de enviar el mensaje a todas las interfaces configuradas con RIP.

Mensaje RIPv1 encapsulado



**Formato de mensajes de RIP: Encabezado de RIP**

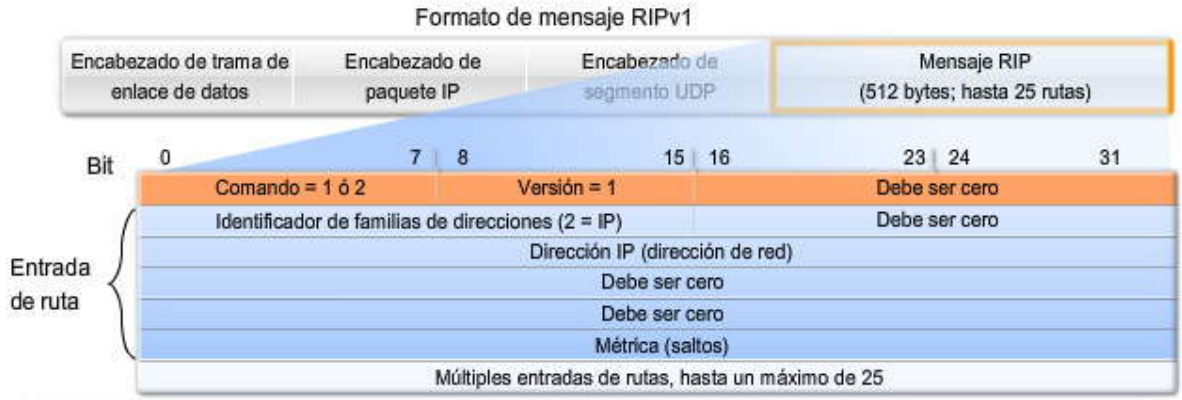
Se especifican tres campos en la porción del encabezado de cuatro bytes que se muestra en la figura de color anaranjado. El campo Comando especifica el tipo de mensaje, que se discute más detalladamente en la próxima sección. El campo Versión se establece en 1 para la versión 1 de RIP. El tercer campo se rotula Debe ser cero. Los campos "Debe ser cero" ofrecen espacio para la futura expansión del protocolo.

**Formato de mensajes de RIP: Entrada de ruta**

La porción de la entrada de ruta del mensaje incluye tres campos con contenido: Identificador de familias de direcciones (establecido en 2 para IP, a menos que un router solicite una tabla de enrutamiento completa, en cuyo caso el campo se establece en cero), Dirección IP y Métrica. Esta porción de entrada de ruta representa una ruta de destino con su métrica asociada. Una actualización de RIP puede incluir hasta 25 entradas de ruta. El tamaño máximo del datagrama es de 512 bytes, sin incluir los encabezados IP o UDP.

**¿Por qué hay tantos campos establecidos en cero?**

RIP se desarrolló antes que IP y se utilizó para otros protocolos de red (como XNS). BSD también ejerció su influencia. Al principio, el espacio adicional se agregó con la intención de admitir mayores espacios de direcciones en el futuro. Como veremos en el Capítulo 7, RIPv2 ya ha utilizado la mayoría de dichos campos vacíos.



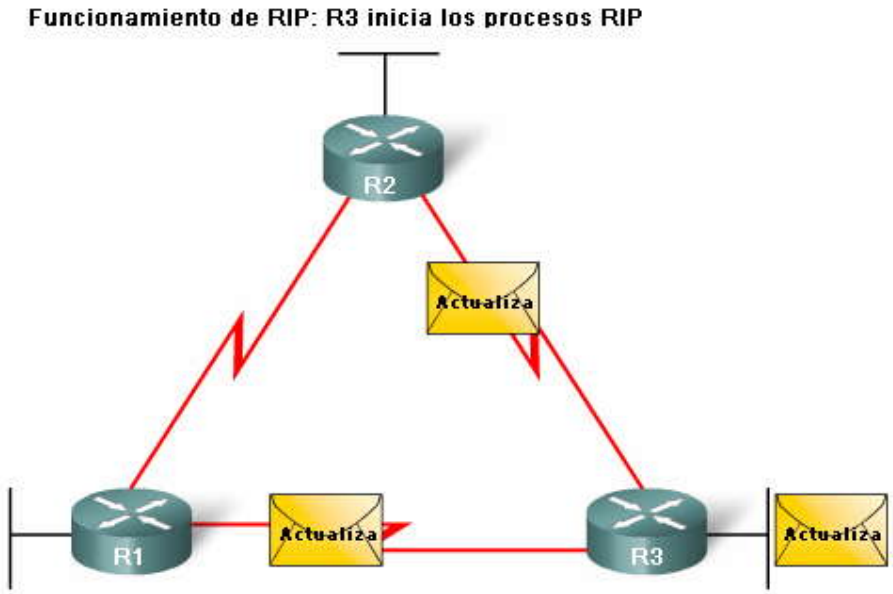

| | |
|---|---|
| **Comando** | 1 para una solicitud o 2 para una respuesta. |
| **Versión** | 1 para RIP v1 ó 2 para RIP v2. |
| **Identificador de familias de direcciones** | 2 para IP a menos que se realice la solicitud de una tabla de enrutamiento completa, en cuyo caso se establece en 0. |
| **Dirección IP** | La dirección de la ruta de destino, que puede ser una red, subred o dirección de host. |
| **Métrica** | Conteo de saltos entre 1 y 16. El router que realiza el envío aumenta la métrica antes de enviar un mensaje. |

### 5.1.3 FUNCIONAMIENTO DE RIP.-

**Proceso de solicitud/respuesta de RIP**

RIP utiliza dos tipos de mensajes especificados en el campo Comando: **Mensaje de solicitud y Mensaje de respuesta**.

**Haga clic en Reproducir para ver el proceso de solicitud/respuesta.**
Cada interfaz configurada con RIP envía un mensaje de solicitud durante el inicio y solicita que todos los RIP vecinos envíen sus tablas de enrutamiento completas. Se envía de regreso un mensaje de respuesta por parte de los vecinos habilitados con RIP. Cuando el router que realiza la solicitud recibe las respuestas, evalúa cada entrada de ruta. Si una entrada de ruta es nueva, el router receptor instala la ruta en la tabla de enrutamiento. Si la ruta ya se encuentra en la tabla, la entrada existente se reemplaza si la nueva entrada tiene un mejor conteo de saltos. El router de inicio luego envía un update disparado a todas las interfaces habilitadas con RIP que incluyen su propia tabla de enrutamiento para que los RIP vecinos puedan recibir la información acerca de todas las nuevas rutas.

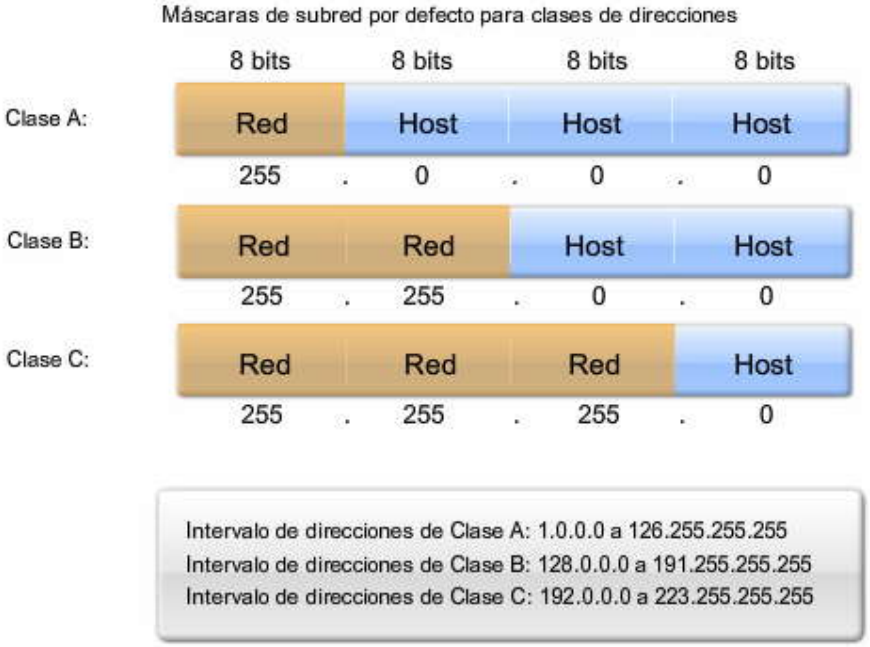



**Clases de direcciones IP y enrutamiento con clase**

Puede recordar a partir de estudios anteriores que las direcciones IP asignadas a los hosts se dividieron inicialmente en 3 clases: clase A, clase B y clase C. A cada clase se le asignó una máscara de subred predeterminada, como se muestra en la figura. Es importante conocer la máscara de subred predeterminada para cada clase a fin de comprender el funcionamiento de RIP.

RIP es un protocolo de enrutamiento con clase. Como puede haberlo notado en la discusión anterior sobre el formato de los mensajes, RIPv1 no envía información sobre la máscara de subred en la actualización. Por lo tanto, un router utiliza la máscara de subred configurada en una interfaz local o aplica la máscara de subred predeterminada según la clase de dirección. Debido a esta limitación, las redes de RIPv1 no pueden ser no contiguas ni pueden implementar VLSM.

El direccionamiento IP se discute más adelante en el Capítulo 6, "VLSM y CIDR". También puede visitar los enlaces que se indican a continuación para obtener una revisión de las clases.

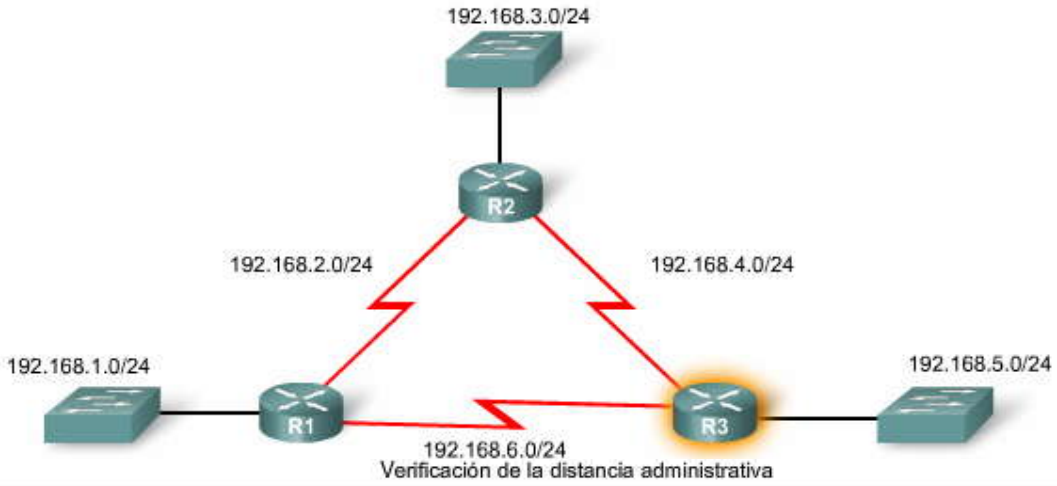



### 5.1.4 DISTANCIA ADMINISTRATIVA.-

Como se vio en el Capítulo 3, "Introducción a los protocolos de enrutamiento dinámicos", la distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. RIP tiene una distancia administrativa predeterminada de 120. Al compararlo con otros protocolos de gateway interior, RIP es el protocolo de enrutamiento menos preferido. IS -IS, OSPF, IGRP y EIGRP tienen valores de AD predeterminados inferiores.

Recuerde que puede verificar la distancia administrativa mediante los comandos show ip route o show ip protocols.

Verificación de la distancia administrativa




Verificación de la distancia administrativa

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    192.168.1.0/24 [120/1] via 192.168.6.2, 00:00:05, Serial0/0/0
R    192.168.2.0/24 [120/1] via 192.168.6.2, 00:00:05, Serial0/0/0
                    [120/1] via 192.168.4.2, 00:00:05, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:05, Serial0/0/1
C    192.168.4.0/24 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
C    192.168.6.0/24 is directly connected, Serial0/0/0
```

show ip route

Verificación de la distancia administrativa

```
R3#show ip protocols
Routing Protocol is "rip"
  <output omitted>
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface              Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0        1     1 2
    Serial0/0/0            1     1 2
    Serial0/0/1            1     1 2
  Automatic network summarization is in effect
  Routing for Networks:
    192.168.4.0
    192.168.5.0
    192.168.6.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.6.2          120      00:00:10
    192.168.4.2          120      00:00:18
  Distance: (default is 120)
```

show ip protocols

## 5.2 CONFIGURACION BÁSICA DEL RIPv1.-

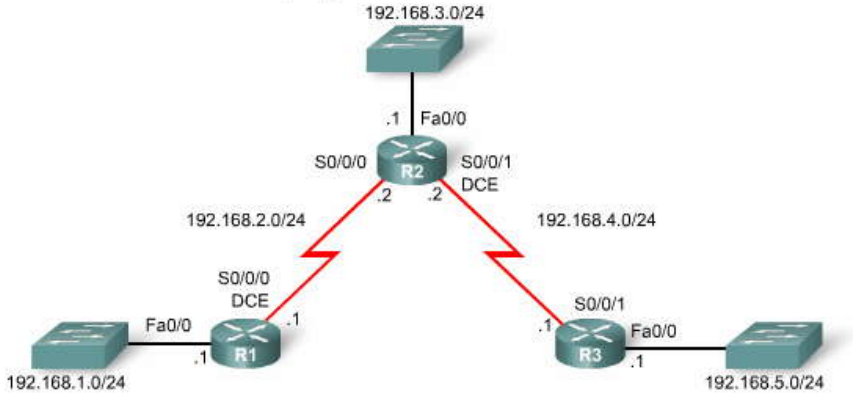
### 5.2.1 ARRANQUE EN FRIO.-

La figura muestra la topología de los tres routers que utilizamos en el Capítulo 2, "Enrutamiento estático". Físicamente, la topología es la misma, excepto que no necesitaremos conectar las PC a las LAN. Sin embargo, lógicamente el esquema de direccionamiento es diferente. Utilizamos cinco direcciones de red clase C.

Tabla de direccionamiento: Situación A

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 192.168.1.1 | 255.255.255.0 |
| | S0/0/0 | 192.168.2.1 | 255.255.255.0 |
| R2 | Fa0/0 | 192.168.3.1 | 255.255.255.0 |
| | S0/0/0 | 192.168.2.2 | 255.255.255.0 |
| | S0/0/1 | 192.168.4.2 | 255.255.255.0 |
| R3 | Fa0/0 | 192.168.5.1 | 255.255.255.0 |
| | S0/0/1 | 192.168.4.1 | 255.255.255.0 |

Topología de RIP: Situación A




### 5.2.2 HABILITACIÓN DE RIP: COMANDO ROUTER RIP.-

Para habilitar un protocolo de enrutamiento dinámico, ingrese en el modo de configuración global y utilice el comando router. Como se muestra en la figura, si escribe un espacio seguido de un signo de interrogación, aparecerá una lista de los protocolos de enrutamiento disponibles admitidos por IOS.

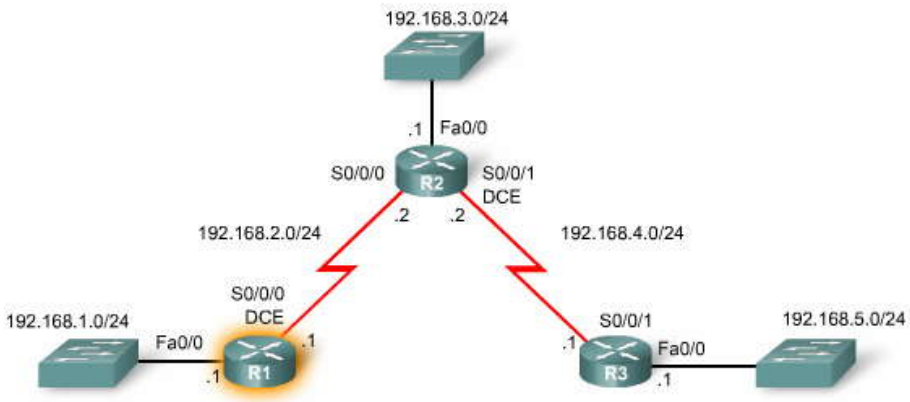
Para ingresar en el modo de configuración del router para RIP, ingrese router rip en la solicitud de configuración global. Observe que la solicitud cambia de una solicitud de configuración global a la siguiente:

R1(config-router)#

Este comando no inicia en forma directa el proceso de RIP. En su lugar, brinda acceso a la configuración de los parámetros del protocolo de enrutamiento. No se envían actualizaciones de enrutamiento.

Si necesita eliminar completamente el proceso de enrutamiento de RIP de un dispositivo, realice la denegación del comando mediante no router rip. Este comando detiene el proceso RIP y elimina todas las configuraciones RIP existentes.

Topología de RIP: Situación A



### 5.2.3 ESPECIFICACIÓN DE REDES.-

Al ingresar en el modo de configuración de router RIP, se brindan instrucciones al router para que ejecute RIP. Pero el router aún necesita conocer las interfaces locales que deberá utilizar para comunicarse con otros routers, así como las redes conectadas en forma local que deberá publicar a dichos routers. Para habilitar el enrutamiento RIP para una red, utilice el comando network en el modo de configuración del router e ingrese la dirección de red con clase para cada red conectada directamente.

Router(config-router)#network dirección de red con clase directamente conectada

El comando **network:**
Habilita el RIP en todas las interfaces que pertenecen a una red específica. Las interfaces asociadas ahora enviarán y recibirán actualizaciones de RIP.
Publica la red especificada en las actualizaciones de enrutamiento RIP enviadas a otros routers cada 30 segundos.

**Nota:** Si ingresa una dirección de subred, IOS la convierte automáticamente en una dirección de red con clase. Por ejemplo, si ingresa el comando network **192.168.1.32**, el router lo convertirá en network 192.168.1.0.

Sintaxis y finalidad del comando `network`

| El comando | |
|---|---|
| **Finalidad** | ▪ Permite el envío y la recepción de actualizaciones RIP para las interfaces que pertenecen a la red especificada<br>▪ Informa la red especificada sobre actualizaciones RIP |
| **Sintaxis** | `Router(config-router)#network` *directly-connected-classful-address* |

En la figura, el comando network se configura en los tres routers para las redes conectadas directamente. Observe que sólo se ingresaron las redes con clase.

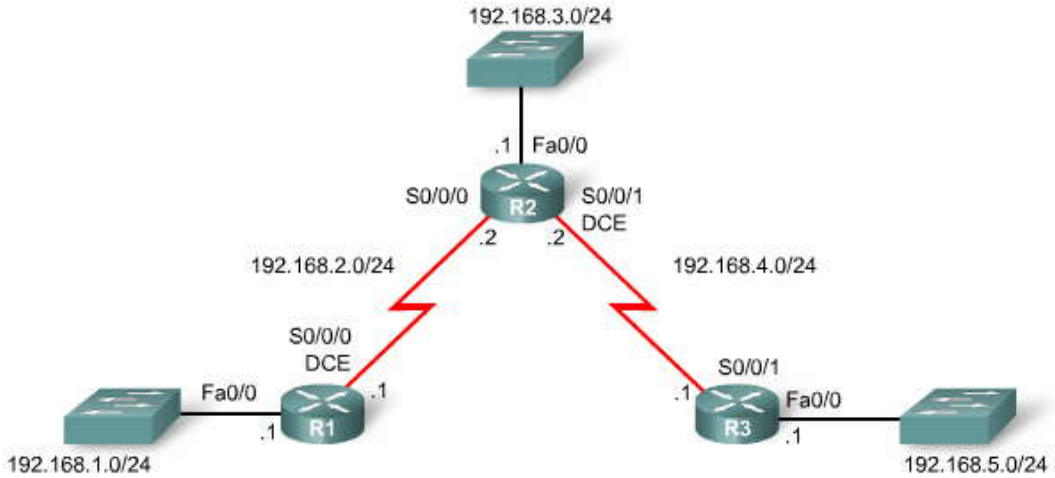
¿Qué ocurre si ingresa una dirección de subred o dirección IP de interfaz en lugar de una dirección de red con clase al utilizar el comando network para configuraciones RIP?

R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.1

En este ejemplo, ingresamos una dirección IP de interfaz en lugar de una dirección de red con clase. Observe que IOS no presenta ningún mensaje de error. En su lugar, IOS corrige la entrada e ingresa la dirección de red con clase. Esto se demuestra con la verificación que se encuentra a continuación.

R3#show running-config
!
router rip
network 192.168.4.0
network 192.168.5.0
!

Topología RIP: Situación A



Comparación de resultado: Habilitación de RIP con el comando **network**

```
R1(config)#router rip
R1(config-router)#network 192.168.1.0
R1(config-router)#network 192.168.2.0
```

```
R2(config)#router rip
R2(config-router)#network 192.168.2.0
R2(config-router)#network 192.168.3.0
R2(config-router)#network 192.168.4.0
```

```
R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
```

## 5.3 VERIFICACIÓN Y RESOLUCIÓN DE PROBLEMAS.-

### 5.3.1 VERIFICACIÓN DE RIP: SHOW IP ROUTE.-

**Poderosos comandos para la resolución de problemas**

Para verificar y solucionar problemas de enrutamiento, primero utilice show ip route y show ip protocols. Si no puede aislar el problema mediante estos dos comandos, utilice debug ip rip para ver qué ocurre exactamente. Estos tres comandos se discuten en un orden sugerido que usted podrá utilizar para verificar y solucionar problemas en una configuración de protocolo de enrutamiento. Recuerde, antes de configurar cualquier enrutamiento, ya sea estático o dinámico, asegúrese de que todas las interfaces necesarias estén "habilitadas" con el comando show ip interface brief.

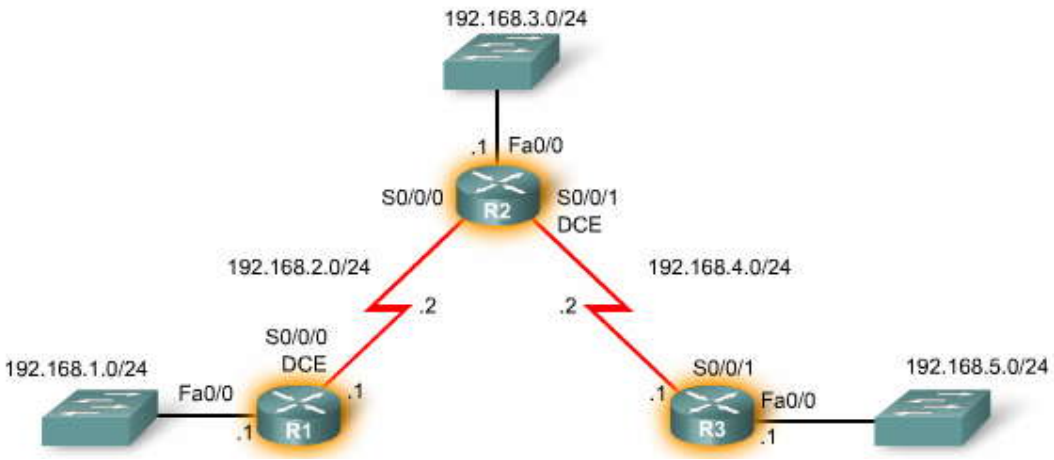
**Haga clic en R1, R2 y R3 para ver las tablas de enrutamiento.**

El comando show ip route verifica que las rutas recibidas por vecinos RIP estén instaladas en una tabla de enrutamiento. Una R en el resultado indica las rutas RIP. Debido a que este comando muestra la tabla de enrutamiento completa, incluidas las rutas estáticas y las conectadas directamente, normalmente éste es el primer comando utilizado para verificar la convergencia. Es posible que las rutas no aparezcan de inmediato cuando ejecute este comando ya que la convergencia de las redes puede tomar cierto tiempo. Sin embargo, una vez que el enrutamiento esté correctamente configurado en todos los routers, el comando show ip route reflejará que cada router cuenta con una tabla de enrutamiento completa, con una ruta para cada red de la topología.

**Haga clic en el botón Topología.**

Como puede ver en la figura, hay cinco redes en la topología. Cada router enumera cinco redes en la tabla de enrutamiento; por lo tanto, podemos decir que los tres routers convergen debido a que cada router tiene una ruta para cada red ilustrada en la topología.

Topología de RIP: Situación A



Verificación de la convergencia de RIP con **show ip route**

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is not set

R    192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:02, Serial0/0/0
R    192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:02, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:02, Serial0/0/0
```

Verificación de la convergencia de RIP con **show ip route**

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.1, 00:00:12, Serial0/0/1
R    192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:24, Serial0/0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
```

Verificación de la convergencia de RIP con **show ip route**

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
R    192.168.1.0/24 [120/2] via 192.168.4.2, 00:00:08, Serial0/0/1
R    192.168.2.0/24 [120/1] via 192.168.4.2, 00:00:08, Serial0/0/1
R    192.168.3.0/24 [120/1] via 192.168.4.2, 00:00:08, Serial0/0/1
```

**Interpretación del resultado de show ip route**

Con la información de la figura, nos enfocaremos en una ruta RIP aprendida mediante R1 e interpretaremos el resultado que aparece en la tabla de enrutamiento.

**R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:23, Serial0/0/0**

La lista de rutas con un código R es una manera rápida de verificar si RIP está realmente en ejecución en este router. Si RIP no se encuentra al menos parcialmente configurado, no verá ninguna ruta RIP.

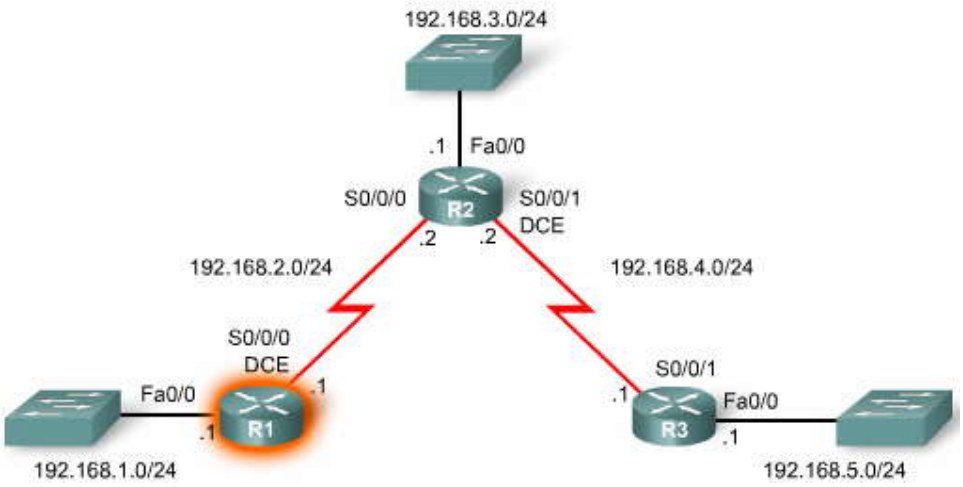
A continuación, se enumeran la dirección de red remota y la máscara de subred (192.168.5.0/24).

Entre paréntesis se muestra el valor AD (120 para RIP) y la distancia a la red (2 saltos).

La dirección IP del siguiente salto del router que realiza la notificación está enumerada (R2 en 192.168.2.2) y la cantidad de segundos que pasaron desde la última actualización (00:00:23, en este caso).

Por último, se enumera la interfaz de salida que utilizará este router para el tráfico destinado a la red remota (Serial 0/0/0).

Topología RIP: Situación A




```
R 192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:23, Serial 0/0/0
```

Interpretación de una ruta RIP en la tabla de enrutamiento

| Resultado | Descripción |
|---|---|
| R | Identifica el origen de la ruta como RIP. |
| 192.168.5.0 | Indica la dirección de la red remota. |
| /24 | La máscara de subred que se usa para esta red |
| [120/2] | La distancia administrativa (120) y la métrica (2 saltos) |
| via 192.168.2.2 | Especifica la dirección del router del siguiente salto (R2) que envía tráfico hacia la red remota. |
| 00:00:23 | Especifica la cantidad de tiempo desde que se actualizó la ruta (aquí, 23 segundos). Otra actualización está programada para dentro de 7 segundos. |
| Serial0/0/0 | Especifica la interfaz local por la cual se puede llegar a la red remota. |

### 5.3.2 VERIFICACIÓN DE RIP: SHOW IP PROTOCOLS.-

**Interpretación del resultado de show ip protocols**

Si falta una red de la tabla de enrutamiento, verifique la configuración de enrutamiento mediant e show ip protocols. El comando show ip protocols muestra el protocolo de enrutamiento configurado actualmente en el router. Este resultado puede usarse para verificar la mayoría de los parámetros RIP a fin de confirmar si:
está configurado el enrutamiento RIP
las interfaces correctas envían y reciben actualizaciones RIP
el router publica las redes correctas
los vecinos RIP envían actualizaciones

Este comando también es muy útil para la verificación de las operaciones de otros protocolos de enrutamiento, c omo veremos más adelante con EIGRP y OSPF.

**Haga clic en el botón 1 en la figura.**

La primera línea de resultados verifica si el enrutamiento RIP está configurado y en ejecución en el router R2. Como vimos en la sección anterior, "Configuración básica del RIPv1", se necesita al menos una interfaz activa con un comando network asociado antes de iniciar el enrutamiento RIP.

**Haga clic en el botón 2 en la figura.**

Éstos son los temporizadores que indican cuándo se enviará la siguiente serie de actualizaciones desde este router, 23 segundos a partir de ahora, en el ejemplo.

**Haga clic en el botón 3 en la figura.**

Esta información se relaciona con las actualizaciones de filtrado y las rutas de redistribución, si están configuradas en este router. El filtrado y la redistribución son dos temas de nivel CCNP.

**Haga clic en el botón 4 en la figura.**

Este bloque de resultados contiene información acerca de la versión RIP que está configurada actualmente y las interfaces que participan en las actualizaciones RIP.

**Haga clic en el botón 5 en la figura.**

Esta parte del resultado muestra que el router R2 actualmente realiza el resumen en el borde de la red con clase y utilizará en forma predeterminada hasta cuatro rutas de igual costo para equilibrar cargas en el tráfico.

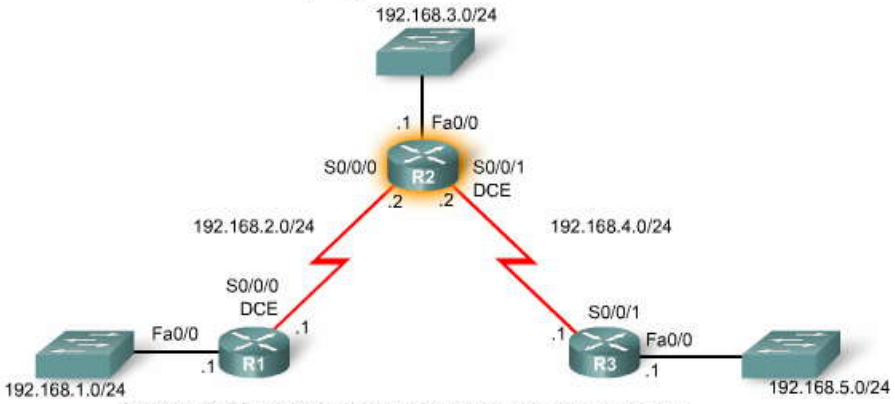
**Haga clic en el botón 6 en la figura.**

Las redes con clase configuradas con el comando network se enumeran a continuación. Éstas son las redes que incluirá R2 en sus actualizaciones RIP.

**Haga clic en el botón 7 en la figura.**

Desplácese hacia abajo para ver el resultado restante. Los vecinos RIP se enumeran aquí como Fuentes de información de enrutamiento. Gateway es la dirección IP del siguiente salto del vecino que envía actualizaciones de R2. Distancia es la AD que utiliza R2 para las actualizaciones enviadas por este vecino. Última actualización son los segundos transcurridos desde que se recibió la última actualización por parte de este vecino.

Topología de RIP: Situación A




Interpretación de resultados de **show ip protocols**

```
R2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 23 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
    Interface                Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0          1        1 2
    Serial0/0/0              1        1 2
    Serial0/0/1              1        1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
    192.168.4.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1          120      00:00:18
    192.168.4.1          120      00:00:22
  Distance: (default is 120)
```

### 5.3.3 VERIFICACIÓN DE RIP: DEBUG IP RIP.-

**Interpretación del resultado de debug ip rip**

La mayoría de los errores de configuración de RIP involucran una configuración de sentencia network, una configuración de sentencia network faltante o la configuración de subredes no contiguas en un entorno con clase. Como se muestra en la figura, un comando efectivo utilizado para reconocer problemas con las actualizaciones RIP es el debug ip rip. Este comando muestra las actualizaciones de enrutamiento RIP a medida que se envían y reciben. Debido a que las actualizaciones son periódicas, necesitará esperar la siguiente serie de actualizaciones antes de ver cualquier resultado.

**Haga clic en el botón 1 en la figura.**

Primero veremos una actualización proveniente de R1 en la interfaz Serial 0/0/0. Observe que R1 sólo envía una ruta a la red 192.168.1.0. No se envían más rutas para no violar la regla de horizonte dividido. R1 no está autorizado a publicar redes nuevamente en R2 que R2 envío previamente a R1.

**Haga clic en el botón 2 en la figura.**

La siguiente actualización que se recibe proviene de R3. Nuevamente, debido a la regla de horizonte dividido, R3 sólo envía una ruta: red 192.168.5.0.

**Haga clic en el botón 3 en la figura.**

R2 envía sus propias actualizaciones. Primero, R2 crea una actualización para enviar a la interfaz FastEthernet0/0. La actualización incluye la tabla de enrutamiento completa, excepto la red 192.168.3.0, que está conectada a FastEthernet0/0.

**Haga clic en el botón 4 en la figura.**

A continuación, R2 crea una actualización para enviar a R3. Se incluyen tres rutas. R2 no publica la red que R2 y R3 comparten ni publica la red 192.168.5.0 debido al horizonte dividido.

**Haga clic en el botón 5 en la figura.**

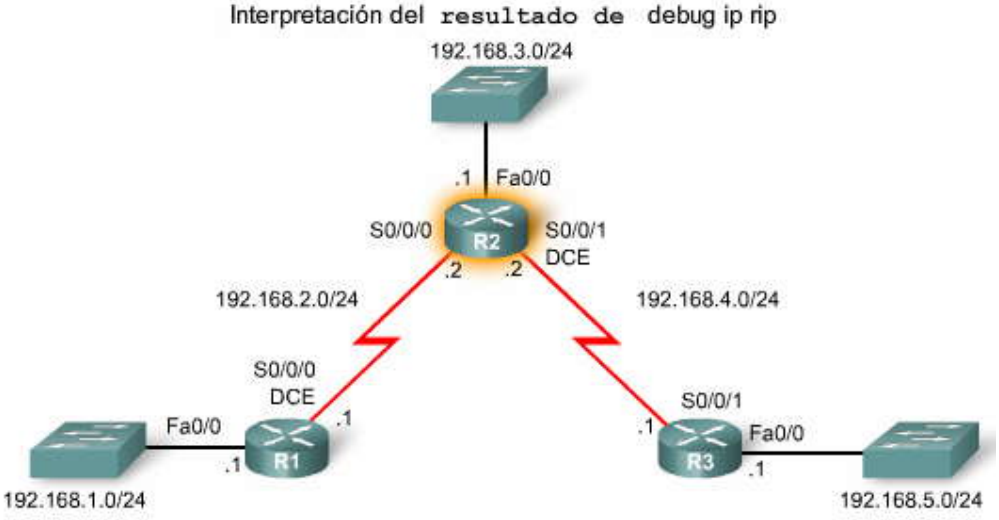
Por último, R2 crea una actualización para enviar a R1. Se incluyen tres rutas. R2 no publica la red que R2 y R1 comparten ni publica la red 192.168.1.0 debido al horizonte dividido.

Nota: Si esperara otros 30 segundos, vería todos los resultados de depuración mostrados en la repetición de la figura debido a que RIP envía actualizaciones periódicas cada 30 segundos.

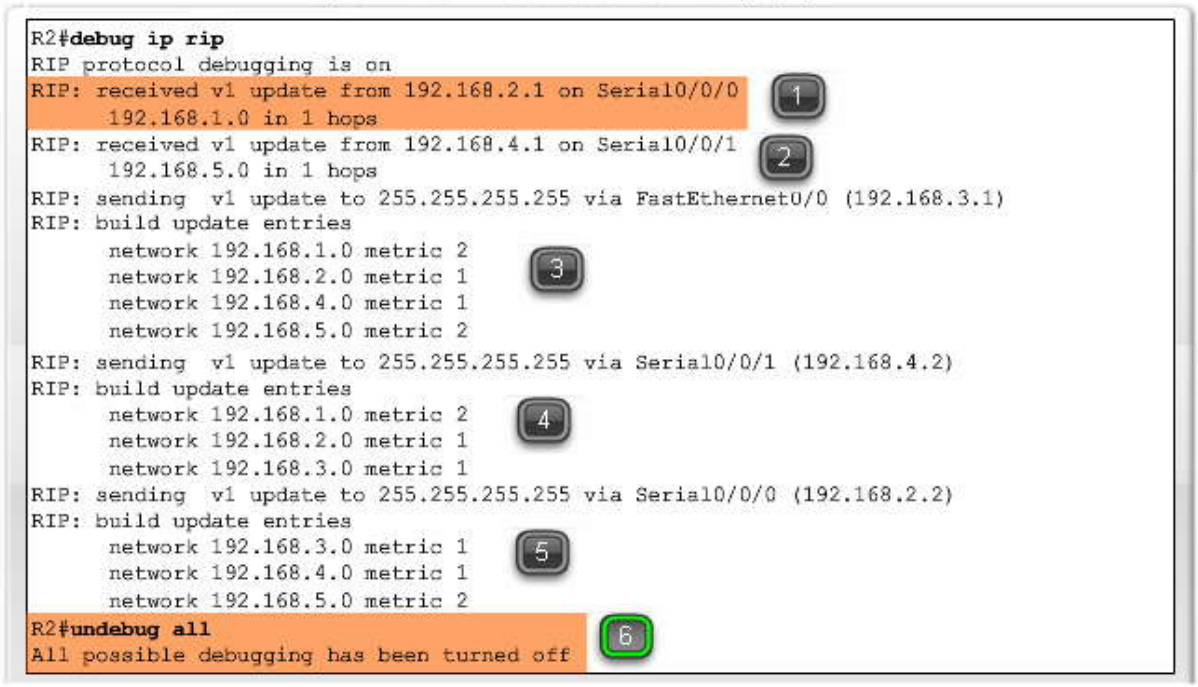
**Haga clic en el botón 6 en la figura.**

Para detener la supervisión de las actualizaciones RIP en R2, ingrese el comando no debug ip rip o simplemente undebug all, como se muestra en la figura.

Al revisar este resultado de depuración, podemos verificar que el enrutamiento RIP es completamente operativo en R2. Pero, ¿encuentra un modo de optimizar el enrutamiento RIP en R2? ¿Necesita R2 enviar actualizaciones fuera de FastEthernet0/0? En el siguiente tema veremos cómo pueden prevenirse las actualizaciones innecesarias.



Interpretación del resultado de debug ip rip




### 5.3.4 INTERFACES PASIVAS.-

**Las actualizaciones RIP innecesarias influyen en la red**

Como vio en el ejemplo anterior, R2 envía actualizaciones fuera de FastEthernet0/0 a pesar de que no existe ningún dispositivo RIP en dicha LAN. R2 no tiene modo de conocer esto y, como consecuencia, envía una actualización cada 30 segundos. El envío de actualizaciones innecesarias a una LAN influye en la red de tres maneras:

1. Se desperdicia el ancho de banda al transportar actualizaciones innecesarias. Debido a la transmisión de las actualizaciones RIP, los switches reenviarán las actualizaciones a todos los puertos.

2. Todos los dispositivos de la LAN deben procesar la actualización hasta las capas de transporte, donde el dispositivo receptor desechará la actualización.

3. La publicación de actualizaciones en una red de broadcast representa un riesgo para la seguridad. Las actualizaciones RIP pueden interceptarse con software de detección de paquetes. Las actualizaciones de enrutamiento pueden modificarse y enviarse nuevamente al router, con lo cual se corrompería la tabla de enrutamiento con métricas falsas que encaminan el tráfico en forma errónea.

**Detención de actualizaciones RIP innecesarias**

Es posible que piense que puede detener las actualizaciones retirando la red 192.168.3.0 de la configuración mediante el comando no network 192.168.3.0, pero entonces R2 no publicará esta LAN como una ruta en las actualizaciones enviadas a R1 y R3. La solución correcta es utilizar el comando passive-interface, que evita la transmisión de las actualizaciones de enrutamiento a través de una interfaz de router pero aun así permite la notificación de dicha red en otros routers. Ingrese el comando passive-interface en el modo de configuración de router.

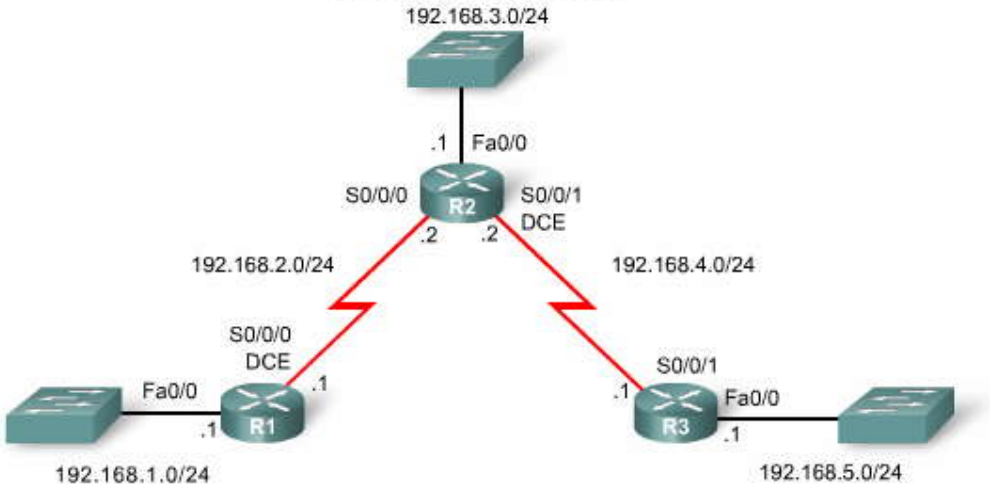
Router(config-router)#passive-interface interface-type interface-number

Este comando detiene las actualizaciones de enrutamiento de la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada aún se publicará en las actualizaciones de enrutamiento enviadas a otras interfaces.

En la figura, R2 se configura inicialmente con el comando passive-interface para prevenir las actualizaciones de enrutamiento en FastEthernet0/0 debido a la falta de vecinos RIP en la LAN. El comando show ip protocols se utiliza luego para verificar la interfaz pasiva. Observe que la interfaz ya no se enumera en Interfaz, sino en una nueva sección denominada Interfaces pasivas. Asimismo, observe que la red 192.168.3.0 aún se encuentra en Enrutamiento para redes, lo cual significa que esta red aún está incluida como una entrada de ruta en las actualizaciones RIP que se envían a R1 y R3.

Todos los protocolos de enrutamiento admiten el comando passive-interface. Se espera que se utilice el comando passive-interface cuando corresponda como parte de la configuración normal de enrutamiento.

Topología RIP: Situación A




Inhabilitación de actualizaciones con el comando `passive-interface`

```
R2(config)#router rip
R2(config-router)#passive-interface FastEthernet 0/0
R2(config-router)#end
R2#show ip protocols
Routing Protocol is "rip"
    Sending updates every 30 seconds, next due in 14 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
    Outgoing update filter list for all interfaces is
    Incoming update filter list for all interfaces is
    Redistributing: rip
    Default version control: send version 1, receive any version
        Interface             Send  Recv  Triggered RIP  Key-chain
        Serial0/0/0           1     1 2
        Serial0/0/1           1     1 2
    Automatic network summarization is in effect
    Routing for Networks:
        192.168.2.0
        192.168.3.0
        192.168.4.0
```

Observe que FastEthernet 0/0 ya no se menciona debajo de "Default version control:"
Sin embargo, R2 sigue siendo el enrutamiento para 192.168.3.0 y ahora menciona a FastEthernet debajo de "Passive Interfaces:"

## 5.4 RESUMEN AUTOMÁTICO.-

### 5.4.1 TOPOLOGIA MIDIFICADA: ESCENARIO B.-

Para prestar ayuda con la discusión de resumen automático, la topología RIP mostrada en la figura se modificó con los siguientes cambios:

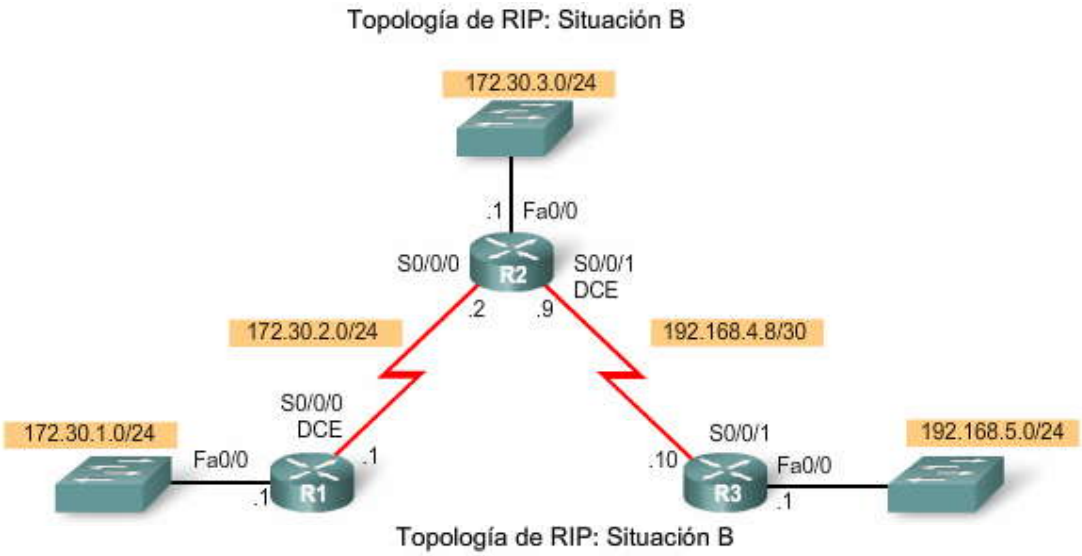
Se utilizan tres redes con clase:
172.30.0.0/16
192.168.4.0/24
192.168.5.0/24

La red 172.30.0.0/16 se divide en tres subredes:
172.30.1.0/24
172.30.2.0/24
172.30.3.0/24

Los siguientes dispositivos forman parte de la dirección de red con clase 172.30.0.0/16:
Todas las interfaces en R1

S0/0/0 y Fa0/0 en R2

La red 192.168.4.0/24 se divide como una única subred 192.168.4.8/30




Topología de RIP: Situación B

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 172.30.1.1 | 255.255.255.0 |
| | S0/0/0 | 172.30.2.1 | 255.255.255.0 |
| R2 | Fa0/0 | 172.30.3.1 | 255.255.255.0 |
| | S0/0/0 | 172.30.2.2 | 255.255.255.0 |
| | S0/0/1 | 192.168.4.9 | 255.255.255.252 |
| R3 | Fa0/0 | 192.168.5.1 | 255.255.255.0 |
| | S0/0/1 | 192.168.4.10 | 255.255.255.252 |

Haga clic en R1, R2 y R3 para ver los detalles de configuración de cada router.

Observe que los comandos no shutdown y clock rate no son necesarios debi do a que dichos comandos aún se configuran desde el Escenario A. Sin embargo, debido a que se agregaron nuevas redes, el proceso de enrutamiento RIP se eliminó por completo con el comando no router rip antes de habilitarlo nuevamente.

Haga clic en R1 en la figura.

En el resultado de R1, observe que ambas subredes están configuradas con el comando network. Esta configuración es técnicamente incorrecta ya que RIPv1 envía la dirección de red con clase en sus actualizaciones y no la subred. Por lo tanto, IOS cambió la configuración para reflejar la configuración con clase correcta, como puede verse con el resultado de show run.

Haga clic en R2 en la figura.

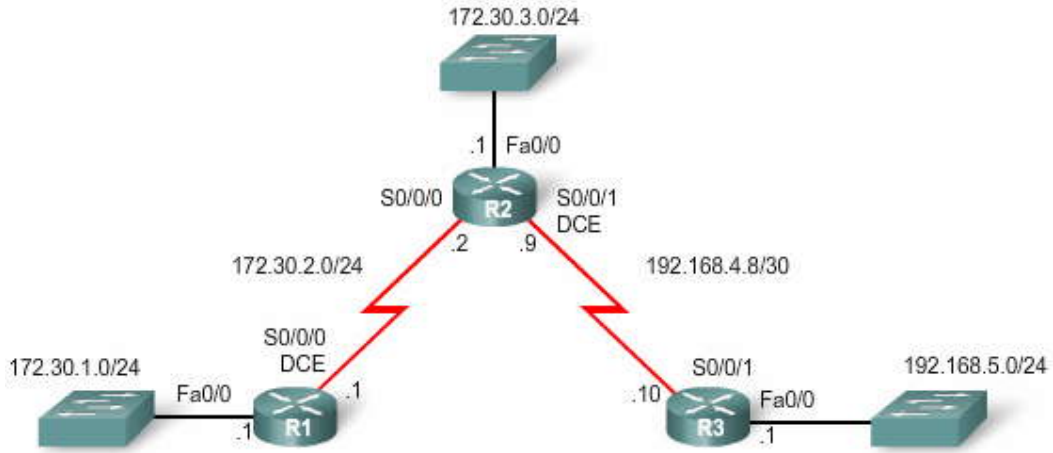
En el resultado para R2, observe que la subred 192.168.4.8 se configuró con el comando network. Nuevam ente, esta configuración es técnicamente incorrecta y el IOS la cambió a 192.168.4.0 en la configuración en ejecución.

Haga clic en R3 en la figura.

La configuración de enrutamiento para R3 es correcta. La configuración en ejecución coincide con la ingre sada en el modo de configuración de router.

Nota: En los exámenes de evaluación y certificación, ingresar una dirección de subred en lugar de una dirección de red con clase en un comando network se considera una respuesta incorrecta.

Topología RIP: Situación B




Topología RIP: Situación B

```
R1(config)#interface fa0/0
R1(config-if)#ip address 172.30.1.1 255.255.255.0
R1(config-if)#interface S0/0/0
R1(config-if)#ip address 172.30.2.1 255.255.255.0
R1(config-if)#no router rip
R1(config)#router rip
R1(config-router)#network 172.30.1.0
R1(config-router)#network 172.30.2.0
R1(config-router)#passive-interface FastEthernet 0/0
R1(config-router)#end
R1#show run
<output omitted>
!
router rip
 passive-interface FastEthernet0/0
 network 172.30.0.0
!
<output omitted>
```

Topología RIP: Situación B

```
R2(config)#interface S0/0/0
R2(config-if)#ip address 172.30.2.2 255.255.255.0
R2(config-if)#interface fa0/0
R2(config-if)#ip address 172.30.3.1 255.255.255.0
R2(config-if)#interface S0/0/1
R2(config-if)#ip address 192.168.4.9 255.255.255.252
R2(config-if)#no router rip
R2(config)#router rip
R2(config-router)#network 172.30.0.0
R2(config-router)#network 192.168.4.8
R2(config-router)#passive-interface FastEthernet 0/0
R2(config-router)#end
R2#show run
<output omitted>
!
router rip
 passive-interface FastEthernet0/0
 network 172.30.0.0
```

Topología RIP: Situación B

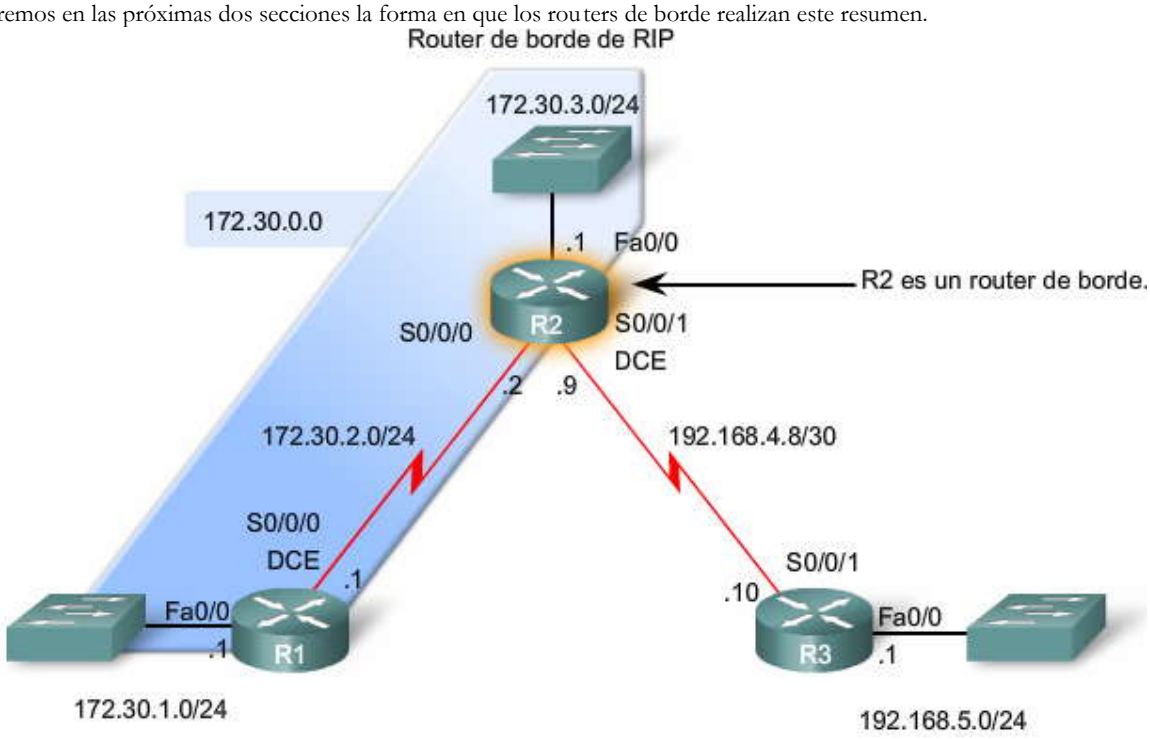
```
R3(config)#interface fa0/0
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#interface S0/0/1
R3(config-if)#ip address 192.168.4.10 255.255.255.252
R3(config-if)#no router rip
R3(config)#router rip
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#passive-interface FastEthernet 0/0
R3(config-router)#end
R3#show run
<output omitted>
!
router rip
 passive-interface FastEthernet0/0
 network 192.168.4.0
 network 192.168.5.0
!
```

### 5.4.2 ROUTERS DE BORDE Y RESUMEN AUTOMÁTICO.-

Como sabe, RIP es un protocolo de enrutamiento con clase que resume automáticamente redes con clase en los bordes de redes principales. En la figura, puede ver que R2 posee interfaces en más de una red principal con clase. Esto convierte a R2 en un router de borde en RIP. Las interfaces Serial 0/0/0 y FastEthernet 0/0 en R2 se encuentran dentro del borde 172.30.0.0. La interfaz Serial 0/0/1 está dentro del borde 192.168.4.0.

Debido a que los routers de borde resumen subredes RIP de una red principal a otra, las actualizaciones para las redes 172.30.1.0, 172.30.2.0 y 172.30.3.0 se resumirán automáticamente en 172.30.0.0 cuando se envíe la interfaz Serial 0/0/1 de R2.

Veremos en las próximas dos secciones la forma en que los routers de borde realizan este resumen.




### 5.4.3 PROCESAMIENTO DE ACTUALIZACIONES RIP.-

**Reglas para el procesamiento de actualizaciones RIPv1**

Las siguientes dos reglas regulan las actualizaciones RIPv1:

- Si una actualización de enrutamiento y la interfaz que la recibe pertenecen a la misma red principal, la máscara de subred de la interfaz se aplica a la red de la actualización de enrutamiento.

- Si una actualización de enrutamiento y la interfaz que la recibe pertenecen a diferentes redes principales, la máscara de subred con clase de la red se aplica a la red de la actualización de enrutamiento.

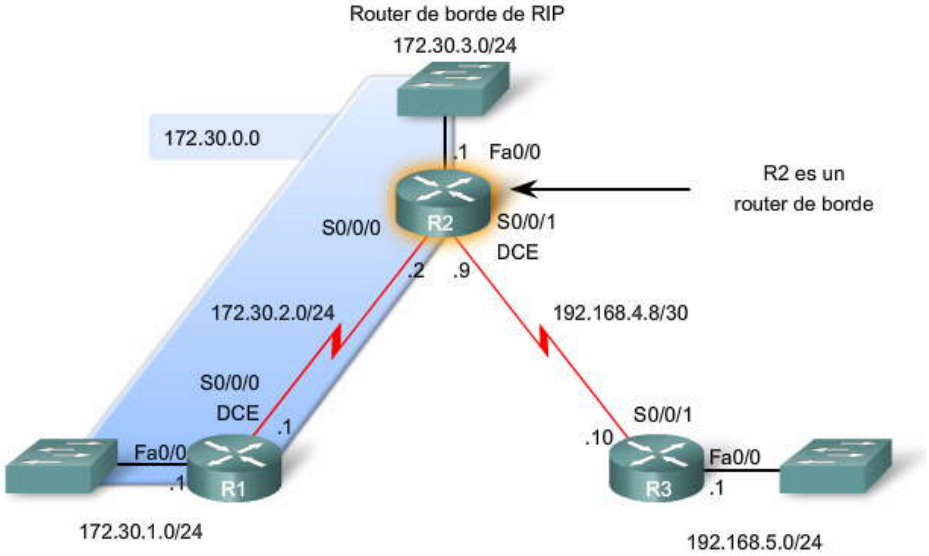
**Ejemplo de actualizaciones de procesamiento de RIPv1**

En la figura, R2 recibe una actualización de R1 e ingresa la red en la tabla de enrutamiento. ¿Cómo sabe R2 que esta subred tiene una máscara de subred /24 (255.255.255.0)? Lo sabe debido a que:

- R2 recibió dicha información en una interfaz que pertenece a la misma red con clase (172.30.0.0) que la de la actualización 172.30.1.0 entrante.
- La dirección IP para la que R2 recibió el mensaje "172.30.1.0 in 1 hops" (172.30.1.0 en 1 salto) se encontraba en Serial 0/0/0 con una dirección IP de 172.30.2.2 y una máscara de subred de 255.255.255.0 (/24).
- R2 utiliza su propia máscara de subred en esta interfaz y la aplica a ésta y a todas las demás subredes 172.30.0.0 que ésta recibe en esta interfaz; en este caso, 172.30.1.0.
- La subred 172.30.1.0 /24 se agregó a la tabla de enrutamiento.

Los routers que ejecutan RIPv1 se limitan a la utilización de la misma máscara de subred para todas las subredes con la misma red con clase.

Como aprenderá en los siguientes capítulos, los protocolos de enrutamiento sin clase como RIPv2 permiten que la misma red principal (con clase) utilice diferentes máscaras de subred en diferentes subredes, más conocida como Máscara de subred de longitud variable (VLSM).




```
R2#debug ip rip
RIP protocol debugging is on
RIP: received v1 update from 172.30.2.1 on Serial0/0/0
      172.30.1.0 in 1 hops
<output omitted>
R2#undebug all
All possible debugging has been turned off
R2#show ip route
<output omitted>

Gateway of last resort is not set

     172.30.0.0/24 is subnetted, 3 subnets
R       172.30.1.0 [120/1] via 172.30.2.1, 00:00:18, Serial0/0/0
C       172.30.2.0 is directly connected, Serial0/0/0
C       172.30.3.0 is directly connected, FastEthernet0/0
     192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
R    192.168.5.0/24 [120/1] via 192.168.4.10, 00:00:16, Serial0/0/1
R2#
```

### 5.4.4 ENVIO DE ACTUALIZACIONES RIP.-

**Utilización de la depuración para ver el resumen automático**

Al enviar una actualización, el router de borde R2 incluirá la dirección de red y la métrica asoci ada. Si la entrada de ruta es para una actualización enviada a una red principal diferente, luego la dirección de red en la entrada de ruta se resume en la dirección de red principal o con clase. Esto es exactamente lo que hace R2 para 192.168.4.0 y 192.16 8.5.0. Envía dichas redes con clase a R1.

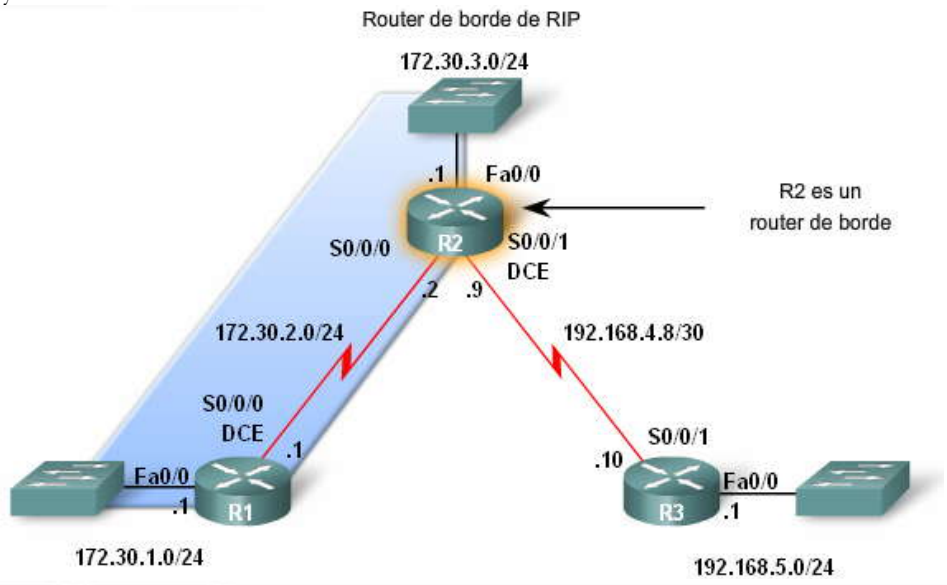
R2 también tiene rutas para las subredes 172.30.1.0/24, 172.30.2.0/24 y 172.30.3.0/24. En la actualización de enrutamiento de R2 a R3 en Serial0/0/1, R2 sólo envía un resumen de la dirección de red con clase de 17 2.30.0.0.

Si la entrada de ruta es para una actualización enviada dentro de una red principal, la máscara de subred de la interfaz saliente se utiliza para determinar la dirección de red para publicar. R2 envía la subred 172.30.3.0 a R1 mediante la máscar a de subred en Serial0/0/0 para determinar la dirección de subred para publicar.

R1 recibe la actualización 172.30.3.0 en la interfaz Serial0/0/0, que posee una dirección de interfaz de 172.30.2.1/24. Ya que la actualización de enrutamiento y la interfaz pertenecen a la misma red principal, R1 aplica su máscara /24 a la ruta 172.30.3.0.

**Haga clic en las tablas de enrutamiento R1 y R3 en la figura para comparar las tablas de enrutamiento.**

Observe que R1 tiene tres rutas para la red principal 172.30.0.0, que se ha dividido en subredes a /24 ó 255.255.255.0. R3 sólo tiene una ruta hacia la red 172.30.0.0 y la red no se ha dividido en subredes. R3 tiene la red principal en su tabla de enrutamiento. Sin embargo, sería un error asumir que R3 no cuenta con cone ctividad total. R3 enviará cualquier paquete destinado para las redes 172.30.1.0/24, 172.30.2.0/24 y 172.30.3.0/24 hacia R2, ya que esas tres redes pertenecen a 172.30.0.0/16 y son alcanzables a través de R2.




```
R2#debug ip rip
RIP protocol debugging is on
RIP: sending  v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.2)
RIP: build update entries
      network 172.30.3.0 metric 1
      network 192.168.4.0 metric 1
      network 192.168.5.0 metric 2
RIP: sending  v1 update to 255.255.255.255 via Serial0/0/1 (192.168.4.9)
RIP: build update entries
      network 172.30.0.0 metric 1
R2#undebug all
All possible debugging has been turned off
R2#
```

Rutas enviadas hacia R1.

Compare las rutas de R1 y R3 para la red 172.30.0.0

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <remaining codes omitted>

Gateway of last resort is not set

     172.30.0.0/24 is subnetted, 3 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, Serial0/0/0
R       172.30.3.0 [120/1] via 172.30.2.2, 00:00:17, Serial0/0/0
R    192.168.4.0/24 [120/1] via 172.30.2.2, 00:00:17, Serial0/0/0
R    192.168.5.0/24 [120/2] via 172.30.2.2, 00:00:17, Serial0/0/0

R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <remaining codes omitted>
```

Compare las rutas de R1 y R3 para la red 172.30.0.0

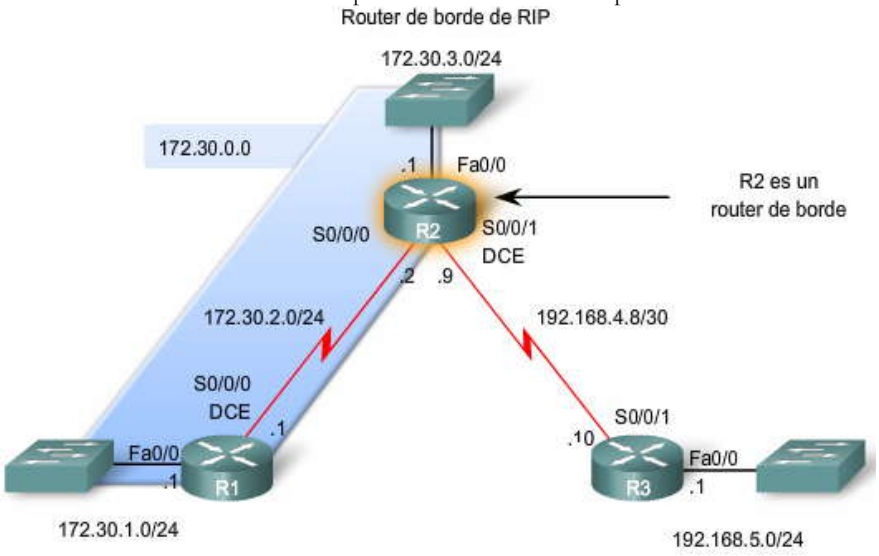
### 5.4.5 VENTAJAS Y DESVENTAJAS DEL RESUMEN AUTOMATICO.-

**Ventajas del resumen automático**

Como se vio con R2 en la figura anterior, RIP resume automáticamente las actualizaciones entre redes con clase. Debido a que la actualización 172.30.0.0 se envía fuera de una interfaz (Serial 0/0/1) en una red con clase diferente (192.168.4.0), RIP envía sólo una actualización única para toda la red con clase en lugar de enviar una para cada una de las diferentes subredes. Este proceso es similar al que realizamos al resumir varias rutas estáticas en una única ruta estática. ¿Por que el resumen automático constituye una ventaja?

Se envían y reciben actualizaciones de enrutamiento menores, que utilizan menor ancho de banda para las actualizaciones de enrutamiento entre R2 y R3.

R3 tiene una ruta única para la red 172.30.0.0/16, independientemente de la cantidad de subredes que haya o cómo se divida en subredes. La utilización de una única ruta ofrece un proceso de consulta más rápido en la tabla de enrutamiento para R3.



Ventajas del resumen automático

```
R3#show ip route
Codes: C - connected, S - static, I -IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSFP inter area
       N1 - OSPF NSSA externasl type 1, N2 - OSPF NSSA external type2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, II - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    172.30.0.0/16 [120/1] via 192.168.4.9, 00:00:15, Serial0/0/1
     192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

R3 recibe una sola ruta resumida.

¿Existe alguna desventaja en el resumen automático? Sí, cuando hay redes no contiguas configuradas en la topología.

Desventaja del resumen automático

Como puede ver en la figura, el esquema de direccionamiento cambió. Esta topología se utilizará para mostrar una desventaja principal con los protocolos de enrutamiento con clase como RIPv1: su falta de compatibilidad con redes no contiguas.

Los protocolos de enrutamiento con clase no incluyen la máscara de subred en las actualizaciones de enrutamiento. Las redes se resumen automáticamente a través de los bordes de redes principales, ya que el router receptor no puede determinar la máscara de la ruta. Esto se debe a que la interfaz receptora puede tener una máscara diferente de las rutas divididas en subredes.

Observe que R1 y R3 tienen subredes provenientes de la red principal 172.30.0.0/16, a diferencia de R2. Fundamentalmente, R1 y R3 son routers de borde para 172.30.0.0/16 ya que están separados por otra red principal, 209.165.200.0/24. Esta separación crea una red no contigua, debido a que dos grupos de subredes 172.30.0.0/24 están separados al menos por otra red principal. 172.30.0.0/16 es una red no contigua.

Topología: Desventajas del resumen automático

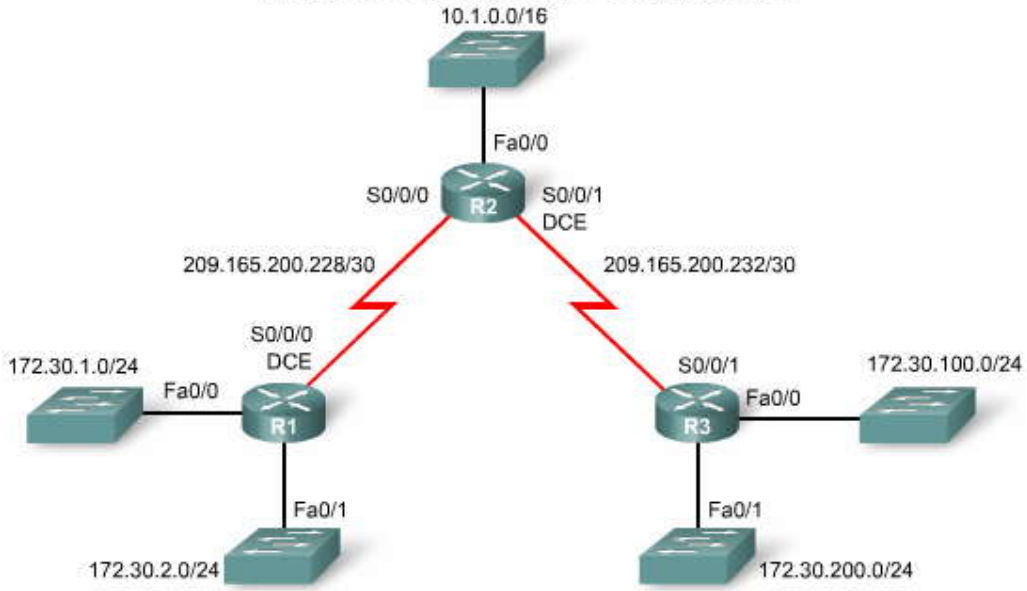


Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 172.30.1.1 | 255.255.255.0 |
| | Fa0/1 | 172.30.2.1 | 255.255.255.0 |
| | S0/0/0 | 209.165.200.229 | 255.255.255.252 |
| R2 | Fa0/0 | 10.1.0.1 | 255.255.255.0 |
| | S0/0/0 | 209.165.200.230 | 255.255.255.252 |
| | S0/0/1 | 209.165.200.233 | 255.255.255.252 |
| R3 | Fa0/0 | 172.30.100.1 | 255.255.255.0 |
| | Fa0/0 | 172.30.200.1 | 255.255.255.0 |
| | S0/0/1 | 209.165.200.234 | 255.255.255.252 |

**Las topologías no contiguas no convergen con RIPv1**

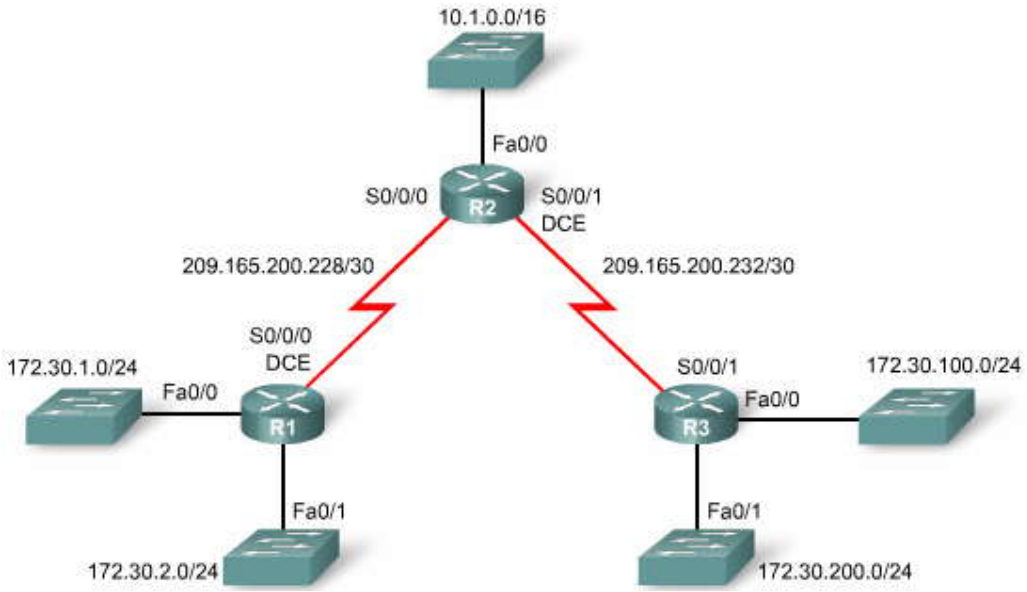
La figura muestra la configuración RIP para cada router según la topología. La configuración RIPv1 es correcta, pero no puede determinar todas las redes en esta topología no contigua. Para comprender los motivos, recuerde que un router sólo publicará las direcciones de red principales en las interfaces que no pertenecen a la ruta publicada. Como consecuencia, R1 no publicará 172.30.1.0 ni 172.30.2.0 para R2 a través de la red 209.165.200.0. R3 no publicará 172.30.100.0 ni 172.30.200.0 para R2 a través de la red 209.165.200.0. Sin embargo, ambos routers publicarán la dirección de la red principal 172.30.0.0, una ruta resumida para R3.

¿Cuál es el resultado? Sin la inclusión de la máscara de subred en la actualización de enrutamiento, RIPv1 no puede publicar información de enrutamiento específica que permitirá a los routers realizar el enrutamiento correctamente para las subredes 172.30.0.0/24.

**Haga clic en los botones show ip route para R1, R2 y R3 en la figura y revise las rutas.**

- R1 no tiene ninguna ruta hacia las LAN conectadas a R3.
- R3 no tiene ninguna ruta hacia las LAN conectadas a R1.
- R2 tiene dos rutas de igual costo hacia la red 172.30.0.0.
- R2 equilibrará cargas en el tráfico destinado a cualquier subred de 172.30.0.0. Esto significa que R1 obtendrá la mitad del tráfico y R3 obtendrá la otra mitad del tráfico, independientemente de si el destino del tráfico es una de sus LAN o no.

En el Capítulo 7, "RIPv2," verá una versión de esta topología. Se la utilizará para mostrar la diferencia entre enrutamiento con clase y sin clase.



```
R1(config)#router rip
R1(config-router)#network 172.30.0.0
R1(config-router)#network 209.165.200.0
```

```
R2(config)#router rip
R2(config-router)#network 172.30.0.0
R2(config-router)#network 209.165.200.0
```

```
R3(config)#router rip
R3(config-router)#network 172.30.0.0
R3(config-router)#network 209.165.200.0
```

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 209.165.200.230, 00:00:26, Serial0/0/0
     172.30.0.0/24 is subnetted, 3 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, FastEthernet0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
R       209.165.200.232 [120/1] via 209.165.200.230, 00:00:26, Serial0/0/0
```

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
R    172.30.0.0/16 [120/1] via 209.165.200.234, 00:00:14, Serial0/0/1
                   [120/1] via 209.165.200.229, 00:00:19, Serial0/0/0
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.228 is directly connected, Serial0/0/0
C       209.165.200.232 is directly connected, Serial0/0/1
```

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    10.0.0.0/8 [120/1] via 209.165.200.233, 00:00:24, Serial0/0/1
     172.30.0.0/24 is subnetted, 3 subnets
C       172.30.100.0 is directly connected, FastEthernet0/0
C       172.30.200.0 is directly connected, FastEthernet0/1
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.228 [120/1] via 209.165.200.233, 00:00:24, Serial0/0/1
C       209.165.200.232 is directly connected, Serial0/0/1
```

## 5.5 RUTA POR DEFECTO Y RIPv1.-

### 5.5.1 TOPOLOGIA MODIFICADA: ESCENARIO C.-

**Agregar acceso a Internet a la topología**

RIP fue el primer protocolo de enrutamiento dinámico y se utilizó ampliamente en las implementaciones iniciales entre clientes e ISP, así como entre diferentes ISP. Sin embargo, en las redes actuales, los clientes no necesariamente tienen que intercambiar actualizaciones de enrutamiento con sus ISP. Los routers de clientes que se conectan a un ISP no necesitan una lista para cada ruta en Internet. En su lugar, estos routers tienen una ruta por defecto que envía todo el tráfico al router ISP cuando el router del cliente no tiene una ruta a un destino. El ISP configura una ruta estática que apunta al router del cliente en busca de direcciones dentro de la red del cliente.

En el escenario C, R3 es el proveedor de servicios con acceso a Internet, como lo indica la nube. R3 y R2 no intercambian actualizaciones de RIP. En su lugar, R2 utiliza una ruta por defecto para alcanzar la LAN de R3 y todos los demás destinos que no están enumerados en su tabla de enrutamiento. R3 utiliza una ruta estática de resumen para alcanzar las subredes 172.30.1.0, 172.30.2.0 y 172.30.3.0.

Para preparar la topología, podemos dejar el direccionamiento en su lugar; es el mismo que se utilizó en el Escenario B. Sin embargo, también necesitamos completar los siguientes pasos:

**Haga clic en Configuración RIP en la figura.**

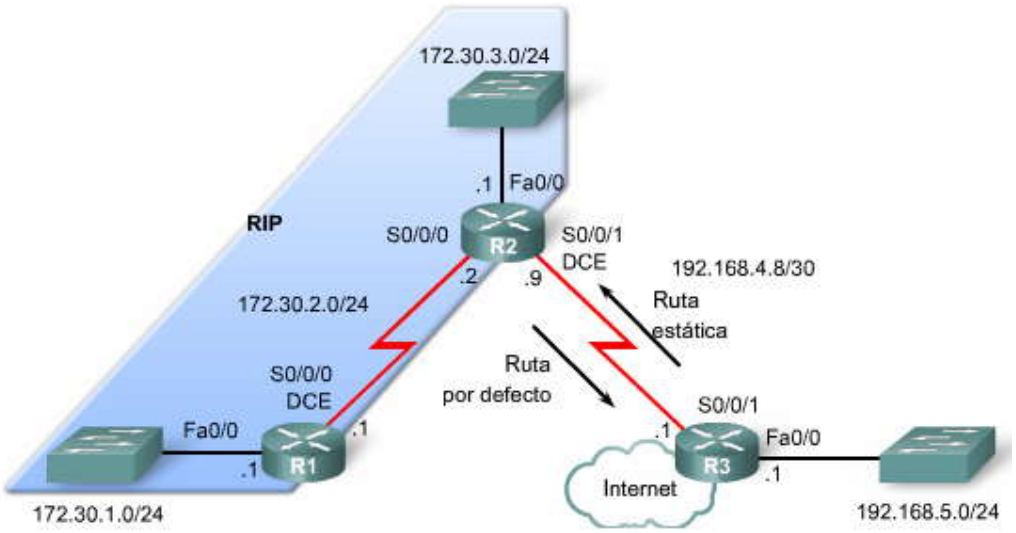
1. Desactive el enrutamiento RIP para la red 192.168.4.0 en R2.

2. Configure R2 con una ruta estática por defecto para enviar el tráfico predeterminado a R3.

3. Desactive completamente el enrutamiento RIP en R3.

4. Configure R3 con una ruta estática a las subredes 172.30.0.0.

**Haga clic en la ficha show ip route en la figura del router correspondiente para ver el resultado.**




## Configuración de RIP

- Inhabilite el enrutamiento RIP en R2 sólo para la red 192.168.4.0.
- Configure el R2 con una ruta por defecto dirigida hacia R3.

```
R2(config)#router rip
R2(config-router)#no network 192.168.4.0
R2(config-router)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 serial 0/0/1
```

- Inhabilite completamente el enrutamiento RIP en R3.
- Configure el R3 con una ruta estática dirigida hacia R2.

```
R3(config)#no router rip
R3(config)#ip route 172.30.0.0 255.255.252.0 serial 0/0/1
```

## R1 show ip route

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/24 is subnetted, 3 subnets
C       172.30.1.0 is directly connected, FastEthernet0/0
C       172.30.2.0 is directly connected, Serial0/0/0
R       172.30.3.0 [120/1] via 172.30.2.2, 00:00:05, Serial0/0/0
```

R2 show ip route

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.30.0.0/24 is subnetted, 3 subnets
R       172.30.1.0 [120/1] via 172.30.2.1, 00:00:03, Serial0/0/0
C       172.30.2.0 is directly connected, Serial0/0/0
C       172.30.3.0 is directly connected, FastEthernet0/0
     192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

R3 show ip route

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/22 is subnetted, 1 subnets
S       172.30.0.0 is directly connected, Serial0/0/1
     192.168.4.0/30 is subnetted, 1 subnets
C       192.168.4.8 is directly connected, Serial0/0/1
C    192.168.5.0/24 is directly connected, FastEthernet0/0
```

### 5.5.2 PROPAGACION DE LA RUTA POR DEFECTO EN RIPv1.-

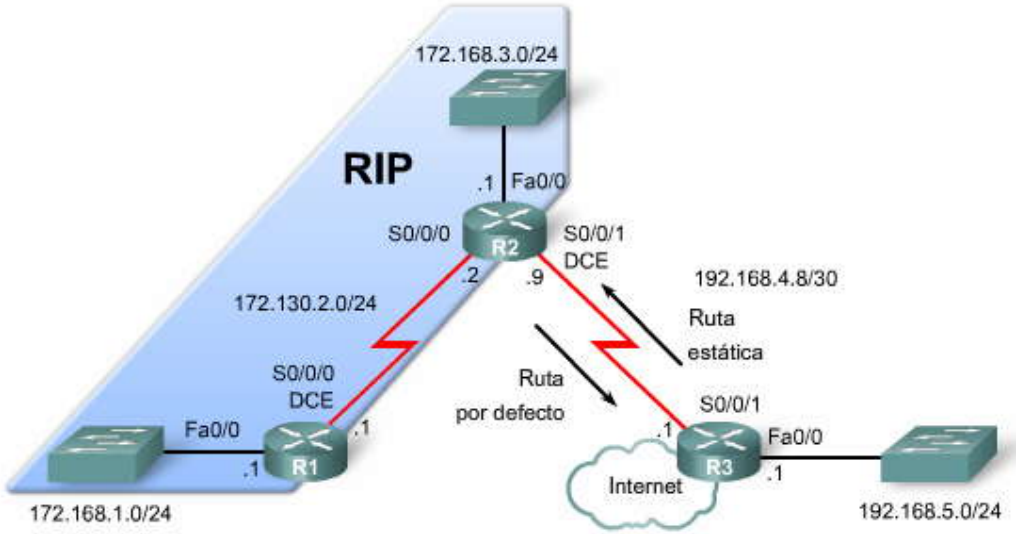
Para brindar conectividad a Internet a todas las demás redes del dominio de enrutamiento RIP, la ruta estática por defecto debe publicarse a todos los demás routers que utilizan el protocolo de enrutamiento dinámico. Podría con figurar una ruta estática por defecto en R1 apuntando a R2, pero dicha técnica no es escalable. Cada vez que agregue un router al dominio de enrutamiento RIP, tendría que configurar otra ruta estática por defecto. ¿Por qué no dejar que el protocolo de enru tamiento haga el trabajo por usted?

En varios protocolos de enrutamiento, incluido RIP, usted puede utilizar el comando default -information originate en el modo de configuración de router para especificar que este router originará la información predeterm inada, al propagar la ruta estática por defecto en las actualizaciones RIP. En la figura, R2 se configuró con el comando default -information originate. Observe a partir del resultado de debug ip rip que éste ahora envía una ruta estática por defecto "quad -zero" a R1.

Haga clic en show ip route en la figura.

En la tabla de enrutamiento para R1, podrá ver que hay una ruta candidata por defecto, como se indica a través del código R*. La ruta estática por defecto en R2 se propagó hacia R1 en una actualización RIP. R1 tiene conectividad a la LAN en R3 y a cualquier destino en Internet.

Propagación de una ruta por defecto con `default-information originate`




Propagación de una ruta por defecto con `default-information originate`

```
R2(config)#router rip
R2(config-router)#default-information originate
R2(config-router)#end
R2#debug ip rip
RIP protocol debugging is on
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (172.30.2.2)
RIP: build update entries
           subnet 0.0.0.0 metric 1
           subnet 172.30.3.0 metric 2
R2#undebug all
All possible debugging has been turned off
```

R2 ahora envía una ruta "quad-zero" hacia R1.

`show ip route`

Propagación de una ruta por defecto con `default-information originate`

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B- BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.30.2.2 to network 0.0.0.0

   172.30.0.0/24 is subnetted, 3 subnets
C  172.30.2.0 is directly connected, Serial0/0/0
R  172.30.3.0 [120/1] via 172.30.2.2 00:00:16, Serial0/0/0
C  172.30.1.0 is directly connected, Fast Ethernet0/0
R* 0.0.0.0/0 [120/1] via 172.30.2.2, 00:00:16, Serial0/0/0
```

R1 posee un "gateway de último recurso", una ruta candidata por defecto.

# CAPITULO VI – "VLSM Y CIDR"

## 6.0 INTRODUCCION DEL CAPITULO.-

### 6.0.1 INTRODUCCIÓN DEL CAPITULO.-

Antes de 1981, las direcciones IP usaban sólo los primeros 8 bits para especificar la porción de red de la dirección, lo que limitaba Internet, entonces conocida como ARPANET, a 256 redes. Pronto fue evidente que este espacio de dirección no iba a ser suficiente.

En 1981, la RFC 791 modificó la dirección IPv4 de 32 bits para permitir tres clases o tamaños distintos de redes: clase A, clase B y clase C. Las direcciones de clase A usaban 8 bits para la porción de red de la dirección, las de clase B usaban 16 bits y las de clase C usaban 24 bits. Este formato se hizo conocido como direccionamiento IP con clase.

El desarrollo inicial del direccionamiento con clase resolvió el problema de límite de 256 redes, por un tiempo. Una década más tarde, fue evidente que el espacio de dirección IP se estaba reduciendo rápidamente. En respuesta, el Grupo de trabajo de ingeniería de Internet (IETF) introdujo Classless Inter-domain Routing (CIDR), que utilizaba una máscara de subred de longitud variable (VLSM) para ayudar a conservar el espacio de dirección.

Con la introducción de CIDR y VLSM, los ISP ahora podían asignar una parte de una red con clase a un cliente y otra parte diferente a otro cliente. Esta asignación no contigua de direcciones de los ISP era análoga al desarrollo de los protocolos de enrutamiento sin clase. Para comparar: los protocolos de enrutamiento con clase siempre resumen el borde con clase y no incluyen la máscara de subred en actualizaciones de enrutamiento. Los protocolos de enrutamiento sin clase sí incluyen la máscara de subred en las actualizaciones de enrutamiento y no deben realizar el resumen. Los protocolos de enrutamiento sin clase que se discuten en este curso son los RIPv2, EIGRP y OSPF.

Con la introducción de VLSM y CIDR, los administradores de red tuvieron que usar habilidades relacionadas con la división en subredes adicionales. VLSM simplemente subdivide una subred. Las subredes, a su vez, se pueden dividir en subredes en varios niveles, como aprenderá en este capítulo. Además de la división en subredes, se hizo posible resumir una gran colección de redes con clase en una ruta agregada o superred. En este capítulo, también revisará las habilidades relacionadas con el resumen de ruta.

**En este capítulo, aprenderá a:**

- Comparar y contrastar direccionamientos IP con y sin clase.
- Repasar la VLSM y explicar los beneficios del direccionamiento IP sin clase.
- Describir la función del estándar Classless Inter-Domain Routing (CIDR) para hacer que el uso de direcciones IPv4 escasas sea más eficiente.

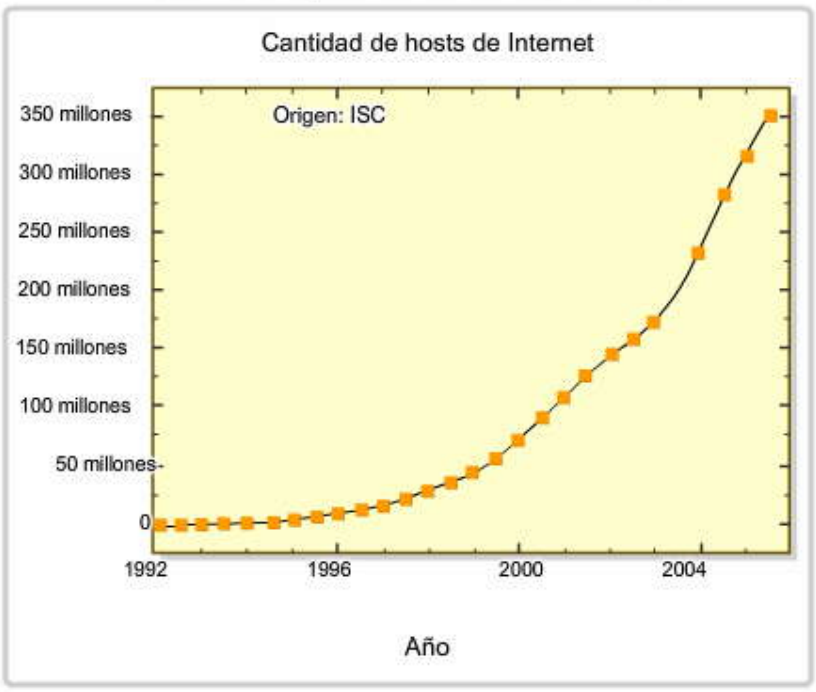
## 6.1 DIRECCIONAMIENTO CON CLASE Y SIN CLASE.-

### 6.1.1 DIRECCIONAMIENTO IP CON CLASE.-

Cuando en 1969 se puso en funcionamiento ARPANET, nadie imaginó que Internet superaría de tal forma los humildes comienzos de este proyecto de investigación. En el año 1989, ARPANET se había transformado en lo que hoy conocemos como Internet. En la siguiente década, la cantidad de hosts de Internet creció de manera exponencial, de 159 000, en octubre de 1989, a más de 72 millones a fines del milenio. A partir de enero de 2007, había más de 433 millones de hosts en Internet.

Sin la introducción de la notación CIDR y VLSM en 1993 (RFC 1519), la traducción de direcciones de nombre (NAT) en 1994 (RFC 1631) y el direccionamiento privado en 1996 (RFC 1918), el espacio de dirección IPv4 de 32 bits estaría agotado.

Crecimiento exponencial de los hosts en Internet




**Bits de orden superior**

Inicialmente, las direcciones IPv4 se asignaban en función de la clase. En la especificación original de IPv4 (RFC 791) que se lanzó en 1981, los autores establecieron las clases para ofrecer tres tamaños distintos de redes para organizaciones grandes, medianas y pequeñas. Por ende, se definieron las direcciones de clase A, B y C con un formato específico para los bits de orden superior. Los bits de orden superior son los bits que se encuentran más a la izquierda en una dirección de 32 bits.

Como se muestra en la figura:

- Las direcciones de clase A empiezan con un bit 0. Por lo tanto, todas las direcciones de 0.0.0.0 a 127.255.255.255 pertenecen a la clase A. La dirección 0.0.0.0 se reserva para el enrutamiento predeterminado y la dirección 127.0.0.0 se reserva para la prueba de loopback.
- Las direcciones de clase B empiezan con un bit 1 y un bit 0. Por lo tanto, todas las direcciones de 128.0.0.0 a 191.255.255.255 pertenecen a la clase B.
- Las direcciones de clase C empiezan con dos bits 1 y un bit 0. Las direcciones de clase C comprenden de 192.0.0.0 a 223.255.255.255.

Las direcciones restantes se reservaron para multicasting y futuros usos. Las direcciones multicast empiezan con tres bits 1 y un bit 0. Las direcciones multicast se usan para identificar un grupo de hosts que son parte de un grupo multicast. Esto ayuda a reducir la cantidad de procesamientos de paquetes que realizan los hosts, especialmente en los medios de broadcast. En este curso, verá que los protocolos de enrutamiento RIPv2, EIGRP y OSPF usan direcciones multicast designadas.

Las direcciones IP que empiezan con cuatro bits 1 se han reservado para uso futuro.

Bits de alto nivel

| Clase | Bits de alto nivel | Inicio | Final |
|---|---|---|---|
| Clase A | 0 | 0.0.0.0 | 127.255.255.255 |
| Clase B | 10 | 128.0.0.0 | 191.255.255.255 |
| Clase C | 110 | 192.0.0.0 | 223.255.255.255 |
| Multicast | 1110 | 224.0.0.0 | 239.255.255.255 |
| Experimental | 1111 | 240.0.0.0 | 255.255.255.255 |

**Estructura del direccionamiento con clase IPv4**

Las designaciones de los bits de red y de los bits de host se establecieron en la RFC 790 (publicada con la RFC 791). Como se muestra en la figura, las redes de clase A usaban el primer octeto para la asignación de red, que se traducía a una máscara de subred con clase 255.0.0.0. Debido a que sólo se dejaron 7 bits en el primer octeto (recuerde que el primer bit es siempre 0), esto dio como resultado 2 a la 7ma potencia o bien 128 redes.

Con 24 bits en la porción de host, cada dirección de clase A tenía capacidad para más de 16 millones de direcciones host individuales. Antes de CIDR y VLSM, a las organizaciones se les asignaba una dirección de red con clase completa. ¿Qué iba a hacer una organización con 16 millones de direcciones? Ahora puede entender el enorme desperdicio de espacio de direcciones que se produjo durante los comienzos de Internet, cuando las empresas recibían direcciones de clase A. Algunas empresas y organizaciones gubernamentales aún tienen direcciones de clase A. Por ejemplo, General Electric posee 3.0.0.0/8, Apple Computer posee 17.0.0.0/8 y el Servicio Postal de los Estados Unidos posee 56.0.0.0/8. (Consulte el enlace "Internet Protocol v4 Address Space" [Espacio de dirección del Protocolo de Internet v4] que figura a continuación para ver una lista de todas las asignaciones de IANA.)

La clase B no era mucho mejor. La RFC 790 especificaba los primeros dos octetos como red. Con los primeros dos bits ya establecidos en 1 y 0, quedaban 14 bits en los primeros dos octetos para asignar redes, lo que produjo 16 384 direcciones de red de clase B. Debido a que cada dirección de red de clase B contenía 16 bits en la porción de host, controlaba 65 534 direcciones. (Recuerde que se reservaban 2 direcciones para las direcciones de red y de broadcast). Sólo las organizaciones más grandes y los gobiernos podían llegar a usar alguna vez las 65 000 direcciones. Como en la clase A, el espacio de dirección de clase B se desperdiciaba.

Para empeorar la situación, ¡las direcciones de clase C generalmente eran muy pequeñas! La RFC 790 especificaba los primeros tres octetos como red. Con los primeros tres bits establecidos en 1 y 1, y 0, quedaban 21 bits para asignar redes para más de 2 millones de redes de clase C. Pero cada red de clase C sólo tenía 8 bits en la porción de host o 254 direcciones host posibles.

Máscara de subred basada en la clase

| | 1.er octeto | 2.º octeto | 3.er octeto | 4.º octeto | Máscara de subred |
|---|---|---|---|---|---|
| Clase A | Red | Host | Host | Host | 255.0.0.0 o /8 |
| Clase B | Red | Red | Host | Host | 255.255.0.0 o /16 |
| Clase C | Red | Red | Red | Host | 255.255.255.0 o /24 |

Cantidad de redes y hosts por red para cada clase

| Clase de dirección | Rango del primer octeto | Cantidad de redes posibles | Cantidad de hosts por red |
|---|---|---|---|
| Clase A | 0 a 127 | 128 (2 están reservados) | 16,777,214 |
| Clase B | 128 a 191 | 16,384 | 65,534 |
| Clase C | 192 a 223 | 2,097,152 | 254 |

### 6.1.2 PROTOCOLO DE ENTURAMIENTO CON CLASE.-

**Ejemplo de protocolos de enrutamiento con clase**

Usar direcciones IP con clase significaba que la máscara de subred podía determinarse con el valor del primer octeto, o más precisamente, con los primeros tres bits de la dirección. Los protocolos de enrutamiento, como RIPv1 sólo necesitaban propagar la dirección de red de las rutas conocidas y no necesitaban incluir la máscara de subred en la actualización de enrutamiento. Esto se debe a que el router que recibía la actualización de enrutamiento podía determinar la máscara de

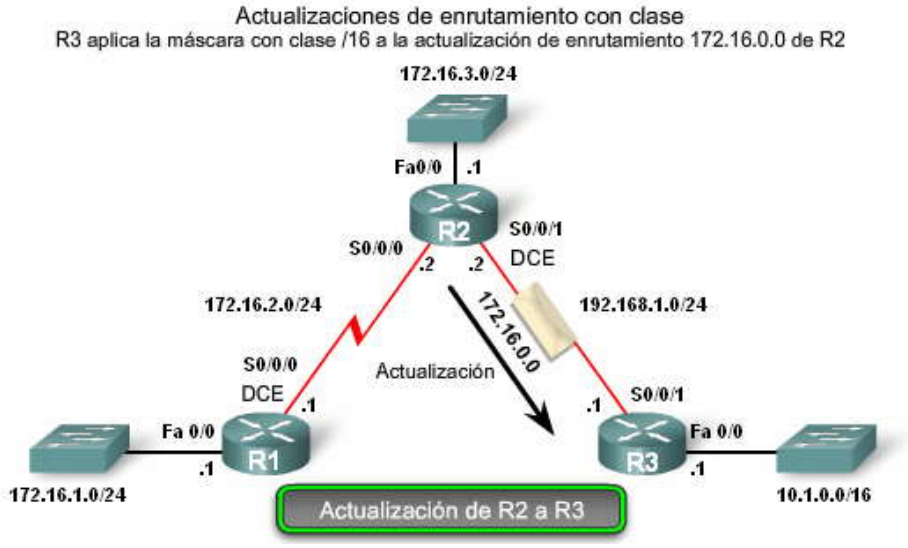
subred simplemente examinando el valor del primer octeto de la dirección de red o aplicando su máscara de subred de ingreso para las rutas divididas en subredes. La máscara de subred estaba directamente relacionada con la dirección de red.

**Haga clic en Actualización de R1 a R2 en la figura.**

En el ejemplo, R1 sabe que la subred 172.16.1.0 pertenece a la misma red principal con clase que la interfaz saliente. Por lo tanto, le envía una actualización RIP a R2 que contiene la subred 172.16.1.0. Cuando R2 recibe la actualización, aplica la máscara de subred de la interfaz de recepción (/24) a la actualización y agrega 172.16.1.0 a la tab la de enrutamiento.

**Haga clic en Actualización de R2 a R3 en la figura.**

Cuando se envían actualizaciones a R3, R2 resume las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24 en la red principal con clase 172.16.0.0. Debido a que R3 no tiene ninguna subred que pertenezca a 172.16.0.0, aplica la máscara con clase a la red de clase B, /16.


### 6.1.3 DIRECCIONAMIENTO IP SIN CLASE.-

**Avance hacia el direccionamiento sin clase**

En 1992, los miembros del IETF (Grupo de Trabajo de ingeniería de Internet) estaban muy preocupados por el crecimiento exponencial de Internet y la escalabilidad limitada de las tablas de enrutamiento de Internet. También estaban preocupados por el eventual agotamiento del espacio de dirección IPv4 de 32 bits. El agotamiento del espacio d e dirección de clase B se estaba produciendo tan rápidamente que en dos años no habría direcciones de clase B disponibles (RFC 1519). Este agotamiento se estaba produciendo porque cada organización que solicitaba la aprobación de espacio de dirección IP y lo obtenía, recibía una dirección de red con clase completa; ya fuera una clase B con 65 534 direcciones host o una clase C con

254 direcciones host. Una de las causas fundamentales de este problema era la falta de flexibilidad. No existía ninguna clase que sirviera a una organización de tamaño mediano que necesitara miles de direcciones IP, pero no 65 000.

En 1993, el IETF introdujo el Classless Inter-Domain Routing o CIDR (RFC 1517). CIDR permitía:

- Un uso más eficiente del espacio de dirección IPv4
- La agregación de prefijo, lo que reducía el tamaño de las tablas de enrutamiento

Para los routers compatibles con CIDR, la clase de dirección no tiene sentido. A la porción de red de la dirección la determina la máscara de subred de la red, también conocida como prefijo de red o duración de prefijo (/8, /19, etc.). La clase de dirección ya no determina la dirección de red.

Los ISP ahora podían asignar espacio de dirección de manera más eficiente usando cualquier duración de prefijo, comenzando con /8 y más grandes (/8, /9, /10, etc.). Los ISP ya no estaban limitados a una máscara de subred de /8, /16 o /24 Los bloques de direcciones IP podían asignarse a una red basándose en los requerimientos del cliente, que podían ir desde unos pocos hosts hasta cientos o miles de hosts.

**CIDR (RFC 1519) se permite para:**

- un uso más eficaz del espacio de dirección IPv4
- agregación de prefijos, que reduce el tamaño de las tablas de enrutamiento

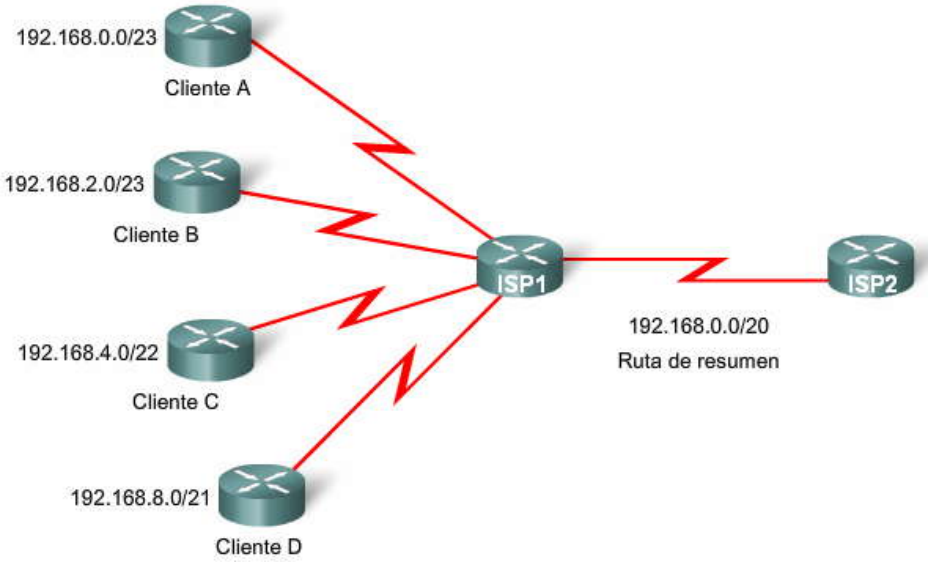
**CIDR y resumen de ruta**

CIDR usa Máscaras de subred de longitud variable (VLSM) para asignar direcciones IP a subredes de acuerdo con la necesidad individual en lugar de hacerlo por la clase. Este tipo de asignación permite que el borde de la red/del host se produzca en cualquier bit de la dirección. Las redes, a su vez, se pueden subdividir o dividir en subredes cada vez más pequeñas.

Del mismo modo que Internet estaba creciendo a un ritmo exponencial a principios de la década de 1990, el tamaño de las tablas de enrutamiento que los routers de Internet mantenían también estaba creciendo bajo el direccionamiento IP con clase. CIDR permitía la agregación de prefijo, que ya se conoce como resumen de ruta. Recuerde del Capítulo 2, "Enrutamiento estático", que se puede crear una única ruta estática para varias redes. Las tablas de enrutamiento de Internet ahora podían beneficiarse del mismo tipo de agregación de rutas. La capacidad de las rutas para ser resumidas como una sola ruta ayuda a reducir el tamaño de las tablas de enrutamiento de Internet.

En la figura, observe que ISP1 tiene cuatro clientes, cada uno con una cantidad variable de espacio de dirección IP. Sin embargo, todo el espacio de dirección de los clientes puede resumirse en una única notificación a ISP2. La ruta 192.168.0.0/20 resumida o agregada incluye todas las redes que pertenecen a los Clientes A, B, C y D. Este tipo de ruta se conoce como ruta de superred. Una superred resume varias direcciones de red con una máscara menor que la máscara con clase.

Propagar la VLSM y las rutas de superred requiere un protocolo de enrutamiento sin clase porque la máscara de subred ya no puede determinarse con el valor del primer octeto. La máscara de subred ahora necesita incluirse con la dirección de red. Los protocolos de enrutamiento sin clase incluyen la máscara de subred con la dirección de red en la actualización de enrutamiento.



### 6.1.4 PROTOCOLO DE ENRUTAMIENTO SIN CLASE.-

Los protocolos de enrutamiento sin clase incluyen RIPv2, EIGRP, OSPF, IS-IS y BGP. Estos protocolos de enrutamiento incluyen la máscara de subred con la dirección de red en sus actualizaciones de enrutamiento. Los protocolos de enrutamiento sin clase son necesarios cuando la máscara no puede suponerse ni determinarse con el valor del primer octeto.

Por ejemplo, las redes 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16 y 172.19.0.0/16 pueden resumirse como 172.16.0.0/14.

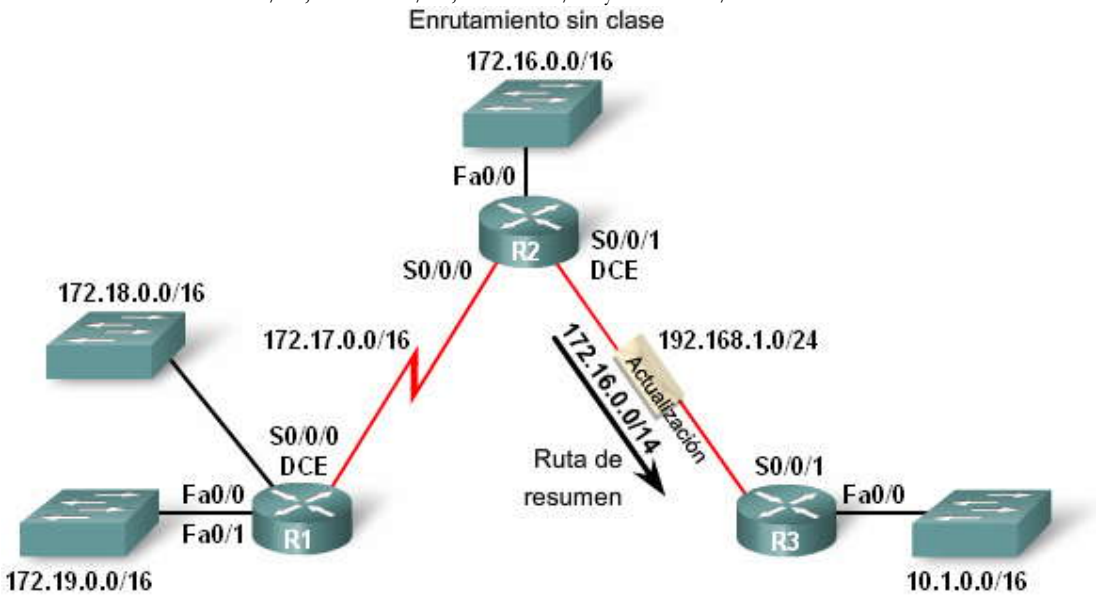
Si R2 envía la ruta resumida 172.16.0.0 sin la máscara de /14, R3 sólo sabe aplicar la máscara con clase predeterminada de /16. En un escenario de protocolos de enrutamiento con clase, R3 no tiene conocimiento de las redes 172.17.0.0/16, 172.18.0.0/16 y 172.19.0.0/16.

**Nota:** Con un protocolo de enrutamiento con clase, R2 puede enviar estas redes individuales sin resumen, pero se pierden los beneficios del resumen.

Los protocolos de enrutamiento con clase no pueden enviar rutas de superred porque el router de recepción aplicará la ruta con clase predeterminada a la dirección de red en la actualización de enrutamiento. Si nuestra topología tuviera un protocolo de enrutamiento con clase, entonces R3 sólo instalaría 172.16.0.0/16 en la tabla de enrutamiento.

**Nota:** Cuando una ruta de superred se encuentra en una tabla de enrutamiento, por ejemplo, como una ruta estática, un protocolo de enrutamiento con clase no incluirá esa ruta en sus actualizaciones.

Con un protocolo de enrutamiento sin clase, R2 publicará la red 172.16.0.0 conjuntamente con la máscara de /14 a R3. Entonces, R3 podrá instalar la ruta de superred 172.16.0.0/14 en su tabla de enrutamiento, lo que le dará la posibilidad de conexión con las redes 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16 y 172.19.0.0/16.




### 6.2 VLSM.-

### 6.2.1 VLSM EN ACCION.-

En un curso anterior, usted aprendió cómo una Máscara de subred de longitud variable (VLSM) permite usar distintas máscaras para cada subred. Después de que una dirección de red se divide en subredes, esas subredes también se pueden dividir en subredes. **Como seguramente recuerda, VLSM simplemente subdivide una subred. La VLSM puede imaginarse como la división en subredes.**

**Haga clic en Reproducir para ver la animación.**

La figura muestra la red 10.0.0.0/8 que se ha dividido en subredes usando la máscara de subred de /16, lo que produce 256 subredes.

10.0.0.0/16
10.1.0.0/16
10.2.0.0/16
.
.
.

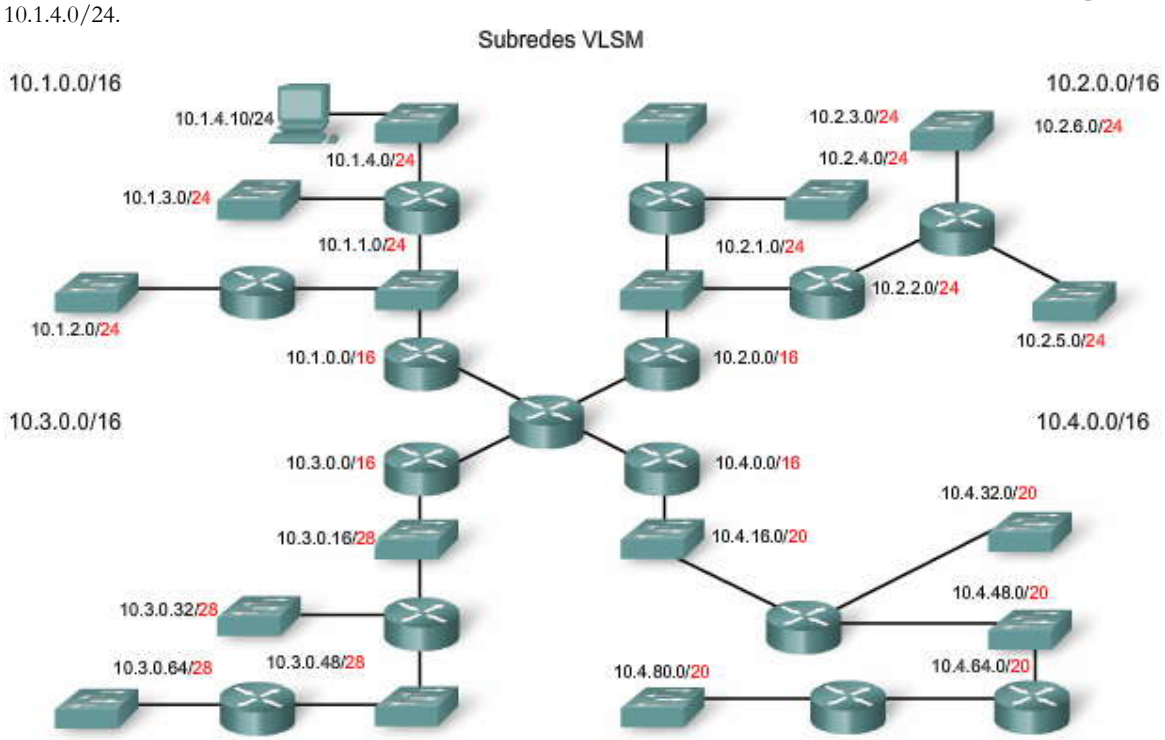
10.255.0.0/16

Cualquiera de estas subredes de /16, a su vez , se puede dividir en subredes. Por ejemplo, en la figura, la subred 10.1.0.0/16 se divide en subredes nuevamente usando la máscara de /24, lo que produce las siguientes subredes adicionales.

10.1.1.0/24
10.1.2.0/24
10.1.3.0/24
.
.
.
10.1.255.0/24

La subred 10.2.0.0/16 también se divide en subredes con una máscara de /24. La subred 10.3.0.0/16 se divide en subredes nuevamente con la máscara de /28 y la subred 10.4.0.0/16 se divide en subredes nuevamente con la máscara de /20.

Las direcciones host individuales se asignan a partir de las direcciones de "sub-subredes". Por ejemplo, la figura muestra la subred 10.1.0.0/16 dividida en subredes de /24. La dirección 10.1.4.10 sería ahora miembro de la subred más específica 10.1.4.0/24.




### 6.2.2 VLSM Y DIRECIONES IP.-

Otra forma de ver las subredes VLSM es enumerar cada subred y sus subredes. En la figura, la red 10.0.0.0/8 es el espacio de dirección inicial. Está dividido en subredes con una máscara de /16 en la primera serie de división en subredes. Usted ya sabe que al pedir prestados 8 bits (al pasar de /8 a /16) se crean 256 subredes. Con el enrutamiento con clase, eso es lo máximo que puede lograr. Sólo puede elegir una única máscara para todas sus redes. Con VLSM y enrutamiento sin clase, usted tiene más flexibilidad para crear direcciones de red adicionales y usar una máscara que se adecue a sus necesidades.

**Haga clic en 10.1.0.0/16 en la figura.**

Para la subred 10.1.0.0/16, nuevamente, se piden prestados 8 bits para crear 256 subredes con una máscara de /24. Esto permitirá que haya 254 direcciones host por subred. Las subredes comprendidas entre 10.1.0.0/24 y 10.1.255.0/24 son subredes de la subred 10.1.0.0/16.

**Haga clic en 10.2.0.0/16 en la figura.**

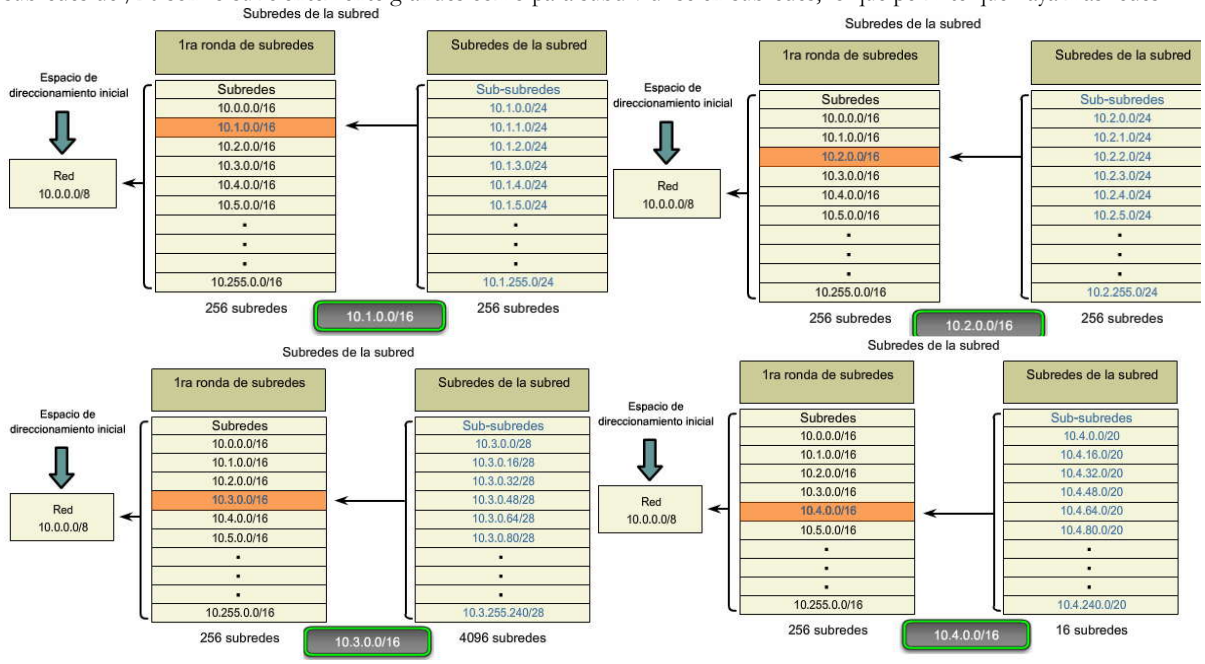
La subred 10.2.0.0/16 también se subdivide además en subredes con una máscara de /24. Las subredes comprendidas entre 10.2.0.0/24 y 10.2.255.0/24 son subredes de la subred 10.1.0.0/16.

**Haga clic en 10.3.0.0/16 en la figura.**

La subred 10.3.0.0/16 también se subdivide en subredes con una máscara de /28. Esto permitirá que haya 14 direcciones host por subred. Se piden prestados doce bits y se crean 4096 subredes que van de 10.3.0.0/28 a 10.3.255.240/28.

**Haga clic en 10.4.0.0/16 en la figura.**

La subred 10.4.0.0/16 además se subdivide en subredes con una máscara de /20. Esto permitirá que haya 2046 direcciones host por subred. Se piden prestados cuatro bits y se crean 16 subredes que van de 10.4.0.0/20 a 10.4.240.0/20. Estas subredes de /20 son lo suficientemente grandes como para subdividirse en subredes, lo que permite que haya más redes.




## 6.3 CIDR-

### 6.3.1 RESUMEN DE RUTA.-

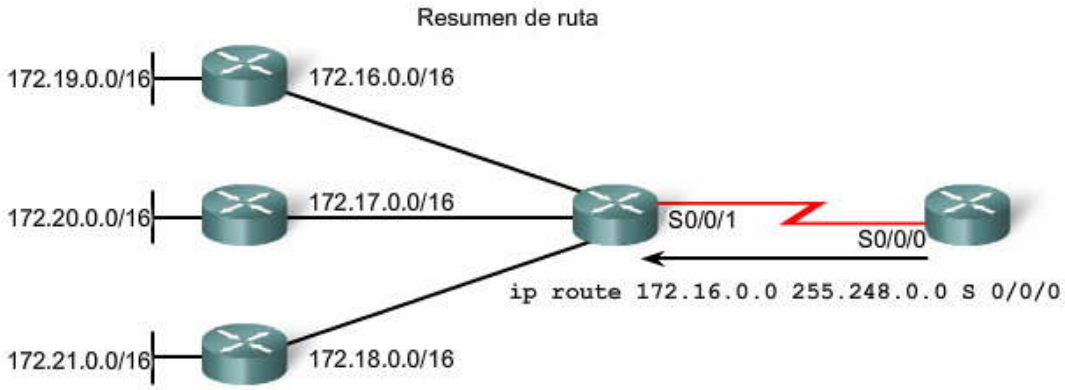
Como ha aprendido anteriormente, el resumen de ruta, también conocido como agregación de ruta, es el proceso de publicar un conjunto de direcciones contiguas como una única dirección con una máscara de subred más corta y menos específica. Recuerde que CIDR es una forma de resumen de ruta y es sinónimo del término creación de superredes.

Ya se debe haber familiarizado con el resumen de ruta que realizan los protocolos de enrutamiento con clase como RIPv1. RIPv1 resume las subredes en una única dirección con clase de red principal cuando envía la actualización de RIPv1 de una interfaz que pertenece a otra red principal. Por ejemplo, RIPv1 resumirá las subredes 10.0.0.0/24 (de 10.0.0.0/24 a 10.255.255.0/24) como 10.0.0.0/8.

CIDR ignora la limitación de los bordes con clase y permite el resumen con las máscaras que son menores que las de la máscara con clase predeterminada. Este tipo de resumen ayuda a reducir la cantidad de entradas en las actualizaciones de enrutamiento y disminuye la cantidad de entradas en las tablas de enrutamiento locales. También ayuda a reducir la utilización de ancho de banda para las actualizaciones de enrutamiento y da como resultado búsquedas de la tabla de enrutamiento más rápidas.

La figura muestra una única ruta estática con la dirección 172.16.0.0 y la máscara 255.248.0.0 que resume todas las redes con clase de 172.16.0.0/16 a 172.23.0.0/16. Si bien 172.22.0.0/16 y 172.23.0.0/16 no se muestran en el gráfico, éstas también se incluyen en la ruta resumida. Observe que la máscara de /13 (255.248.0.0) es menor que la máscara con clase predeterminada de /16 (255.255.0.0).

Nota: Debe recordar que una superred es siempre una ruta resumida, pero una ruta resumida no siempre es una superred. Es posible que un router tenga una entrada de ruta específica y una entrada de ruta resumida que cubra la misma red. Supongamos que el router X tiene una ruta específica para 172.22.0.0/16 que usa serial 0/0/1 y una ruta resumida de 172.16.0.0/14 que usa serial 0/0/0. Los paquetes con la dirección IP de 172.22.n.n coinciden con ambas entradas. Estos paquetes destinados para 172.22.0.0 se enviarían desde la interfaz serial 0/0/1 porque hay una coincidencia más específica de 16 bits, que con los 14 bits de la ruta resumida 172.16.0.0/14.




### 6.3.2 CALCULO DEL RESUMEN DE RUTA.-

El cálculo de los resúmenes de rutas y superredes es idéntico al proceso que ya aprendió en el Capítulo 2, "Enrutamiento estático". Por lo tanto, el siguiente ejemplo se presenta como revisión rápida.

El resumen de redes en una sola dirección y máscara puede realizarse en tres pasos. Observemos las siguientes cuatro redes:
172.20.0.0/16
172.21.0.0/16
172.22.0.0/16
172.23.0.0/16

**Haga clic en Paso 1 en la figura.**

El primer paso es enumerar las redes en formato binario. La figura muestra las cuatro redes en formato binario.

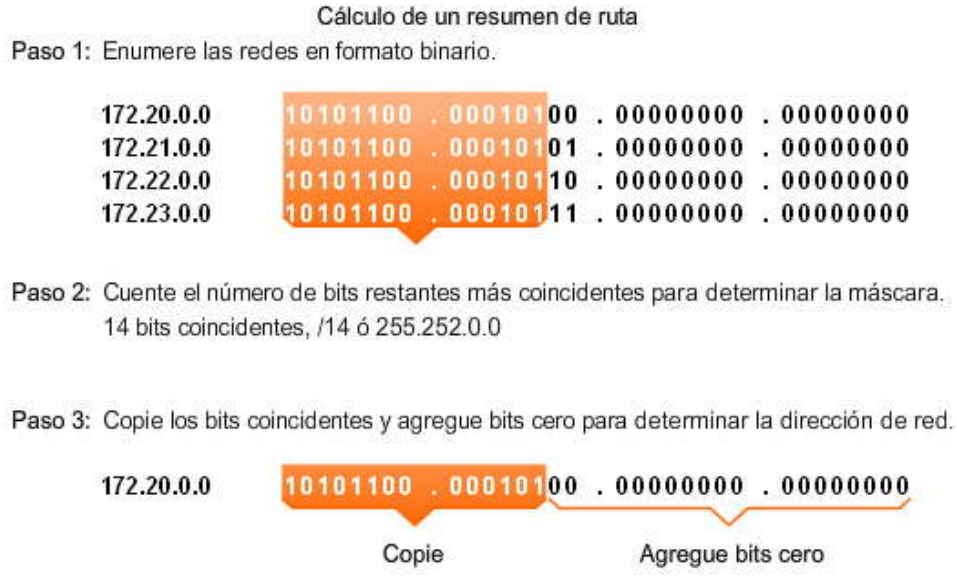
**Haga clic Paso 2 en la figura.**

El segundo paso es contar la cantidad de bits coincidentes que se encuentran más a la izquierda para determinar la máscara para la ruta resumida. Puede ver en la figura que coinciden los primeros 14 bits coincidentes que se encuentran más a la izquierda. Éste es el prefijo o máscara de subred para la ruta resumida: /14 ó 255.252.0.0.

**Haga clic en Paso 3 en la figura.**

El tercer paso es copiar los bits coincidentes y luego agregar bits cero al resto de la dirección para determinar la dirección de red resumida. La figura muestra que los bits coincidentes con ceros al final producen la dirección de red 172.20.0.0. Las cuatro redes (172.20.0.0/16, 172.21.0.0/16, 172.22.0.0/16 y 172.23.0.0/16) pueden resumirse en una única dirección de red y prefijo 172.20.0.0/14.

Las actividades de la siguiente sección le ofrecen la oportunidad de practicar el diseño y la resolución de problemas en esquemas de direccionamiento VLSM. También practicará la creación y resolución de problemas en resúmenes de ruta.



# CAPITULO VII – "RIPv2"

## 7.0 INTRODUCCION DEL CAPITULO.-

### 7.0.1 INTRODUCCIÓN DEL CAPITULO.-

La versión 2 de RIP (RIPv2) se define en RFC 1723. Éste es el primer protocolo de enrutamiento sin clase que se discute en el curso. La figura ubica a RIPv2 en su propia perspectiva con respecto a otros protocolos de enrutamiento. Si bien RIPv2 es un protocolo de enrutamiento apropiado para algunos ambientes, pierde popularidad cuando se compara con protocolos de enrutamiento tales como EIGRP, OSPF e IS-IS, que ofrecen más funciones y son más escalables.

Aunque puede ser menos popular que otros protocolos de enrutamiento, ambas versiones de RIP aún son apropiadas para algunas situaciones. Si bien RIP carece de las capacidades de muchos protocolos posteriores, su simplicidad y amplia utilización en varios sistemas operativos lo convierten en un candidato ideal para las redes homogéneas más pequeñas, donde es necesaria la compatibilidad con varios fabricantes, especialmente dentro de los ambientes UNIX.

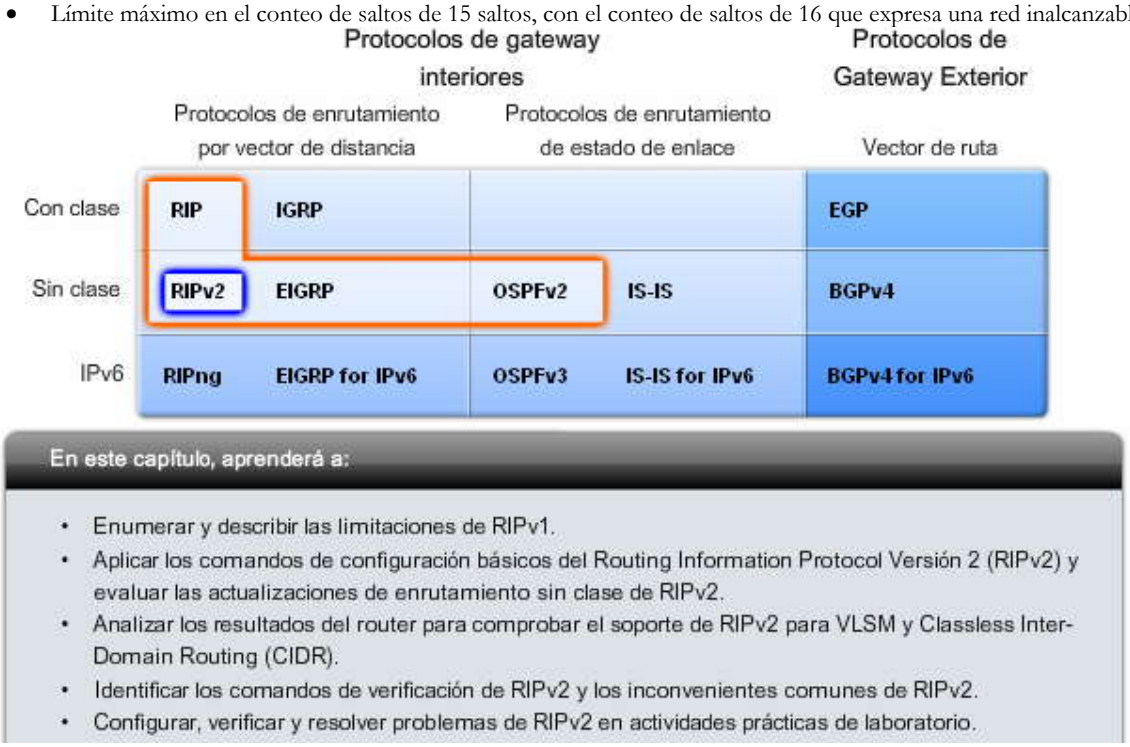
Debido a que necesitará entender RIPv2, incluso si no lo usa, este capítulo se concentrará en las diferencias entre un protocolo de enrutamiento con clase (RIPv1) y un protocolo de enrutamiento sin clase (RIPv2), más que en los detalles de RIPv2. La limitación principal de RIPv1 es que es un protocolo de enrutamiento con clase. Como usted sabe, los protocolos de enrutamiento con clase no incluyen la máscara de subred con la dirección de red en las actualizaciones de enrutamiento, lo que puede ocasionar problemas con las redes o subredes no contiguas que usan la Máscara de subred de longitud variable (VLSM). Como RIPv2 es un protocolo de enrutamiento sin clase, las máscaras de subred se incluyen en las actualizaciones de enrutamiento, lo que hace que RIPv2 sea más compatible con los ambientes de enrutamiento modernos.

En realidad, RIPv2 es una mejora de las funciones y extensiones de RIPv1, más que un protocolo completamente nuevo. Algunas de estas funciones mejoradas incluyen:

- Direcciones de siguiente salto incluidas en las actualizaciones de enrutamiento
- Uso de direcciones multicast al enviar actualizaciones
- Opción de autenticación disponible

Como RIPv1, RIPv2 es un protocolo de enrutamiento por vector de distancia. Las dos versiones de RIP tienen las siguientes funciones y limitaciones:

- Uso de temporizadores de espera y otros temporizadores para ayudar a impedir routing loops.
- Uso de horizonte dividido u horizonte dividido con envenenamiento en reversa para ayudar también a impedir routing loops.
- Uso de updates disparados cuando hay un cambio en la topología para lograr una convergencia más rápida.
- Límite máximo en el conteo de saltos de 15 saltos, con el conteo de saltos de 16 que expresa una red inalcanzable.




En este capítulo, aprenderá a:

- Enumerar y describir las limitaciones de RIPv1.
- Aplicar los comandos de configuración básicos del Routing Information Protocol Versión 2 (RIPv2) y evaluar las actualizaciones de enrutamiento sin clase de RIPv2.
- Analizar los resultados del router para comprobar el soporte de RIPv2 para VLSM y Classless Inter-Domain Routing (CIDR).
- Identificar los comandos de verificación de RIPv2 y los inconvenientes comunes de RIPv2.
- Configurar, verificar y resolver problemas de RIPv2 en actividades prácticas de laboratorio.

## 7.1 LIMITACIONES DE RIPv1.-

### 7.1.1 TOPOLOGIA DE LABORATORIO.-

La figura muestra la topología y el esquema de direccionamiento que se usa en este capítulo. Este escenario es similar al dominio de enrutamiento con tres routers que se usó al final del Capítulo 5, "RIPv1". Recuerde que los routers R1 y R3 tienen subredes que forman parte de la red principal con clase 172.30.0.0/16 (clase B). También recuerde que R1 y R3 están conectados a R2 con subredes de la red principal con clase 209.165.200.0/24 (clase C). Esta topología es no contigua y no convergerá porque 172.30.0.0/16 está dividida por 209.165.200.0/24.

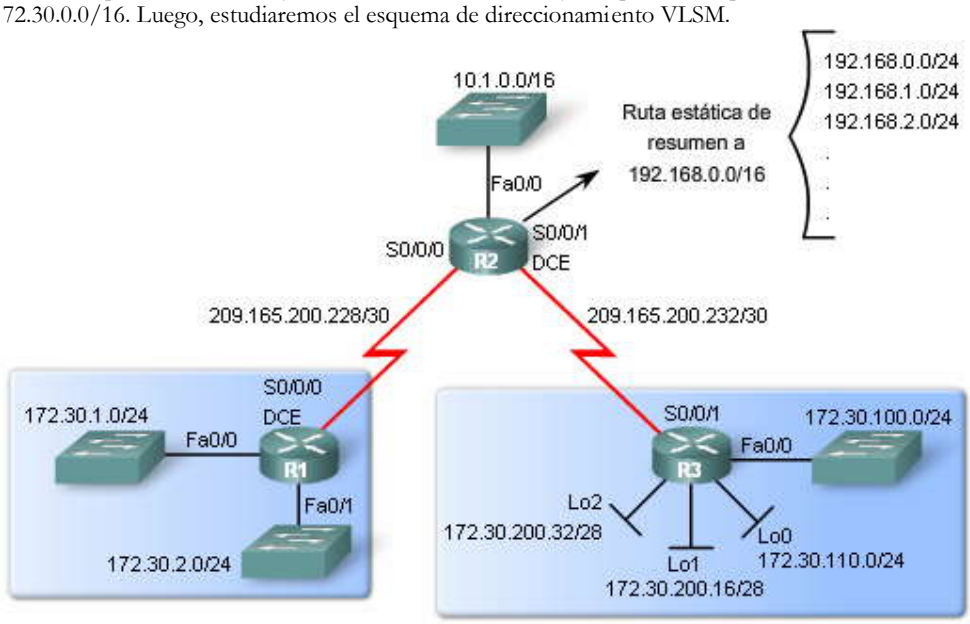
**Haga clic en R1, R2 y R3 para ver la configuración de inicio de cada router.**

**Ruta resumida**

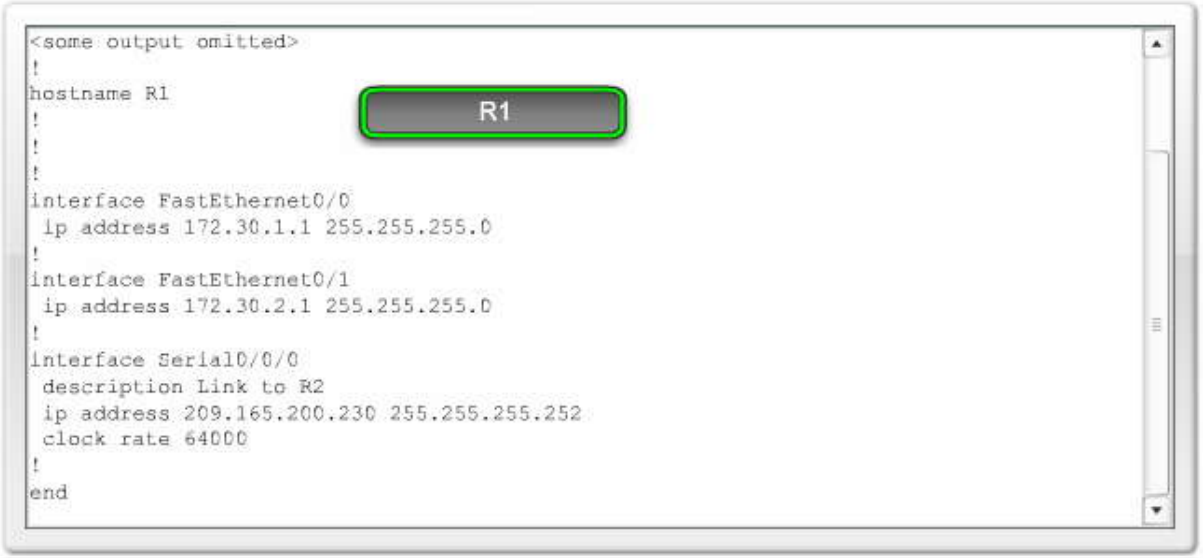
La topología muestra que R2 tiene una ruta resumida estática hacia la red 192.168.0.0/16. La configuración de esta ruta resumida se mostrará más adelante en esta sección.

El concepto y la configuración de las rutas resumidas estáticas se discutió en el Capítulo 2, "Enrutamiento estático". Podemos inyectar información de rutas estáticas en las actualizaciones de protocolo de enrutamiento . Esto se denomina redistribución y también se discutirá más adelante en esta sección. Por ahora, debe comprender que esta ruta resumida ocasionará problemas con RIPv1 porque 192.168.0.0/16 no es una dirección principal con clase e incluye todas las versio nes de /24 de 192.168.0.0/16, como se muestra en la topología.

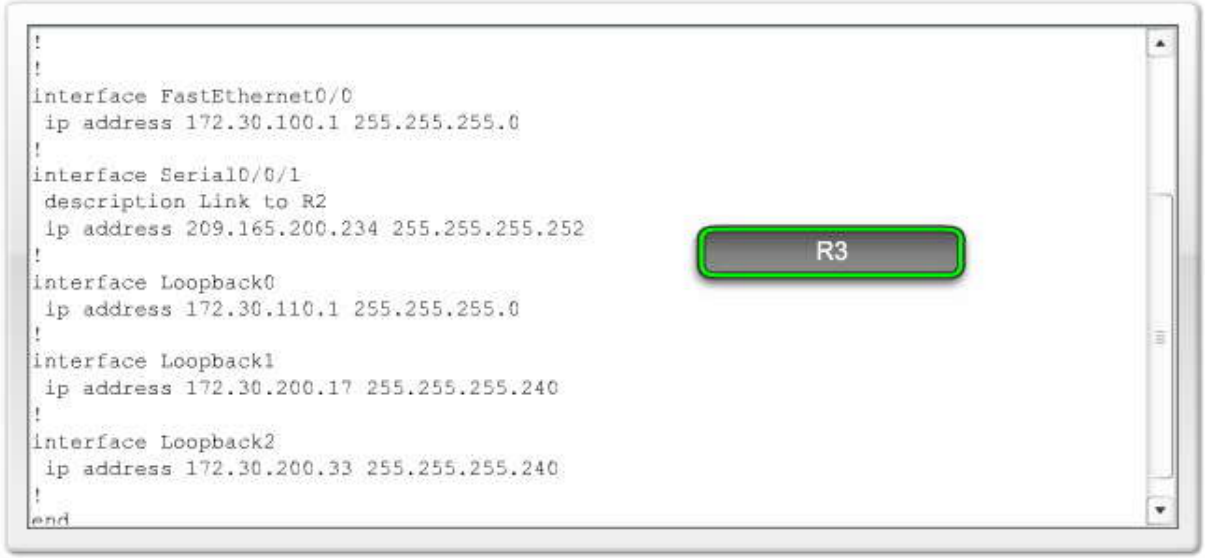
Finalmente, observe que los routers R1 y R3 contienen redes VLSM y comparten el espacio de dirección de la red principal con clase 172.30.0.0/16. Luego, estudiaremos el esquema de direccionamiento VLSM.




| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 172.30.1.1 | 255.255.255.0 |
| | Fa0/1 | 172.30.2.1 | 255.255.255.0 |
| | S0/0/0 | 209.165.200.230 | 255.255.255.252 |
| R2 | Fa0/0 | 10.1.0.1 | 255.255.0.0 |
| | S0/0/0 | 209.165.200.229 | 255.255.255.252 |
| | S0/0/1 | 209.165.200.233 | 255.255.255.252 |
| R3 | Fa0/0 | 172.30.100.1 | 255.255.255.0 |
| | Lo0 | 172.30.110.1 | 255.255.255.0 |
| | Lo1 | 172.30.200.17 | 255.255.255.240 |
| | Lo2 | 172.30.200.33 | 255.255.255.240 |
| | S0/0/1 | 209.165.200.234 | 255.255.255.252 |








**VLSM**

Revise el esquema de direccionamiento VLSM de la figura. Como se muestra en el gráfico superior, tanto R1 como R3 han dividido la red 172.30.0.0/16 en subredes de /24. Cuatro de estas subredes de /24 se asignan: dos a R1 (172.30.1.0/24 y 172.30.2.0/24) y dos a R3 (172.30.100.0/24 y 172.30.110.0/24).

En la parte inferior del gráfico, hemos tomado la subred 172.30.200.0/24 y la hemos subdividido nuevamente, usando los primeros cuatro bits para las subredes y los cuatro últimos bits para los hosts. El resultado es una máscara de 255.255.255.240 o de /28. La Subred 1 y la Subred 2 se asignan a R3. Esto significa que la subred 172.30.200.0/24 ya no puede usarse, a pesar de que las subredes de /28 restantes pueden usarse.

| Asignada a | Subred | Red | Rango de host | Broadcast |
|---|---|---|---|---|
| | 0 | 172.30.0.0 | 172.30.0.1 to 172.30.0.254 | 172.30.0.255 |
| R1 Fa0/0 | 1 | 172.30.1.0 | 172.30.1.1 to 172.30.1.254 | 172.30.1.255 |
| R1 Fa0/1 | 2 | 172.30.2.0 | 172.30.2.1 to 172.30.2.254 | 172.30.2.255 |
| | 3 | 172.30.3.0 | 172.30.3.1 to 172.30.3.254 | 172.30.3.255 |
| | 4 | 172.30.4.0 | 172.30.4.1 to 172.30.4.254 | 172.30.4.255 |
| | . | | | |
| R3 Fa0/0 | 100 | 172.30.100.0 | 172.30.100.1 to 172.30.100.254 | 172.30.100.255 |
| | . | | | |
| R3 Lo0 | 110 | 172.30.110.0 | 172.30.110.1 to 172.30.110.254 | 172.30.110.255 |
| | . | | | |
| Nuevamente dividida en | 200 | 172.30.200.0 | 172.30.200.1 to 172.30.200.254 | 172.30.200.255 |
| subredes | . | | | |
| | 255 | 172.30.255.0 | 172.30.255.1 to 172.30.255.254 | 172.30.255.255 |

256 subredes /24

| | Subred | Red | Rango de host | Broadcast |
|---|---|---|---|---|
| | 0 | 172.30.200.0 | 172.30.200.1 to 172.30.200.14 | 172.30.200.15 |
| R3 Lo1 | 1 | 172.30.200.16 | 172.30.200.17 to 172.30.200.30 | 172.30.200.31 |
| R3 Lo2 | 2 | 172.30.200.32 | 172.30.200.33 to 172.30.200.46 | 172.30.200.47 |
| | 3 | 172.30.200.48 | 172.30.200.49 to 172.30.200.62 | 172.30.200.63 |
| | . | | | |
| | 15 | 172.30.200.240 | 172.30.200.241 to 172.30.200.254 | 172.30.200.255 |

16 subredes /28

**Direcciones privadas de RFC 1918**

Usted ya se debe haber familiarizado con RFC 1918 y la lógica que existe detrás del direccionamiento privado. Todos los ejemplos del plan de estudios usan direcciones IP privadas para el ejemplo de direccionamiento interno.

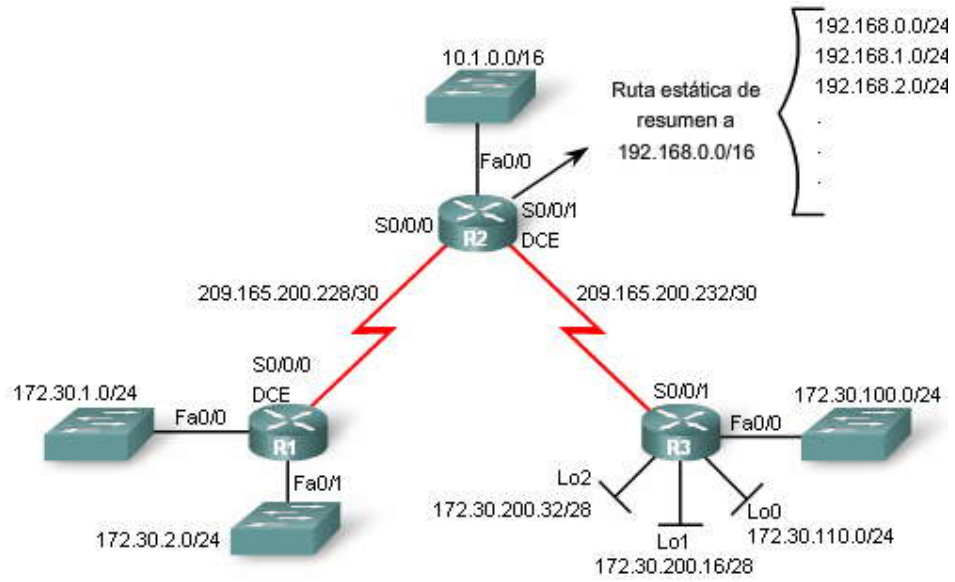
En la tabla se muestran las direcciones que cumplen con RFC 1918. Pero cuando se realiza el enrutamiento del tráfico IP por los enlaces WAN a través de un ISP o cuando los usuarios internos necesitan ingresar en sitios externos, debe usarse una dirección IP pública.

**Direcciones IP de un ejemplo de Cisco**

Usted debe haber observado que los enlaces WAN entre R1, R2 y R3 utilizan direcciones IP públicas. Si bien según la RFC 1918, estas direcciones IP no son direcciones privadas, Cisco ha adquirido un cierto espacio de direcciones públicas para usar con los ejemplos.

Las direcciones que se muestran en la figura son todas direcciones IP públicas válidas con las que se puede realizar el enrutamiento en Internet. Cisco ha reservado estas direcciones con fines educativos. Por lo tanto, este curso y los cursos futuros usarán estas direcciones cuando sea necesario utilizar direcciones públicas.

En la figura, R1, R2 y R3 se conectan usando el espacio de direcciones públicas de Cisco 209.165.200.224/27. Debido a que los enlaces WAN sólo necesitan dos direcciones, la 209.165.200.224/27 se subdivide en subredes con una máscara de /30. En la topología, la subred 1 se asigna al enlace WAN entre R1 y R2. La subred 2 se asigna al enlace WAN entre R2 y R3.




Direcciones privadas de RFC 1918

| Clase | Prefijo/Máscara | Rango de direcciones |
|---|---|---|
| A | 10.0.0.0/8 | 10.0.0.0 to 10.255.255.255 |
| B | 172.16.0.0/12 | 172.16.0.0 to 172.31.255.255 |
| C | 192.168.0.0/16 | 192.168.0.0 to 192.168.255.255 |

Utilizado para direccionamiento IP privado

Direcciones IP de ejemplo de Cisco

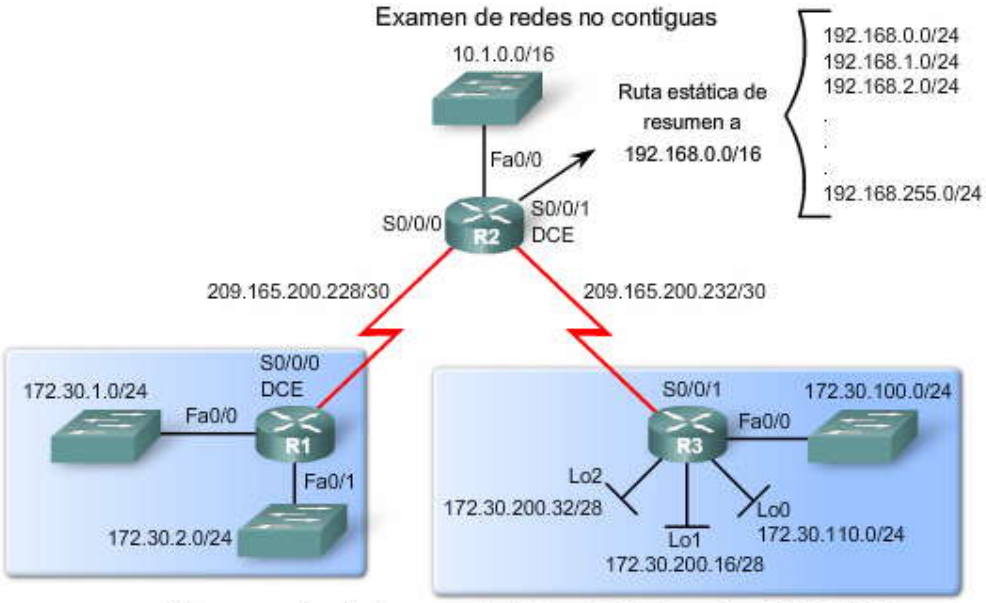
| Prefijo/Máscara | Rango de direcciones |
|---|---|
| 209.165.200.224/27 | 209.165.200.224 to 209.165.200.255 |
| 209.165.201.0/27 | 209.165.201.0 to 209.165.201.31 |
| 209.165.202.128/27 | 209.165.202.128 to 209.165.202.159 |

Utilizado para direccionamiento IP privado cuando se requiere como ejemplo.

**Interfaces loopback**

Observe que R3 utiliza interfaces loopback (Lo0, Lo1 y Lo2). Una interfaz loopback es una interfaz de software que se usa para emular una interfaz física. Como a otras interfaces, se le puede asignar una dirección IP. Otros protocolos de enrutamiento, tales como OSPF, también usan las interfaces loopback para distintos fines. Estos usos se discutirán en el Capítulo 11, OSPF.

En un ambiente de laboratorio, las interfaces loopback son útiles para crear redes adicionales sin tener que agregar más interfaces físicas al router. Se puede hacer ping en una interfaz loopback y la subred puede publicarse en las actualizaciones de enrutamiento. Por lo tanto, las interfaces loopback son ideales para simular múltiples redes conectadas al mismo router. En nuestro ejemplo, R3 no necesita cuatro interfaces LAN para realizar una demostración de múltiples subredes y VLSM. En cambio, usamos interfaces loopback.




Ambos grupos de subredes son parte de la red principal con clase 172.30.0.0/16

Examen de redes no contiguas

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 172.30.1.1 | 255.255.255.0 |
| | Fa0/1 | 172.30.2.1 | 255.255.255.0 |
| | S0/0/0 | 209.165.200.230 | 255.255.255.252 |
| R2 | Fa0/0 | 10.1.0.1 | 255.255.255.0 |
| | S0/0/0 | 209.165.200.229 | 255.255.255.252 |
| | S0/0/1 | 209.165.200.233 | 255.255.255.252 |
| R3 | Fa0/0 | 172.30.100.1 | 255.255.255.0 |
| | Lo0 | 172.30.110.1 | 255.255.255.0 |
| | Lo1 | 172.30.200.17 | 255.255.255.240 |
| | Lo2 | 172.30.200.33 | 255.255.255.240 |
| | S0/0/1 | 209.165.200.234 | 255.255.255.252 |

### 7.1.2 LIMITACIONES DE TOPOLOGIA RIPv1.-

**Rutas estáticas e interfaces nulas**

Para configurar la ruta de superred estática en R2, se usa el siguiente comando:

R2(config)#ip route 192.168.0.0 255.255.0.0 Null0

Recuerde que el resumen de ruta permite una única entrada de ruta de alto nivel para representar muchas rutas de nivel bajo y, por consiguiente, reducir el tamaño de las tablas de enrutamiento. La ruta estática de R2 usa una máscara de /16 para resumir las 256 redes comprendidas entre 192.168.0.0/24 y 192.168.255.0/24.

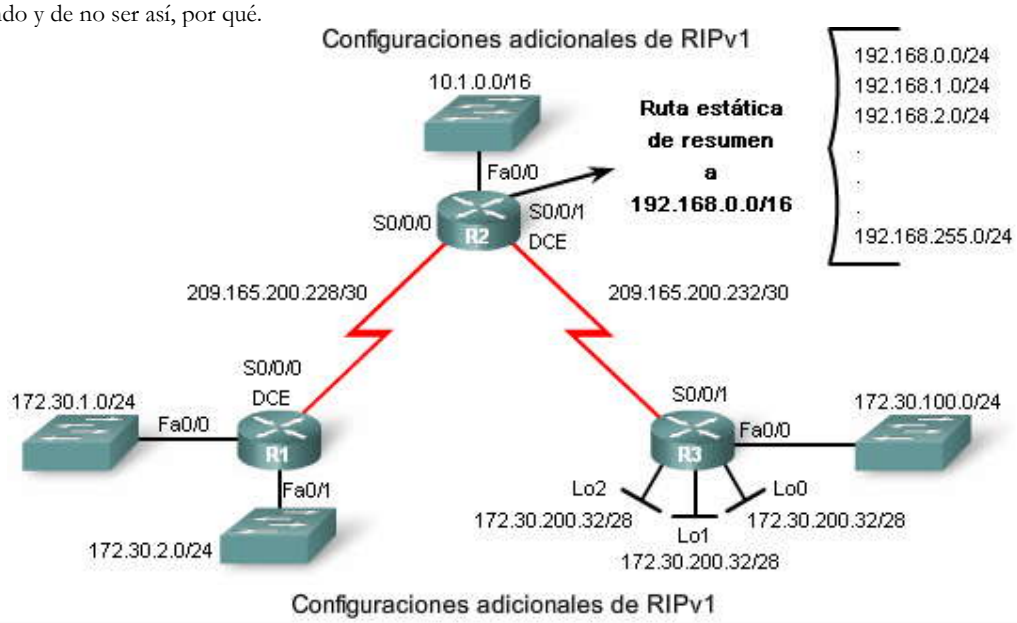
El espacio de dirección que representa la ruta resumida estática 192.168.0.0/16 en realidad no existe. Para simular esta ruta estática, usamos una interfaz nula como interfaz de salida. No es necesario que usted ingrese ningún comando para crear o configurar la interfaz nula. Siempre se encuentra activa pero no reenvía ni recibe tráfico. El tráfico que se envía a la interfaz nula se desecha. Para nuestros fines, la interfaz nula servirá de interfaz de salida de la ruta estática. Recuerde del Capítulo 2, "Enrutamiento estático", que una ruta estática debe tener una interfaz de salida activa antes de ser instalada en la tabla de enrutamiento. El uso de la interfaz nula permitirá a R2 publicar la ruta estática en RIP a pesar de que las redes que pertenecen al resumen 192.168.0.0/16 en realidad no existen.

**Redistribución de ruta**

El segundo comando que debe ingresarse es el comando redistribute static:

R2(config-router)#redistribute static

La redistribución implica tomar las rutas de una fuente de enrutamiento y enviarlas a otra fuente de enrutamiento. En nuestra topología de ejemplo, queremos que el proceso RIP en R2 redistribuya nuestra ruta estática (192.168.0.0/16) importando la ruta en RIP y luego enviándola a R1 y R3 mediante el proceso RIP. Veremos si en realidad esto está sucediendo y de no ser así, por qué.




Configuraciones adicionales de RIPv1

```
R1(config)#router rip
R1(config-router)#network 172.30.0.0
R1(config-router)#network 209.165.200.0
```

```
R2(config)#ip route 192.168.0.0 255.255.0.0 null0
R2(config)#router rip
R2(config-router)#redistribute static
R2(config-router)#network 10.0.0.0
R2(config-router)#network 209.165.200.0
```

Ruta estática configurada y redistribuida.

```
R3(config)#router rip
R3(config-router)#network 172.30.0.0
R3(config-router)#network 209.165.200.0
```

**Verificación y prueba de conectividad**

Para probar si la topología tiene conectividad completa, primero verificamos que los dos enlaces seriales de R2 estén activos usando el comando show ip interface brief como se muestra en la figura para los enlaces de R2. Si un enlace está desactivado, el campo Estado o el campo Protocolo (o ambos) mostrarán down (desactivado) en el resultado del comando. Si un enlace está activado, ambos campos mostrarán up, como se muestra aquí. R2 tiene conectividad directa a R1 y R3 por los enlaces seriales.

Pero ¿puede R2 hacer ping en las LAN de R1 y R3? ¿Hay algún problema de conectividad con un protocolo de enrutamiento con clase y las subredes no contiguas de 172.30.0.0? Probemos las comunicaciones entre los routers usando ping.

**Haga clic en Pings de R2 en la figura.**

Este resultado muestra a R2 intentando hacer ping en la interfaz 172.30.1.1 de R1 y en la interfaz 172.30.100.1 de R3. Cuando R2 hace ping en cualquiera de las subredes 172.30.0.0 de R1 o R3, sólo aproximadamente el 50% de los mensajes ICMP son exitosos.

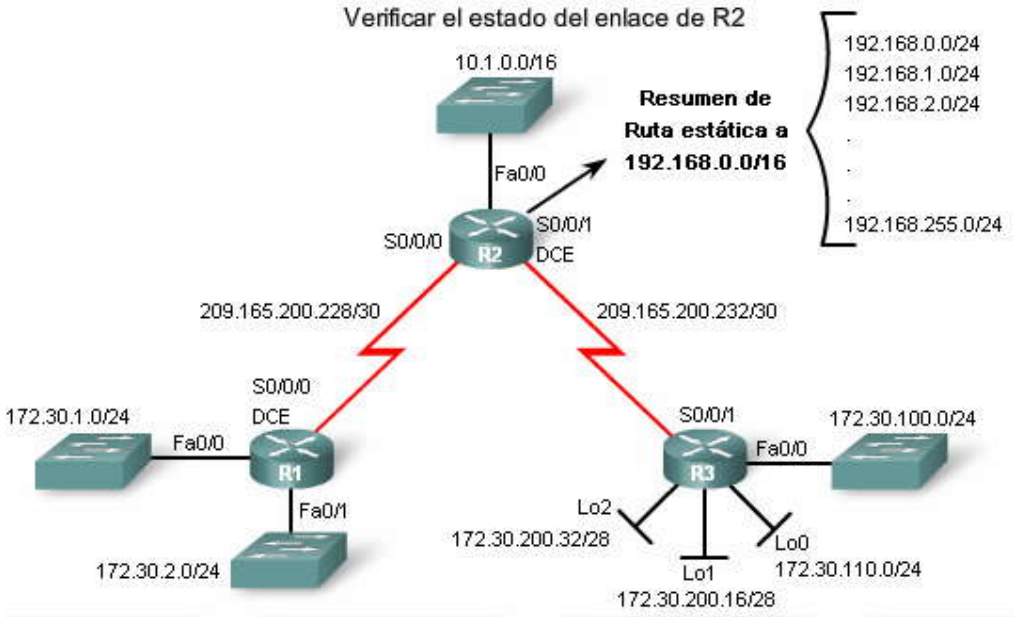
**Haga clic en Pings de R1 en la figura.**

Este resultado muestra que R1 puede hacer ping en 10.1.0.1, pero no tiene éxito cuando intenta hacer ping en la interfaz 172.30.100.1 de R3.

**Haga clic en Pings de R3 en la figura.**

Este resultado muestra que R3 puede hacer ping en 10.1.0.1, pero no tiene éxito cuando intenta hacer ping en la interfaz 172.30.1.1 de R1.

Como puede ver, hay un problema obvio cuando intenta comunicarse con las subredes no contiguas 172.30.0.0. En las siguientes secciones examinaremos las tablas de enrutamiento y actualizaciones de enrutamiento para investigar más este problema e intentar resolverlo.




Verificar el estado del enlace de R2

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        10.1.0.1        YES manual up                    up
Serial0/0/0            209.165.200.229 YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
Serial0/0/1            209.165.200.233 YES manual up                    up
```

R2 cuenta con enlaces activos a R1 y R3.

Verificar el estado del enlace de R2

```
R2#ping 172.30.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.1.1, timeout is 2 seconds:
!U!.!
Success rate is 60 percent (3/5), round-trip min/avg/max = 28/29/32 ms

R2#ping 172.30.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.100.1, timeout is 2 seconds:
!U!.!
Success rate is 60 percent (3/5), round-trip min/avg/max = 28/28/28 ms
R2#
```

Los pings de R2 a las subredes 172.30.0.0 sólo son exitosos de manera parcial.

Verificar el estado del enlace de R2

```
R1#ping 10.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R1#ping 172.30.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.100.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R1#
```

R1 no puede llegar a la red 172.30.100.0 en R3.

Verificar el estado del enlace de R2

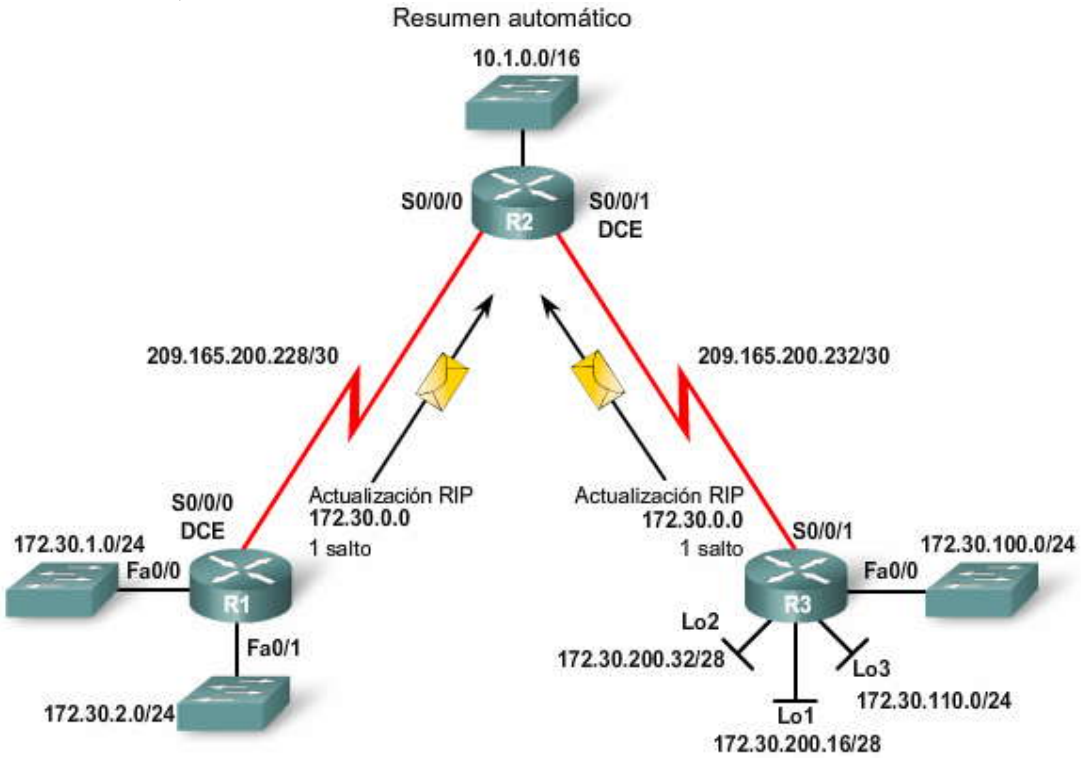
```
R3#ping 10.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms

R3#ping 172.30.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.1.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
R3#
```

R3 no puede llegar a la red 172.30.1.0 en R1.

### 7.1.3 RIPv1: REDES NO CONTIGUAS.-

Usted ya sabe que RIPv1 es un protocolo de enrutamiento con clase. Como puede ver en el formato de mensaje del RIPv1, en sus actualizaciones de enrutamiento no se incluyen las máscaras de subred. Por lo tanto, RIPv1 no puede admitir redes no contiguas, VLSM ni superredes Classless Inter-Domain Routing (CIDR). Sin embargo, ¿podría haber espacio para expandir el formato de mensaje del RIPv1 a fin de poder incluir la máscara de subred para que verdaderamente podamos tener una configuración de red no contigua? ¿Cómo cambiaría el formato de este mensaje en la figura para incluir la máscara de subred?


Debido a que la máscara de subred no está incluida en la actualización, RIPv1 y otros protocolos de enrutamiento con clase deben resumir las redes en los bordes de redes principales. Como puede ver en la figura, el RIPv1 de los routers R1 y R3 resumirá sus subredes 172.30.0.0 a la dirección con clase de red principal de 172.30.0.0 cuando envíe actualizaciones de enrutamiento a R2. Desde la perspectiva de R2, ambas actualizaciones tienen el mismo costo de 1 salto para alcanzar la red 172.30.0.0/16. Como verá, R2 instala ambas rutas en la tabla de enrutamiento.




**Examen de las tablas de enrutamiento**

Como se ha visto, R2 obtiene resultados incoherentes cuando intenta hacer ping en la dirección en una de las subredes 172.30.0.0.

**Haga clic en Rutas de R2 en la figura.**

Observe que R2 tiene dos rutas de igual costo hacia la red 172.30.0.0/16. Esto se debe a que tanto R1 como R3 están enviando a R2 una actualización RIPv1 para la red con clase 172.30.0.0/16 con una métrica de 1 salto. Como R1 y R3 resumieron automáticamente las subredes individuales, la tabla de enrutamiento de R2 sólo contiene la red principal con clase de 172.30.0.0/16.

Podemos examinar los contenidos de las actualizaciones de enrutamiento ya que las actualizaciones se envían y reciben con el comando debug ip rip.

**Haga clic en Depuración 1 de R2 en la figura.**

El resultado de este comando muestra que R2 recibe dos rutas de igual costo 172.30.0.0 con una métrica de 1 salto. R2 recibe una única ruta en Serial 0/0/0 desde R1 y otra ruta en Serial 0/0/1 desde R3. Observe que la máscara de subred no se incluye con la dirección de red en la actualización.

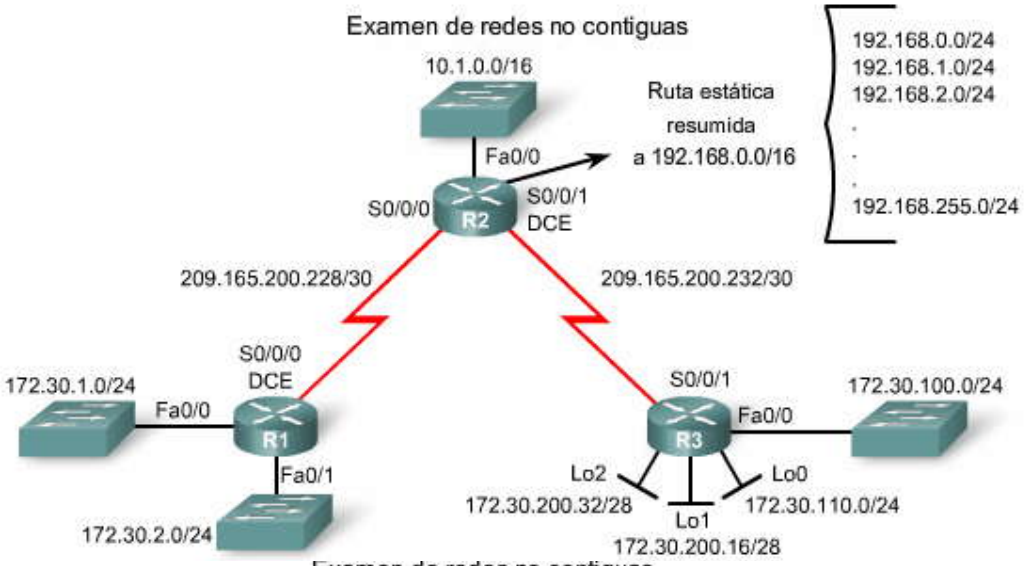
¿Qué ocurre con R1 y R3? ¿Reciben mutuamente la subred 172.30.0.0 de la otra?

**Haga clic en Rutas de R1 en la figura.**

Aquí vemos que R1 tiene sus propias rutas 172.30.0.0: 172.30.2.0/24 y 172.30.1.0/24. Pero R1 no envía esas subredes a R2. R3 tiene una tabla de enrutamiento similar. Tanto R1 como R3 son routers de borde y sólo envían la red 172.30.0.0 resumida a R2 en sus actualizaciones de enrutamiento de RIPv1. Por ende, R2 sólo conoce la red con clase 172.30.0.0/16 y no tiene conocimiento de ninguna subred 172.30.0.0.

**Haga clic en Depuración 2 de R2 en la figura.**

Observe en el resultado de debug ip rip de R2 que no incluye la red 172.30.0.0 en sus actualizaciones a R1 ni a R3. ¿Por qué no? Porque tiene vigencia la regla de horizonte dividido. R2 ha detectado a 172.30.0.0/16 en las interfaces Serial 0/0/0 y Serial 0/0/1. Debido a que R2 detectó a 172.30.0.0 en estas interfaces, no incluye esa red en las actualizaciones que envía desde estas mismas interfaces.




```
R2#ping 172.30.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.1.1, timeout is 2 seconds:
!U!.!
Success rate is 60 percent (3/5), round-trip min/avg/max = 28/29/32 ms

R2#ping 172.30.100.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.100.1, timeout is 2 seconds:
!U!.!
Success rate is 60 percent (3/5), round-trip min/avg/max = 28/28/28 ms
R2#
```

Prueba de conectividad.

Nota: Para algunos routers, será necesario deshabilitar IP CEF para visualizar los resultados como se muestran.

Examen de redes no contiguas

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:09, Serial0/0/0
                   [120/1] via 209.165.200.234, 00:00:11, Serial0/0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.232 is directly connected, Serial0/0/1
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
S    192.168.0.0/16 is directly connected, Null0
```

R2 cuenta con rutas del mismo costo a 172.30.0.0.

Examen de redes no contiguas

```
R2#debug ip rip
RIP protocol debugging is on

RIP: received v1 update from 209.165.200.230 on Serial0/0/0
     172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
     172.30.0.0 in 1 hops
R2#
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (209.165.200.229)
RIP: build update entries
        network 10.0.0.0 metric 1
        subnet 209.165.200.232 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/0/1 (209.165.200.233)
RIP: build update entries
        network 10.0.0.0 metric 1
        subnet 209.165.200.228 metric 1
R2#
```

Ruta 172.30.0.0 desde R1 y R3.

Examen de redes no contiguas

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/24 is subnetted, 2 subnets
C       172.30.2.0 is directly connected, Loopback0
C       172.30.1.0 is directly connected, FastEthernet0/0
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:16, Serial0/0/0
C       209.165.200.228 is directly connected, Serial0/0/0
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:16, Serial0/0/0
R1#
```

R1 sólo cuenta con rutas a las subredes 172.30.0.0 locales.

Examen de redes no contiguas

```
R2#debug ip rip
RIP protocol debugging is on

RIP: received v1 update from 209.165.200.230 on Serial0/0/0
     172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
     172.30.0.0 in 1 hops
R2#
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (209.165.200.229)
RIP: build update entries
        network 10.0.0.0 metric 1
        subnet 209.165.200.232 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/0/1 (209.165.200.233)
RIP: build update entries
        network 10.0.0.0 metric 1
        subnet 209.165.200.228 metric 1
R2#
```

R2 no notifica a 172.30.0.0 a R1 ni a R3.

### 7.1.4 RIPv1: INCOMPATIBILIDAD CON VLSM.-

Debido a que RIPv1 no envía la máscara de subred en las actualizaciones de enrutamiento, no puede admitir VLSM. El router R3 está configurado con las subredes VLSM, que son miembros de la red clase B 172.30.0.0/16:

- 172.30.100.0/24 (FastEthernet 0/0)
- 172.30.110.0/24 (Loopback 0)
- 172.30.200.16/28 (Loopback 1)
- 172.30.200.32/28 (Loopback 2)

Como vimos con las actualizaciones 172.30.0.0/16 a R2 de R1 y R3, RIPv1 resume las subredes hacia el borde con clase o usa la máscara de subred de la interfaz saliente para determinar qué subredes publicar.

**Haga clic en Topología en la figura.**

Para demostrar de qué manera RIPv1 usa la máscara de subred de la interfaz saliente, R4 se agrega a la topología conectada a R3 a través de la interfaz FastEthernet0/0 en la red 172.30.100.0/24.

Haga clic en Resultado del router en la figura.

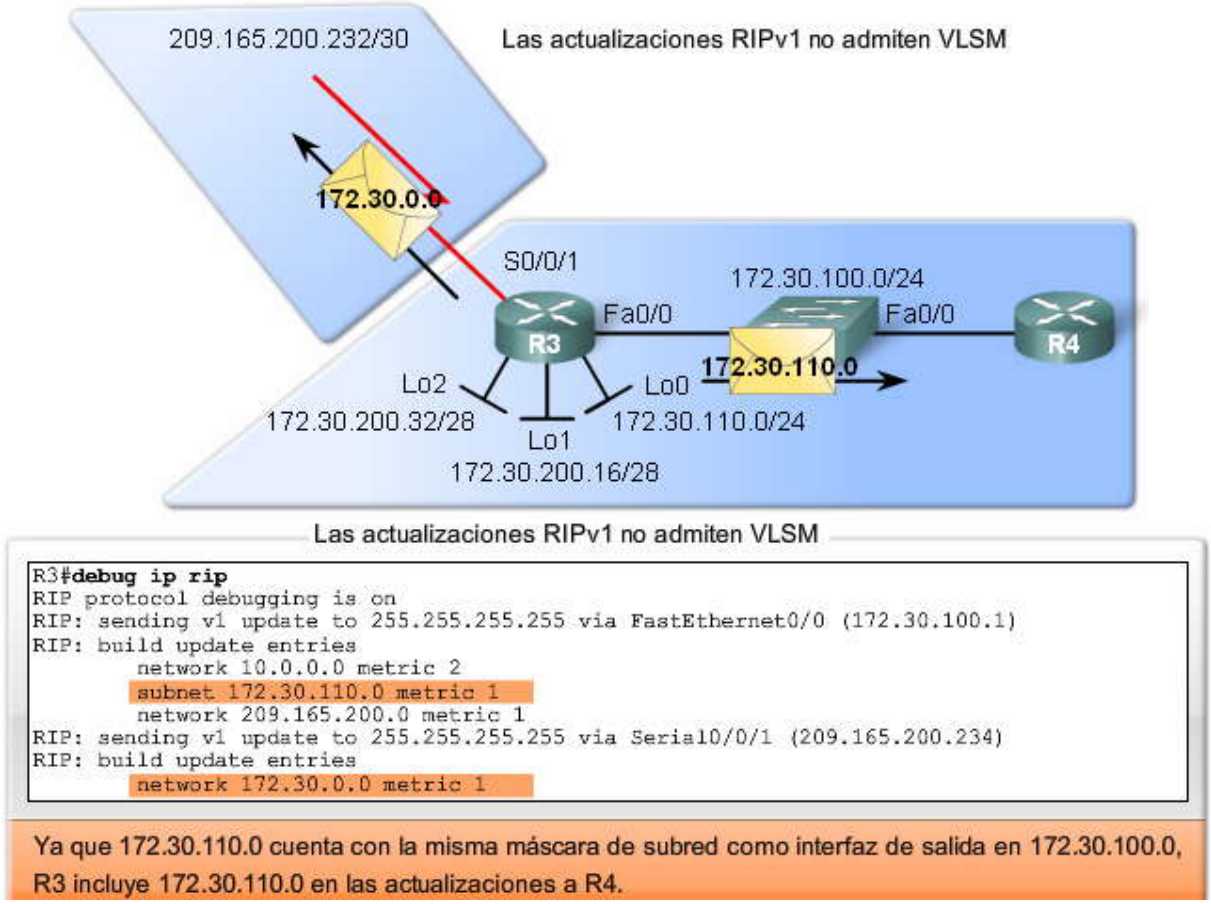
Consulte debug ip rip en la figura. Observe que la única subred 172.30.0.0 que se envía al router R4 es 172.30.110.0. También observe que R3 envía toda la red principal con clase 172.30.0.0 de Serial 0/0/1.

¿Por qué RIPv1 de R3 no incluye las otras subredes, 172.30.200.16/28 y 172.30.200.32/28, en las actualizaciones a R4? Esas subredes no tienen la misma máscara de subred que FastEthernet 0/0. Por eso todas las subredes deben usar la misma máscara de subred cuando se implementa un protocolo de enrutamiento con clase en la red.

**Una explicación más detallada**

R3 necesita determinar qué subredes 172.30.0.0 incluir en las actualizaciones que salen de su interfaz FastEthernet 0/0 con la dirección IP 172.30.100.1/24. Sólo incluirá esas rutas 172.30.0.0 en su tabla de enrutamiento con la misma máscara que la interfaz de salida. Debido a que la interfaz es 172.30.100.1 con una máscara de /24, sólo incluirá subredes 172.30.0.0 con una máscara de /24. La única que cumple con esta condición es 172.30.110.0.

Las otras subredes 172.30.0.0, 172.30.200.16/28 y 172.30.200.32/28, no se incluyen porque las máscaras de /28 no coinciden con la máscara de /24 de la interfaz saliente. El router receptor, R4, sólo puede aplicar su propia máscara de interfaz de /24 a las notificaciones de la ruta de RIPv1 con subredes 172.30.0.0. Con máscaras de /28, R4 aplicaría la máscara de /24 incorrecta a estas subredes.




### 7.1.5 RIPv1: INCOMPATIBILIDAD CON CIDR.-

**La ruta estática 192.168.0.0/16**

Hasta ahora, la mayoría de la información le debe ser familiar del Capítulo 5, "RIPv1". Sin embargo, hay un tema que aún no hemos tratado.

**Haga clic en Enrutamiento de R2 en la figura.**

Configuramos una ruta estática hacia la red 192.168.0.0/16 de R2 y le ordenamos a RIP que incluya esa ruta en sus actualizaciones con el comando redistribute static, como se muestra en la figura. Esta ruta estática es un resumen de las subredes 192.168.0.0/24 comprendidas entre 192.168.0.0/24 y 192.168.255.0/24.

R2(config)#ip route 192.168.0.0 255.255.0.0 Null0

**Haga clic en Rutas de R2 en la figura.**

Podemos ver que la ruta estática está incluida en la tabla de enrutamiento de R2.

**Haga clic en Rutas de R1 en la figura.**

Si observamos la tabla de enrutamiento de R1, veremos que R1 no está recibiendo la ruta 192.168.0.0/16 en sus actualizaciones de RIP de R2, si bien nosotros esperábamos que sí lo estuviera haciendo.

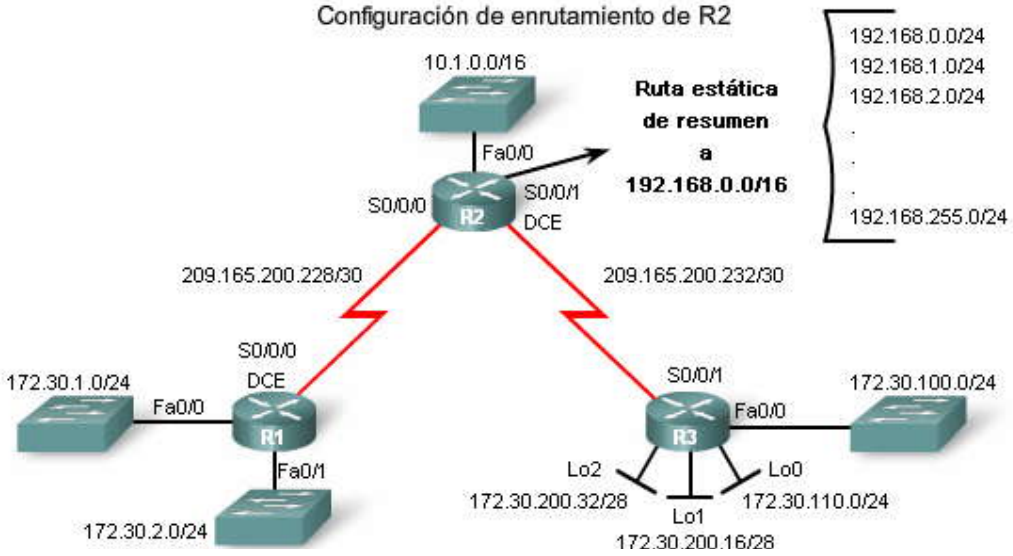
**Haga clic en Depuración de R2 en la figura.**

Si usamos debug ip rip en R2, observamos que RIPv1 no incluye la ruta 192.168.0.0/16 en sus actualizaciones de RIP para R1 o R3. ¿Sabe por qué no se incluye esta ruta? Observe la ruta 192.168.0.0/16. ¿Qué clase de ruta es? ¿Clase A, B o C? ¿Cuál es la máscara que se usa en la ruta estática? ¿Coincide con la clase? ¿Es la máscara de la ruta estática menor que la máscara con clase?

Configuramos la ruta estática 192.168.0.0 con una máscara de /16. Ésta tiene menos bits que la máscara de clase C con clase de /24. Debido a que la máscara no coincide con la clase ni la subred de la clase, RIPv1 no incluirá esta ruta en sus actualizaciones a otros routers.

RIPv1 y otros protocolos de enrutamiento con clase no pueden admitir rutas CIDR que sean rutas resumidas con una máscara de subred menor que la máscara con clase de la ruta. RIPv1 ignora estas subredes en la tabla de enrutamiento y no las incluye en las actualizaciones a otros routers. Esto se debe a que el router receptor sólo podrá aplicar la máscara con clase más grande a la actualización y no la máscara de /16 más corta.

Nota: Si la ruta estática 192.168.0.0 se configurara con una máscara de /24 o más grande, esta ruta se incluiría en las actualizaciones de RIP. Los routers receptores aplicarían la máscara con clase de /24 a esta actualización.




Configuración de enrutamiento de R2

```
R2(config)#router rip
R2(config-router)#redistribute static
R2(config-router)#network 10.0.0.0
R2(config-router)#network 209.165.200.0
R2(config-router)#exit
R2(config)#ip route 192.168.0.0 255.255.0.0 null0
```

R2 cuenta con una ruta estática y se configura para redistribuir dicha ruta estática en las actualizaciones RIP.

Configuración de enrutamiento de R2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>
R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:09, Serial0/0/0
                   [120/1] via 209.165.200.234, 00:00:11, Serial0/0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.232 is directly connected, Serial0/0/1
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
S    192.168.0.0/16 is directly connected, Null0
```

La ruta estática se encuentra en la tabla de enrutamiento para R2.

Configuración de enrutamiento de R2

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/24 is subnetted, 2 subnets
C       172.30.2.0 is directly connected, FastEthernet0/1
C       172.30.1.0 is directly connected, FastEthernet0/0
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:16, Serial0/0/0
C       209.165.200.228 is directly connected, Serial0/0/0
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:16, Serial0/0/0
```

R1 no recibe la ruta estática de R2.

Configuración de enrutamiento de R2

```
R2#debug ip rip
RIP protocol debugging is on
<some output omitted>
RIP: received v1 update from 209.165.200.230 on Serial0/0/0
     172.30.0.0 in 1 hops
RIP: received v1 update from 209.165.200.234 on Serial0/0/1
     172.30.0.0 in 1 hops
R2#
RIP: sending v1 update to 255.255.255.255 via Serial0/0/0 (209.165.200.229)
RIP: build update entries
        network 10.0.0.0 metric 1
        subnet 209.165.200.232 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0/0/1 (209.165.200.233)
RIP: build update entries
        network 10.0.0.0 metric 1
        subnet 209.165.200.228 metric 1
R2#
```

R2 no envía la ruta estática a R1 o a R3.

### 7.2 CONFIGURACION DE RIPv2.-

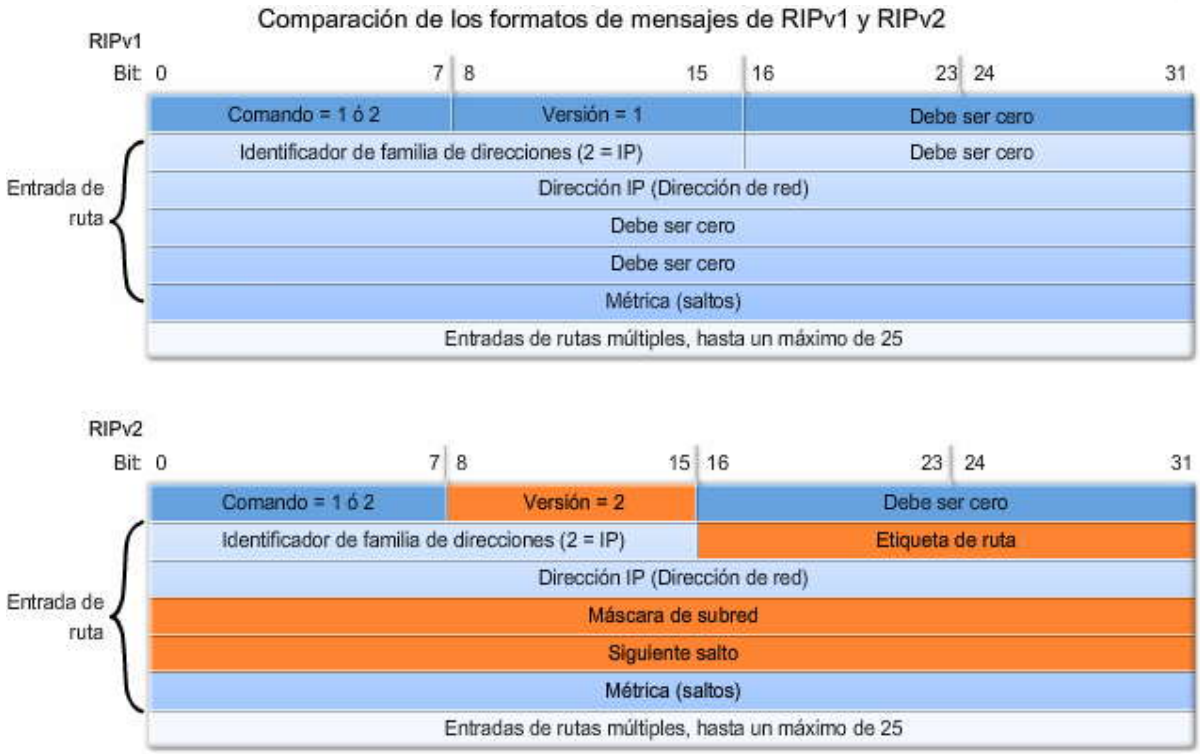
#### 7.2.1 HABILITACION Y VERIFICAION DEL RIPv2.-

**Comparación de los formatos de mensajes de RIPv1 y RIPv2**

RIPv2 se define en RFC 1723. Al igual que la versión 1, RIPv2 se encapsula en un segmento UDP mediante el puerto 520 y puede transportar hasta 25 rutas. Si bien RIPv2 tiene el mismo formato de mensaje básico que RIPv1, se agregan dos extensiones importantes.

La primera extensión en el formato de mensaje de RIPv2 es el campo de la máscara de subred que permite que una máscara de 32 bits se incluya en la entrada de ruta de RIP. Por ende, el router receptor ya no depende de la máscara de subred de la interfaz entrante ni de la máscara con clase al determinar la máscara de subred para una ruta.

La segunda extensión importante para el formato de mensaje de RIPv2 es la adición de la dirección del siguiente salto. La dirección del siguiente salto se usa para identificar una dirección del siguiente salto mejor que la dirección del router emisor, si es que existe. Si el campo se establece todo en ceros (0.0.0.0), la dirección del router emisor es la mejor dirección del siguiente salto. La información detallada sobre cómo se usa la dirección del siguiente salto se encuentra más allá del alcance de este curso. Sin embargo, puede encontrar un ejemplo en RFC 1722 o en Routing TCP/IP Volumen 1 de Jeff Doyle.




**Versión 2**

En forma predeterminada, cuando un proceso de RIP se encuentra configurado en un router Cisco, éste ejecuta RIPv1. Sin embargo, a pesar de que el router sólo envía mensajes de RIPv1, puede interpretar los mensajes de RIPv1 y RIPv2. Un router de RIPv1 simplemente ignorará los campos de RIPv2 en la entrada de ruta.

**Haga clic en RIPv1 de R2 en la figura.**

El comando show ip protocols verifica que R2 esté configurado para RIPv1, pero recibe mensajes de RIP para ambas versiones.

**Haga clic en Configuraciones de RIPv2 en la figura.**

Observe que el comando version 2 se usa para modificar RIP para que utilice la versión 2. Este comando debe configurarse en todos los routers del dominio de enrutamiento. El proceso de RIP ahora incluirá la máscara de subred en todas las actualizaciones, lo que hará que RIPv2 sea un protocolo de enrutamiento sin clase.

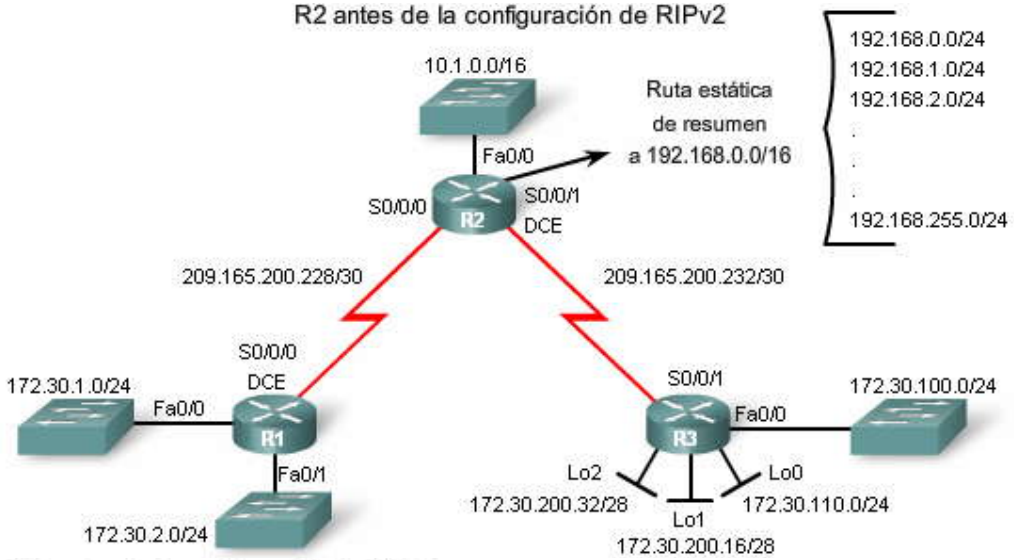
**Haga clic en RIPv2 de R2 en la figura.**

Como puede ver en el resultado, cuando un router está configurado para la versión 2, sólo se envían y reciben mensajes de RIPv2.

**Haga clic en Volver a RIPv1 en la figura.**

El comportamiento predeterminado de RIPv1 puede restaurarse usando el comando version 1 o el comando no version en el modo de configuración de router.

## R2 antes de la configuración de RIPv2




## R2 antes de la configuración de RIPv2

```
R2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 1 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: static, rip
  Default version control: send version 1, receive any version
    Interface              Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0            1     1 2
    Serial0/0/1            1     1 2
  Automatic network summarization is in effect
  Routing for Networks:
    10.0.0.0
    209.165.200.0
  Passive Interface(s):
```

Configuración de RIPv2:

R2 envía las actualizaciones RIPv1 pero recibe tanto actualizaciones RIPv1 como RIPv2.

## R2 antes de la configuración de RIPv2

```
R1(config)#router rip
R1(config-router)#version 2
```

```
R2(config)#router rip
R2(config-router)#version 2
```

```
R3(config)#router rip
R3(config-router)#version 2
```

R2 antes de la configuración de RIPv2

```
R2#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 1 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Redistributing: static, rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    Serial0/0/0            2     2
    Serial0/0/1            2     2
  Automatic network summarization is in effect
  Routing for Networks:
    10.0.0.0
    209.165.200.0
  Passive Interface(s):
```

R2 después de la configuración de RIPv2:
RIPv2 ignora las actualizaciones RIPv1

R2 antes de la configuración de RIPv2

```
R1(config)#router rip
R1(config-router)#version 1
!
!or
!
```

```
R2(config)#router rip
R2(config-router)#version 1
!
!or
!
```

```
R3(config)#router rip
R3(config-router)#version 1
!
!or
!
```

### 7.2.2 AUTORESUMEN Y RIPv2.-

**Examen de las tablas de enrutamiento**

Como RIPv2 es un protocolo de enrutamiento sin clase, es posible que se vean las subredes 172.30.0.0 individuales en las tablas de enrutamiento. Sin embargo, cuando examinamos la tabla de enrutamiento para R2 en la figura, aún vemos la ruta 172.30.0.0/16 resumida con las mismas dos rutas de igual costo. Los routers R1 y R3 aún no incluyen las subredes 172.30.0.0 del otro router.

**Haga clic en Rutas de R1 en la figura.**

La única diferencia que hay hasta ahora entre RIPv1 y RIPV2 es que R1 y R3 cuentan cada uno con una ruta a la superred 192.168.0.0/16. Esta ruta era la ruta estática configurada en R2 y redistribuida por RIP

**Haga clic en Depuración 1 de R1 en la figura.**

Entonces, ¿qué está sucediendo? Para examinar qué rutas de RIPv2 se están enviando y recibiendo, usaremos debug ip rip. La figura muestra el resultado debug ip rip para R1. Observe que RIPv2 envía la dirección de red y la máscara de subred:

RIP: sending v2 update to 224.0.0.9 via Serial0/0 (209.165.200.230)
172.30.0.0/16 via 0.0.0.0, metric 1, tag 0

Sin embargo, observe que la ruta que se envió es la dirección de red con clase resumida, 172.30.0.0/16, y no las subredes individuales 172.30.1.0/24 y 172.30.2.0/24.

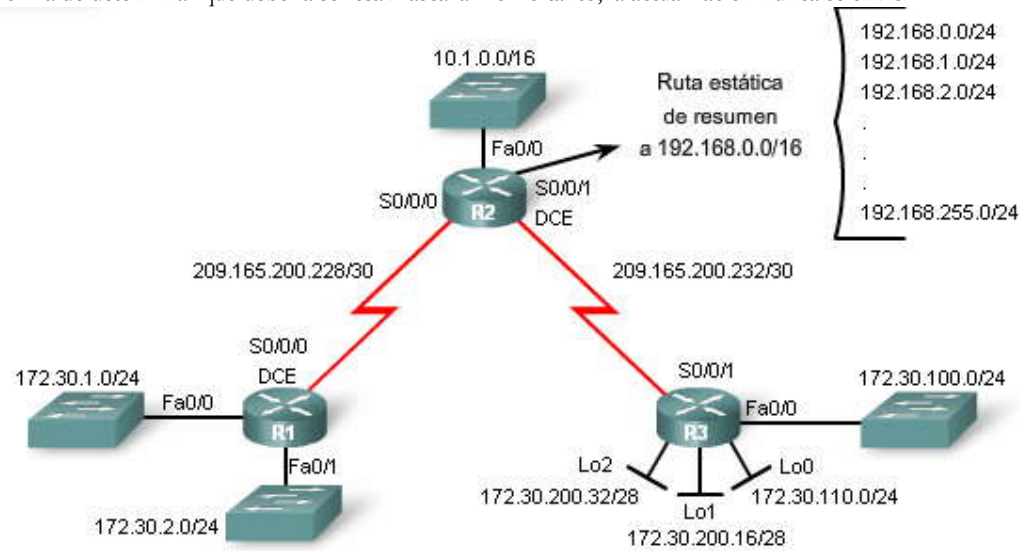
**Haga clic en Autoresumen en la figura**

**De manera predeterminada, RIPv2 resume automáticamente las redes en los bordes de redes principales, como RIPv1.** Los routers R1 y R3 todavía resumen sus subredes 172.30.0.0 a la dirección de clase B de 172.30.0.0 cuando envían las actualizaciones de sus interfaces de las redes 209.165.200.228 y 209.165.200.232, respectivamente. El coman do show ip protocols verifica que el "resumen automático tenga vigencia".

**Haga clic en Depuración 2 de R1 en la figura.**

El único cambio producto del comando version 2 es que R2 ahora incluye la red 192.168.0.0/16 en sus actualizaciones. Esto se debe a que RIPv2 incluye la máscara 255.255.0.0 con la dirección de red 192.168.0.0 en la actualización. Tanto R1 como R3 ahora recibirán esta ruta estática redistribuida a través de RIPv2 y la ingresarán en sus tablas de enrutamiento.

Nota: Recuerde que la ruta 192.168.0.0/16 no pudo distribuirse con RIPv1 porque la máscara de subred era menor que la máscara con clase. Debido a que la máscara no está incluida en las actualizaciones de RIPv1, el router de RIPv1 no tenía forma de determinar qué debería ser esa máscara. Por lo tanto, la actualización nunca se envió.




```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

R    172.30.0.0/16 [120/1] via 209.165.200.230, 00:00:28, Serial0/0/0
                   [120/1] via 209.165.200.234, 00:00:18, Serial0/0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.232 is directly connected, Serial0/0/1
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
S    192.168.0.0/16 is directly connected, Null0
```

Rutas de R2

R2 aún cuenta con rutas del mismo costo.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/24 is subnetted, 2 subnets
C       172.30.2.0 is directly connected, Loopback0
C       172.30.1.0 is directly connected, FastEthernet0/0
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:04, Serial0/0/0
C       209.165.200.228 is directly connected, Serial0/0/0
R    10.0.0.0/8 [120/1] via 209.165.200.229, 00:00:04, Serial0/0/0
R    192.168.0.0/16 [120/1] via 209.165.200.229, 00:00:04, Serial0/0/0
```

Rutas de R1

R1 ahora cuenta con superred.

```
R1#debug ip rip
RIP protocol debugging is on
R1#
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (209.165.200.230)
RIP: build update entries
        172.30.0.0/16 via 0.0.0.0, metric 1, tag 0
R1#
<output omitted for brevity>
RIP: received v2 update from 209.165.200.229 on Serial0/0/0
     10.0.0.0/8 via 0.0.0.0 in 1 hops
     192.168.0.0/16 via 0.0.0.0 in 1 hops
     209.165.200.232/30 via 0.0.0.0 in 1 hops
<output omitted for brevity>
R1#
```

Depuración de R1

R1 aún envía la ruta de resumen pero ahora con máscara de subred /16.

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 20 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0        2     2
    FastEthernet0/1        2     2
    Serial0/1/0            2     2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    172.30.0.0
    209.165.200.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.165.200.229         120      00:00:08
  Distance: (default is 120)
```

El comando **show ip protocols** verifica el resumen automático.

```
R1#debug ip rip
RIP protocol debugging is on
R1#
RIP: sending v2 update to 224.0.0.9 via Serial0/1/0 (209.165.200.230)
RIP: build update entries
        172.30.0.0/16 via 0.0.0.0, metric 1, tag 0
R1#
<output omitted for brevity>
RIP: received v2 update from 209.165.200.229 on Serial0/1/0
     10.0.0.0/8 via 0.0.0.0 in 1 hops
     192.168.0.0/16 via 0.0.0.0 in 1 hops
     209.165.200.232/30 via 0.0.0.0 in 1 hops
<output omitted for brevity>
R1#
```

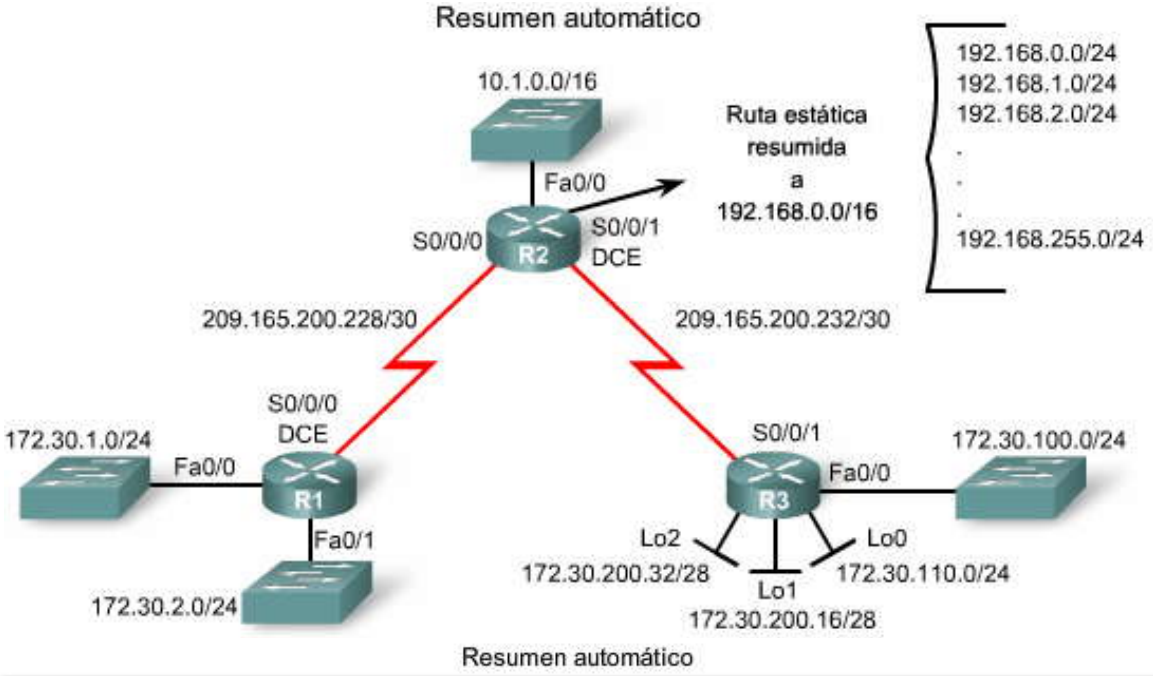
Depuración 2 de R1

Las superredes ahora se incluyen en las actualizaciones RIPv2.

### 7.2.3 DESACTIVAION DE AUTORESUMEN EN RIPv2.-

Como puede ver en la figura, para modificar el comportamiento predeterminado de resumen automático de RIPv2, use el comando no auto-summary en el modo de configuración de router. Este comando no es válido con RIPv1. A pesar de que el IOS de Cisco le permitirá configurar no auto-summary para RIPv1, el comando no tiene ningún efecto. También debe configurar la versión 2 antes de que el IOS de Cisco cambie la forma en la que envía las actualizaciones de RIP.

Una vez que el resumen automático esté desactivado, RIPv2 ya no resumirá las redes a su dirección con clase en routers de borde. RIPv2 ahora incluirá todas las subredes y sus máscaras apropiadas en sus actualizaciones de enrutamiento. El comando show ip protocols puede usarse para verificar que "el resumen automático de la red no tiene efecto".




```
R1(config)#router rip
R1(config-router)#no auto-summary
R1(config-router)#end
R1#show ip protocols
Routing Protocol is "rip"
<output omitted for brevity>
  Default version control: send version 2, receive version 2
    Interface             Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0       2     2
    FastEthernet0/1       2     2
    Serial0/1/0           2     2
  Automatic network summarization is not in effect
  <output omitted for brevity>
```

```
R2(config)#router rip
R2(config-router)# no auto-summary
```

```
R3(config)#router rip
R3(config-router)#no auto-summary
```

### 7.2.4 VERIFICACION DE LAS ACTUALIZACIONES DE RIPv2.-

Ahora que utilizamos un protocolo de enrutamiento sin clase RIPv2 y también que hemos desactivado el resumen automático, ¿qué podemos esperar ver en las tablas de enrutamiento?

En la figura, la tabla de enrutamiento de R2 ahora contiene las subredes individuales para 172.30.0.0/16. Observe que ya no hay una única ruta resumida con dos rutas de igual costo. Cada subred y máscara tiene su propia entrada específica, junto con la interfaz de salida y la dirección del siguiente salto para llegar a esa subred.

**Haga clic en Rutas de R1 en la figura.**

La tabla de enrutamiento de R1 contiene todas las subredes para 172.30.0.0/16, incluidas las subredes de R3.

**Haga clic en Rutas de R3 en la figura.**

La tabla de enrutamiento de R3 contiene todas las subredes para 172.30.0.0/16, incluidas las subredes de R1. Esta red es convergente.

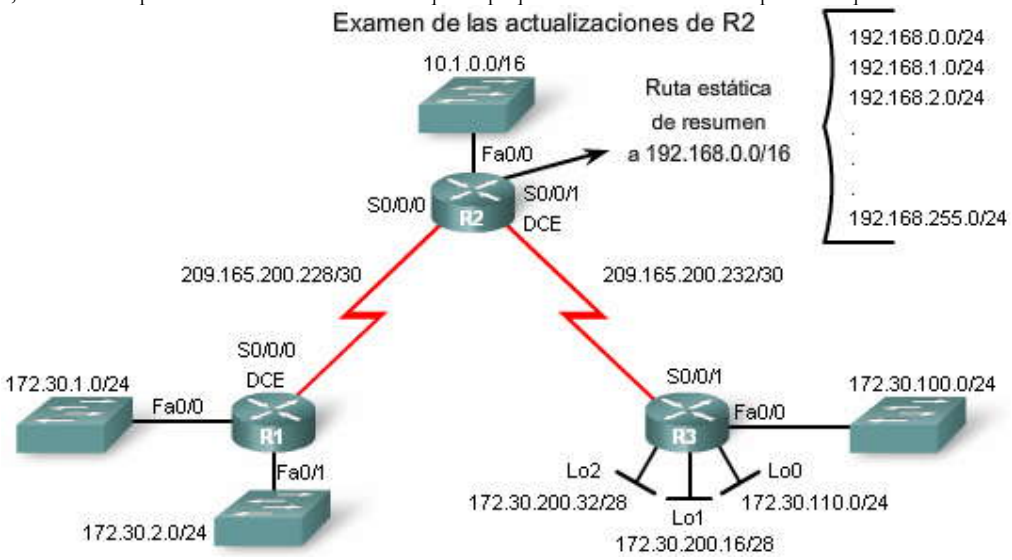
**Haga clic en Depuración de R2 en la figura.**

Podemos verificar que el protocolo de enrutamiento sin clase RIPv2 realmente está enviando y recibiendo información sobre la máscara de subred en las actualizaciones de enrutamiento usando debug ip ri p. Observe que cada entrada de ruta ahora incluye la notación de barra para la máscara de subred.

También podemos ver que una actualización en una interfaz hace que su métrica se incremente antes de enviarla a otra interfaz. Por ejemplo, la actualización que se recibió en Serial 0/0/1 para la red 172.30.100.0/24 con 1 salto se envía a otras interfaces, como Serial 0/0/0, con una métrica de 2, o 2 saltos.

RIP: received v2 update from 209.165.200.234 on Serial0/0/1
172.30.100.0/24 via 0.0.0.0 in 1 hops
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (209.165.200.229)
172.30.100.0/24 via 0.0.0.0, metric 2, tag 0

También observe que las actualizaciones se envían usando la dirección multicast 224.0.0.9. RIPv1 envía actualizaciones como un broadcast 255.255.255.255. Usar una dirección multicast tiene muchas ventajas. Los detalles sobre el direccionamiento multicast se encuentran más allá del alcance de este curso; sin embargo, en general, multicast puede ocupar menos ancho de banda en la red. Además, las actualizaciones de multicast requieren menos procesamiento de los dispositivos no habilitados con RIP. Con RIPv2, cualquier dispositivo que no esté configurado para RIP descartará la trama de la capa de Enlace de datos. Con las actualizaciones de broadcast en configuraciones de RIPv1, todos los dispositivos de una red de broadcast como Ethernet deben procesar una actualización RIP por completo hasta llegar a la capa de Transporte, donde el dispositivo finalmente descubre que el paquete está destinado a un proc eso que no existe.



Examen de las actualizaciones de R2

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

     172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.30.200.32/28 [120/1] via 209.165.200.234, 00:00:09, Serial0/0/1
R       172.30.200.16/28 [120/1] via 209.165.200.234, 00:00:09, Serial0/0/1
R       172.30.2.0/24 [120/1] via 209.165.200.230, 00:00:03, Serial0/0/0
R       172.30.1.0/24 [120/1] via 209.165.200.230, 00:00:03, Serial0/0/0
R       172.30.100.0/24 [120/1] via 209.165.200.234, 00:00:09, Serial0/0/1
R       172.30.110.0/24 [120/1] via 209.165.200.234, 00:00:09, Serial0/0/1
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.232 is directly connected, Serial0/0/1
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
C       10.1.0.0 is directly connected, FastEthernet0/0
S    192.168.0.0/16 is directly connected, Null0
```

R2 ahora cuenta con todas las subredes en su tabla de enrutamiento.

Examen de las actualizaciones de R2

```
R1#show ip route
<output omitted>

Gateway of last resort is not set

     172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
C       172.30.2.0/24 is directly connected, Loopback0
C       172.30.1.0/24 is directly connected, FastEthernet0/0
R       172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
R       10.1.0.0 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
R    192.168.0.0/16 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
```

R1 ahora cuenta con todas las subredes en su tabla de enrutamiento.

Examen de las actualizaciones de R2

```
R3#show ip route
<output omitted>

Gateway of last resort is not set

     172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
C       172.30.200.32/28 is directly connected, Loopback2
C       172.30.200.16/28 is directly connected, Loopback1
R       172.30.2.0/24 [120/2] via 209.165.200.233, 00:00:01, Serial0/0/1
R       172.30.1.0/24 [120/2] via 209.165.200.233, 00:00:01, Serial0/0/1
C       172.30.100.0/24 is directly connected, FastEthernet0/0
C       172.30.110.0/24 is directly connected, Loopback0
     209.165.200.0/30 is subnetted, 2 subnets
C       209.165.200.232 is directly connected, Serial0/0/1
R       209.165.200.228 [120/1] via 209.165.200.233, 00:00:02, Serial0/0/1
     10.0.0.0/16 is subnetted, 1 subnets
R       10.1.0.0 [120/1] via 209.165.200.233, 00:00:02, Serial0/0/1
R    192.168.0.0/16 [120/1] via 209.165.200.233, 00:00:02, Serial0/0/1
```

R3 ahora cuenta con todas las subredes en su tabla de enrutamiento.

Examen de las actualizaciones de R2

```
R2#debug ip rip
RIP protocol debugging is on
<some output omitted for brevity>
R2#
RIP: received v2 update from 209.165.200.234 on Serial0/0/1
     172.30.100.0/24 via 0.0.0.0 in 1 hops
     172.30.110.0/24 via 0.0.0.0 in 1 hops
     172.30.200.16/28 via 0.0.0.0 in 1 hops
     172.30.200.32/28 via 0.0.0.0 in 1 hops
R2#
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (209.165.200.229)
RIP: build update entries
        10.1.0.0/16 via 0.0.0.0, metric 1, tag 0
        172.30.100.0/24 via 0.0.0.0, metric 2, tag 0
        172.30.110.0/24 via 0.0.0.0, metric 2, tag 0
```

R2 recibe la ruta de R3 como 1 salto.

R2 envía la ruta a R1 como 2 saltos.

### 7.3 VLSM Y CIDR-

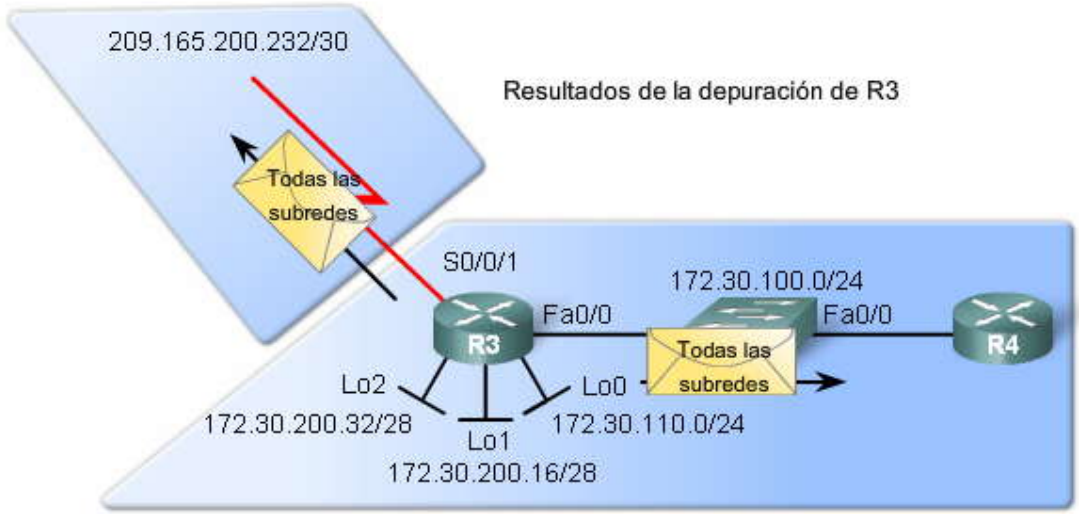
#### 7.3.1 RIPv2 Y VLSM.-

Debido a que los protocolos de enrutamiento sin clase como RIPv2 pueden transportar la dirección de red y la máscara de subred, no necesitan resumir estas redes a sus direcciones con clase en los bordes de redes principales. Por lo tanto, los protocolos de enrutamiento sin clase admiten VLSM. Los routers que usan RIPv2 ya no necesitan usar la máscara de la interfaz saliente para determinar la máscara de subred en la notificación de la ruta. La red y la máscara están incluidas de manera explícita en todas las actualizaciones de enrutamiento.

En las redes que usan un esquema de direccionamiento VLSM, un protocolo de enrutamiento sin clase es esencial para propagar todas las redes junto con las máscaras de subred correctas. Si observamos el resultado de debug ip rip para R3 en la figura, podemos ver que RIPv2 incluye las redes y sus máscaras de subred en las actualizaciones de enrutamiento.

También observe en la figura que una vez más hemos agregado el router R4 en la topología. Recuerde que con RIPv1, R3 sólo enviará a R4 las rutas 172.30.0.0 que tenían la misma máscara que la interfaz de salida FastEthernet 0/0. Debido a que la interfaz es 172.30.100.1 con una máscara de /24, RIPv1 sólo incluyó subredes 172.30.0.0 con una máscara de /24. La única ruta que cumplía con esta condición era 172.30.110.0.

Sin embargo, con RIPv2, R3 ahora puede incluir todas las subredes 172.30.0.0 en sus actualizaciones de enrutamiento a R4, como se muestra en el resultado de depuración en la figura. Esto se debe a que RIPv2 puede incluir la máscara de subred correcta con la dirección de red en la actualización.



Resultados de la depuración de R3

```
R3#debug ip rip
RIP protocol debugging is on
R3#
RIP: received v2 update from 209.165.200.233 on Serial0/0/1
     10.1.0.0/16 via 0.0.0.0 in 1 hops
     172.30.1.0/24 via 0.0.0.0 in 2 hops
     172.30.2.0/24 via 0.0.0.0 in 2 hops
     192.168.0.0/16 via 0.0.0.0 in 1 hops
     209.165.200.228/30 via 0.0.0.0 in 1 hops
R3#
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (172.30.100.1)
RIP: build update entries
        10.1.0.0/16 via 0.0.0.0, metric 2, tag 0
        172.30.1.0/24 via 0.0.0.0, metric 3, tag 0
        172.30.2.0/24 via 0.0.0.0, metric 3, tag 0
        172.30.110.0/24 via 0.0.0.0, metric 1, tag 0
        172.30.200.16/28 via 0.0.0.0, metric 1, tag 0
        172.30.200.32/28 via 0.0.0.0, metric 1, tag 0
        192.168.0.0/16 via 0.0.0.0, metric 2, tag 0
        209.165.200.228/30 via 0.0.0.0, metric 2, tag 0
```

RIPv2 admite VLSM

### 7.3.2 RIPv2 Y CIDR.-

Uno de los objetivos de Classless Inter-Domain Routing (CIDR), según lo que establece RFC 1519, es "proporcionar un mecanismo para la agregación de información de enrutamiento". Este objetivo incluye el concepto de creación de superredes. Una superred es un bloque de redes con clase contiguas que se direcciona como una única red. En el router R2, configuramos una superred, una ruta estática a una única red que se usa para representar varias redes o subredes.

Las superredes tienen máscaras que son más pequeñas que la máscara con clase (de /16 en este caso, en lugar de la máscara con clase de /24). Para que la superred se incluya en una actualización de enrutamiento, el protocolo de enrutamiento debe tener la capacidad de transportar esa máscara. Es decir que debe ser un protocolo de enrutamiento sin clase, como RIPv2.

La ruta estática de R2 sí incluye una máscara que es menor que la máscara con clase:

R2(config)#ip route 192.168.0.0 255.255.0.0 Null0

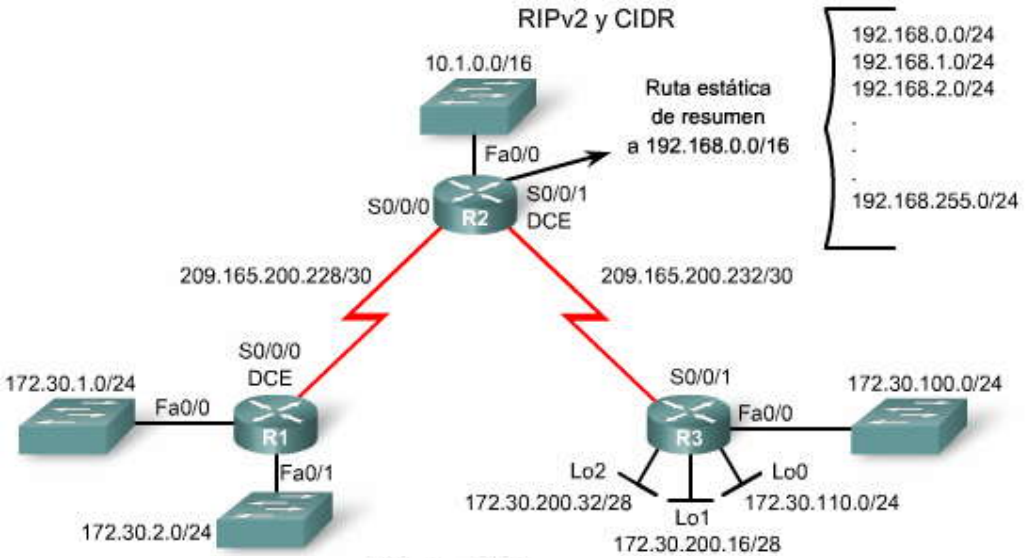
En un ambiente con clase, la dirección de red 192.168.0.0 se asocia con la máscara clase C con clase de /24 ó 255.255.255.0. En las redes actuales, ya no relacionamos las direcciones de red con las máscaras con clase. En este ejemplo, la red 192.168.0.0 tiene una máscara de /16 ó 255.255.0.0. Esta ruta puede representar una serie de redes 192.168.0.0/24 o cualquier número de distintos rangos de direcciones. La única forma en la que puede incluirse esta ruta en una actualización de enrutamiento dinámica es con un protocolo de enrutamiento sin clase que incluya la máscara de /16.

**Haga clic en Depuración de R2 en la figura.**

Con debug ip rip podemos ver que esta superred CIDR está incluida en la actualización de enrutamiento que envió R2. No es necesario desactivar el resumen automático en RIPv2 ni en ningún protocolo de enrutamiento sin clase para que las superredes se incluyan en las actualizaciones.

**Haga clic en Rutas de R1 en la figura.**

La tabla de enrutamiento para R1 muestra que ha recibido la ruta de superred de R2.




RIPv2 y CIDR

```
R2(config)#router rip
R2(config-router)#redistribute static
R2(config-router)#network 10.0.0.0
R2(config-router)#network 209.165.200.0
R2(config-router)#exit
R2(config)#ip route 192.168.0.0 255.255.0.0 null0
```

Superred

192.168.0.0/16 es una superred.

RIPv2 y CIDR

```
R2#debug ip rip
RIP protocol debugging is on
R2#
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (209.165.200.229)
RIP: build update entries
       10.1.0.0/16 via 0.0.0.0, metric 1, tag 0
       172.30.100.0/24 via 0.0.0.0, metric 2, tag 0
       172.30.110.0/24 via 0.0.0.0, metric 2, tag 0
       172.30.200.16/28 via 0.0.0.0, metric 2, tag 0
       172.30.200.32/28 via 0.0.0.0, metric 2, tag 0
       192.168.0.0/16 via 0.0.0.0, metric 1, tag 0
       209.165.200.232/30 via 0.0.0.0, metric 1, tag 0
<output omitted for brevity>
R2#
```

Depuración de R2

La superred es enviada por R2.

RIPv2 y CIDR

```
R1#show ip route
<output omitted>

Gateway of last resort is not set

     172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
C       172.30.2.0/24 is directly connected, Loopback0
C       172.30.1.0/24 is directly connected, FastEthernet0/0
R       172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
R       10.1.0.0 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
R    192.168.0.0/16 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
```

Rutas de R1

La superred se encuentra en la tabla de enrutamiento de R1.

## 7.4 VERIFICACION Y RESOLUCION DE PROBLEMAS RIPv2.-

### 7.4.1 COMANDOS PARFA LA VERIFICACION Y RESOLUCION DE PROBLEMAS.-

Existen muchas formas de verificar y resolver los problemas de RIPv2. Muchos de los mismos comandos que se usan para RIPv2 pueden utilizarse para verificar y resolver los problemas de otros protocolos de enrutamiento.

Siempre se recomienda comenzar con los principios básicos:

1. Asegúrese de que todos los enlaces (interfaces) estén activados y en funcionamiento.

2. Verifique el cableado.

3. Verifique que tiene la máscara de subred y dirección IP correcta en cada interfaz.

4. Elimine los comandos de configuración que sean innecesarios o se hayan reemplazado con otros comandos.

**Haga clic en show ip route en la figura.**

Éste es el primer comando que se usa para verificar la convergencia de red. Mientras examina la tabla de enrutamiento, es importante que busque tanto las rutas que espera que estén en la tabla de enrutamiento, como así también las que no deberían estar allí.

**Haga clic en show ip interface brief en la figura.**

Si está faltando una red en la tabla de enrutamiento, generalmente es porque una interfaz está de sactivada o mal configurada. El comando show ip interface brief verifica rápidamente el estado de todas las interfaces.

**Haga clic en show ip protocols en la figura.**

El comando show ip protocols verifica varios elementos esenciales y también verifica que RIP esté habilitado, la versión de RIP, el estado del resumen automático y las redes que se incluyeron en las sentencias de red. Las fuentes de información de enrutamiento enumeradas en la parte inferior del resultado son los vecinos de RIP de donde este r outer está recibiendo actualizaciones.

**Haga clic en debug ip rip en la figura.**

Como se demostró a lo largo del capítulo, debug ip rip es un excelente comando para examinar los contenidos de las actualizaciones de enrutamiento que un router envía y recibe. Es posible que en algún momento un router reciba una ruta pero no la agregue en la tabla de enrutamiento. Uno de los motivos puede ser que la ruta estática también esté configurada para la misma red que se publica. En forma predeterminada, una ruta estática tiene una distancia administrativa menor que cualquier protocolo de enrutamiento dinámico y tendrá prioridad al ser agregada a la tabla de enrutamiento.

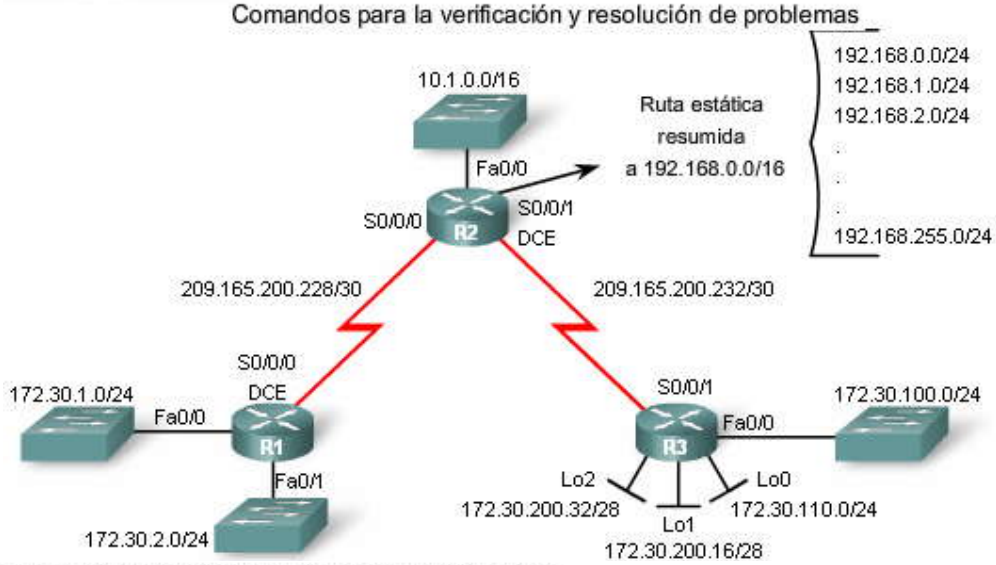
**Haga clic en ping en la figura.**

Una manera fácil de verificar la conectividad completa es con el comando ping. Si la conectividad de extremo a extremo no es satisfactoria, comience haciendo ping en las interfaces locales. Si es satisfactoria, haga ping en las interfaces del router en las redes conectadas directamente. Si eso también es satisfactorio, continúe haciendo ping en las interfaces de cada router sucesivo. Una vez que un ping no es satisfactorio, examine ambos routers y todos los routers intermedios para determinar dónde y por qué está fallando el ping.

**Haga clic en show running-config en la figura.**

El comando show running-config puede usarse para verificar todos los comandos configurados en ese momento. Generalmente, otros comandos son más eficientes y proporcionan más información que una simple lista de la configuración actual. Sin embargo, show running-config es útil para determinar si un elemento esencial se ha olvidado o está mal configurado.

## Comandos para la verificación y resolución de problemas




## Comandos para la verificación y resolución de problemas

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/16 is variably subnetted, 6 subnets, 2 masks
R       172.30.200.32/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.200.16/28 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
C       172.30.2.0/24 is directly connected, Loopback0
C       172.30.1.0/24 is directly connected, FastEthernet0/0
R       172.30.100.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
R       172.30.110.0/24 [120/2] via 209.165.200.229, 00:00:01, Serial0/0/0
     209.165.200.0/30 is subnetted, 2 subnets
R       209.165.200.232 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
C       209.165.200.228 is directly connected, Serial0/0/0
     10.0.0.0/16 is subnetted, 1 subnets
R       10.1.0.0 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
R    192.168.0.0/16 [120/1] via 209.165.200.229, 00:00:02, Serial0/0/0
```

Verificar la tabla de enrutamiento

## Comandos para la verificación y resolución de problemas

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            172.30.1.1      YES NVRAM  up                    up
FastEthernet0/1            172.30.2.1      YES NVRAM  up                    up
Serial0/0/0                209.165.200.230 YES NVRAM  up                    up
Serial0/0/1                unassigned      YES NVRAM  down                  down
```

Verificar que las interfaces estén activas

```
R1#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 29 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface              Send  Recv  Triggered RIP  Key-chain
    FastEthernet0/0        2     2
    FastEthernet0/1        2     2
    Serial0/0/0            2     2
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    172.30.0.0
    209.165.200.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.165.200.229      120      00:00:18
  Distance: (default is 120)
```

Verificar la configuración de enrutamiento

```
R1#debug ip rip
RIP protocol debugging is on
R1#
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/1 (172.30.2.1)
RIP: build update entries
        10.1.0.0/16 via 0.0.0.0, metric 2, tag 0
        172.30.1.0/24 via 0.0.0.0, metric 1, tag 0
        172.30.100.0/24 via 0.0.0.0, metric 3, tag 0
        172.30.110.0/24 via 0.0.0.0, metric 3, tag 0
        172.30.200.16/28 via 0.0.0.0, metric 3, tag 0
        172.30.200.32/28 via 0.0.0.0, metric 3, tag 0
        192.168.0.0/16 via 0.0.0.0, metric 2, tag 0
        209.165.200.228/30 via 0.0.0.0, metric 1, tag 0
        209.165.200.232/30 via 0.0.0.0, metric 2, tag 0
R1#
RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0 (172.30.1.1)
RIP: build update entries
        10.1.0.0/16 via 0.0.0.0, metric 2, tag 0
        172.30.2.0/24 via 0.0.0.0, metric 1, tag 0
        172.30.100.0/24 via 0.0.0.0, metric 3, tag 0
        172.30.110.0/24 via 0.0.0.0, metric 3, tag 0
        172.30.200.16/28 via 0.0.0.0, metric 3, tag 0
        172.30.200.32/28 via 0.0.0.0, metric 3, tag 0
        192.168.0.0/16 via 0.0.0.0, metric 2, tag 0
        209.165.200.228/30 via 0.0.0.0, metric 1, tag 0
        209.165.200.232/30 via 0.0.0.0, metric 2, tag 0
R1#
RIP: sending v2 update to 224.0.0.9 via Serial0/0/0 (209.165.200.230)
RIP: build update entries
        172.30.1.0/24 via 0.0.0.0, metric 1, tag 0
        172.30.2.0/24 via 0.0.0.0, metric 1, tag 0
```

Resolver problemas en la configuración de enrutamiento

```
R2#ping 172.30.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
```

```
R1#ping 172.30.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.100.1, timeout is 2 seconds:
```

```
R3#ping 172.30.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.1.1, timeout is 2 seconds:
```

```
R1#show running-config
Building configuration...
!
hostname R1
!
interface FastEthernet0/0
 ip address 172.30.1.1 255.255.255.0
!
interface FastEthernet0/1
 ip address 172.30.2.1 255.255.255.0
!
interface Serial0/0/0
 ip address 209.165.200.230 255.255.255.252
 clock rate 64000
!
router rip
 version 2
 network 172.30.0.0
 network 209.165.200.0
 no auto-summary
!
<some output omitted for brevity>
!
end
```

Resolver problemas en la configuración de enrutamiento

### 7.4.2 PROBLEMAS COMUNES DE RIPv2.-

Cuando se resuelven problemas específicos de RIPv2, hay varias áreas para examinar.

**Versión**

Un buen lugar para comenzar la resolución de problemas en una red que está ejecutando RIP es verificar que la versión 2 esté configurada en todos los routers. A pesar de que RIPv1 y RIPv2 son compatibles, RIPv1 no admite subredes no contiguas, VLSM ni rutas de superred CIDR. Siempre es mejor usar el mismo protocolo de enrutamiento en todos los routers a menos que exista una razón específica para no hacerlo.

**Sentencias de red**

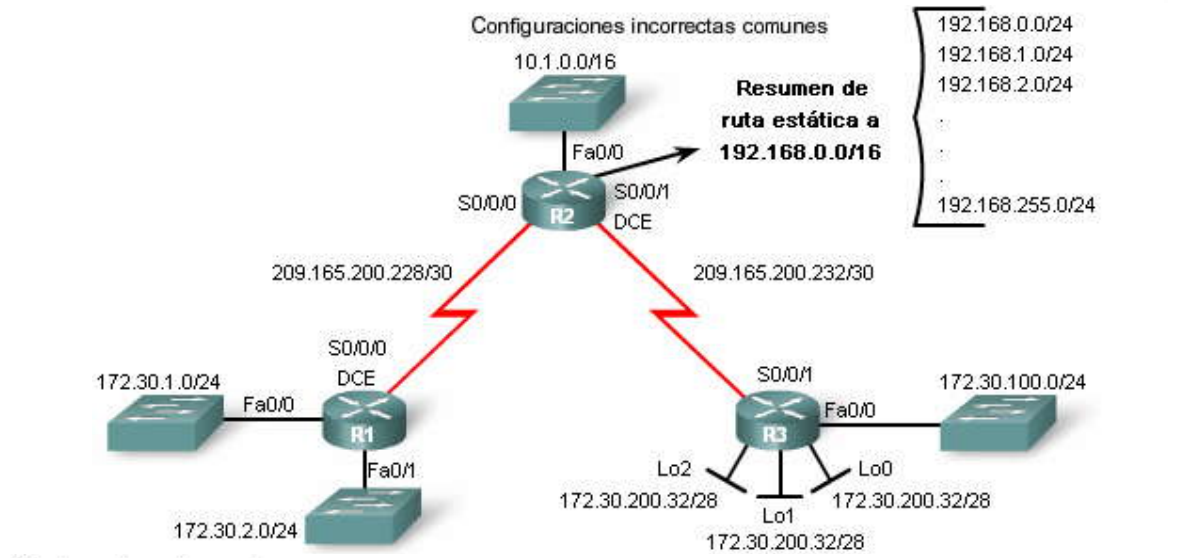
Otra fuente de problemas pueden ser las sentencias de red incorrectas o faltantes. Recuerde que la sentencia de red hace dos cosas:

- Le permite al protocolo de enrutamiento enviar y recibir actualizaciones en cualquier interfaz local que pertenezca a esa red.
- Incluye esa red en sus actualizaciones de enrutamiento a los routers vecinos.

- Una sentencia de red incorrecta o faltante ocasionará la pérdida de actualizaciones de enrutamiento y provocará que las actualizaciones de enrutamiento no se envíen o no se reciban en una interfaz.

**Resumen automático**

Si necesita o desea enviar subredes específicas y no simplemente rutas resumidas, asegúrese de que el resumen automático esté desactivado.




Configuraciones incorrectas comunes

```
R1#show running-config
Building configuration...
 !
hostname R1
 !
interface FastEthernet0/0
 ip address 172.30.1.1 255.255.255.0
 !
interface FastEthernet0/1
 ip address 172.30.2.1 255.255.255.0
 !
interface Serial0/0/0
 ip address 209.165.200.230 255.255.255.252
 clock rate 64000
 !
router rip
 version 2
 network 172.30.0.0
 network 209.165.200.0
 no auto-summary
 !
***resultado omitido***
 !
end
```

### 7.4.3 AUTENTIFICACION.-

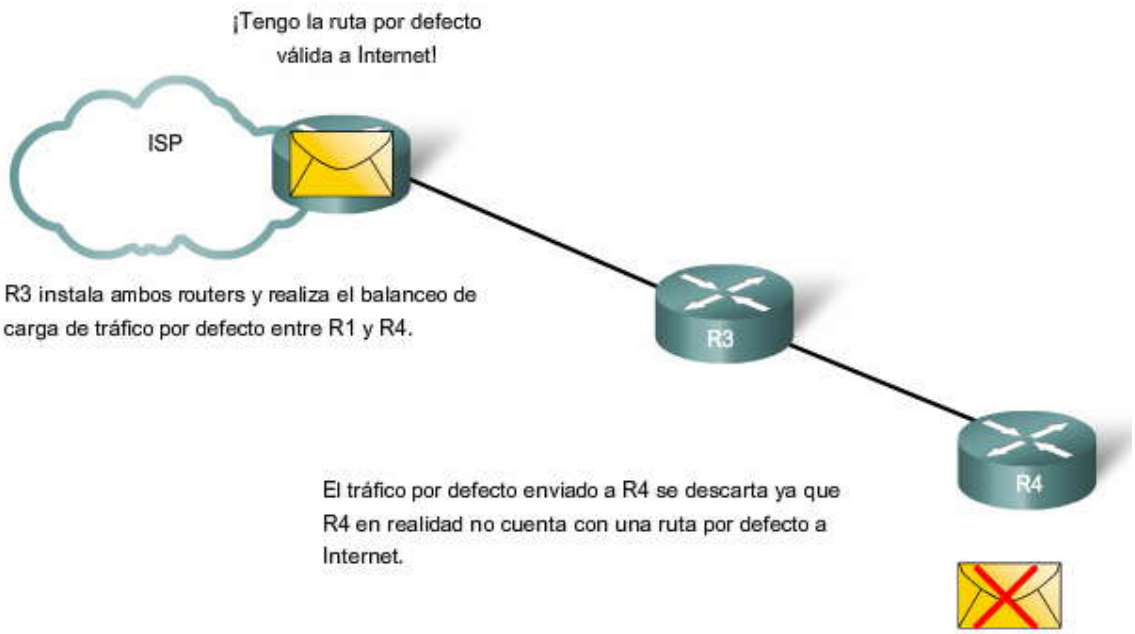
La mayoría de los protocolos de enrutamiento envían sus actualizaciones y otra información de enrutamiento con IP (en paquetes IP). El IS-IS es la excepción más evidente y se discute en los cursos de CCNP. Uno de los problemas de seguridad en cualquier protocolo de enrutamiento es la posibilidad de aceptar actualizaciones de enrutamiento inválidas. La fuente de estas actualizaciones de enrutamiento inválidas puede ser un atacante que intenta maliciosamente afectar la red o capturar paquetes engañando al router para que envíe sus actualizaciones al destino equivocado. Otra fuente de actualizaciones inválidas puede ser un router mal configurado. O bien puede ser que un host esté conectado a la red y, sin que el usuario lo sepa, el host ejecuta el protocolo de enrutamiento de la red local.

Por ejemplo, en la figura, R1 está propagando una ruta por defecto a todos los otros routers de este d ominio de enrutamiento. Sin embargo, alguien ha agregado por error el router R4 a la red, lo que también propaga una ruta por defecto. Algunos routers pueden reenviar tráfico predeterminado a R4 en lugar de hacia el verdadero router de gateway, R1. Estos paquetes pueden "perderse" y no verse nunca más.

Independientemente del motivo, es aconsejable autenticar la información de enrutamiento que se transmite entre routers. RIPv2, EIGRP, OSPF, IS-IS y BGP pueden configurarse para autenticar la información de enrutamiento. Esto garantiza que los routers sólo aceptarán información de enrutamiento de otros routers que estén configurados con la misma contraseña o información de autenticación. Nota: La autenticación no encripta la tabla de enrutamiento.

Nota: Debido a que RIP ha dado lugar a protocolos de enrutamiento más populares, las funciones de configuración detalladas para la autenticación en RIPv2 no se discuten en este capítulo. En su lugar, la configuración de protocolos de enrutamiento para usar autenticación se discutirá en un curso posterior con otros temas de seguridad.

¿Qué router cuenta con la ruta por defecto correcta?



# CAPITULO VIII – "LA TABLA DE ENRUTAMIENTO: UN ESTUDIO DETALLADO"

## 8.0 INTRODUCCION DEL CAPITULO.-

### 8.0.1 INTRODUCCIÓN DEL CAPITULO.-

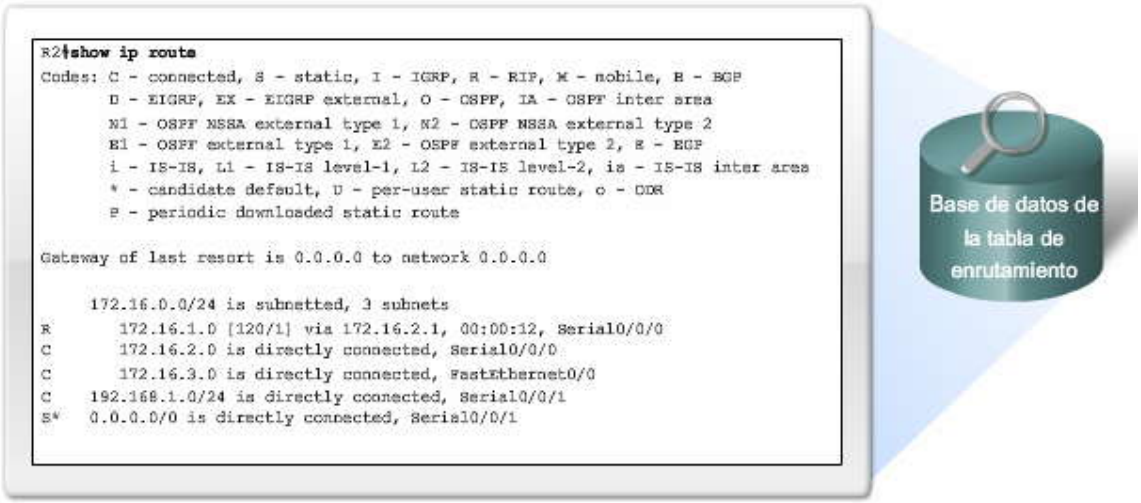
En los capítulos anteriores, examinamos la tabla de enrutamiento con el comando show ip route. Vimos cómo las rutas dinámicas, estáticas y las conectadas directamente se agregan y eliminan de la tabla de enrutamiento.

Como administrador de red, es importante conocer la tabla de enrutamiento en profundidad cuando se resuelven problemas de red. Comprender la estructura y el proceso de búsqueda de la tabla de enrutamiento lo ayudará a diagnosticar cualquier problema en la tabla de enrutamiento, independientemente de su nivel de familiaridad con el protocolo de enrutamiento en particular. Por ejemplo, puede encontrarse con una situación en la que la tabla de enrutamiento tenga todas las rutas que esperaría ver, pero el reenvío de paquetes no funciona como está previsto. Conocer cómo manejarse en el proceso de búsqueda de una dirección IP de destino de un paquete le dará la posibilidad de determinar si el paquete se está reenviando como está previsto, si el paquete se está reenviando a otro lugar y por qué o si el paquete se ha descartado.

En este capítulo, analizaremos más detalladamente la tabla de enrutamiento. La primera parte del capítulo se concentra en la estructura de la tabla de enrutamiento IP de Cisco. Examinaremos el formato de la tabla de enrutamiento y estudiaremos las rutas de nivel 1 y 2. La segunda parte del capítulo analiza el proceso de búsqueda de la tabla de enrutamiento. Analizaremos el comportamiento del enrutamiento con clase, como así también el comportamiento del enrutamiento sin clase, que usa los comandos no ip classless e ip classless.

En este capítulo, se han omitido muchos de los detalles sobre la estructura y el proceso de búsqueda de la tabla de enrutamiento IP de Cisco. Si le interesa leer más sobre este tema y sobre el funcionamiento interno del IOS de Cisco relativo al enrutamiento, consulte Cisco IP Routing, de Alex Zinin (ISBN 0-201-60473-6).

Nota: Este libro no es un libro sobre protocolos de enrutamiento para principiantes, sino que es un examen meticuloso de los procesos, protocolos y algoritmos que usa el IOS de Cisco.




**En este capítulo, aprenderá a:**

- Describir los distintos tipos de rutas que pueden encontrarse en la estructura de la tabla de enrutamiento.
- Describir el proceso de búsqueda de ruta.
- Describir el comportamiento de enrutamiento en redes enrutadas.

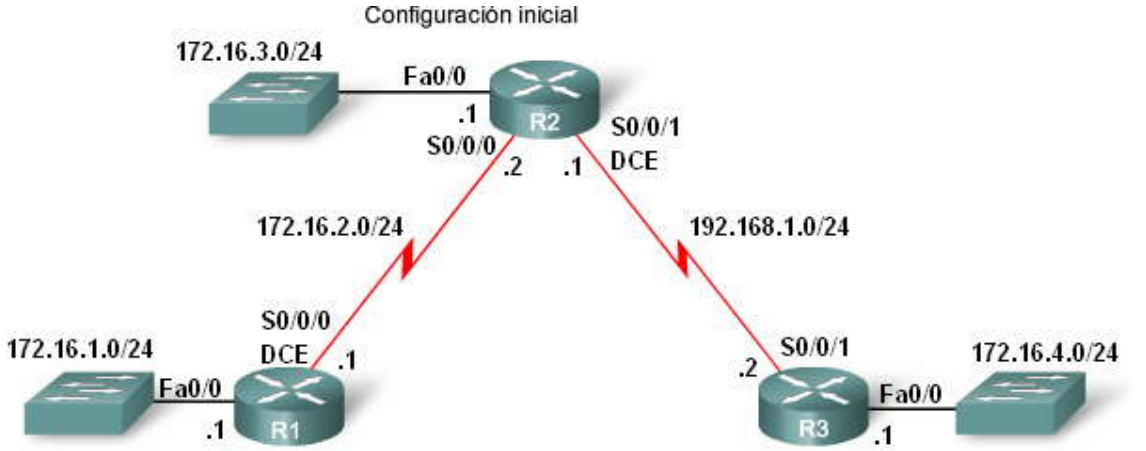
## 8.1 ESTRUCTURA DE LA TABLA DE ENRUTAMIENTO.-

### 8.1.1 TOPOLOGIA DE LABORATORIO.-

En este capítulo, usaremos una red simple de tres routers, como se muestra en la figura. R1 y R2 comparten una red 172.16.0.0/16 común con las subredes 172.16.0.0/24. R2 y R3 están conectados por la red 192.168.1.0/24. Observe que R3 también tiene una subred 172.16.4.0/24 desconectada, o no contigua, de la red 172.16.0.0 que comparten R1 y R2. Los efectos de esta subred no contigua se examinarán luego en este capítulo cuando veamos el proceso de búsqueda de rutas.

**Haga clic en R1 y R3 en la figura.**

Las configuraciones de interfaz de R1 y R3 también se muestran en la figura. En una sección posterior, configuraremos las interfaces de R2.




```
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#interface Serial0/0/0
R1(config-if)#ip address 172.16.2.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#end
R1#copy run start
```

R1

```
R3(config)#interface FastEthernet0/0
R3(config-if)#ip address 172.16.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface Serial0/0/1
R3(config-if)#ip address 192.168.1.2 255.255.255.0
R3(config-if)#clock rate 64000
R3(config-if)#no shutdown
R3(config-if)#end
R3#copy run start
```

R3

### 8.1.2 ENTRADAS DE LA TABLA DE ENRUTAMIENTO.-

El ejemplo de la tabla de enrutamiento de la figura consta de entradas de ruta de los siguientes orígenes:

- Redes conectadas directamente
- Rutas estáticas
- Protocolos de enrutamiento dinámicos

El origen de la ruta no afecta la estructura de la tabla de enrutamiento. La figura muestra un ejemplo de tabla de enrutamiento con rutas dinámicas, estáticas y conectadas directamente. Observe que las subredes 172.16.0.0/24 tienen una combinación de los tres tipos de orígenes de enrutamiento.

Nota: La jerarquía de la tabla de enrutamiento en el IOS de Cisco se implementó originalmente con el esquema de enrutamiento con clase. Si bien la tabla de enrutamiento incorpora el direccionamiento con clase y sin clase, la estructura general aún se construye en base a este esquema con clase.

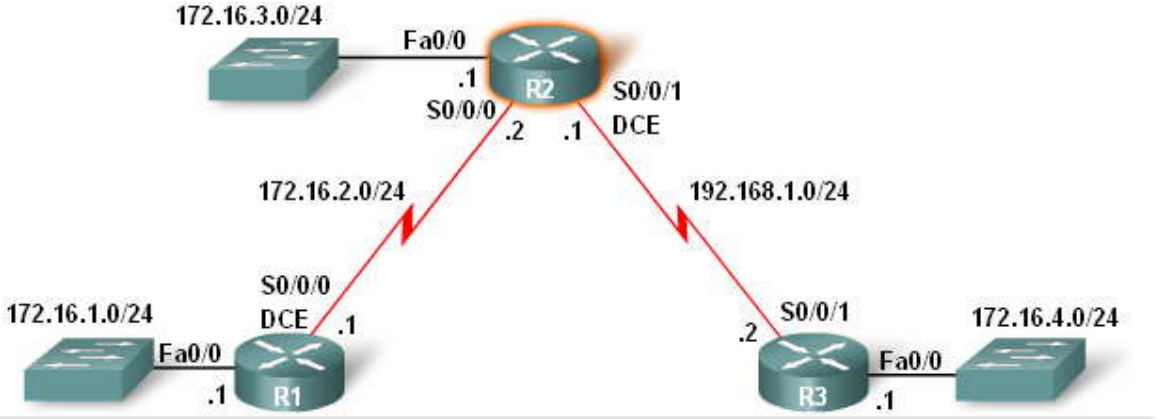
Tabla de enrutamiento de ejemplo

```
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
<output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 4 subnets
S       172.16.4.0 is directly connected, Serial0/0/1
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:08, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
     10.0.0.0/16 is subnetted, 1 subnets
S       10.1.0.0 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
S    192.168.100.0/24 is directly connected, Serial0/0/1
Router#
```

### 8.1.3 RUTAS DE NIVEL 1.-

Los routers R1 y R3 ya tienen sus interfaces configuradas con las direcciones IP y las máscaras de subred apropiadas. Ahora configuraremos las interfaces de R2 y usaremos debug ip routing para ver el proceso de la tabla de enrutamiento que se usa para agregar estas entradas.

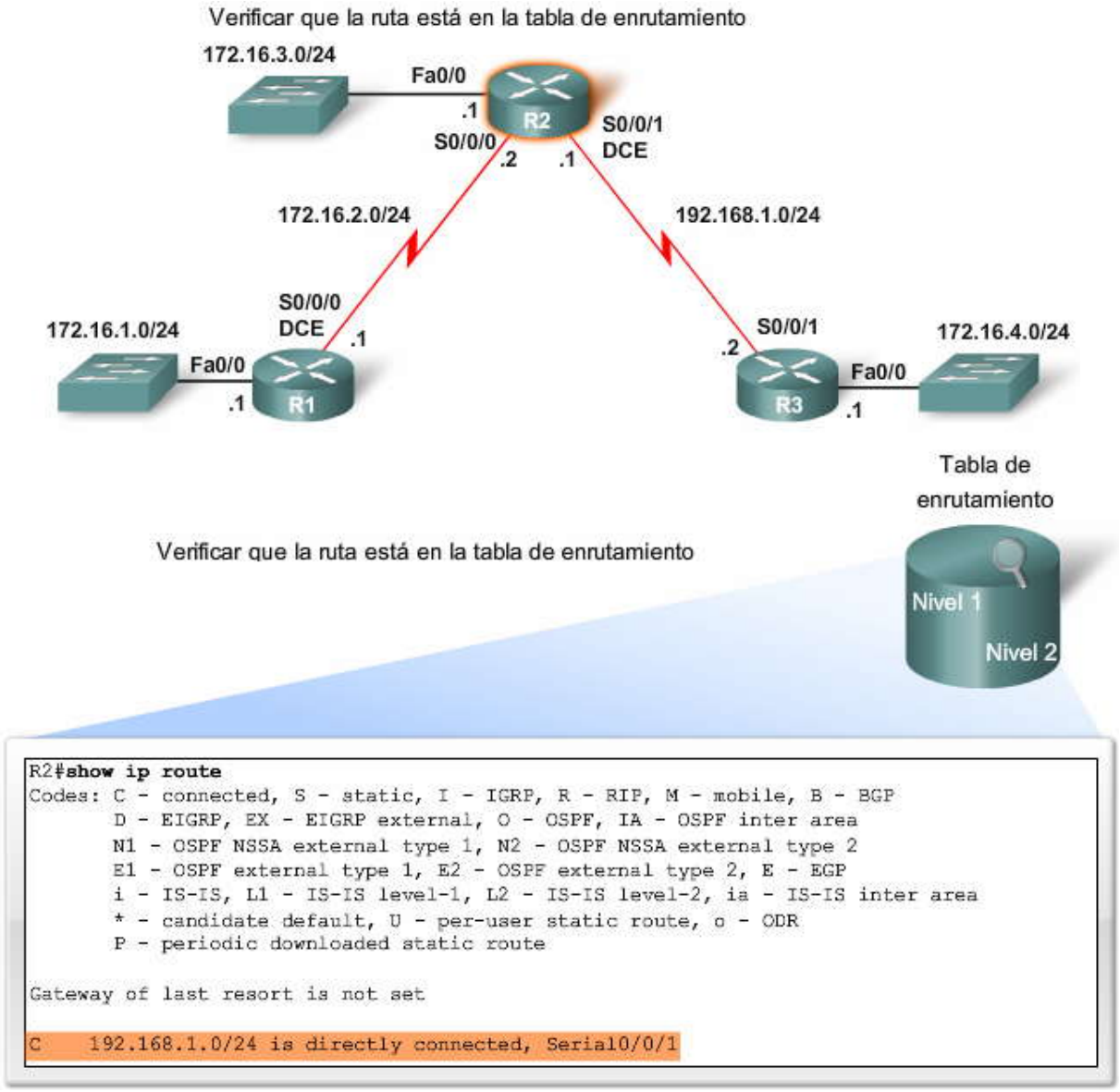
La figura muestra lo que sucede cuando la interfaz Serial 0/0/1 de R2 se configura con la dirección 192.168.1.1/24. Tan pronto como se ingresa no shutdown, el resultado de debug ip routing muestra que se ha agregado esta ruta a la tabla de enrutamiento.




```
R2#debug ip routing
IP routing debugging is on
R2#conf t
R2(config)#interface serial 0/0/1
R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#
00:11:06: %LINK-3-UPDOWN: Interface Serial0/0/1, changed state to up
R2(config-if)#
RT: add 192.168.1.0/24 via 0.0.0.0, connected metric [0/0]
RT: interface Serial 0/0/1 added to routing table
R2(config-if)#end
R2#undebug all
All possible debugging has been turned off
```

En la figura, show ip route muestra la red conectada directamente a la tabla de enrutamiento que recién agregamos a R2.

La tabla de enrutamiento IP de Cisco no es una base de datos plana. La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes. Dentro de esta estructura, la jerarquía incluye varios niveles. Para simplificar el tema, analizaremos todas las rutas en función de dos niveles: nivel 1 o nivel 2.




Aprendamos sobre las rutas de nivel 1 y de nivel 2 revisando la entrada de la tabla de enrutamiento con mayor detalle.

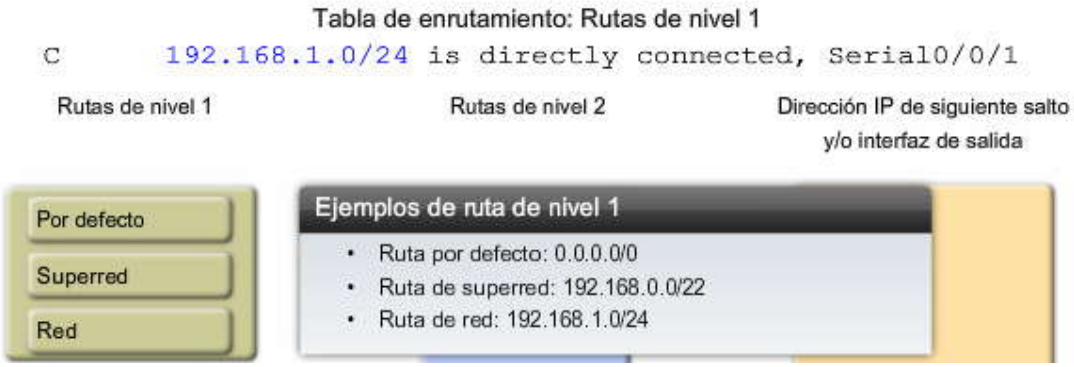
C 192.168.1.0/24 está conectada directamente, Serial0/0/1

**Una ruta de nivel 1 es una ruta con una máscara de subred igual o inferior a la máscara con clase de la dirección de red.** 192.168.1.0/24 es una ruta de red de nivel 1 porque la máscara de subred es igual a la máscara con clase de la red. /24 es la máscara con clase de las redes de clase C, tal como la red 192.168.1.0.

Una ruta de nivel 1 puede funcionar como:

- Ruta por defecto: una ruta por defecto es una ruta estática con la dirección 0.0.0.0/0.
- Ruta de superred: una ruta de superred es una dirección de red con una máscara menor que la máscara con clase.
- Ruta de red: una ruta de red es una ruta que tiene una máscara de subred igual a la de la máscara con clase. Una ruta de red también puede ser una ruta principal. Las rutas principales se analizarán en la siguiente sección.

El origen de la ruta de nivel 1 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico.




**Ruta final**

La ruta 192.168.1.0/24 de nivel 1 también se puede definir como una ruta final. Una ruta final es una ruta que incluye:
una dirección IP del siguiente salto (otra ruta)
y/o una interfaz de salida

La red 192.168.1.0/24 conectada directamente es una ruta de red de nivel 1 porque tiene una máscara de subred que es igual a su máscara con clase. Esta misma ruta también es una ruta final porque contiene la interfaz de salida Serial 0/0/1.

C 192.168.1.0/24 está conectada directamente, Serial0/0/1

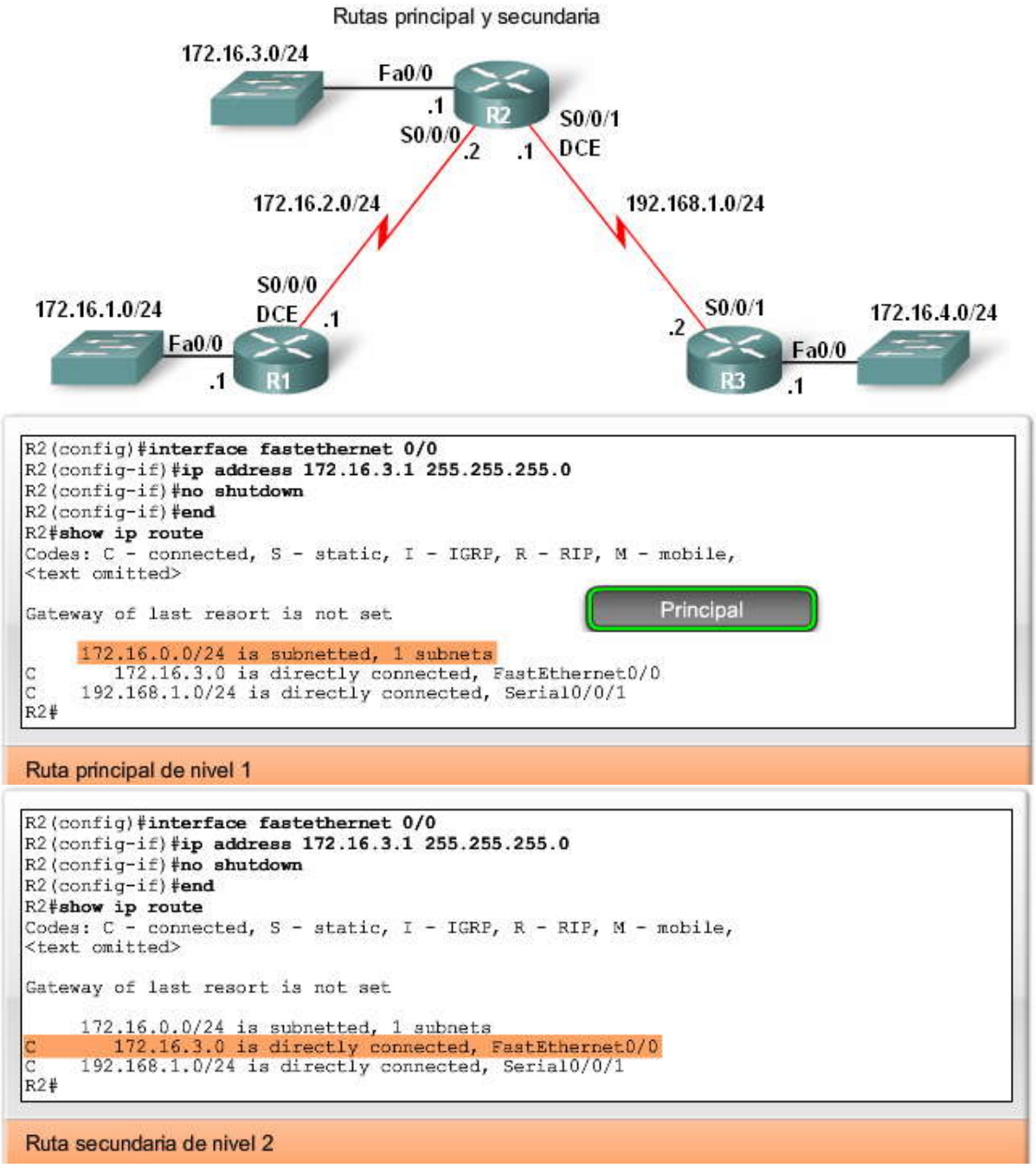
En el siguiente tema, veremos que las rutas de nivel 2 también son rutas finales.


### 8.1.4 RUTAS PRINCIPALES Y SECUNDARIAS: REDES CONCLASE.-

En el tema anterior, vimos una ruta de red de nivel 1 que también era una ruta final. Ahora analicemos otro tipo de ruta de red de nivel 1, una ruta principal. La figura muestra la configuración de la interfaz 172.16.3.1/24 en R2 y el resultado del comando show ip route. Observe que, en realidad, hay dos entradas adicionales en la tabla de enrutamiento. Una entrada es la ruta principal y la otra entrada es la ruta secundaria. ¿Por qué hay dos entradas en lugar de una?

Haga clic en Principal y secundaria en la figura.

Cuando la máscara de subred 172.16.3.0 se agregó a la tabla de enrutamiento, también se agregó otra ruta, la 172.16.0.0. La primera entrada, 172.16.0.0/24, no contiene ninguna dirección IP de siguiente salto ni información de la interfaz de salida. Esta ruta se conoce como ruta principal de nivel 1.



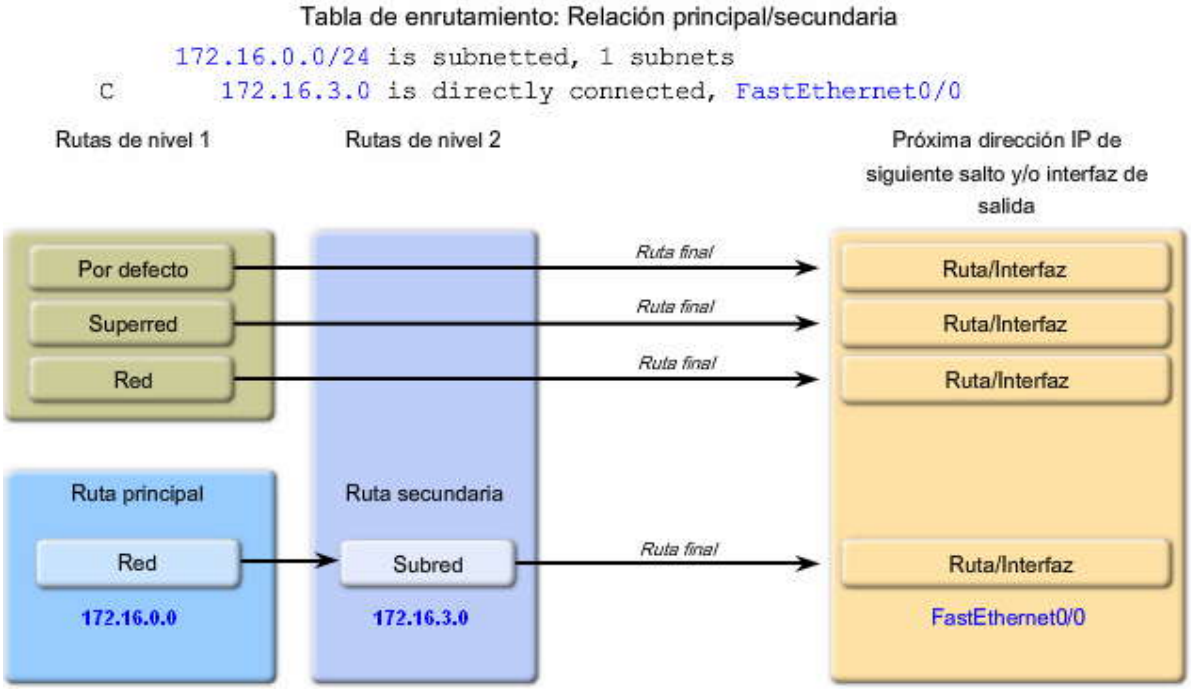

**Una ruta principal de nivel 1 es una ruta de red que no contiene ninguna dirección IP del siguiente salto ni ninguna interfaz de salida para ninguna red.** Una ruta principal es, en realidad, un encabezado que indica la presencia de rutas de nivel 2, también conocidas como rutas secundarias. Una ruta principal de nivel 1 se crea automáticamente cuando se agrega una subred en la tabla de enrutamiento. Es decir que una ruta principal se crea siempre que se ingresa en la tabla de enrutamiento una ruta con una máscara más grande que la máscara con clase. La subred es la ruta secundaria de nivel 2 de la ruta primaria. En este caso, la ruta principal de nivel 1 que se creó automáticamente es:

172.16.0.0/24 está dividida en subredes, subredes 1

**Una ruta de nivel 2 es una ruta que es una subred de una dirección de red con clase.** Al igual que las rutas de nivel 1, el origen de una ruta de nivel 2 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico. En este caso, la ruta de nivel 2 es la ruta de subred real que se agregó a la red cuando configuramos la interfaz FastEthernet 0/0:

C 172.16.3.0 está conectada directamente, FastEthernet0/0

Nota: Recuerde que la jerarquía de la tabla de enrutamiento en el IOS de Cisco tiene un esquema de enrutamiento con clase. Una ruta principal de nivel 1 es la dirección de red con clase de la ruta de subred. Esto es así incluso si un protocolo de enrutamiento sin clase es el origen de la ruta de subred.




**Haga clic en Reproducir para ver la animación.**

Analicemos las entradas de la tabla de enrutamiento para la ruta principal de nivel 1 y la ruta secundaria de nivel 2 (subred)

**Ruta principal de nivel 1**

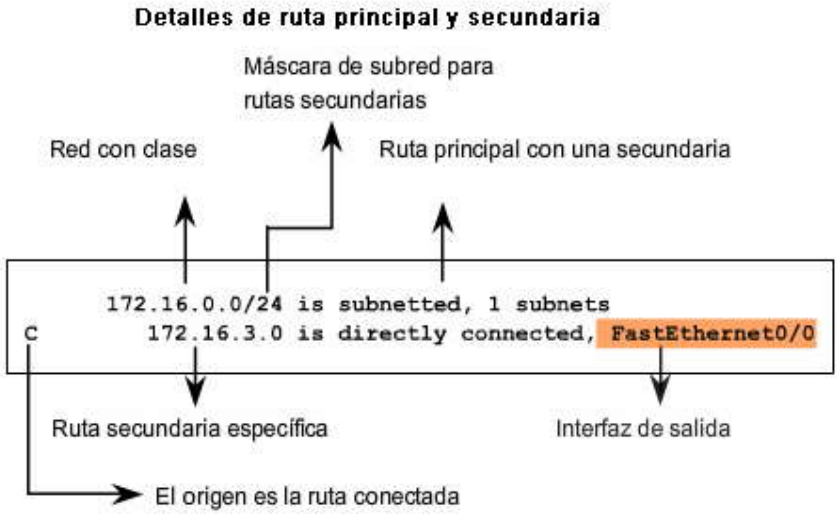
Esta ruta principal contiene la siguiente información:
172.16.0.0: la dirección de red con clase para nuestra subred. Recuerde que la tabla de enrutamiento IP de Cisco está estructurada con clase.
/24: la máscara de subred para todas las rutas secundarias. Si las rutas secundarias tienen máscaras de subred de longitud variable (VLSM), la máscara de subred se excluirá de la ruta principal y se incluirá en las rutas secundarias individuales. Esto se analizará en una sección posterior.
está dividida en subredes, 1 subred: esta parte de la ruta especifica que ésta es una ruta principal y, en este caso, tiene una ruta secundaria, es decir, una subred.

**Ruta secundaria de nivel 2**

La entrada secundaria, 172.16.3.0, es la ruta real para nuestra red conectada directamente. Ésta es una ruta de nivel 2, también conocida como ruta secundaria, y contiene la siguiente información:
C: el código de ruta para una red conectada directamente.
172.16.3.0: la entrada de ruta específica.
está conectada directamente: junto con el código de ruta de C, especifica que ésta es una red conectada directamente con una distancia administrativa de 0.
FastEthernet0/0: la interfaz de salida para reenviar los paquetes que coinciden con esta entrada de ruta específica.

La ruta secundaria de nivel 2 es la entrada de ruta específica para la subred 172,16.3.0/24. Observe que la máscara de subred no está incluida en la subred, la ruta secundaria de nivel 2. La máscara de subred para esta ruta secundaria (subred) es la máscara /24 incluida en su ruta principal, 172.16.0.0.

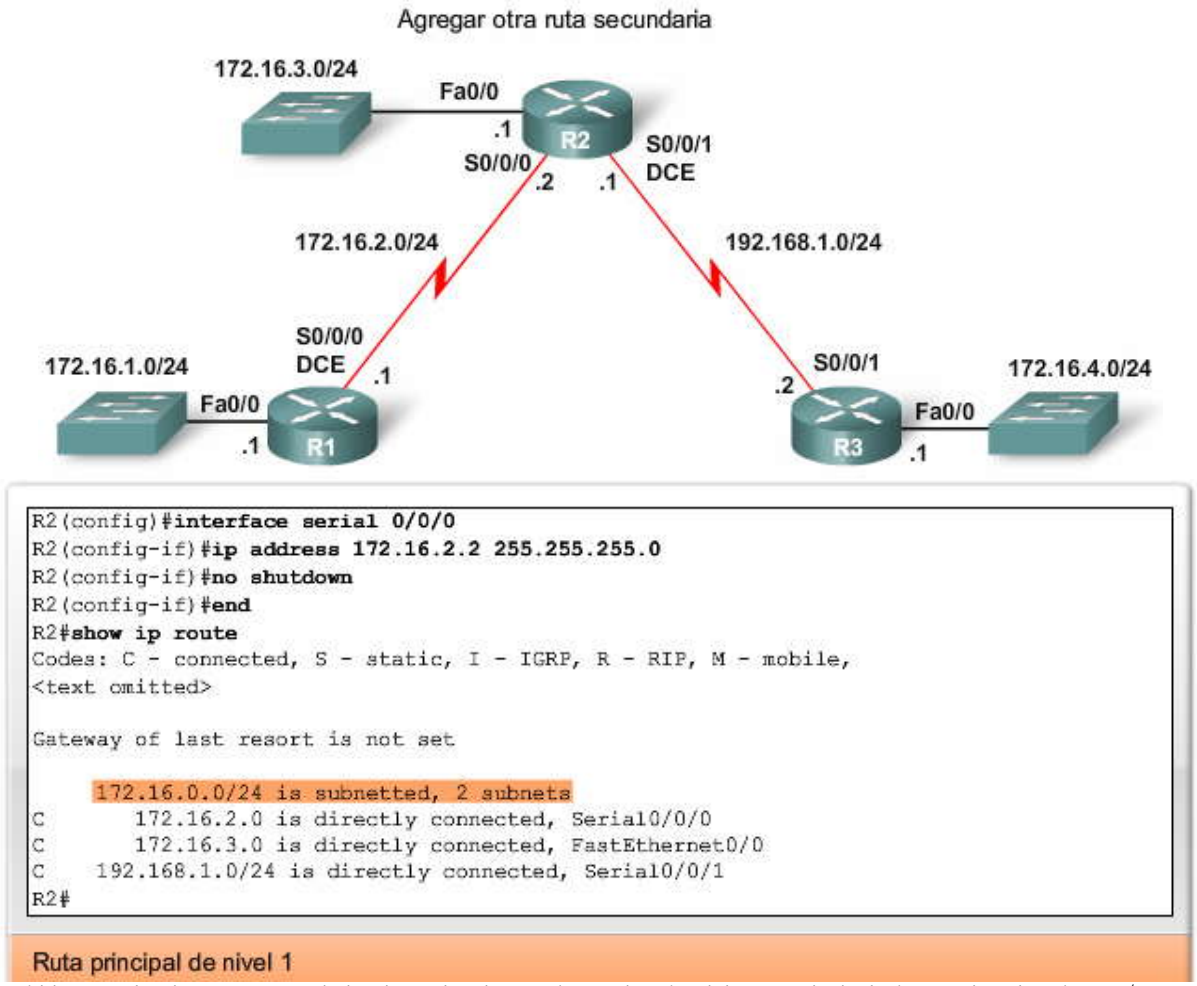
Las rutas secundarias de nivel 2 contienen el origen de la ruta y la dirección de red de la ruta. Las rutas secundarias de nivel 2 también se consideran rutas finales porque contienen la dirección IP del siguiente salto y/o la interfaz de salida.




La figura muestra la configuración de la interfaz Serial 0/0/0 en R2.

Haga clic en 2 y 3 en la figura.

La tabla de enrutamiento muestra dos rutas secundarias para la misma ruta principal 172.16.0.0/24. Tanto 172.16.2.0 como 172.16.3.0 son miembros de la misma ruta principal, porque son miembros de la red con clase 1 72.16.0.0/16.

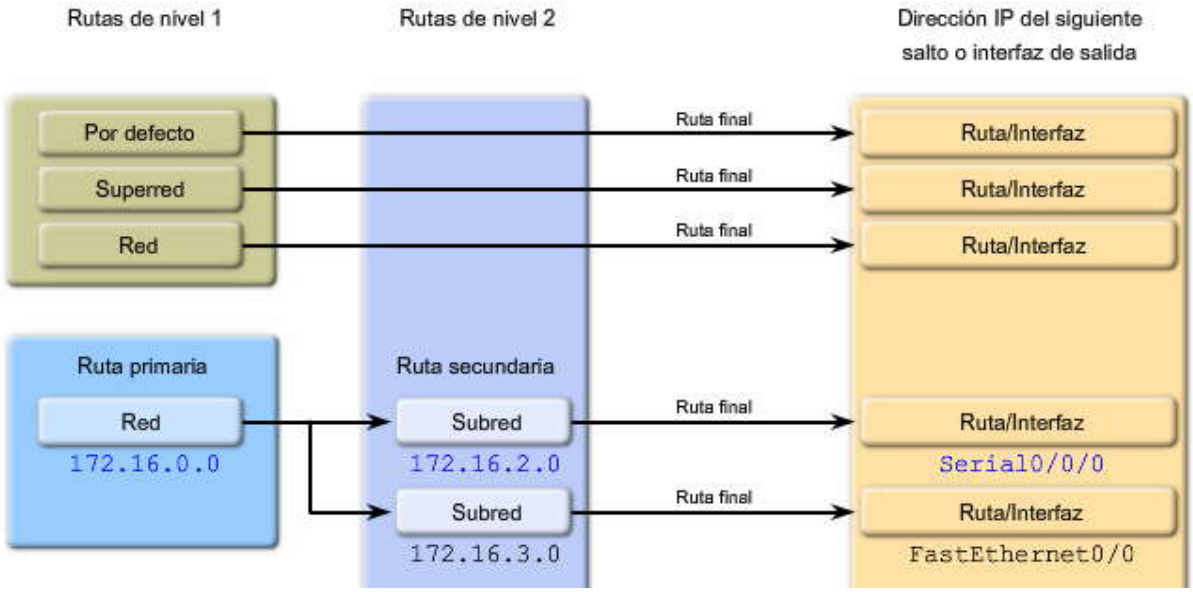



Debido a que las dos rutas secundarias tienen la misma máscara de subred, la ruta principal aún mantiene la máscara /24, pero ahora muestra 2 subredes. El rol de la ruta principal se examinará cuando analicemos el proceso de búsqueda de rutas.

Nota: Si hay una sola ruta secundaria de nivel 2 y esa ruta se retira, la ruta principal de nivel 1 se eliminará automáticamente. Una ruta principal de nivel 1 existe sólo cuando hay al menos una ruta secundaria de nivel 2.

Tabla de enrutamiento: Relación principal/secundaria

```
    172.16.0.0/24 is subnetted, 2 subnets
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
```




### 8.1.5 RUTAS PRINCIPALES Y SECUNDARIAS: REDES SIN CLASE.-

Para esta discusión, usaremos la topología que se muestra en la figura. Si usamos el RouterX con la configuración VLSM que se muestra, podemos examinar el efecto de VLSM en la tabla de enrutamiento. El RouterX tiene tres redes conectadas directamente. Las tres subredes pertenecen a la red con clase 172.16.0.0/16 y son, por lo tanto, rutas secundarias de nivel 2.

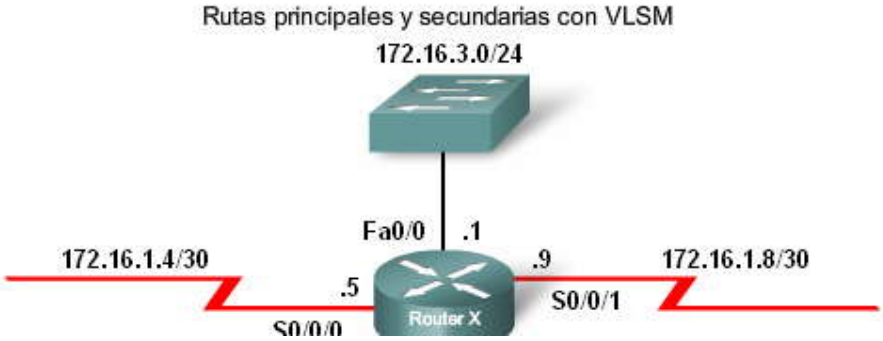
**Haga clic en 2, 3 y 4 en la figura.**

Observe que nuestras rutas secundarias no comparten la misma máscara de subred, como en el caso del ejemplo con clase. En este caso, implementamos un esquema de direccionamiento de red con VLSM.

**Haga clic en la figura.**

Siempre que haya dos o más rutas secundarias con máscaras de subred diferentes que pertenecen a la misma red con clase, la tabla de enrutamiento presentará una visión ligeramente distinta que indica que esta red principal se encuentra dividida en redes en forma variable.

Aunque la relación principal/secundaria utiliza una estructura con clase para mostrar las redes y sus subredes, este formato puede utilizarse con el direccionamiento con clase y sin clase. Sin importar el esquema de direccionamiento que use la red (sin clase o con clase), la tabla de enrutamiento usará el esquema con clase.



```
RouterX#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
<output omitted>

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.4/30 is directly connected, Serial0/0/0
C       172.16.1.8/30 is directly connected, Serial0/0/1
C       172.16.3.0/24 is directly connected, FastEthernet0/0
RouterX#
```

Ruta principal de nivel 1

**Haga clic en Reproducir para ver la animación.**

Comparado con el ejemplo de rutas con clase que se analizó anteriormente, hay varias diferencias visibles con esta ruta principal y sus rutas secundarias. Primero, la ruta principal de 172.16.0.0 ahora contiene la máscara con clase /16. En el ejemplo de rutas con clase anterior, la máscara con clase no se mostró.

También observe que la ruta principal establece que las rutas secundarias están "divididas en redes en forma variable". Al igual que el ejemplo con clase, la ruta principal muestra la cantidad de subredes, pero ahora también incluye la cantidad de máscaras de rutas secundarias diferentes.

La diferencia final entre las redes con clase y sin clase radica en las rutas secundarias. Cada ruta secundaria ahora contiene la máscara de subred para esa ruta específica. En el ejemplo sin VLSM, las dos rutas secundarias compartían la misma máscara de subred y la principal mostraba su máscara de subred común. Con VLSM, las distintas máscaras de subred se muestran con las rutas secundarias específicas.

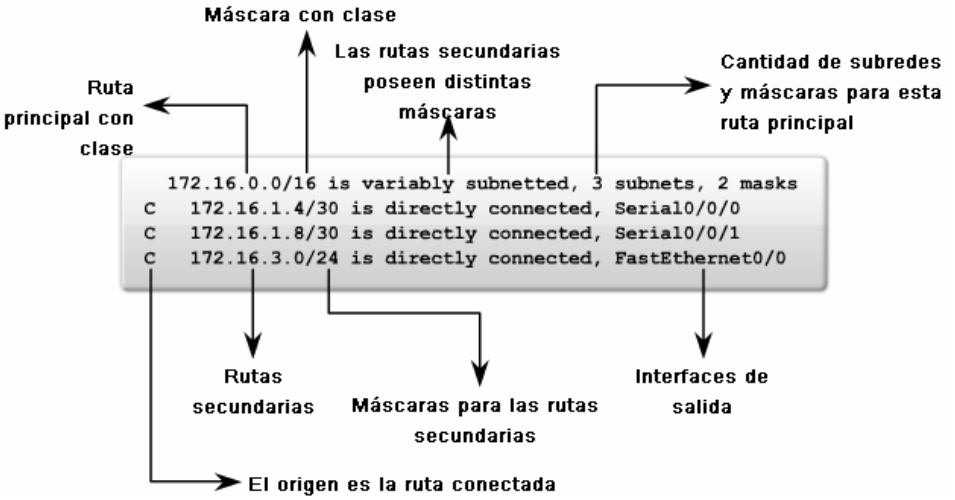
La ruta principal contiene la siguiente información:

- 172.16.0.0: la ruta principal, la dirección de red con clase relacionada con todas las rutas secundarias.
- /16: la máscara de subred con clase de la ruta principal.
- divididas en redes en forma variable: indica que las rutas secundarias están divididas en redes en forma variable y que hay varias máscaras para esta red con clase.
- 3 subredes, 2 máscaras: indica la cantidad de subredes y la cantidad de máscaras de subred distintas para las rutas secundarias de esta ruta principal.

Si usamos una de las rutas secundarias como ejemplo, podremos ver la siguiente información:

- C: el código de ruta para una red conectada directamente.
- 172.16.1.4: la entrada de ruta específica.
- /30: la máscara de subred para esta ruta específica.
- está conectada directamente: junto con el código de ruta de C, especifica que ésta es una red conectada directamente con una distancia administrativa de 0.
- Serial0/0/0: la interfaz de salida para reenviar los paquetes que coinciden con esta entrada de ruta específica.

Por lo tanto, ¿por qué Cisco usa el formato de tabla de enrutamiento con clase? Comprenderemos la respuesta a esta pregunta en las siguientes secciones, cuando analicemos el proceso de búsqueda de rutas.



## 8.2 PROCESO DE BUSQUEDA EN LA TABLA DE ENRUTAMIENTO.-

### 8.2.1 PASOS EN EL PROCESO DE BUSQUEDA DE RUTAS.-

En esta topología, RIPv1, un protocolo de enrutamiento con clase, está ahora configurado. Observe que hemos elegido específicamente un protocolo de enrutamiento con clase con nuestras subredes 172.16.0.0 no contiguas. El motivo se hará evidente en una sección posterior.

**Haga clic en los botones de la figura para revisar la configuración de RIP y las tablas de enrutamiento resultantes.**

Como se supone que sucedería con este esquema de direccionamiento y con los protocolos de enrutamiento con clase, hay problemas con la posibilidad de conexión. Ni R1 ni R2 tienen una ruta hacia 172.16.4.0. R3 tampoco tiene rutas a las subredes 172.16.1.0/24, 172.16.2.0/24 ó 172.16.3.0/24.

Examinemos en mayor profundidad cómo los routers determinan cuáles son las mejores rutas para usar al enviar paquetes y por qué los protocolos de enrutamiento con clase no funcionan con diseños no contiguos. Consideraremos:

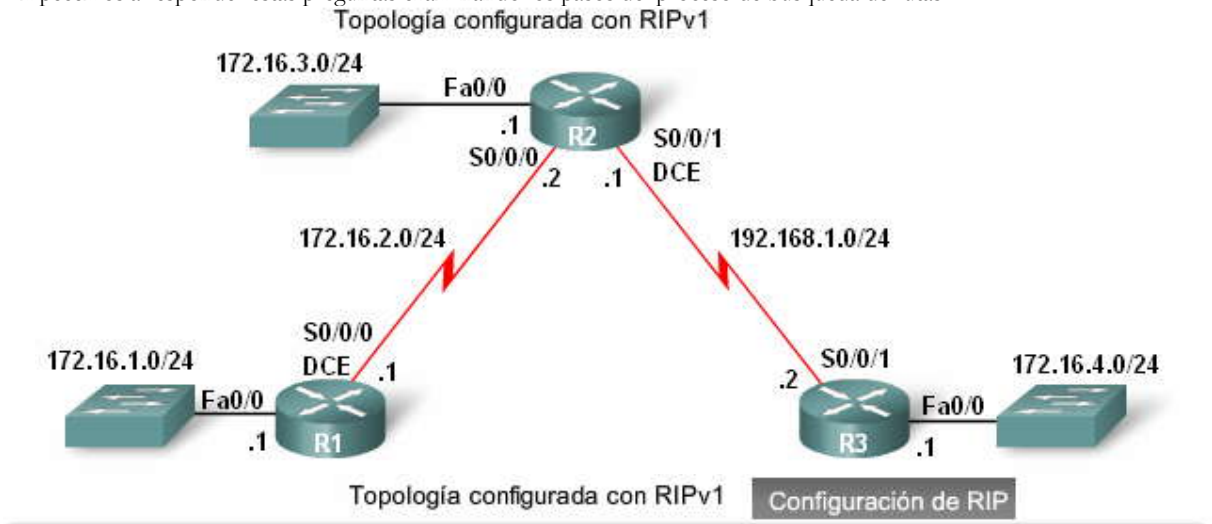
1. ¿Qué sucede cuando un router recibe un paquete IP, examina la dirección IP de destino y busca esa dirección en la tabla de enrutamiento?

2. ¿Cómo decide el router qué ruta de la tabla de enrutamiento es la mejor coincidencia?

3. ¿Qué efecto tiene la máscara de subred en el proceso de búsqueda de la tabla de enrutamiento?

4. ¿Cómo decide el router si usa una superred o una ruta por defecto si no encuentra una coincidencia mejor?

Empecemos a responder estas preguntas examinando los pasos del proceso de búsqueda de rutas.




```
R1(config)#router rip
R1(config-router)#network 172.16.0.0
```

```
R2(config)#router rip
R2(config-router)#network 172.16.0.0
R2(config-router)#network 192.168.1.0
```

```
R3(config)#router rip
R3(config-router)#network 172.16.0.0
R3(config-router)#network 192.168.1.0
```

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
R       172.16.3.0 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
R    192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
```

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:07, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
```

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.4.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
```

**Proceso de búsqueda de rutas**

Siga estos pasos en la figura para ver el proceso de búsqueda de rutas. No se preocupe si no comprende completamente los pasos en este momento. Entenderá mejor este proceso cuando examinemos algunos ejemplos de las siguientes secciones.

**Haga clic en Paso 1.**

El router examina las rutas de nivel 1, incluidas las rutas de red y las rutas de superred, en busca de la mejor coincidencia con la dirección IP de destino del paquete.

**Haga clic en Paso 1a.**

Si la mejor coincidencia es una ruta final de nivel 1 (superred, red con clase o ruta por defecto) esta ruta se usa para reenviar el paquete.

**Haga clic en Paso 1b.**

Si la mejor coincidencia es una ruta principal de nivel 1, continúe con el Paso 2.

**Haga clic en Paso 2.**

El router examina las rutas secundarias (las rutas de subred) de la ruta principal en busca de una mejor coincidencia.

**Haga clic en Paso 2a.**

Si hay una coincidencia con una ruta secundaria de nivel 2, esa subred se usará para reenviar el paquete.

**Haga clic en Paso 2b.**

Si no hay coincidencia con ninguna de las rutas secundarias de nivel 2, continúe con el Paso 3. ¿El router está implementando un comportamiento de enrutamiento con clase o sin clase?

**Haga clic en Paso 3a.**

Comportamiento del enrutamiento con clase: Si el comportamiento del enrutamiento con clase está en vigencia, termine el proceso de búsqueda y descarte el paquete.

**Haga clic en Paso 3b.**

Comportamiento del enrutamiento sin clase: Si el comportamiento de enrutamiento sin clase está en vigencia, continúe buscando las rutas de superred de nivel 1 en la tabla de enrutamiento para ver si hay alguna coincidencia, incluida la ruta por defecto, si así fuera.

**Haga clic en Paso 4.**

Si ahora hay una coincidencia menor con las rutas por defecto o de superred de nivel 1, el router usa esa ruta para reenviar el paquete.

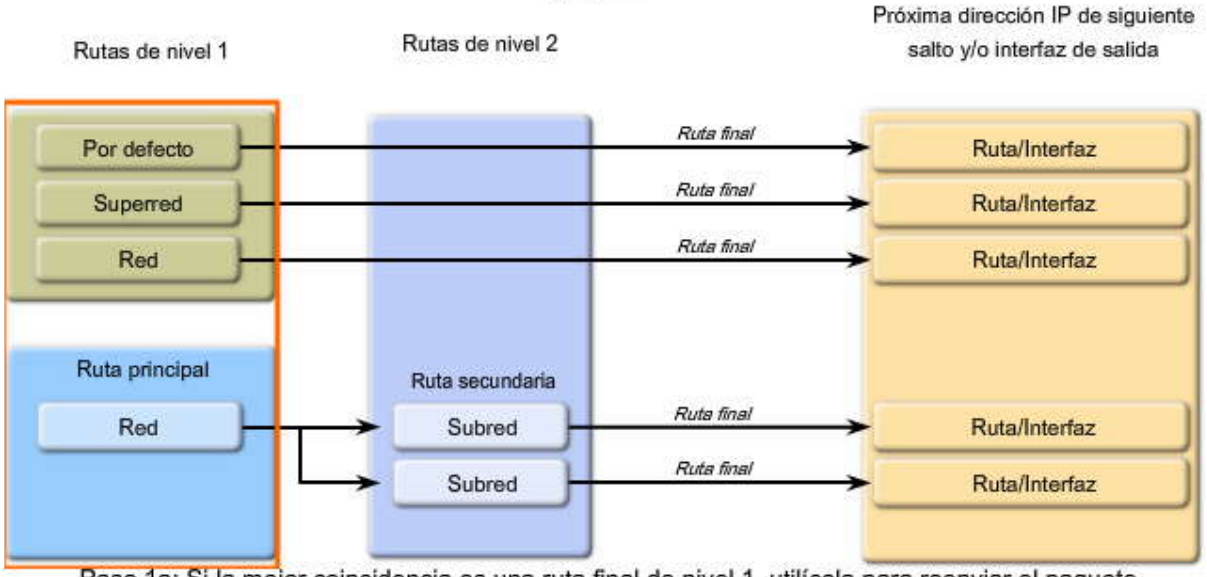
**Haga clic en Paso 5.**

Si no hay coincidencia con ninguna ruta de la tabla de enrutamiento, el router descarta el paquete.

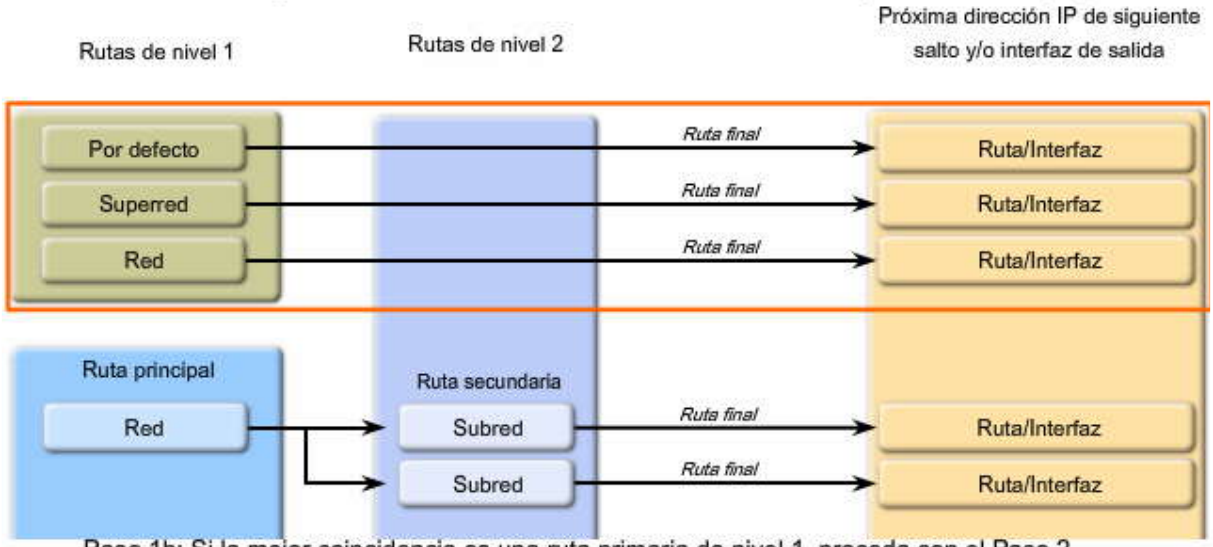
El comportamiento del enrutamiento con clase y sin clase se analizará con mayor detalle en una sección posterior.

**Nota:** Una ruta que sólo hace referencia a una dirección IP de siguiente salto y no a una interfaz de salida debe resolverse con una ruta con una interfaz de salida. Se realiza una búsqueda recurrente en la dirección IP del siguiente salto hasta que la ruta se resuelva con una interfaz de salida.

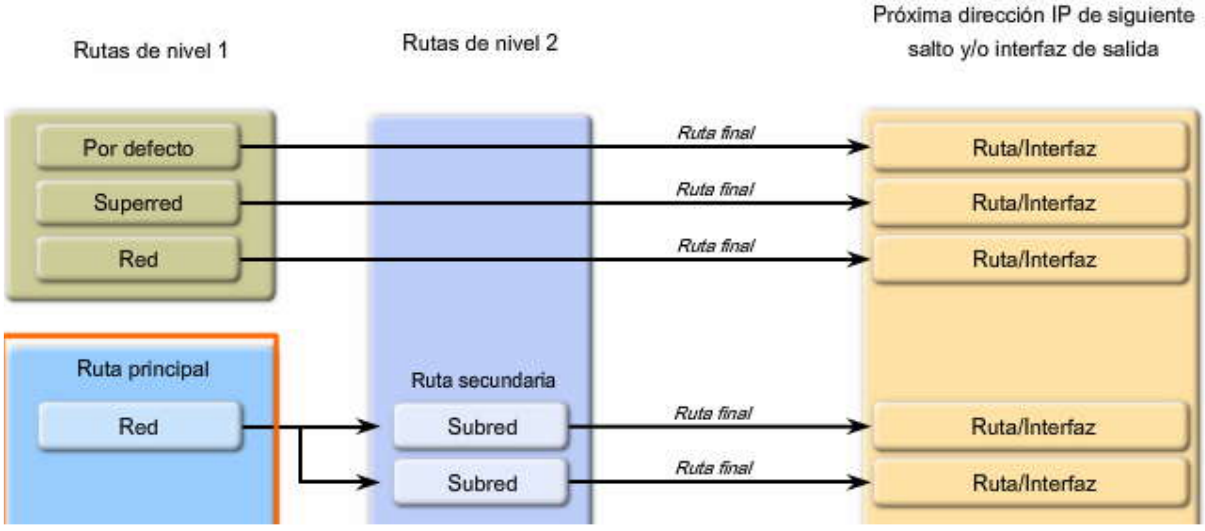
Paso 1: Examine las rutas del nivel 1 para lograr una mejor coincidencia con la dirección de destino del paquete.



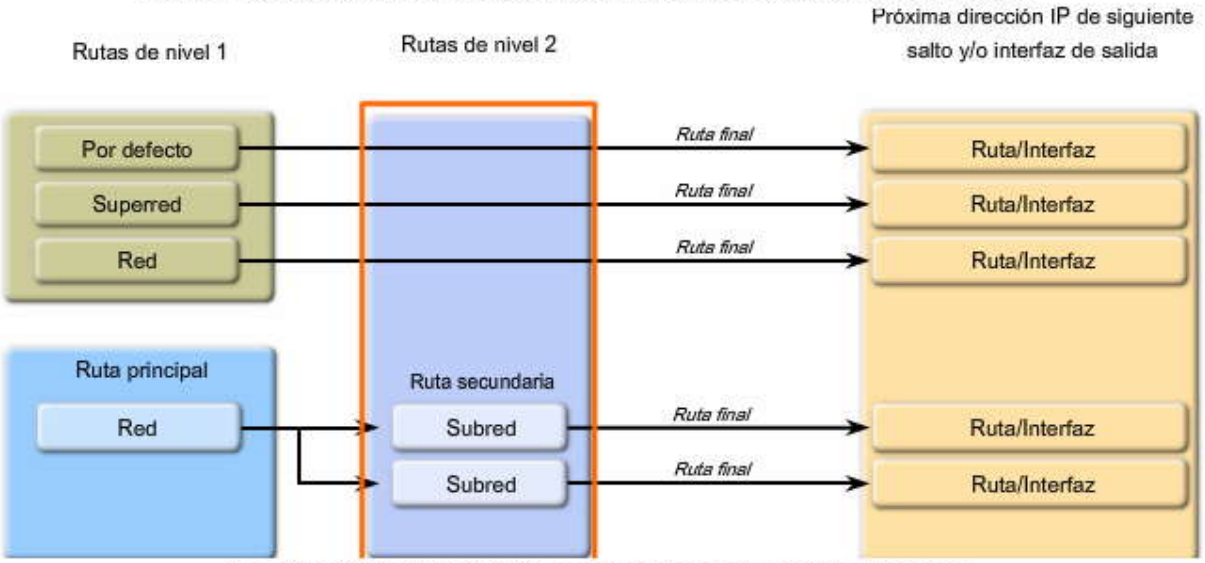

Paso 1a: Si la mejor coincidencia es una ruta final de nivel 1, utilícela para reenviar el paquete.



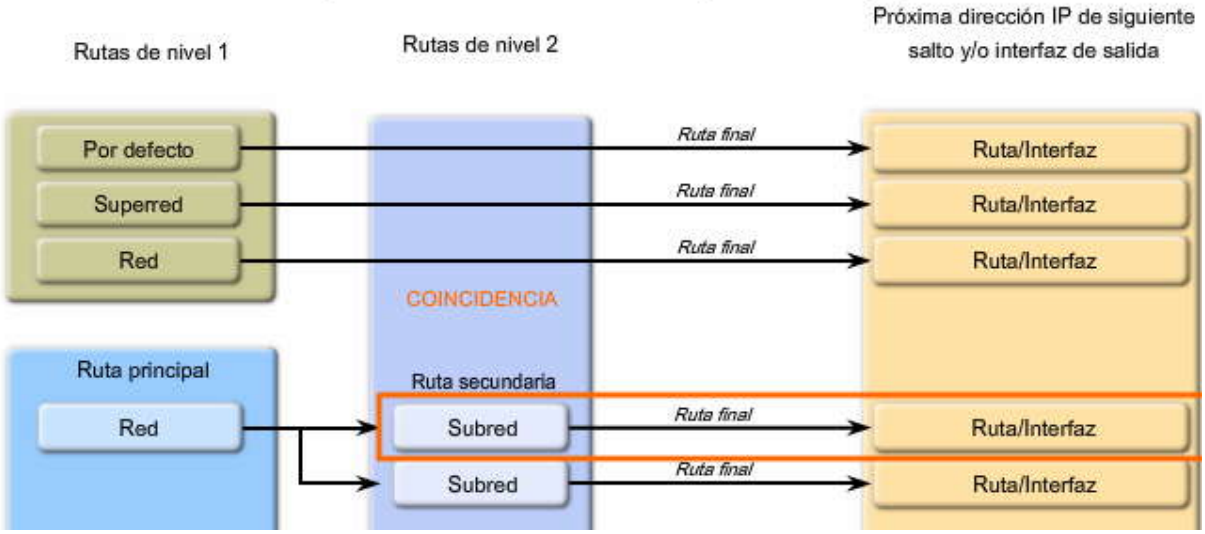

Paso 1b: Si la mejor coincidencia es una ruta primaria de nivel 1, proceda con el Paso 2.



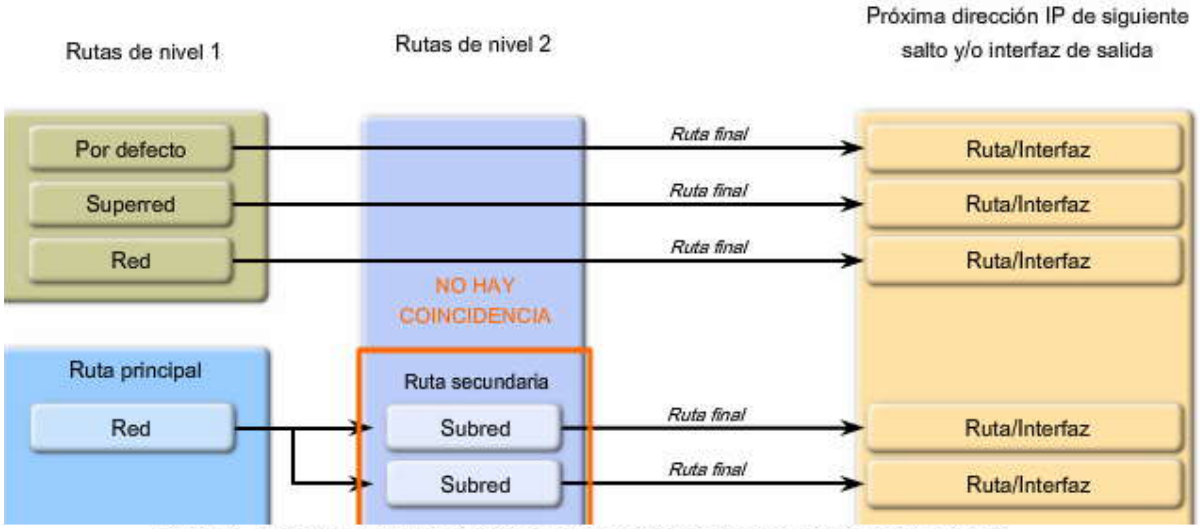
Paso 2: Las rutas secundarias se examinan para lograr una mejor coincidencia.



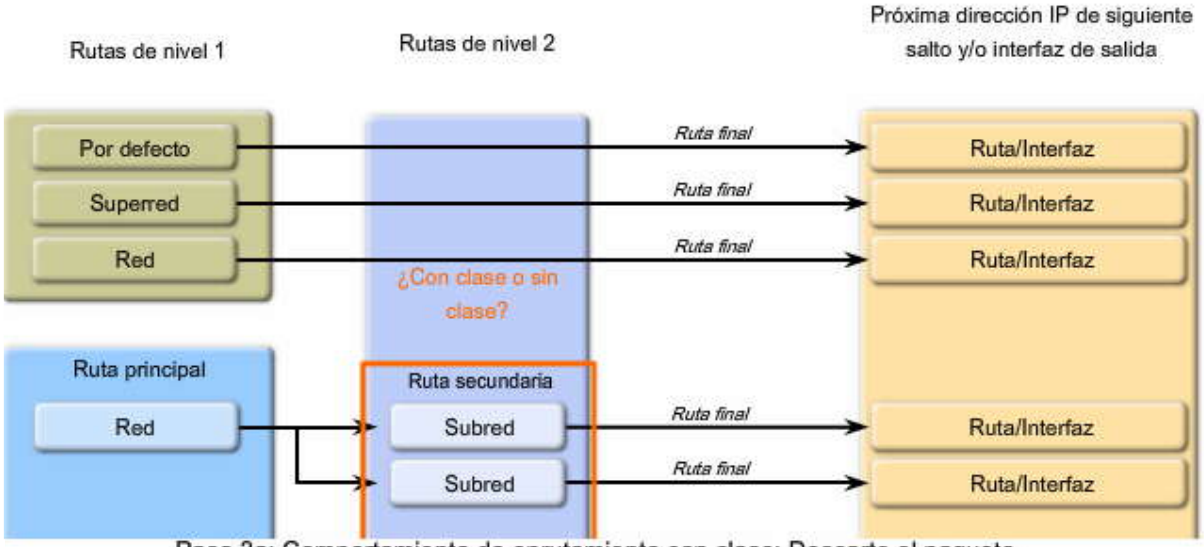

Paso 2a: ¡Coincidencia! Utilice esta subred para enviar el paquete.



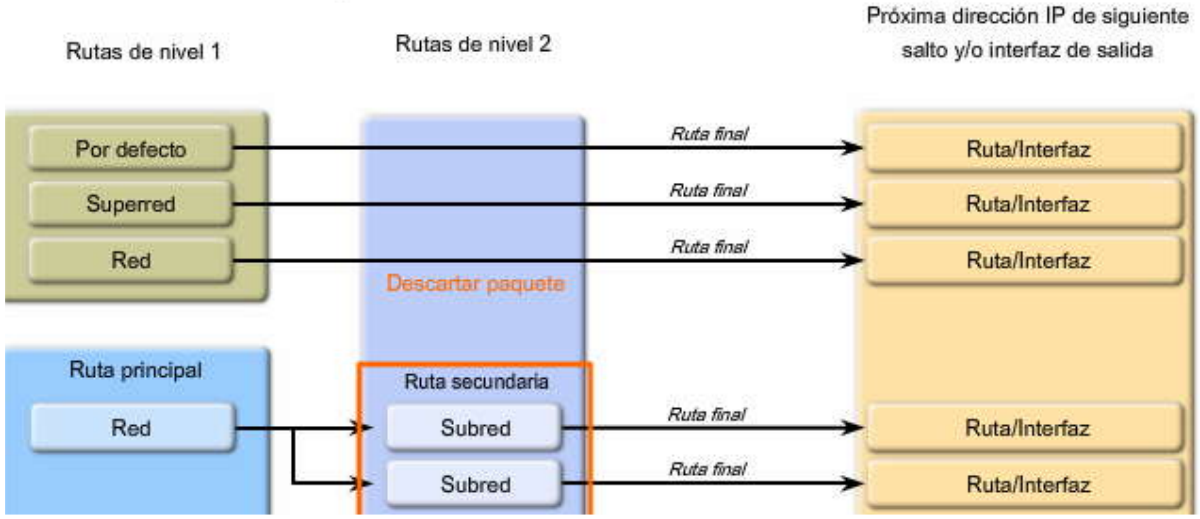
Paso 2b: No hay coincidencia. Proceda con el Paso 3.



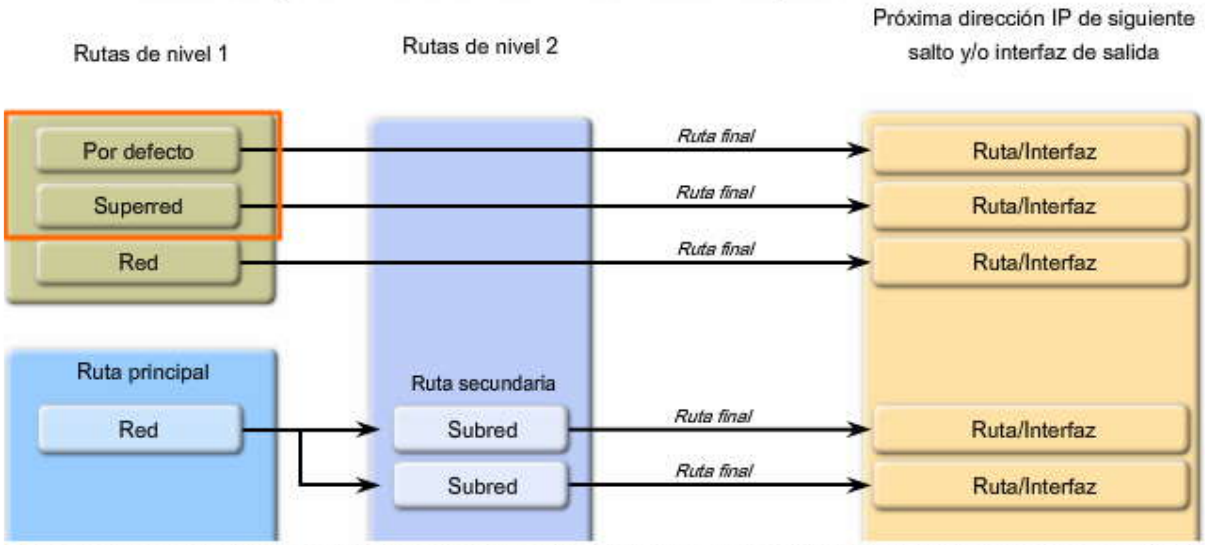

Paso 3: ¿Existe un comportamiento de enrutamiento con clase o sin clase?



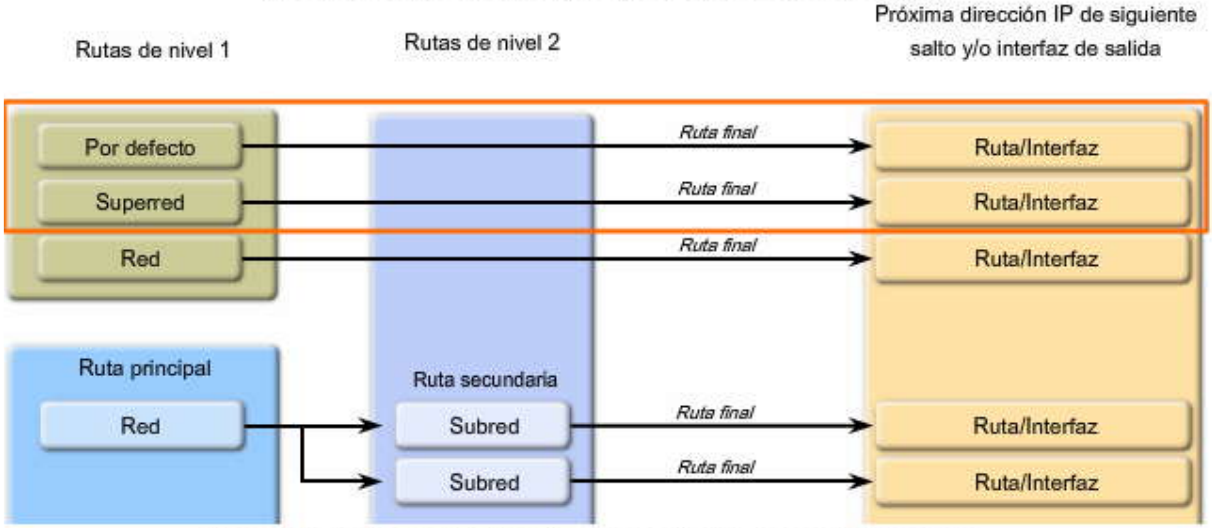

Paso 3a: Comportamiento de enrutamiento con clase: Descarte el paquete



Paso 3b: Comportamiento de enrutamiento sin clase: Busque las rutas del nivel 1

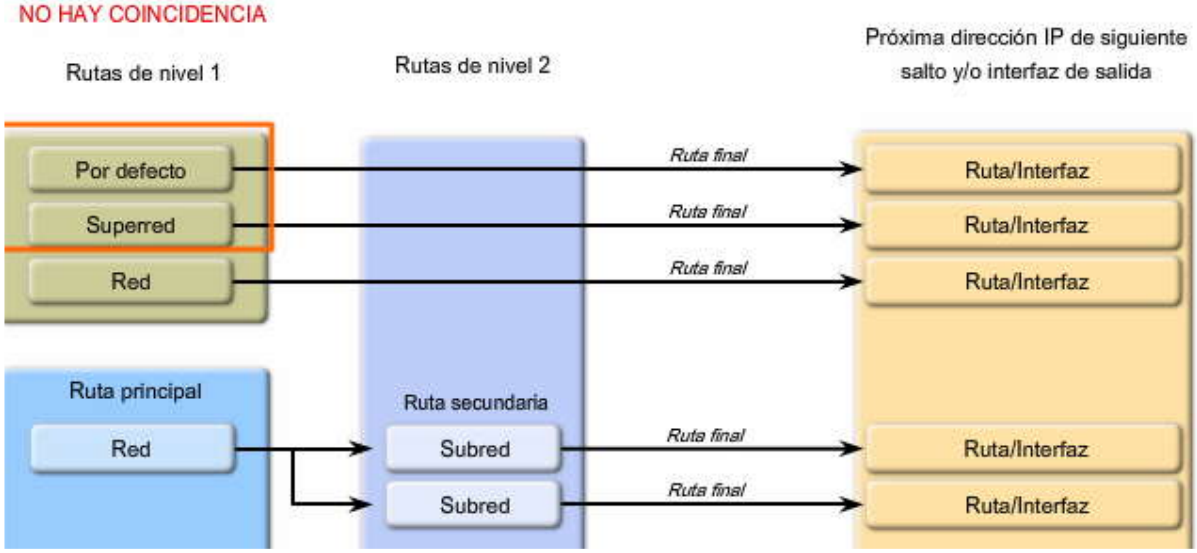



Paso 4: Haga coincidir con superred o por defecto. Utilícela para reenviar el paquete. Primero se verifican las superredes, luego las que son por defecto si es necesario.




Paso 5: No hay coincidencia. No es por defecto. Descarte el paquete.

NO HAY COINCIDENCIA



### 8.2.2 LA COINCIDENCIA MAS LARGA: RUTAS DE VINEL 1.-

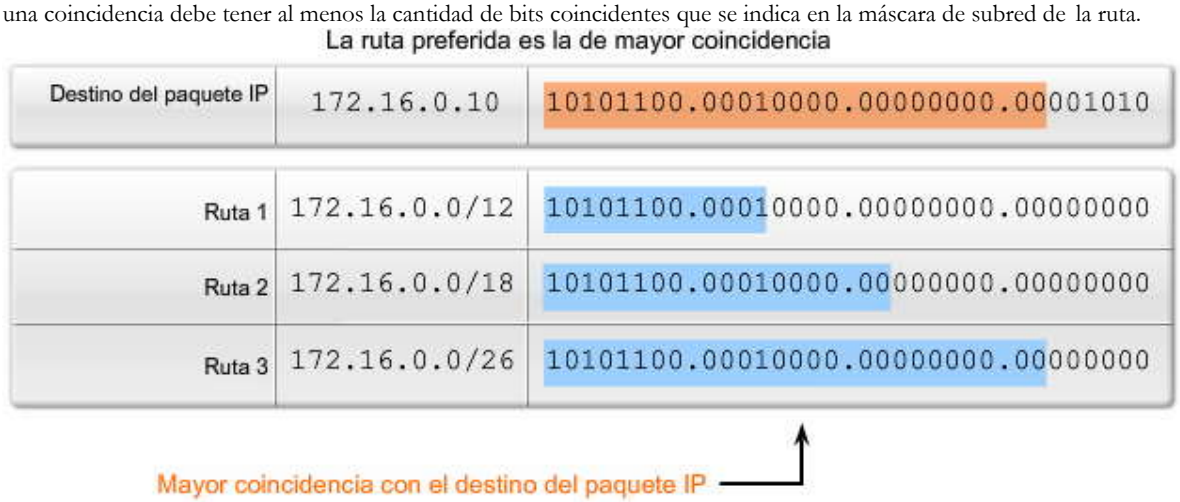
**La coincidencia más larga**

El término mejor coincidencia se usó en el análisis anterior sobre búsqueda de rutas. ¿Qué significa mejor coincidencia? La mejor coincidencia también se denomina coincidencia más larga.

Pero primero, ¿qué es una coincidencia? Para que haya una coincidencia entre la dirección IP de destino de un paquete y una ruta en la tabla de enrutamiento, un número mínimo de los bits que se encuentran más a la izquierda deben coincidir con la dirección IP del paquete y la ruta en la tabla de enrutamiento. La máscara de subred de la ruta en la tabla de enrutamiento se usa para determinar el número mínimo de bits que se encuentran más a la izquierda y que deben coincidir. (Recuerde que un paquete IP sólo contiene la dirección IP y no la máscara de subred).

La mejor coincidencia o la coincidencia más larga es la ruta de la tabla de enrutamiento que contiene la mayor cantidad de bits que se encuentran más a la izquierda y que más coinciden con la dirección IP de destino del paquete. **La ruta con la mayor cantidad de bits equivalentes, que se encuentran más a la izquierda, o la coincidencia más larga es siempre la ruta preferida.**

Por ejemplo, en la figura, tenemos un paquete destinado a 172.16.0.10. Muchas rutas posibles pueden coincidir con este paquete. Se muestran tres rutas posibles que sí coinciden con este paquete: 172.16.0.0/12, 172.16.0.0/18 y 172.16.0.0/26. De las tres rutas, 172.16.0.0/26 tiene la coincidencia más larga. Recuerde que para que cualquiera de estas rutas se considere una coincidencia debe tener al menos la cantidad de bits coincidentes que se indica en la máscara de subred de la ruta.




**Ejemplo: Ruta final de nivel 1**

La máscara de subred que se usa para determinar la coincidencia más larga no siempre es obvia. Examinemos este concepto más en detalle, usando varios ejemplos.

**Haga clic en Reproducir para ver la animación.**

En este ejemplo, la PC1 envía un ping a 192.168.1.2, la interfaz en R3. R1 recibe el paquete.

**Haga clic en Información de ruta y luego en Tabla de enrutamiento de R1 en la figura.**

¿Recuerda la primera parte del Paso 1 en el proceso de búsqueda de rutas? La figura ilustra este paso.

**Haga clic en Paso 1 en la figura.**

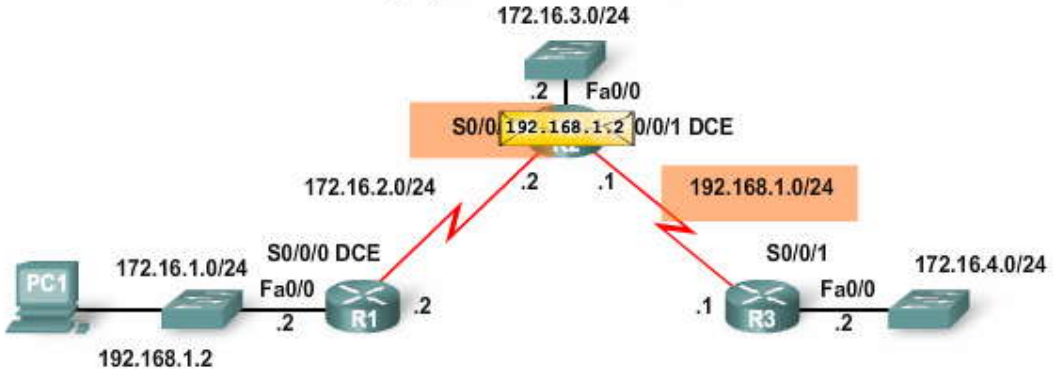
El router primero examina las rutas de nivel 1 en busca de la mejor coincidencia. En nuestro ejemplo, hay una coincidencia entre la dirección IP de destino 192.168.1.2 y la ruta final de nivel 1 de 192.168.1.0/24.

**Haga clic en Paso 1a en la figura.**

R 192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0

R1 usa esta ruta y reenvía el paquete a la interfaz Serial 0/0/0.

## Ejemplo: Ruta final de nivel 1

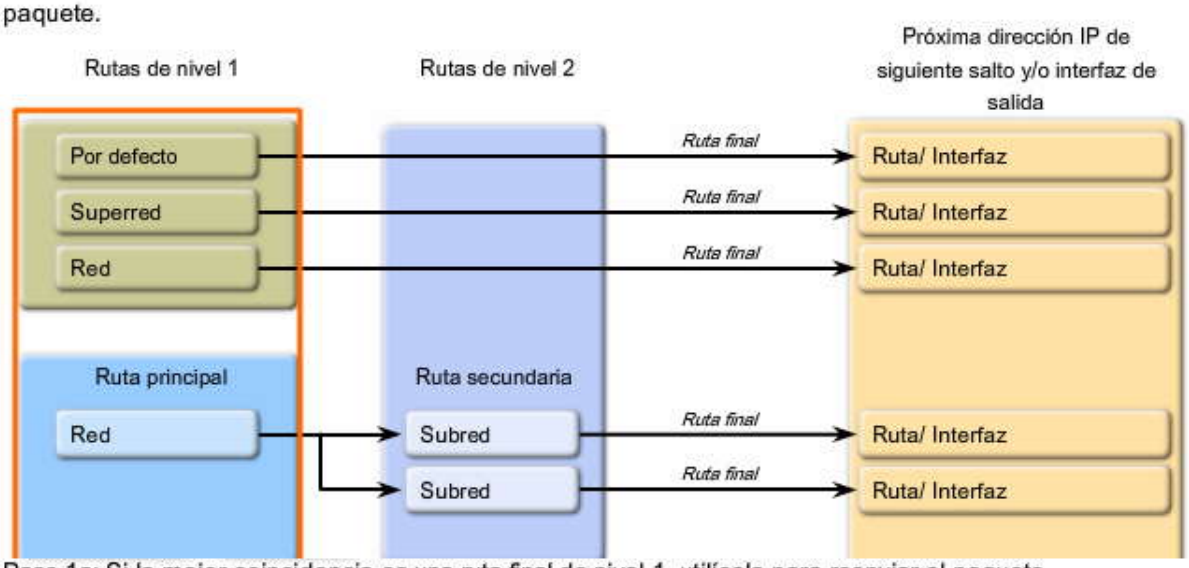



**Paso 1a: Si la mejor coincidencia es una ruta final de nivel 1, utilícela para reenviar el paquete.**

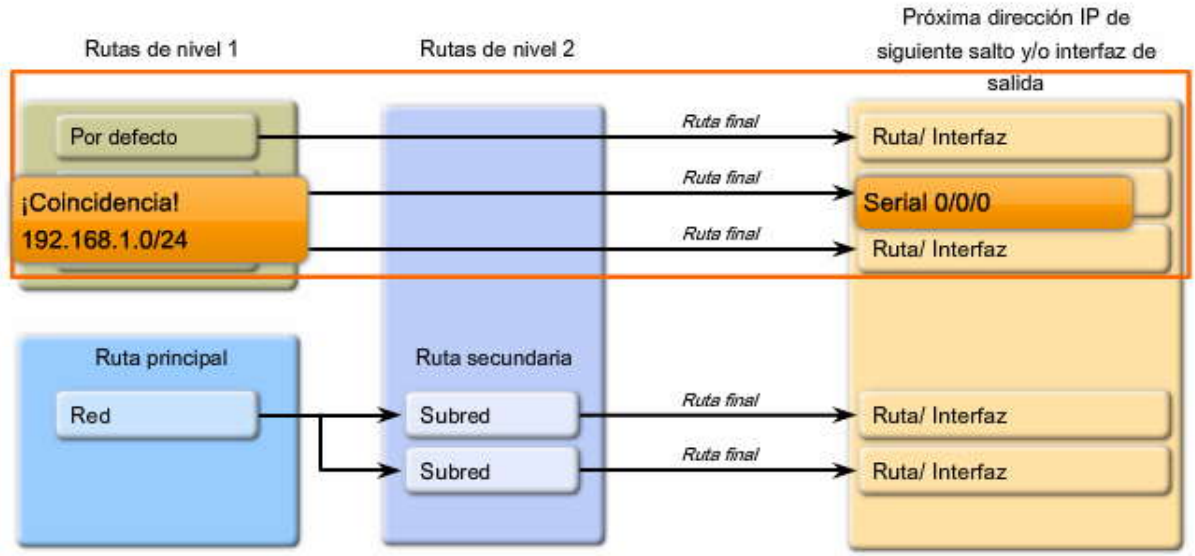
```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       <some output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
R       172.16.3.0 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
R    192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
```

Tabla de enrutamiento de R1

Paso 1: Examine las rutas del nivel 1 para lograr una mejor coincidencia con la dirección de destino del paquete.




Paso 1a: Si la mejor coincidencia es una ruta final de nivel 1, utilícela para reenviar el paquete.



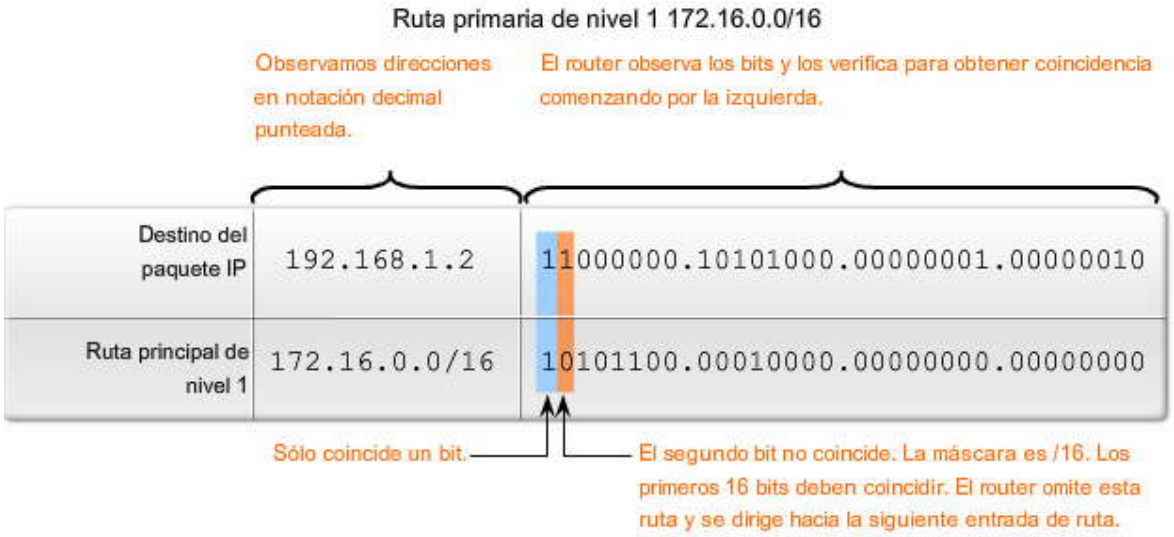

¿Por qué hay una coincidencia con la ruta de nivel 1 192.168.1.0/24 y no con una de las subredes 172.16.0.0? Esto puede parecer obvio. Decimos, "Es obvio que el router usará 192.168.1.0/24". Pero el proceso de búsqueda está comparando direcciones de 32 bits con entradas de ruta de 32 bits en busca de la coincidencia más larga.

El algoritmo que usa el IOS para realizar una búsqueda en la tabla de enrutamiento no se tratará en este capítulo. Lo importante es entender por qué una entrada de ruta coincide o no con la dirección IP de destino del paquete.

¿Por qué no hay coincidencia con ninguna de las subredes 172.16.0.0/24 en la tabla de enrutamiento?

172.16.0.0/24 es una ruta principal con tres subredes o rutas secundarias. Antes de que se examine una ruta secundaria en busca de una coincidencia, debe existir al menos una coincidencia entre la dirección IP de destino del paquete y la dirección con clase de la ruta principal o 172.16.0.0/16.

¿Coinciden, al menos, 16 de los bits que se encuentran más a la izquierda de la ruta principal con los primeros 16 bits de la dirección IP de destino de 192.168.1.2? La respuesta, no, es obvia para nosotros. Pero en la figura, verá que el router, en realidad, verifica el primer bit y encuentra una coincidencia. Luego, el router pasa al segundo bit. Como no hay coincidencia, el proceso de búsqueda se realizará para otras entradas de ruta.




Ahora veamos cómo el router encuentra una coincidencia entre la dirección IP de destino del paquete de 192.168.1.2 y la siguiente ruta en la tabla de enrutamiento, 192.168.1.0/24, una ruta final.

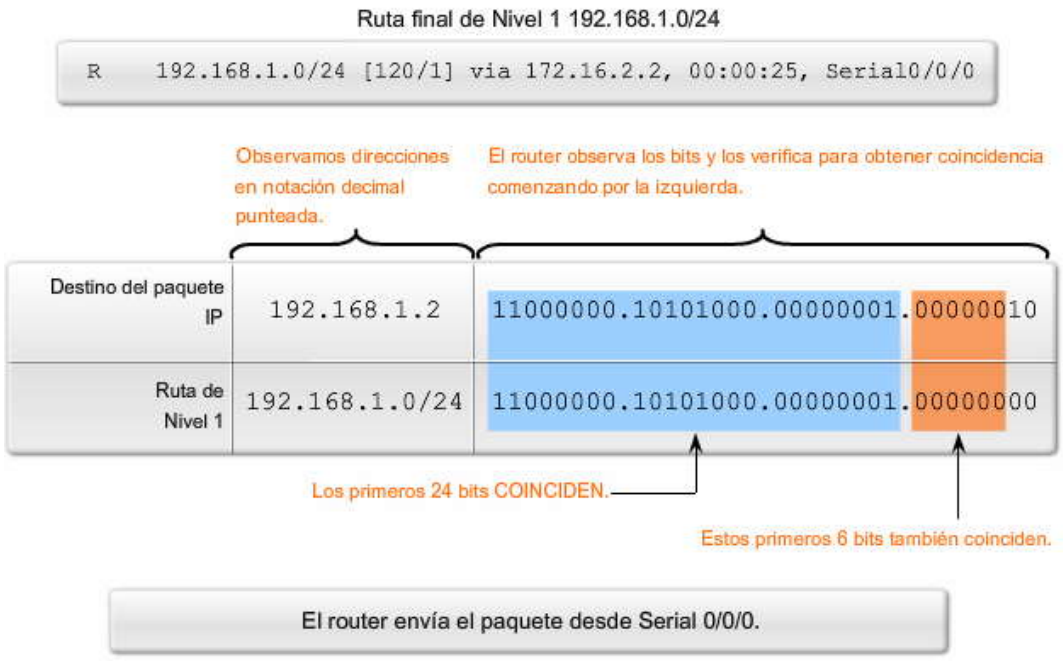
R 192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0

La ruta, 192.168.1.0, es una ruta final de nivel 1 y, por lo tanto, también contiene la máscara de subred, /24. En la figura, observe que al menos los primeros 24 bits que se encuentran más a la izquierda coinciden.

No sólo hay una coincidencia del mínimo de 24 bits, sino que 30 bits coinciden, como se muestra en la figura. ¿Esto es importante? Como veremos más adelante, puede haber situaciones en las que haya varias rutas coincidentes en la tabla de enrutamiento para la misma dirección IP de destino. ¿Cuál es la ruta preferida? La que tenga mayor cantidad de bits coincidentes, la coincidencia más larga.

En este ejemplo, hay una coincidencia entre la dirección IP de destino 192.168.1.0 y la ruta final de nivel 1 192.168.1.0/24. Como no hay una coincidencia más específica y más larga, el paquete se reenvía a la interfaz de salida Serial 0/0/0.

Nota: Recuerde que el proceso de búsqueda de rutas necesitará realizar una búsqueda recurrente en cualquier ruta que haga referencia sólo a la dirección IP del siguiente salto y no a una interfaz de salida. Para obtener una revisión de las búsquedas recurrentes, consulte el Capítulo 2, "Enrutamiento estático".



### 8.2.3 LA COINCIDENCIA MAS LARGA: RUTAS DE VINEL 1 YU SECUNDARIAS DE NIVEL 2.-

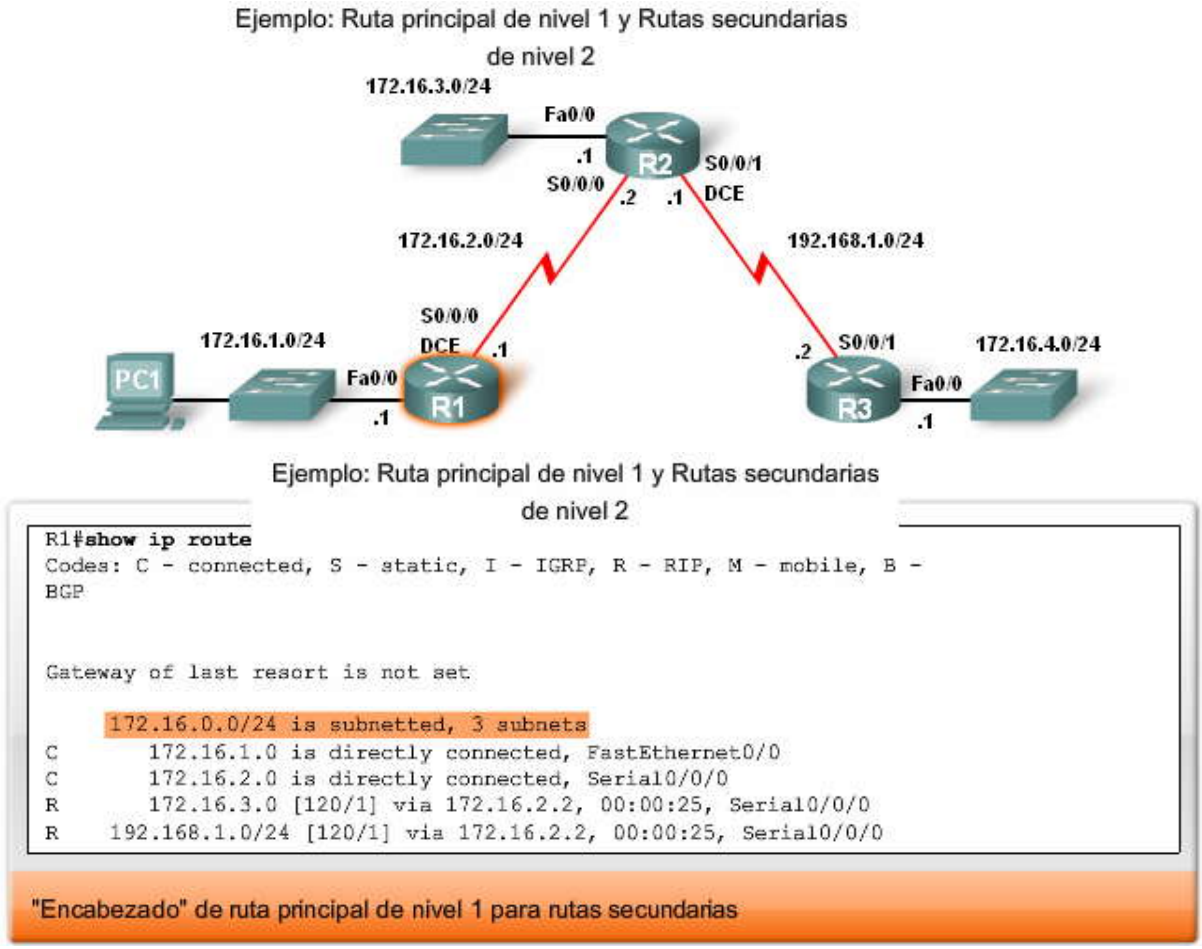
Examinemos lo que sucede cuando hay una coincidencia con una ruta principal de nivel 1.

Haga clic en Información de ruta en la figura.

Como se muestra en la figura, una ruta principal no incluye ninguna dirección de siguiente salto ni ninguna interfaz de salida, sino que sólo es un "encabezado" para sus rutas secundarias de nivel 2, las subredes.

La máscara de subred para las rutas secundarias, /24 en la figura, se muestra en la ruta principal, 172.16.0.0, para subredes que usan la misma máscara de subred.

Antes de que se busque una coincidencia en cualquier ruta secundaria de nivel 2, debe haber una coincidencia entre la dirección con clase de la ruta principal de nivel 1 y la dirección IP de destino del paquete.




**Ejemplo: Ruta principal de nivel 1 y rutas secundarias de nivel 2**

En el ejemplo de la figura, la PC1 envía un ping a la PC2 en 172.16.3.10. R1 recibe el paquete y comienza a buscar una ruta en la tabla de enrutamiento.

**Haga clic en Paso 1b en la figura.**

La primera coincidencia que se produce es con la ruta principal de nivel 1, 172.16.0.0. Recuerde que con las subredes sin VLSM, la máscara con clase de la ruta principal no se muestra en este punto. Antes de que se examinen las rutas secundarias (subredes) en busca de una coincidencia, primero debe haber una coincidencia con la dirección con clase de la ruta principal.

Debido a que la primera entrada de ruta es una ruta principal de nivel 1 que coincide con la dirección de destino (Paso 1b del proceso de búsqueda de rutas), el proceso de búsqueda de rutas continúa con el Paso 2.

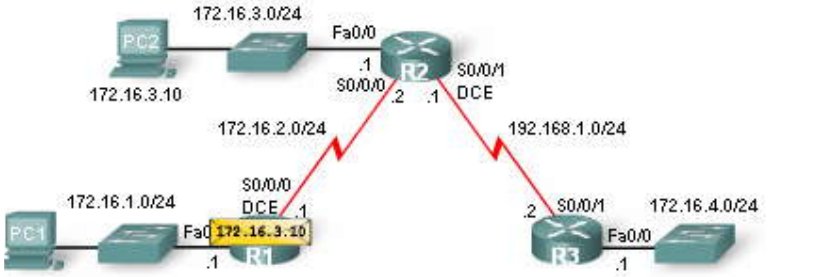
**Haga clic en Paso 2 en la figura.**

Debido a que hay una coincidencia con la ruta principal, se buscará una coincidencia en las rutas secundarias de nivel 2. Sin embargo, esta vez, la máscara de subred de /24 real se usa para la cantidad mínima de bits que se encuentran más a la izquierda y que deben coincidir.

**Haga clic en Paso 2a en la figura.**

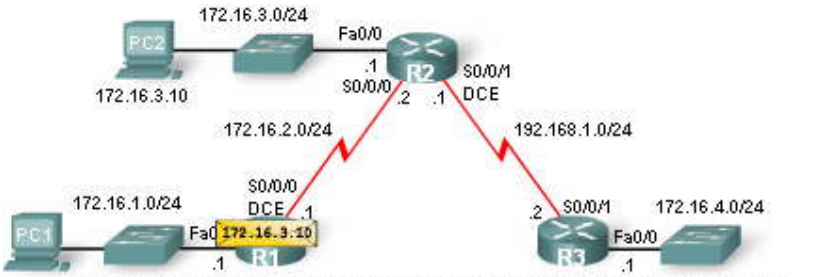
El proceso de búsqueda examina las rutas secundarias en busca de una coincidencia. En este caso, debe haber un mínimo de 24 bits que coincidan.

Ejemplo: Ruta principal de nivel 1 y Rutas secundarias de nivel 2

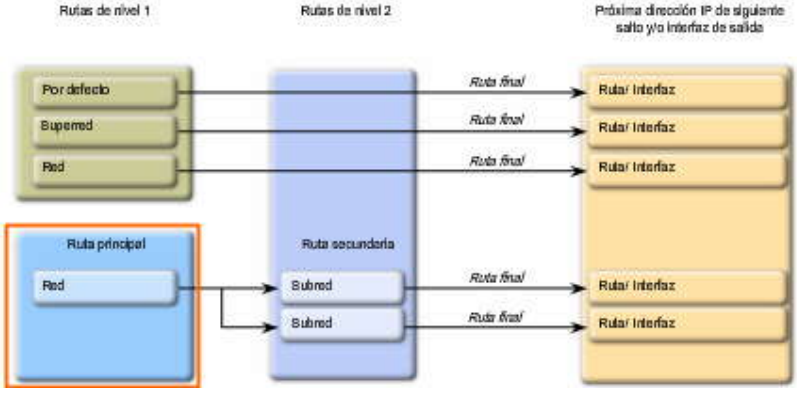


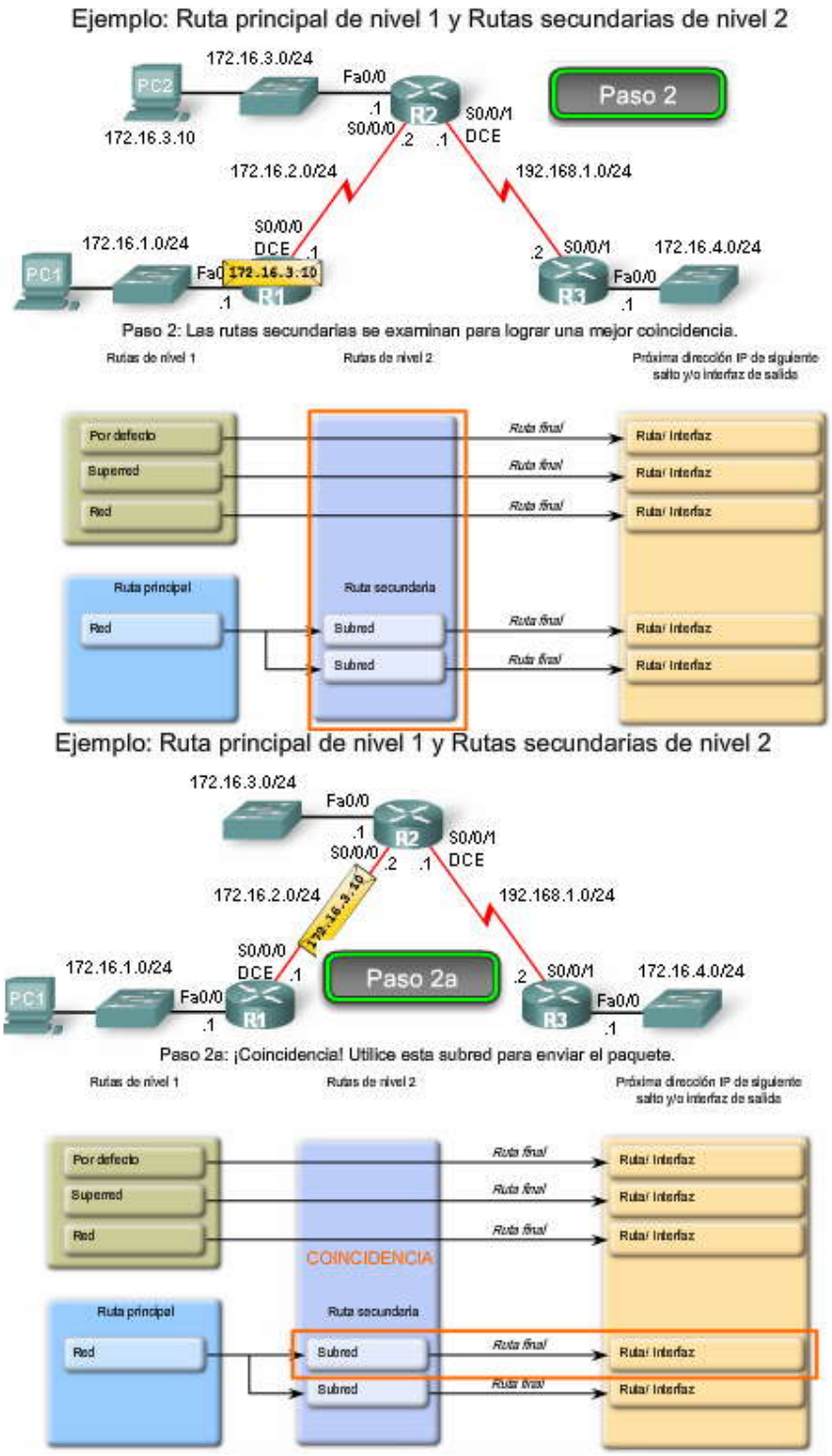

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.1.0 is directly connected, FastEthernet0/0
C       172.16.2.0 is directly connected, Serial0/0/0
R       172.16.3.0 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
R    192.168.1.0/24 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0
```

Ejemplo: Ruta principal de nivel 1 y Rutas secundarias de nivel 2




Paso 1b: Si la mejor coincidencia es una ruta primaria de nivel 1, proceda con el Paso 2.






Examinemos cómo el router encuentra una coincidencia con una de las rutas secundarias de nivel 2.

Primero, el router examina la ruta principal en busca de una coincidencia. En este ejem plo, los primeros 16 bits de la dirección IP deben coincidir con los de la ruta principal. Los 16 bits que se encuentran más a la izquierda deben coincidir porque ésa es la máscara con clase de la ruta principal, /16.

Si hay una coincidencia con la ruta principal, entonces el router verifica la ruta 172.16.1.0. Las rutas secundarias sólo se examinan cuando hay una coincidencia con la máscara con clase de la principal.

Haga clic en 2 en la figura.

Al verificar la primera subred, 172.16.1.0, el bit vigésimo tercero (23) no coincide; por lo tanto, esta ruta se rechaza porque los primeros 24 bits no coinciden.

Haga clic en 3 en la figura.

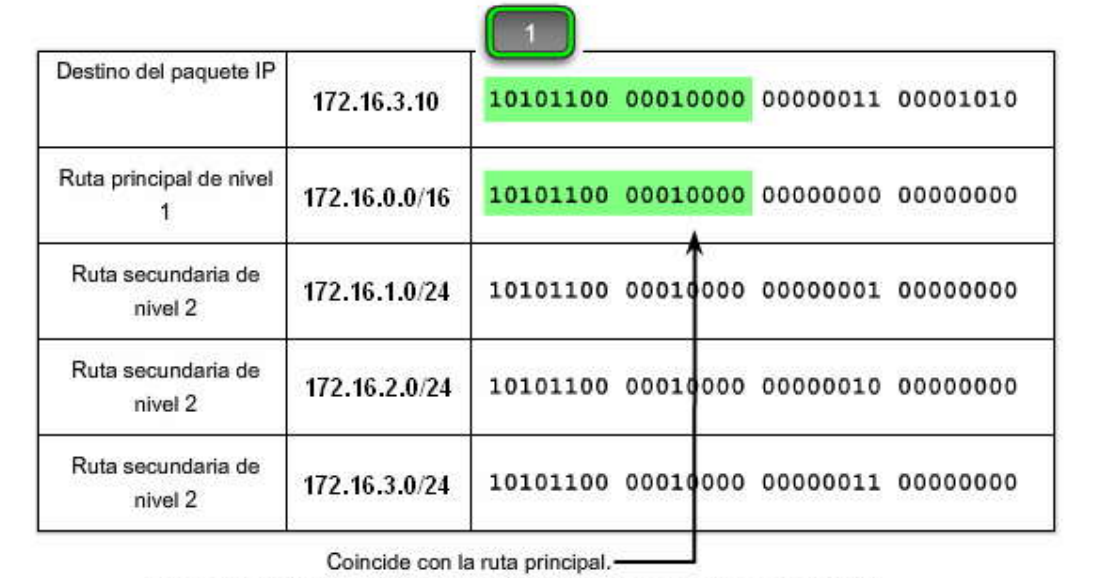
Luego, el router verifica la ruta 172.16.2.0/24. Debido a que el bit vigésimo cuarto (24) no coincide, esta ruta tambi én se rechaza. Los 24 bits deben coincidir.

Haga clic en 4 en la figura.

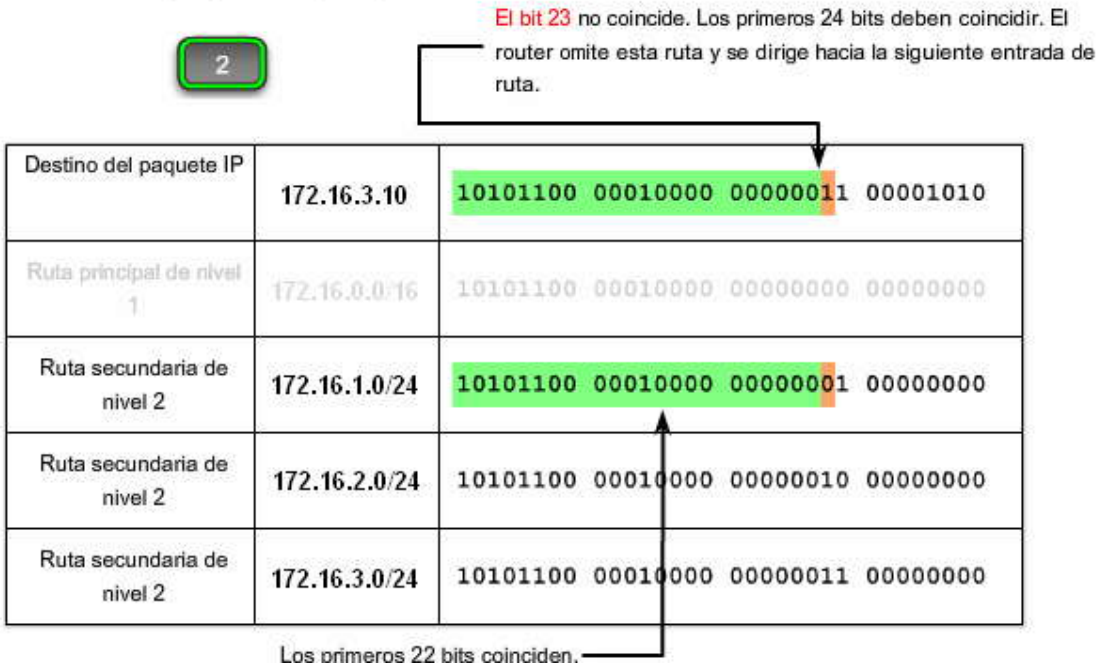
El router verifica la última ruta secundaria de 172.16.3.0/24 y encuentra una coincidencia. Los primeros 24 bits sí coinciden. El proceso de la tabla de enrutamiento usará esta ruta, 172.16.3.0/24, para reenviar el paquete con la dirección IP de destino de 172.16.3.10 a la interfaz de salida de Serial 0/0/0.

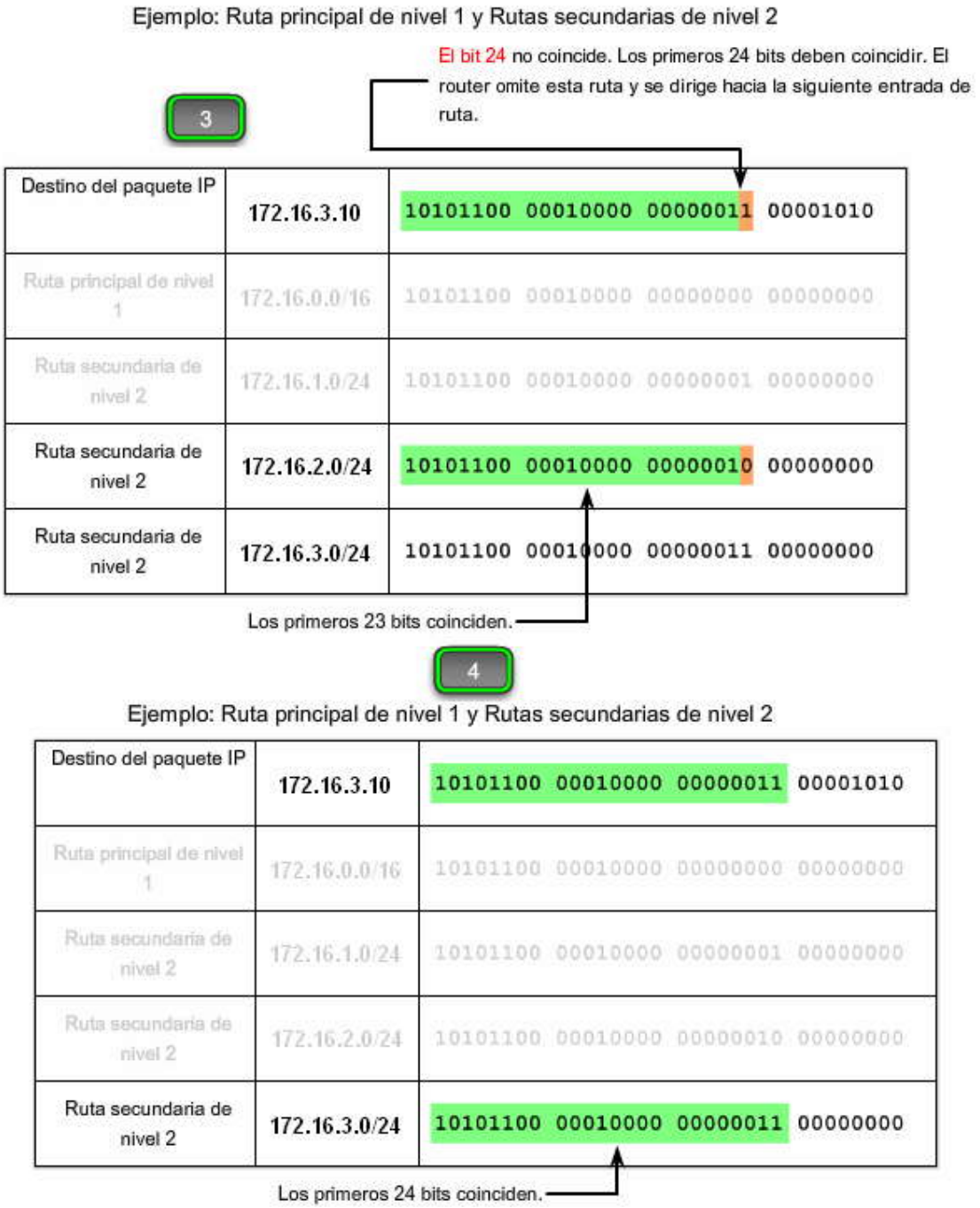
R 172.16.3.0 [120/1] via 172.16.2.2, 00:00:25, Serial0/0/0

¿Qué sucede si el router no tiene una ruta? Entonces descartará el paquete.




Ejemplo: Ruta principal de nivel 1 y Rutas secundarias de nivel 2





Ejemplo: Proceso de búsqueda de rutas con VLSM

¿Qué sucede con nuestra topología de RouterX que utiliza un esquema de direccionamiento VLSM? ¿Cómo cambia esto el proceso de búsqueda?

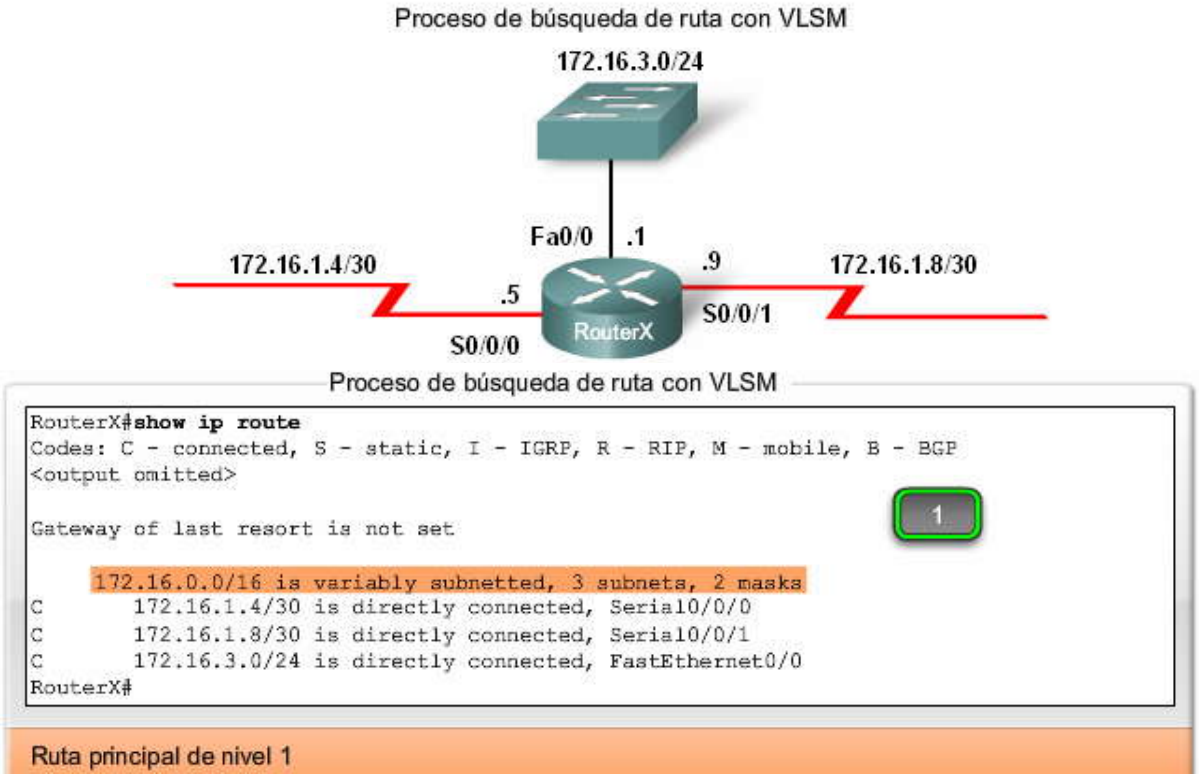
Haga clic en 1 en la figura.

Usar VSLM no cambia el proceso de búsqueda. Con VLSM, la máscara con clase /16 se muestra con la ruta principal de nivel 1 (172.16.0.0/16 en la figura).

Haga clic en 2, 3 y 4 en la figura.

Al igual que con las redes sin VLSM, si hay una coincidencia entre la dirección IP de destino del paquete y la máscara con clase de la ruta principal de nivel 1, se realizará una búsqueda en las rutas secundarias de nivel 2.

La única diferencia con VLSM es que las rutas secundarias muestran sus propias máscaras de subred específicas. Estas máscaras de subred se usan para determinar la cantidad de bits que se encuentran más a la izquierda y que deben coincidir con la dirección IP de destino del paquete. Por ejemplo, para que haya una coincidencia con la ruta secundaria 172.16.1.4, un mínimo de 30 bits que se encuentren más a la izquierda deben coincidir porque la máscara de subred es /30.




### 8.3 COMPORTAMIENTO DE ENRUTAMIENTO.-

#### 8.3.1 COMPORTAMIENTO DE ENRUTAMIENTO CON CLASE Y SIN CLASE.-

El siguiente paso en el proceso de búsqueda de rutas (Paso 3) considera el comportamiento de enrutamiento. El comportamiento de enrutamiento influencia el proceso de búsqueda de la ruta preferida usando los comandos no ip classless o ip classless.

Los comportamientos de enrutamiento sin clase y con clase no son iguales a los protocolos de enrutamiento sin clase y con clase. Los protocolos de enrutamiento sin clase y con clase afectan la forma en que se completa la tabla de enrutamiento. Los comportamientos de enrutamiento con clase y sin clase determinan cómo se realiza una búsqueda en la tabla de enrutamiento después de que se completa. En la figura, las fuentes de enrutamiento (incluidos los protocolos de enrutamiento con clase y sin clase) son las entradas que se usan para completar la tabla de enrutamiento. El comportamiento de enrutamiento, especificados por los comandos ip classless o no ip classless, determina cómo el proceso de búsqueda de rutas pasará al Paso 3.

Como puede ver, los protocolos de enrutamiento y los comportamientos de enrutamiento son completamente independientes entre sí. La tabla de enrutamiento podría completarse con rutas de un protocolo de enrutamiento sin clase como RIPv2; sin embargo, se implementa el comportamiento de enrutamiento con clase porque está configurado el comando no ip classless.

## Comparación entre protocolos de enrutamiento y comportamientos de enrutamiento

**Origen del enrutamiento**

- Redes conectadas directamente
- Rutas estáticas
- Protocolos de enrutamiento con clase
  - RIPv1
  - IGRP
- Protocolos de enrutamiento sin clase
  - RIPv2
  - EIGRP
  - OSPF
  - IS-IS

**Comportamientos de enrutamiento**

- Con clase
  - `no ip classless`
- IP sin clase
  - `ip classless`

- Los orígenes de enrutamiento (incluyendo los protocolos) se utilizan para construir la tabla de enrutamiento.
- Pueden utilizarse múltiples orígenes y protocolos de enrutamiento.

- Los comportamientos de enrutamiento se utilizan para encontrar información en la tabla de enrutamiento.
- Sólo puede utilizarse un único comportamiento de enrutamiento.

Cambios en la topología

En el Capítulo 7, "RIPv2", aprendimos que los protocolos de enrutamiento con clase, tales como RIPv1, no admiten redes no contiguas. A pesar de que nuestra topología actual tiene redes no contiguas, podemos configurar rutas estáticas para alcanzar esas redes.

Haga clic en Configuración de R2 en la figura.

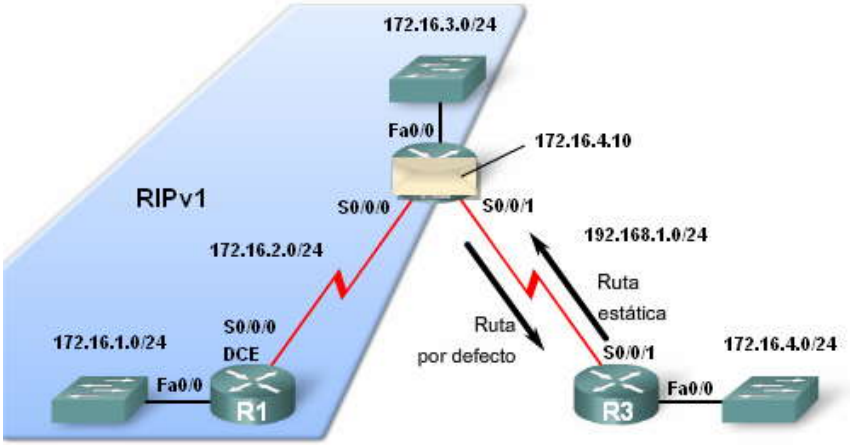
Primero, agregamos una ruta estática "quad-zero" en R2 para enviar el tráfico predeterminado a R3. Luego agregamos el comando default-information originate al proceso de enrutamiento de RIP para que R2 envíe a R1 la ruta por defecto. Esto le dará a R1 y R2 la capacidad de alcanzar otras redes, incluida la 172.16.4.0/24 de R3. Por último, ingresamos el comando no network 192.168.1.0 porque ya no deseamos intercambiar actualizaciones de RIP con R3.

Haga clic en Configuración de R3 en la figura.

Para terminar nuestra configuración, eliminamos el enrutamiento de RIP y agregamos una ruta estática en R3 para enviar tráfico para la red principal 172.16.0.0/16, que no tiene una coincidencia más larga en la tabla de enrutamiento, a R2.

En este momento, no probaremos la conectividad. La conectividad se probará en las siguientes secciones.

Cambios de topología y configuraciones del router



Cambios de topología y configuraciones del router

```
R2(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R2(config)#router rip
R2(config-router)#default-information originate
R2(config-router)#no network 192.168.1.0
R2(config-router)#end
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:00, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Configuración de R2

```
R3(config)#ip route 172.16.0.0 255.255.0.0 s0/0/1
R3(config)#no router rip
R3(config-router)#end
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.4.0/24 is directly connected, FastEthernet0/0
S       172.16.0.0/16 is directly connected, Serial0/0/1
C    192.168.1.0/24 is directly connected, Serial0/0/1
```

Configuración de R3

### 8.3.2 COMPORTAMIENTO DE ENRUTAMIENTO CON CLASE: NO IP CLASSLES.-

Ahora nos concentramos en el Paso 3 del proceso de búsqueda de rutas. Específicamente, nos enfocaremos en qué sucede después del Paso 2b cuando no hay coincidencia con ninguna ruta secundaria de nivel 2 de la principal. Luego, verá un ejemplo específico.

Como seguramente recuerda de la sección anterior, en los Pasos 1 y 2, el router examina las rutas de nivel 1 y secundarias en busca de la mejor coincidencia con la dirección IP de destino del paquete. Supongamos que no hay coincidencia y reanudemos nuestra revisión del proceso de búsqueda de rutas con el Paso 3.

**Haga clic en Pasos 3 y 3a de la figura para revisar cómo el comportamiento de enrutamiento con clase influye en el proceso de de búsqueda de rutas.**

**Haga clic en Paso 3 en la figura.**

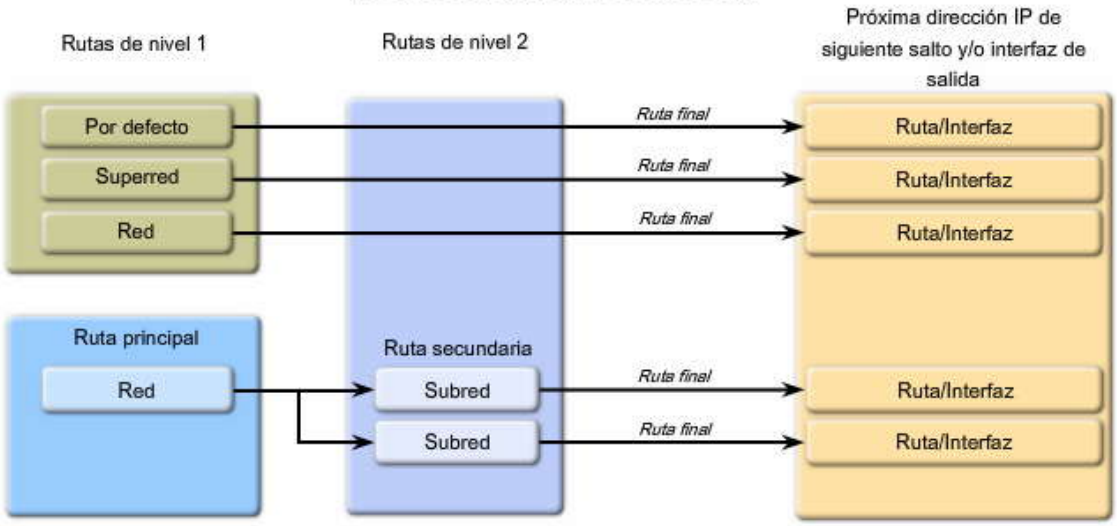
¿El router implementa un comportamiento de enrutamiento con clase o sin clase?

**Haga clic en Paso 3a en la figura.**

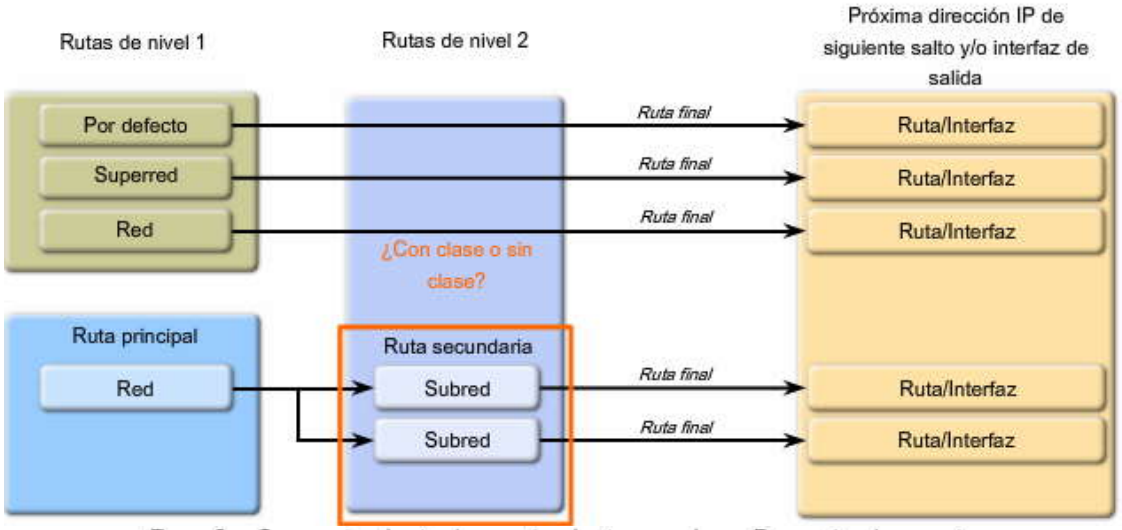
Si el comportamiento del enrutamiento con clase está en vigencia, termine el proceso de búsqueda y descarte el paquete.

Nota: Con el comportamiento de enrutamiento con clase, el proceso nunca llega al Paso 4.

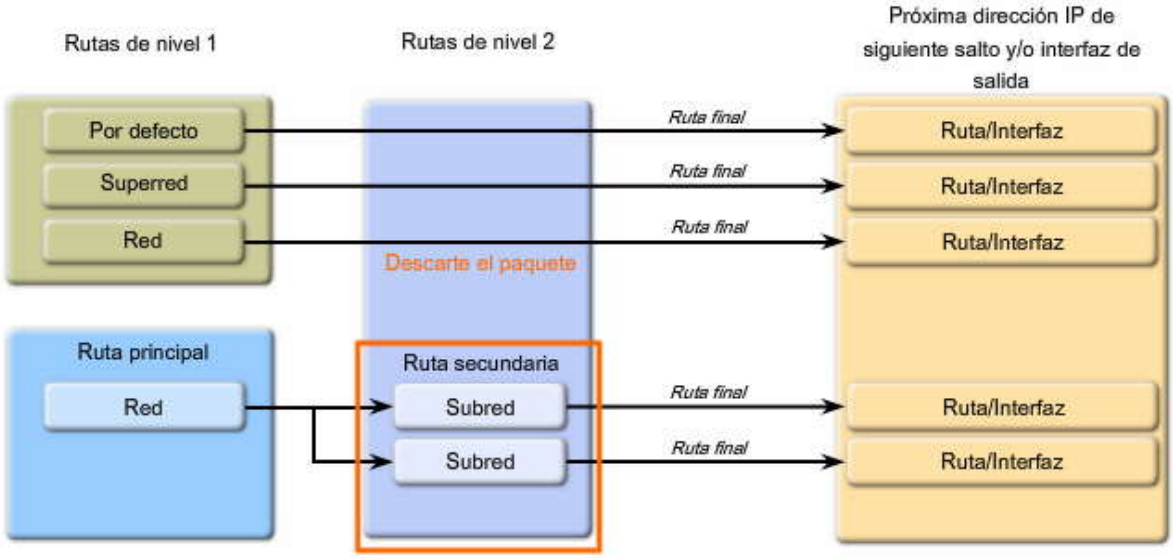
Proceso de búsqueda de tabla de ruta




Paso 3: ¿Comportamiento de enrutamiento con clase o sin clase?




Paso 3a: Comportamiento de enrutamiento con clase: Descarte el paquete



Antes de IOS 11.3, no ip classless era el comportamiento predeterminado de los routers Cisco. El comando no ip classless significa que el proceso de búsqueda de rutas usa búsquedas en la tabla de enrutamiento con clase por defecto. Esto se explicará en las siguientes secciones.

Los comandos no ip classless e ip classless son comandos de configuración global y pueden verse al escribir show running-config. En la versión 11.3 y posteriores de IOS, el comando ip classless es el predeterminado e implementa un proceso de búsqueda de rutas sin clase.

¿Cuál es el efecto del comportamiento del enrutamiento con clase cuando todos los routers se configuran con el comando no ip classless?

R1(config)#no ip classless
R2(config)#no ip classless
R3(config)#no ip classless

Examinemos lo que sucede cuando el router tiene un comportamiento de enrutamiento con clase, es decir, cuando el comando no ip classless está configurado.

Configuración en ejecución con el comando **no ip classless**

```
R2#show running-config
Building configuration...

Current configuration:
!
version 12.2
!
<text omitted>
!
no ip classless
!
<text omitted>
```

### 8.3.3 COMPORTAMIENTO DE ENRUTAMIENTO CON CLASE: PROCESO DE BUSQUEDA.-

En nuestro proceso de búsqueda en la tabla de enrutamiento, el Paso 3a establece que cuando el comportamiento del enrutamiento con clase esté en vigencia (no ip classless) el proceso no seguirá realizando búsquedas de rutas de nivel 1 en la tabla de enrutamiento. Si el paquete no coincide con una ruta secundaria de la ruta de red principal, entonces el router lo descarta. Veamos un ejemplo.

**Ejemplo: R2 en funcionamiento con el comportamiento de enrutamiento con clase**

En este ejemplo, R2 recibe un paquete destinado a la PC3 en 172.16.4.10.

**Haga clic en Tabla de enrutamiento de R2 y principal en la figura.**

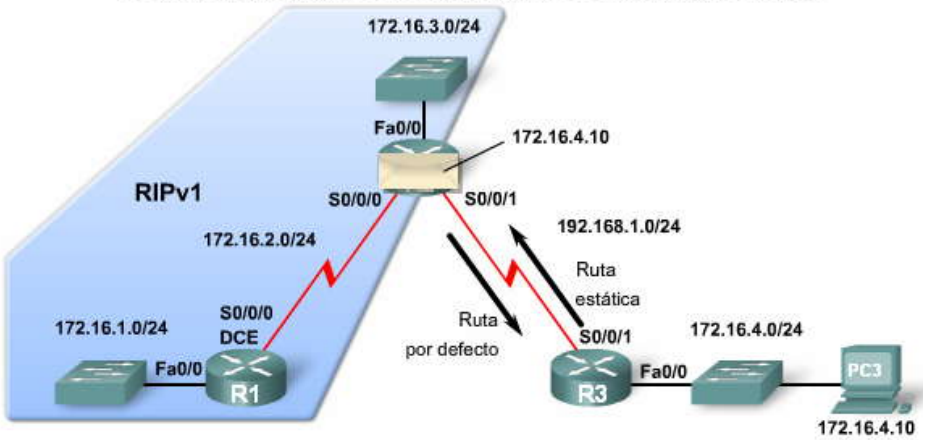
El proceso de enrutamiento realiza una búsqueda en la tabla de enrutamiento y encuentra una coincidencia de 16 bits con la ruta principal 172.16.0.0, como se muestra en la figura. Según el Paso 1b del proceso de enrutamiento, si hay una coincidencia en la ruta principal, las rutas secundarias se verifican.

Ahora observemos el proceso de coincidencia de bits real que tiene lugar mientras se verifican las rutas secundarias.

**Haga clic en 1, 2 y 3 en la figura.**

Observe que ninguno de los 24 bits que se encuentran más a la izquierda de las rutas secundarias coincide con la dirección IP de destino de 172.16.4.10. A lo sumo, sólo 21 bits coinciden. No hay coincidencia con las rutas secundarias de nivel 2.

Ejemplo: R2 funcionando con comportamiento de enrutamiento con clase




```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:12, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Tabla de enrutamiento de R2

Coincidencia

El destino coincide con la ruta principal. R2 ahora verificará las rutas secundarias.

Principal

| | | |
|---|---|---|
| Destino del paquete IP | 172.16.4.10 | 10101100.00010000.00000100.00001010 |
| Ruta principal de nivel 1 | 172.16.0.0/16 | 10101100.00010000.00000000.00000000 |
| Ruta secundaria de nivel 2 | 172.16.1.0/24 | 10101100.00010000.00000001.00000000 |
| Ruta secundaria de nivel 2 | 172.16.2.0/24 | 10101100.00010000.00000010.00000000 |
| Ruta secundaria de nivel 2 | 172.16.3.0/24 | 10101100.00010000.00000011.00000000 |

El bit número 22 *no* coincide. Los primeros 24 bits deben coincidir. El router omite esta ruta y se dirige hacia la siguiente entrada de ruta.

| | | |
|---|---|---|
| Destino del paquete IP | 172.16.4.10 | 10101100.00010000.00000100.00001010 |
| Ruta principal de nivel 1 | 172.16.0.0/16 | 10101100.00010000.00000000.00000000 |
| Ruta secundaria de nivel 2 | 172.16.1.0/24 | 10101100.00010000.00000001.00000000 |
| Ruta secundaria de nivel 2 | 172.16.2.0/24 | 10101100.00010000.00000010.00000000 |
| Ruta secundaria de nivel 2 | 172.16.3.0/24 | 10101100.00010000.00000011.00000000 |

Los primeros 21 bits coinciden.

Por lo tanto, ¿qué sucede después? El Router R2 descarta el paquete.

Haga clic en No hay coincidencias en la figura.

Como el router R2 está usando un comportamiento de enrutamiento con clase, no ip classless, el router no realizará búsquedas más allá de las rutas secundarias para encontrar una coincidencia menor..

Haga clic en Descartar el paquete en la figura.

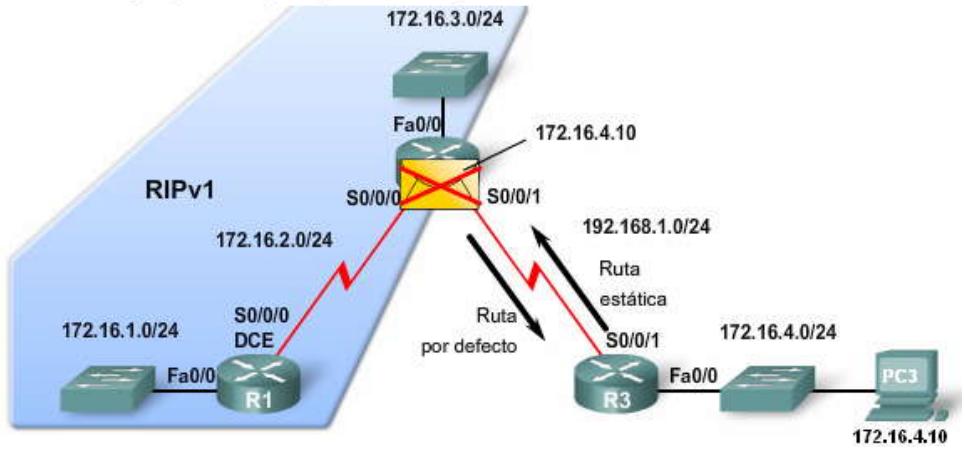
El proceso de la tabla de enrutamiento no usará la ruta por defecto, 0.0.0.0/0, ni ninguna otra ruta.

Un error común es suponer que la ruta por defecto se usa siempre que el router no tiene una ruta mejor. En nuestro ejemplo, la ruta por defecto de R2 no se examina ni se usa, aunque haya una coincidencia. Éste es a menudo un re sultado que sorprende mucho cuando un administrador de red no comprende la diferencia entre comportamiento de enrutamiento con clase y sin clase.

Nota: También veremos otro ejemplo en el Capítulo 9, EIGRP, en el que la comprensión del proceso de búsqueda en la tabla de enrutamiento le ayudará a resolver por qué una ruta por defecto no se usa, incluso con el comportamiento del enrutamiento sin clase.

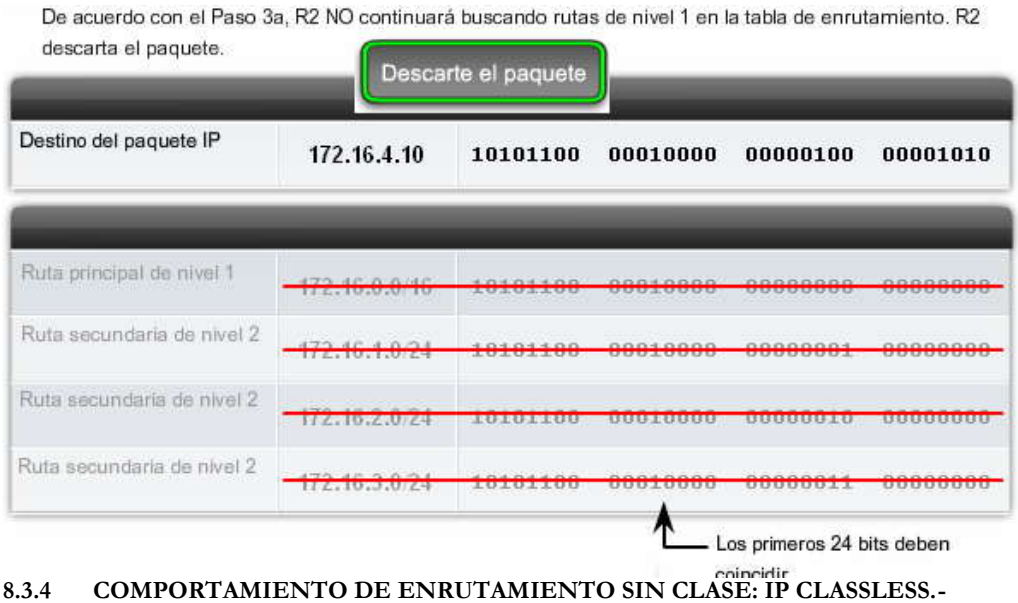
¿Por qué el comportamiento del enrutamiento con clase actúa de esta manera ? La idea general del comportam iento del enrutamiento con clase se originó cuando todas las redes eran con clase. Al comienzo del crecimiento de Internet, una organización recibía una dirección de red principal de clase A, B o C. Una vez que una organización tenía una dirección IP de red principal, esa organización también administraba todas las subredes de esa dirección con clase. Todos los routers que pertenecían a la organización conocían todas las subredes de la red principal. Si una subred no estaba en la tabla de enrutamiento, entonces la subred no existía. Como se vio en el Capítulo 6, "VLSM y CIDR", las direcciones IP ya no se asignan en función de la clase.

Ejemplo: Ruta principal de nivel 1 y Rutas secundarias de nivel 2




Ejemplo: Ruta principal de nivel 1 y Rutas secundarias de nivel 2

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets                    <-- ¡Coincidencia!
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:12, Serial0/0/0   <-- No hay coincidencia
C       172.16.2.0 is directly connected, Serial0/0/0              <-- No hay coincidencia
C       172.16.3.0 is directly connected, FastEthernet0/0          <-- No hay coincidencia
C    192.168.1.0/24 is directly connected, Serial0/0/1             Descarte el paquete
S*   0.0.0.0/0 is directly connected, Serial0/0/1

La ruta por defecto no se utiliza.
```




### 8.3.4 COMPORTAMIENTO DE ENRUTAMIENTO SIN CLASE: IP CLASSLESS.-

A partir de IOS 11.3, Cisco cambió el comportamiento de enrutamiento predeterminado de con clase a sin clase. El comando ip classless se configura en forma predeterminada. El comando show running-config muestra el comportamiento de enrutamiento. Comportamiento de enrutamiento sin clase significa que el proceso de enrutamiento ya no supone que todas las subredes de una red principal con clase sólo pueden alcanzarse dentro de las rutas secundarias a la principal. El comportamiento de enrutamiento sin clase funciona bien para las redes no contiguas y las superredes CIDR.

En esta sección, examinaremos el efecto del comportamiento del enrutamiento sin clase. Todos los routers están configurados con el comando ip classless.

R1(config)#ip classless
R2(config)#ip classless
R3(config)#ip classless

Analizaremos lo que le sucede a un paquete cuando hay una coincidencia con una ruta principal de nivel 1, pero no hay coincidencias con las rutas secundarias de nivel 2 o subredes. Esto nos lleva al Paso 3b, Comportamiento del enrutamiento sin clase.

Configuración en ejecución con el comando **ip classless**

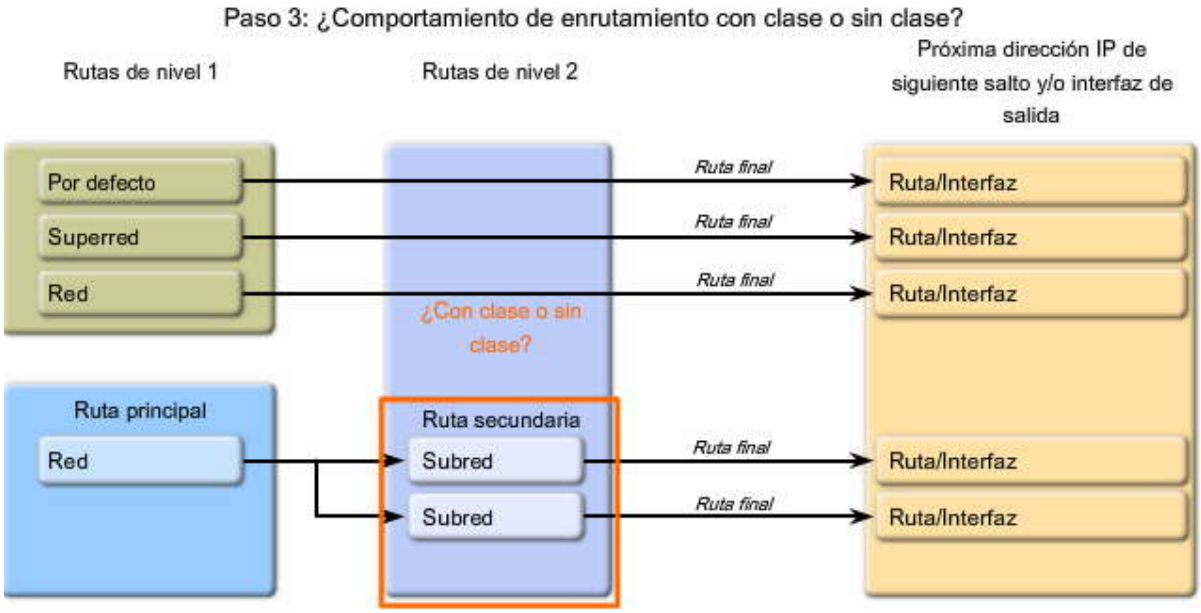
```
R2#show running-config
Building configuration...

Current configuration:
!
version 12.2
!
<text omitted>
!
ip classless
!
<text omitted>
```

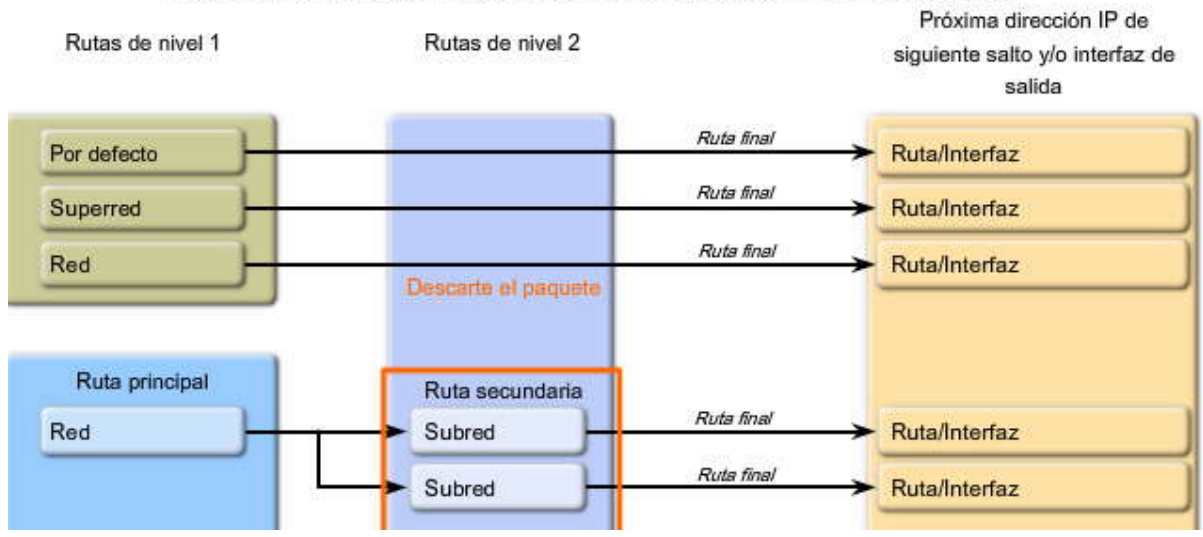
Como seguramente recuerda del proceso de la tabla de enrutamiento, en los Pasos 1 y 2, el proceso de la tabla de enrutamiento examina las rutas secundarias de nivel 1 y de nivel 2 en busca de la mejor coincidencia con la dirección IP de destino del paquete. Supongamos que no hay coincidencia y reanudemos nuestra revisión del proceso de búsqueda de rutas con el Paso 3.

Proceso de búsqueda de rutas:

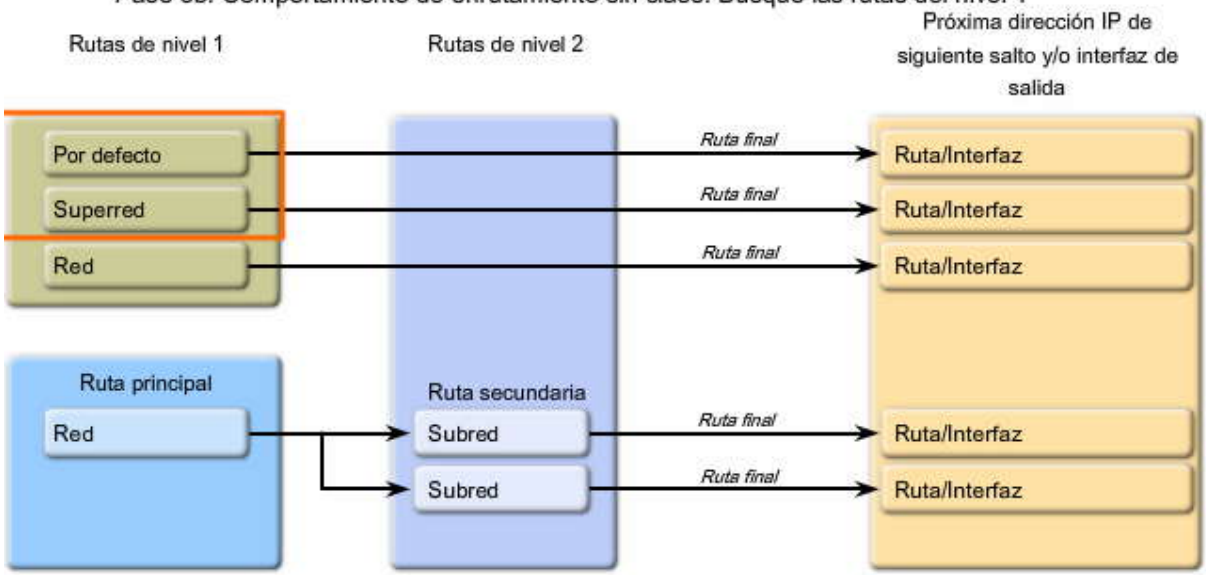
Siga estos pasos en la figura para ver el proceso de búsqueda de rutas:
Haga clic en Paso 3.
¿El router implementa un comportamiento de enrutamiento con clase o sin clase?
Haga clic en Paso 3a.
Comportamiento de enrutamiento con clase: Si el comportamiento del enrutamiento con clase está en vigencia, termine el proceso de búsqueda y descarte el paquete.
Haga clic en Paso 3b.
Comportamiento del enrutamiento sin clase: Si el comportamiento del enrutamiento sin clase está en vigencia, continúe buscando las rutas de superred de nivel 1 en la tabla de enrutamiento para ver si hay alguna coincidencia, incluida la ruta por defecto, de haberla.
Haga clic en Paso 4.
Si ahora hay una coincidencia menor con las rutas por defecto o de superred de nivel 1, el router usa esa ruta para reenviar el paquete.
Haga clic en Paso 5.

Si no hay coincidencia con ninguna ruta de la tabla de enrutamiento, el router descarta el paquete.

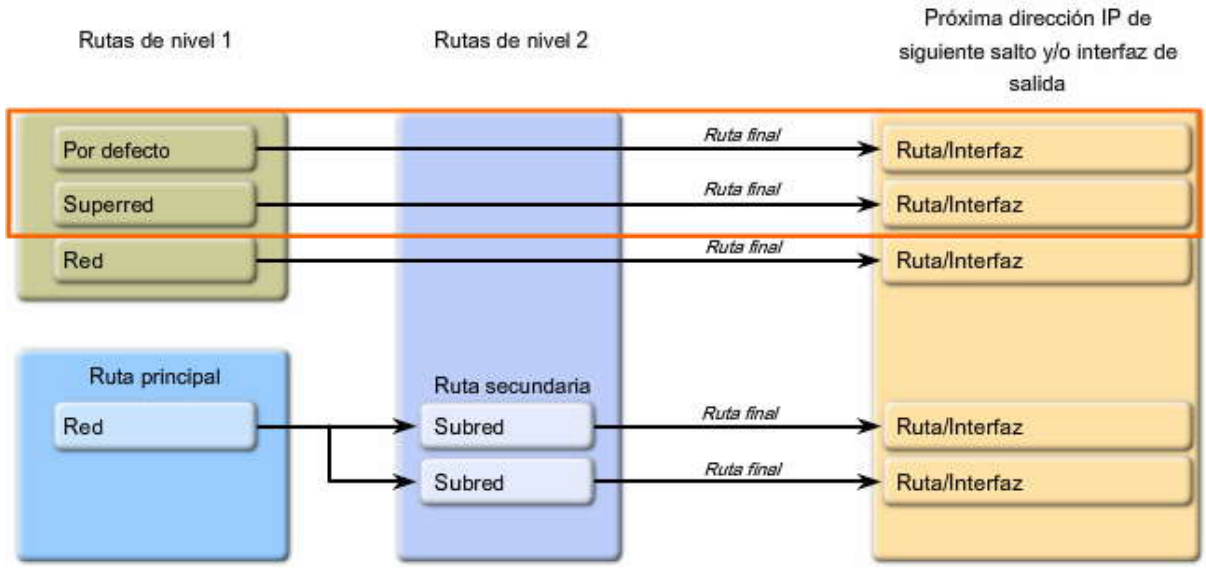


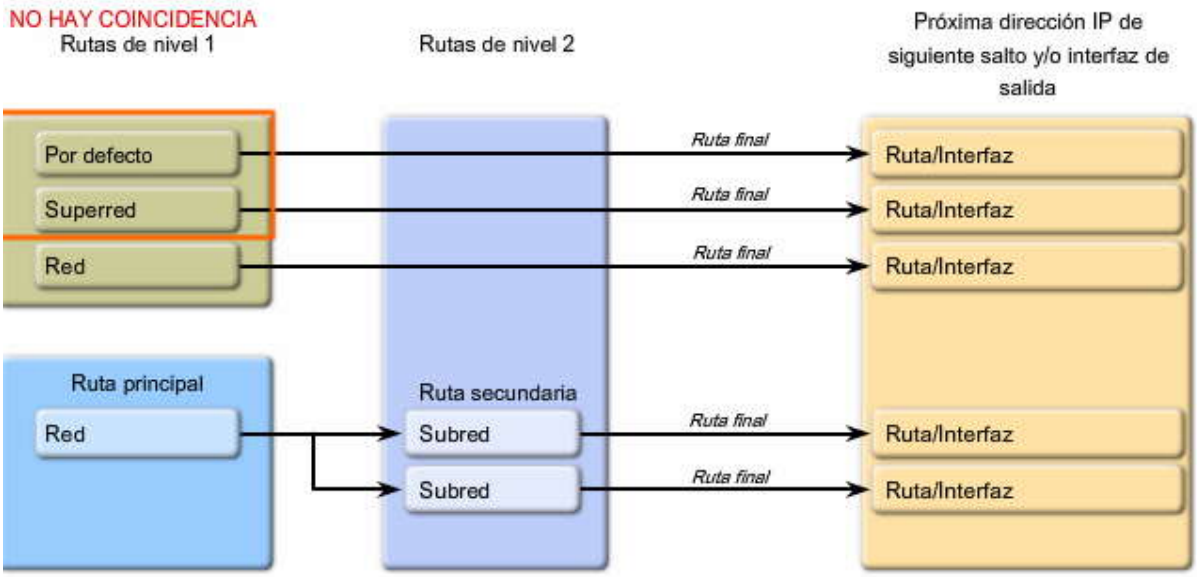
Paso 3b: Comportamiento de enrutamiento sin clase: Busque las rutas del nivel 1




Paso 4: Haga coincidir con superred o por defecto. Utilícela para reenviar el paquete. Primero se verifican las superredes, luego las que son por defecto si es necesario.



Paso 5: No hay coincidencia. No es por defecto. Descarte el paquete.




**8.3.5 COMPORTAMIENTO DE ENRUTAMIENTO SIN CLASE: PROCESO DE BUSQUEDA.-**

Repasemos nuestro ejemplo de topología y observemos la coincidencia de bits que se produce cuando el comportamiento de enrutamiento sin clase (ip classless) está en vigencia.

Ejemplo: R2 en funcionamiento con el comportamiento del enrutamiento sin clase

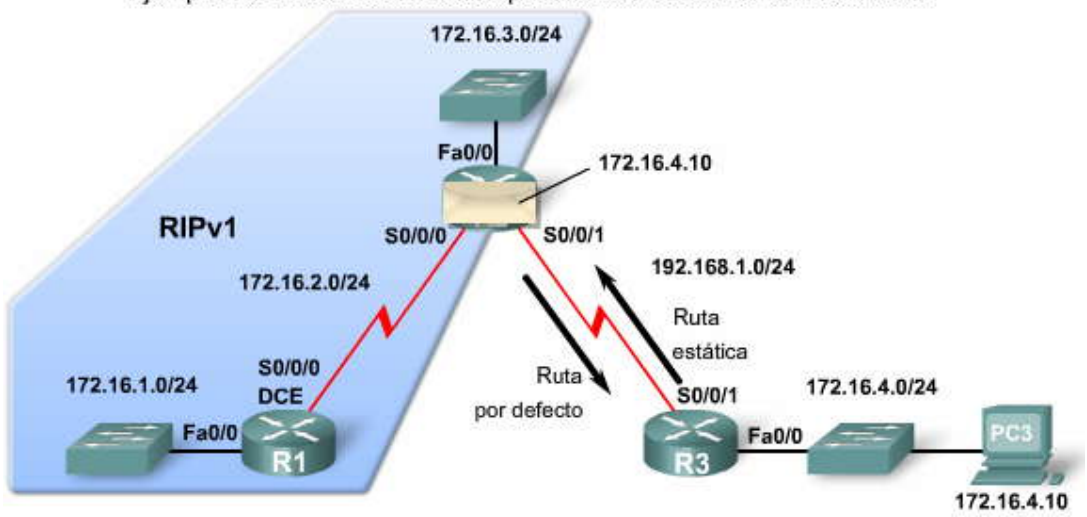
Haga clic en Tabla de enrutamiento de R2 y principal en la figura.

Nuevamente, R2 recibe un paquete destinado a la PC3 en 172.16.4.10. Como sucedía con el comportamiento de enrutamiento con clase, el router realiza una búsqueda en la tabla de enrutamiento y encuentra una coincidencia de 16 bits con la ruta principal 172.16.0.0, como se muestra en la figura. Según el Paso 1b del proceso de enrutamiento, si hay una coincidencia con la ruta principal, entonces, las rutas secundarias se verifican.

Haga clic en 1, 2 y 3 en la figura.

Como antes, ninguno de los 24 bits que se encuentran más a la izquierda de las rutas secundarias coinciden con la dirección IP de destino de 172.16.4.10. A lo sumo, sólo 21 bits coinciden. No hay coincidencia con las rutas secundarias de nivel 2.

Ejemplo: R2 funcionando con comportamiento de enrutamiento sin clase



Ejemplo: R2 funcionando con comportamiento de enrutamiento sin clase

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
R       172.16.1.0 [120/1] via 172.16.2.1, 00:00:12, Serial0/0/0
C       172.16.2.0 is directly connected, Serial0/0/0
C       172.16.3.0 is directly connected, FastEthernet0/0
C    192.168.1.0/24 is directly connected, Serial0/0/1
S*   0.0.0.0/0 is directly connected, Serial0/0/1
```

Tabla de enrutamiento R2

Coincidir

Ejemplo: Ruta primaria de nivel 1 y rutas secundarias de nivel 2

El destino coincide con la ruta principal. R2 ahora verificará las rutas secundarias.

Primaria

| | | |
|---|---|---|
| Destino del paquete IP | 172.16.4.10 | 10101100.00010000.00000100.00001010 |
| Ruta primaria de Nivel 1 | 172.16.0.0/16 | 10101100.00010000.00000000.00000000 |
| Ruta secundaria de Nivel 2 | 172.16.1.0/24 | 10101100.00010000.00000001.00000000 |
| Ruta secundaria de Nivel 2 | 172.16.2.0/24 | 10101100.00010000.00000010.00000000 |
| Ruta secundaria de Nivel 2 | 172.16.3.0/24 | 10101100.00010000.00000011.00000000 |

Debido a que utilizamos el comportamiento de enrutamiento sin clase (ip classless), el router continúa realizando búsquedas en la tabla de enrutamiento, más allá de esta ruta principal y sus rutas secundarias. El proceso de enrutamiento continuará realizando búsquedas en la tabla de enrutamiento para encontrar una ruta con una máscara de subred menor que los 16 bits de la ruta principal anterior. Es decir que el router ahora continuará realizando búsquedas de las otras rutas en la tabla de enrutamiento en la que puede haber menos bits que coincidan, pero también alguna coincidencia.

Haga clic en Ruta de red en la figura.

La ruta 192.168.1.0/24 no tiene 24 bits que se encuentren más a la izquierda y que coincidan con la dirección IP de destino.

C 192.168.1.0/24 está conectada directamente, Serial0/0/1

Haga clic en Ruta por defecto en la figura.

¿Qué sucede con la ruta por defecto? ¿Cuántos bits deben coincidir?

S* 0.0.0.0/0 está conectada directamente, Serial0/0/1

La máscara es /0, lo que significa que no hay necesidad de coincidencia de bits. Una ruta por defecto será la coincidencia con menos bits. En el comportamiento del enrutamiento sin clase, si no hay otra ruta que coincida, la ruta por defecto coincidirá.

Haga clic en Reenviar paquete en la figura.

En este caso, el router usará la ruta por defecto porque es la mejor coincidencia. El paquete se reenviará a la interfaz Seri al 0/0/1.

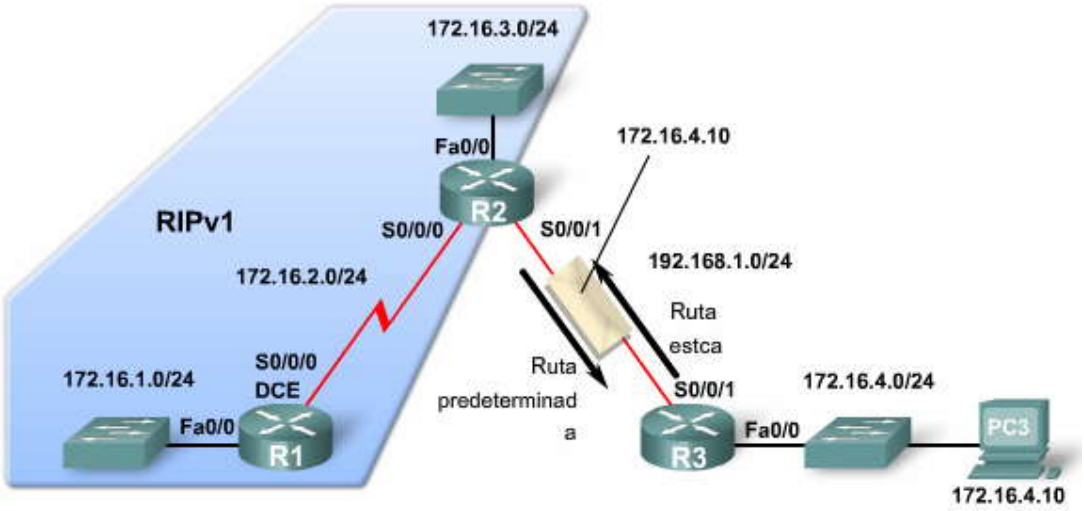
Ruta con clase en R3

Haga clic en Tabla de enrutamiento de R3 en la figura.

¿Qué hace R3 con el tráfico de regreso a la PC2 en 172.16.2.10? En la figura, verá que en la tabla de enrutamiento de R3, la ruta de subred 172.16.4.0/24 y la ruta de red con clase 172.16.0.0/16 son rutas secundarias de nivel 2 de la ruta principal 172.16.0.0/16. Siempre que hay rutas para las subredes de una red con clase y para una ruta de la propia ruta de red con clase, la ruta con clase se considera una ruta secundaria de nivel 2, al igual que las subredes.

En este caso, R3 usa la ruta secundaria 172.16.0.0/16 y reenvía el tráfico de Serial 0/0/1 nuevamente a R2.

Ejemplo: Ruta principal de nivel 2 y rutas secundarias de nivel 2




Ruta de red

Ejemplo: Ruta principal de nivel 2 y rutas secundarias de nivel 2

| | | |
|---|---|---|
| Destino del paquete IP | 172.16.4.10 | 10101100.00010000.00000100.00001010 |
| Ruta de red de Nivel 1 | 192.168.1.0/24 | 11000000.10101000.00000001.00000000 |
| Ruta predeterminada de Nivel 1 | 0.0.0.0/0 | 00000000.00000000.00000000.00000000 |

El segundo bit NO coincide. El router omite esta ruta y pasa a la siguiente entrada de ruta.

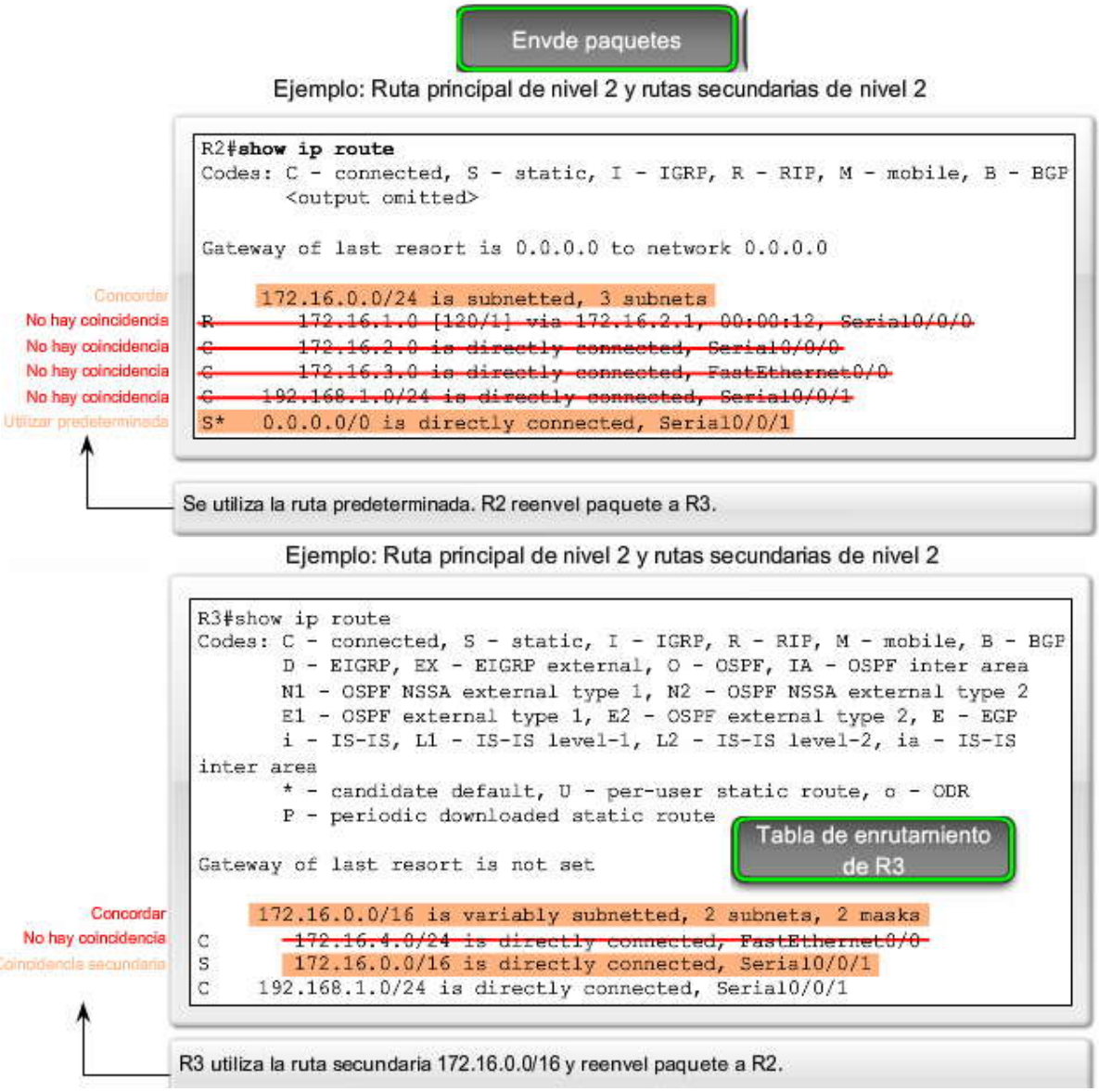
Coincide solamente el primer bit.

Ruta predeterminada

Ejemplo: Ruta principal de nivel 2 y rutas secundarias de nivel 2

Una mara /0 significa que no es necesario que coincidan los bits para usar la ruta predeterminada. R2 utiliza la ruta predeterminada y reenvel paquete.

| | | |
|---|---|---|
| Destino del paquete IP | 172.16.4.10 | 10101100.00010000.00000100.00001010 |
| Ruta de red de Nivel 1 | 192.168.1.0/24 | 11000000.10101000.00000001.00000000 |
| Ruta predeterminada de Nivel 1 | 0.0.0.0/0 | 00000000.00000000.00000000.00000000 |




Comparación del comportamiento del enrutamiento sin clase con el comportamiento del enrutami ento con clase en el mundo real

Recuerde que los comportamientos de enrutamiento con clase y sin clase son independientes de los protocolos de enrutamiento con clase y sin clase. Un router puede configurarse con el comportamiento de enrutamiento con clase (no ip classless) y un protocolo de enrutamiento sin clase, como RIPv2. Un router también puede configurarse con el comportamiento de enrutamiento sin clase (ip classless) y un protocolo de enrutamiento con clase, como RIPv1.

En las redes actuales, se recomienda usar el comportamiento de enrutamiento sin clase para que las rutas por defecto y de superred puedan usarse siempre que se necesiten.

## Comparación entre protocolos de enrutamiento y comportamientos de enrutamiento

Origen del enrutamiento

- Redes conectadas directamente
- Rutas estáticas
- Protocolos de enrutamiento con clase
  - RIPv1
  - IGRP
- Protocolos de enrutamiento sin clase
  - RIPv2
  - EIGRP
  - OSPF
  - IS-IS

- Los orígenes de enrutamiento (incluyendo los protocolos) se utilizan para construir la tabla de enrutamiento.
- Pueden utilizarse múltiples orígenes y protocolos de enrutamiento.

Comportamientos de enrutamiento

- Con clase

```
no ip classless
```

- IP sin clase

```
ip classless
```

- Los comportamientos de enrutamiento se utilizan para encontrar información en la tabla de enrutamiento.
- Sólo puede utilizarse un único comportamiento de enrutamiento.

# CAPITULO IX – "EIGRP"

## 9.0 INTRODUCCION DEL CAPITULO.-

### 9.0.1 INTRODUCCIÓN DEL CAPITULO.-

El Enhanced Interior Gateway Routing Protocol (EIGRP) es un protocolo de enrutamiento por vector de distancia con clase lanzado en 1992 con IOS 9.21. Como su nombre lo sugiere, EIGRP es un IGRP de Cisco mejorado (Interior Gateway Routing Protocol). Los dos son protocolos patentados de Cisco y sólo funcionan con los routers de Cisco.

El propósito principal en el desarrollo de EIGRP de Cisco fue crear una versión con clase de IGRP . EIGRP incluye muchas características que no se encuentran comúnmente en otros protocolos de enrutamiento vector distancia como RIP (RIPv1 y RIPv2) e IGRP. Estas características incluyen:

- Reliable Transport Protocol (RTP)
- Actualizaciones limitadas
- Algoritmo de actualización por difusión (DUAL)
- Establecimiento de adyacencias
- Tablas de topología y de vecinos

Aunque EIGRP puede actuar como un protocolo de enrutamiento de estado de enlace, todavía sigue siendo un protocolo de enrutamiento por vector de distancia.

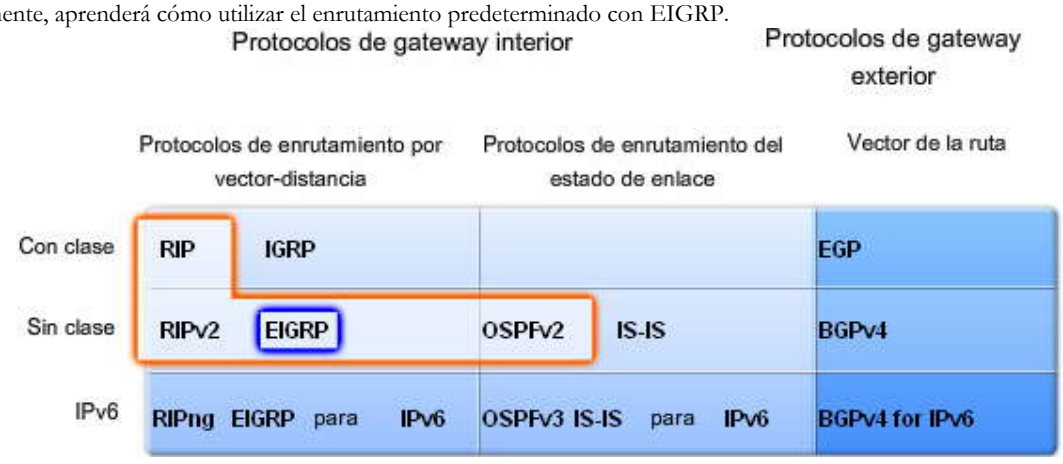
Nota: El término protocolo de enrutamiento híbrido a veces se utiliza para definir a EIGRP. Sin embargo, este término es engañoso porque EIGRP no es un híbrido de un protocolo de enrutamiento por vector de distancia y un protocolo de enrutamiento de estado de enlace, es únicamente un protocolo de enrutamiento por vector de distancia. Por lo tanto, Cisco ya no utiliza este término para referirse a EIGRP.

En este capítulo, aprenderá cómo configurar EIGRP y cómo verificar su configuración EIGRP con nuev os comandos show. También aprenderá la fórmula utilizada por EIGRP para calcular esta métrica compuesta.

El Reliable Transport Protocol (RTP) es exclusivo de EIGRP, el cual proporciona una entrega confiable y no confiable de paquetes EIGRP. Además, EIGRP establece relaciones con routers conectados directamente que también están habilitados para EIGRP. Las relaciones de vecinos se utilizan para llevar un registro del estado de estos vecinos. RTP y el rastreo de las adyacencias de vecinos prepara el terreno para el arma indispensable de EIGRP, el Algoritmo de actualización por difusión (DUAL).

Como motor informático que impulsa a EIGRP, DUAL reside en el centro del protocolo de enrutamiento, y garantiza rutas sin bucles y rutas de respaldo a través del dominio de enrutamiento. Aprenderá exactamente cómo selecciona DUAL una ruta para instalar en la tabla de enrutamiento y qué hace DUAL con las posibles rutas de respaldo.

Como RIPv2, EIGRP funciona con comportamiento de enrutamiento sin clase o con clase. Apr enderá cómo deshabilitar el resumen automático y luego cómo resumir manualmente redes para reducir el tamaño de las tablas de enrutamiento. Finalmente, aprenderá cómo utilizar el enrutamiento predeterminado con EIGRP.



**En este capítulo, aprenderá a:**

- Describa los antecedentes y la historia del EIGRP.
- Describa las características y el funcionamiento del EIGRP.
- Analice los comandos de configuración básica del EIGRP e identifique sus propósitos.
- Calcule la métrica compuesta que utiliza EIGRP.
- Describa los conceptos y el funcionamiento de DUAL.
- Describa los usos de los comandos de configuración adicional en EIGRP.

## 9.1 INTRODUCCION AL EIGRP.-

### 9.1.1 EIGRP: PROTOCOLO DE ENRUTAMIENTO POR VECTOR DE DINTANCIA MEJORADO.-

A pesar de que EIGRP se describe como un protocolo de enrutamiento por vector de distancia mejorado, aún sigue siendo un protocolo de enrutamiento por vector de distancia. Esto a veces puede crear confusión. Para poder apreciar las mejoras de EIGRP y para poder eliminar toda confusión, primero debemos analizar a su predecesor, IGRP.

**Raíces del EIGRP: IGRP**

Cisco desarrolló la patente de IGRP en 1985, en respuesta a algunas de las limitaciones de RIPv1, incluido el uso de la métrica de conteo de saltos y el tamaño máximo de red de 15 saltos.

En lugar del conteo de saltos, IGRP y EIGRP utilizan la métrica compuesta de ancho de banda, retraso, confiabilidad y carga. Los protocolos de enrutamiento utilizan sólo el ancho de banda y el retraso en forma predeterminada. Sin embargo, como IGRP es un protocolo de enrutamiento con clase que utiliza el algoritmo Bellman-Ford y actualizaciones periódicas, su utilidad es limitada en muchas de las redes de la actualidad.

Por lo tanto, Cisco mejoró IGRP con un nuevo algoritmo, DUAL y otras características. Los comandos para IGRP y EIGRP son similares, y en muchos casos idénticos. Esto permite una migración fácil de IGRP a EIGRP. Cisco suspendió IGRP y comenzó con IOS 12.2(13)T y 12.2(R1s4)S.

A pesar de estar analizado más detalladamente a lo largo de este capítulo, examinemos algunas de las diferencias entre un protocolo de enrutamiento por vector de distancia tradicional, tal como RIP e IGRP, y el protocolo de enrutamiento por vector de distancia mejorado, EIGRP.

La figura resume las diferencias más importantes entre el protocolo de enrutamiento por vector de distancia tradicional, tal como RIP, y el protocolo de enrutamiento por vector de distancia mejorado, EIGRP.

**El algoritmo**

Todos los protocolos de enrutamiento por vector de distancia tradicionales utilizan alguna variante del algoritmo Bellman-Ford o Ford-Fulkerson. Estos protocolos, como RIP e IGRP, hacen expirar las entradas de enrutamiento individuales, y por lo tanto deben enviar periódicamente actualizaciones de la tabla de enrutamiento.

EIGRP utiliza el Algoritmo de actualización por difusión (DUAL). Aunque sigue siendo un protocolo de enrutamiento por vector de distancia, EIGRP con DUAL implementa características que no se encuentran en los protocolos de enrutamiento por vector de distancia. EIGRP no envía actualizaciones periódicas y las entradas de ruta no expiran. En su lugar, EIGRP utiliza un protocolo Hello liviano para supervisar el estado de las conexiones con sus vecinos. Sólo los cambios en la información de enrutamiento, tales como un nuevo enlace o un enlace que ya no está disponible, producen una actualización de enrutamiento. Las actualizaciones de enrutamiento EIGRP son todavía vectores de distancia transmitidos a vecinos conectados directamente.

**Determinación de ruta**

Los protocolos de enrutamiento por vector de distancia tradicionales, como RIP e IGRP, llevan un registro sólo de las rutas preferidas; el mejor camino hacia una red de destino. Si la ruta no se encuentra disponible, el router espera otra actualización de enrutamiento con una ruta para esta red remota.

DUAL de EIGRP mantiene una tabla de topología separada de la tabla de enrutamiento, que incluye el mejor camino hacia una red de destino y toda ruta de respaldo que DUAL haya determinado como sin bucles. Sin bucles significa que el vecino no tiene una ruta hacia la red de destino que pase por este router.

Más adelante en este capítulo, verá que para que DUAL considere a una ruta como una ruta de respaldo sin bucles válida, debe cumplir con un requerimiento conocido como condición de factibilidad. Toda ruta de respaldo que cumpla con esta condición tiene la garantía de ser sin bucles. Como EIGRP es un protocolo de enrutamiento por vector de distancia, es posible que haya rutas de respaldo sin bucles hacia una red de destino que no cumplan con la condición de factibilidad. Por lo tanto, DUAL no incluye a estas rutas en la tabla de topología como una ruta de respaldo sin bucles.

Si una ruta no se encuentra disponible, DUAL buscará su tabla de topología en busca de una ruta de respaldo válida. Si existe una, esa ruta ingresa inmediatamente a la tabla de enrutamiento. Si no existe una, DUAL realiza un proceso de descubrimiento de red para ver si por casualidad existe una ruta de respaldo que no cumplió con los requerimientos de la condición de factibilidad. Este proceso se analiza con mayor profundidad más adelante en este capítulo.

**Convergencia**

Los protocolos de enrutamiento por vector de distancia tradicionales, tales como RIP e IGRP, utilizan actualizaciones periódicas. Debido a la naturaleza poco confiable de las actualizaciones periódicas, los protocolos de enrutamiento por vector de distancia tradicionales tienden a tener problemas de routing loops y de cuenta a infinito. RIP e IGRP utilizan varios mecanismos para ayudar a evitar estos problemas, incluidos los temporizadores de espera, que producen tiempos de convergencia más largos.

EIGRP no utiliza temporizadores de espera. En su lugar, las rutas sin bucles se logran a través de un sistema de cálculos de ruta (cálculos por difusión) que se realizan de manera coordinada entre los routers. El detalle de cómo se realiza va más allá del alcance de este curso, pero el resultado es una convergencia más rápida que la de los protocolos de enrutamiento por vector de distancia tradicionales.


Resumen de las operaciones

| Protocolos de enrutamiento por vector de distancia tradicionales | Protocolo de enrutamiento por vector de distancia mejorado: EIGRP |
|---|---|
| • Utilizan el algoritmo de Bellman-Ford o Ford-Fulkerson.<br>• Conservan las entradas de enrutamiento y utilizan actualizaciones periódicas.<br>• Realizan un seguimiento sólo de las mejores rutas; la mejor ruta hacia una red de destino.<br>• Cuando una ruta no está disponible, el router debe esperar una nueva actualización de enrutamiento.<br>• Convergencia más lenta debido a los temporizadores de espera. | • Utiliza el Algoritmo de actualización por difusión (DUAL).<br>• No conserva las entradas de enrutamiento ni utiliza actualizaciones periódicas.<br>• Mantiene una tabla de topología independiente de la tabla de enrutamiento, que incluye la mejor ruta y rutas de respaldo sin bucles.<br>• Cuando una ruta no está disponible, DUAL utilizará una ruta de respaldo, si hubiere alguno en la tabla de topología.<br>• Convergencia más rápida debido a la ausencia de temporizadores de espera y un sistema coordinado de cálculo de rutas. |

### 9.1.2 FORMATO DE MENSAJES DE EIGRP.-

**Coloque el cursor sobre los campos en el Mensaje de EIGRP encapsulado para ver el proceso de encapsulación.**

La porción de datos de un mensaje EIGRP se encapsula en un paquete. Este campo de datos se denomina Tipo/Longitud/Valor o TLV. Como se muestra en la figura, los tipos de TLV relevantes para este curso son Parámetros EIGRP, Rutas internas IP y Rutas externas IP. Los componentes del campo de datos TLV se analizan en mayor profundidad en la próxima página.

El encabezado del paquete EIGRP se encuentra incluido en cada paquete EIGRP, sin importar su tipo. Luego, el encabezado del paquete EIGRP y TLV se encapsulan en un paquete IP. En el encabezado del paquete IP, el campo Protocolo se establece en 88 para indicar EIGRP, y la dirección de destino se establece en multicast 224.0.0.10. Si el paquete

EIGRP se encapsula en una trama de Ethernet, la dirección MAC de destino es también una dirección multicast: 01-00-5E-00-00-0A.


**Nota:** En el siguiente análisis de los mensajes EIGRP, muchos campos se encuentran más allá del alcance de este curso. Se muestran todos los campos a fin de brindar una imagen exacta del formato del mensaje EIGRP. Sin embargo, sólo se analizan los campos relevantes al candidato CCNA.

**Haga clic en Encabezado de paquetes EIGRP en la figura.**

Cada mensaje EIGRP incluye el encabezado. Los campos importantes para nuestro análisis incluyen el campo Código de operación y el campo Número de sistema autónomo. El Código de operación especifica el tipo de paquete EIGRP:

- Actualización
- Consulta
- Respuesta
- Saludo

El número de sistema autónomo (AS) especifica el proceso de enrutamiento EIGRP. A diferencia de RIP, los routers de Cisco pueden ejecutar múltiples instancias de EIGRP. El número de AS se utiliza para rastrear instancias múltiples de EIGRP.

Los tipos de paquetes EIGRP se analizan más adelante en este capítulo.

**Haga clic en TLV: Parámetros de EIGRP en esta figura.**

Los mensajes de los parámetros EIGRP incluyen la ponderación que EIGRP utiliza para su métrica compuesta. Solo el ancho de banda y el retraso se ponderan de manera predeterminada. Ambos se ponderan de igual manera, por lo tanto, el campo K1 para el ancho de banda y el campo K3 para el retraso se establecen en 1. Los otros valores K se establecen en cero. Más adelante en este capítulo, se analizan más detalladamente los cálculos métricos.

El Tiempo de espera es la cantidad de tiempo que el vecino EIGRP que recibe este mensaje debe esperar antes de considerar que router que realiza la notificación se encuentra desactivado. Mas adelante en este capítulo, se analiza con mayor detalle el Tiempo de espera.

**Haga clic en TLV: IP interno en esta figura.**

El mensaje IP interno se utiliza para publicar rutas EIGRP dentro de un sistema autónomo. Entre los campos importantes para nuestro análisis se incluyen: los campos de métrica (Retraso y Ancho de banda), el campo de la máscara de subred (Duración de prefijo), y el campo Destino.

El retraso se calcula como la suma de retrasos desde el origen hacia el destino en unidades de 10 microsegundos. El ancho de banda es el que cuenta con la configuración más baja en todas las interfaces de la ruta.

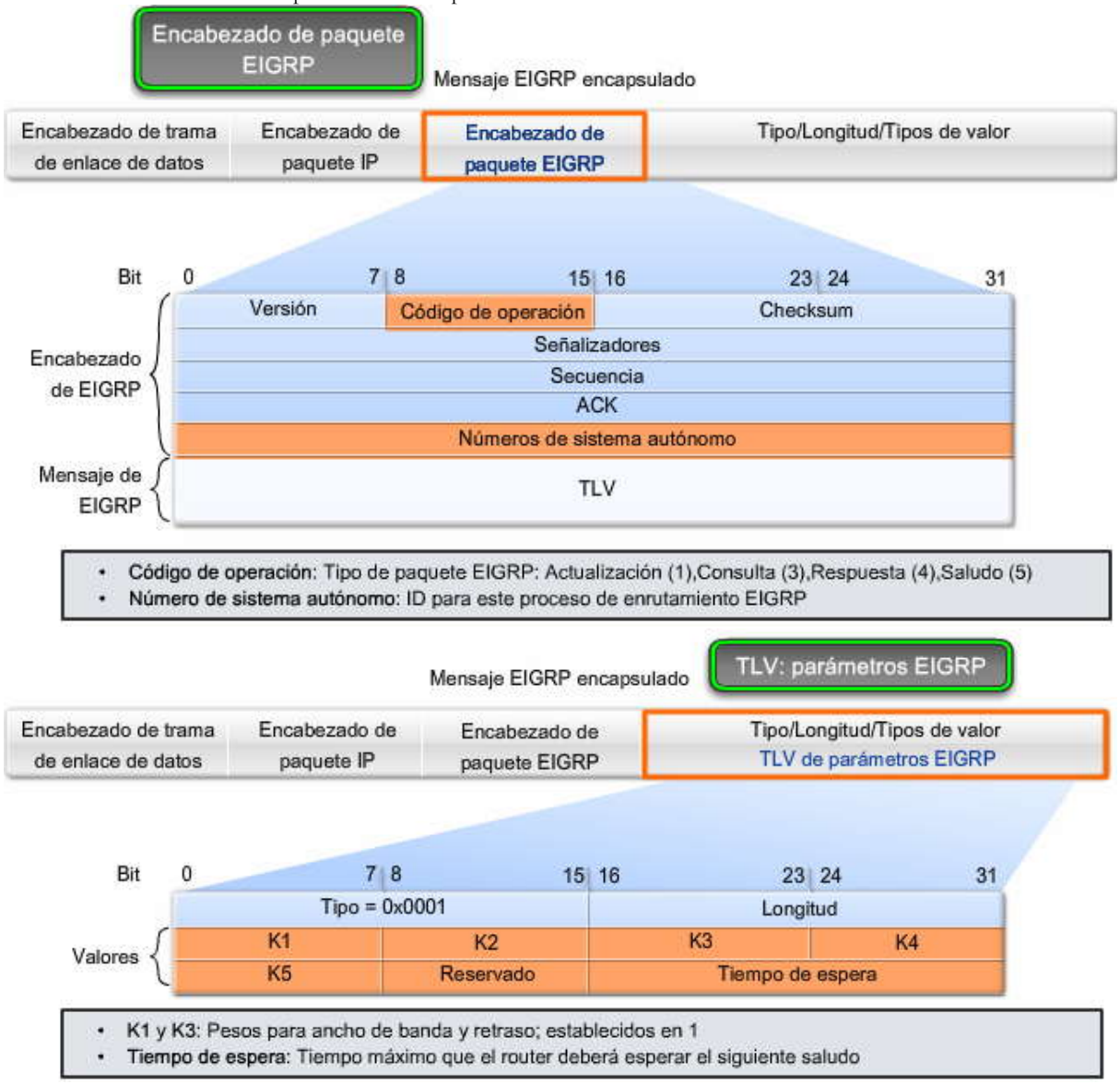
La máscara de subred se especifica como la duración de prefijo o el número de bits de la red en la máscara de subred. Por ejemplo, la duración de prefijo para la máscara de subred 255.255.255.0 es 24 porque 24 es la cantidad de bits de la red.

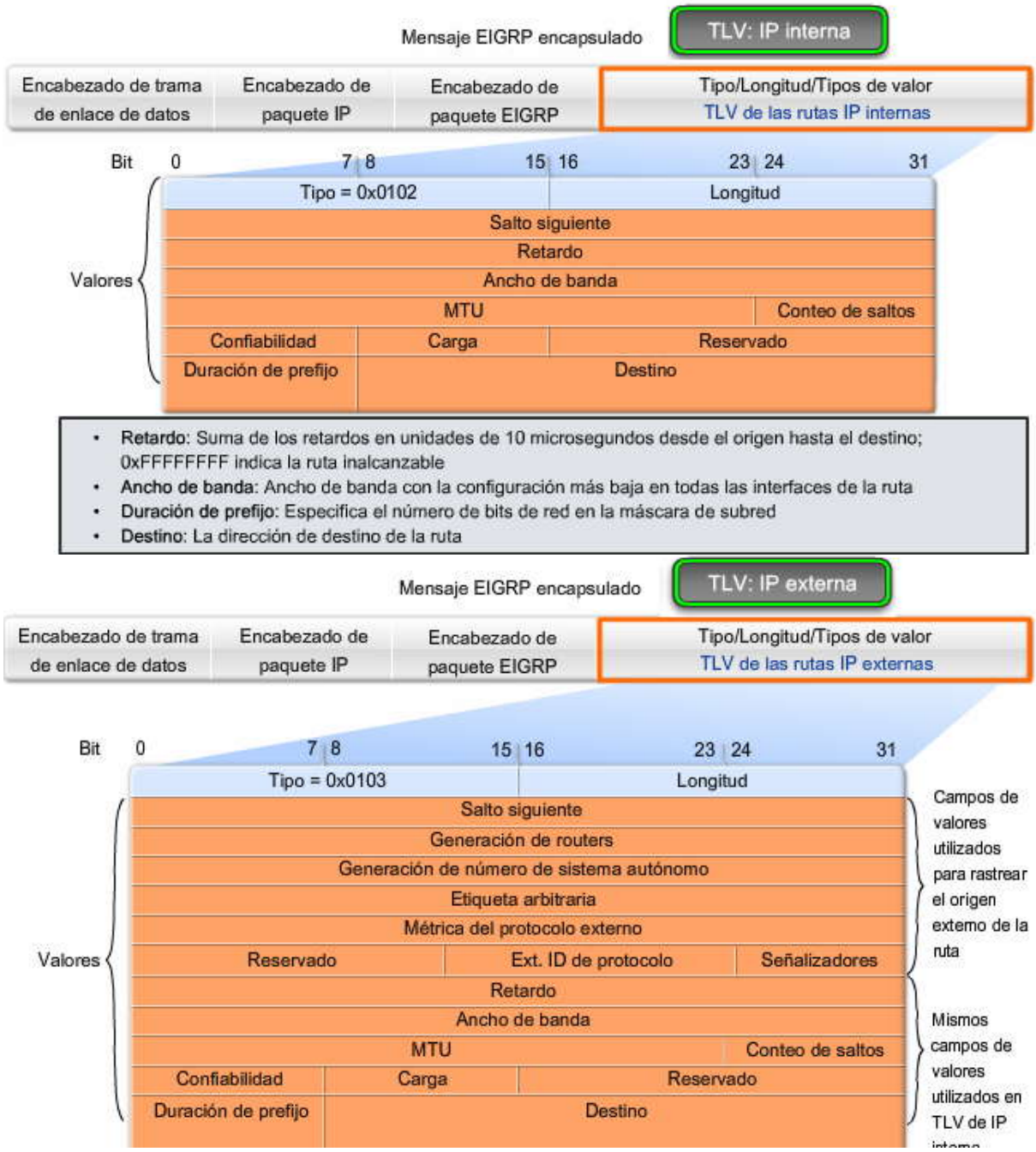
El campo Destino almacena la dirección de la red de destino. A pesar de que se muestran sólo 24 bits en esta figura, este campo varía en función del valor de la porción de red de la dirección de red de 32 bits. Por ejemplo, la porción de red de 10.1.0.0/16 es 10.1. Por lo tanto, el campo Destino almacena los primeros 16 bits. Como la longitud mínima de este campo es de 24 bits, el resto del campo se rellena con ceros. Si una dirección de red es más larga que 24 bits (192.168.1.32/27, por ejemplo), entonces el campo Destino se extiende otros 32 bits más (con un total de 56 bits) y los bits no utilizados se completan con ceros.

**Haga clic en TLV: IP externo en la figura.**

El mensaje IP externo se utiliza cuando las rutas externas se importan en el proceso de enrutamiento EI GRP. En este capítulo, importaremos o redistribuiremos una ruta estática por defecto en EIGRP. Observe que la mitad inferior del TLV de IP externo incluye todos los campos utilizados por el TLV de IP interno.

**Nota:** Algunos libros sobre EIGRP pueden afirmar incorrectamente que la Unidad máxima de transmisión (MTU) es una de las métricas utilizadas por EIGRP. MTU no es una métrica utilizada por EIGRP. MTU está incluida en las actualizaciones de enrutamiento pero no se utiliza para determinar la métrica de enrutamiento.

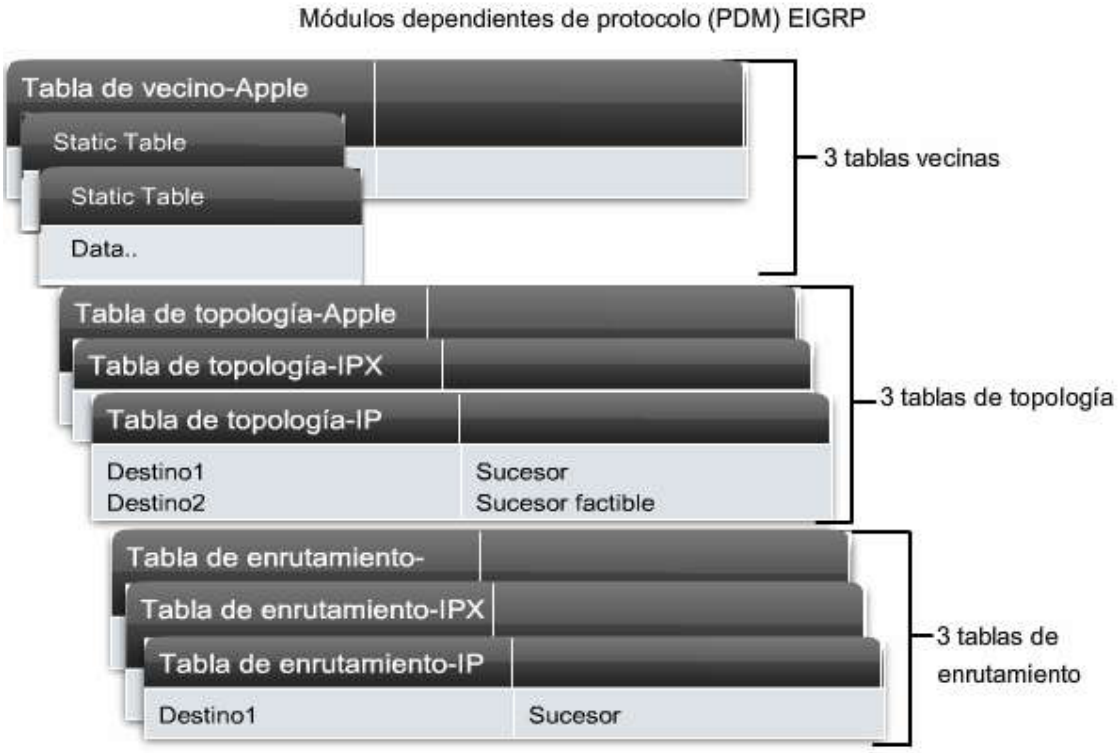





### 9.1.3 MODULOS DEPENDIENTES DE PROTOCOLO (PDM).-

EIGRP tiene la capacidad de realizar el enrutamiento de distintos protocolos, incluidos IP, IPX y Apple Talk, mediante el uso de módulos dependientes de protocolo (PDM). Los PDM son responsables de las tareas de enrutamiento específicas de cada protocolo de capa de Red.

Por ejemplo:
El módulo IP-EIGRP es responsable de enviar y recibir paquetes EIGRP encapsulados en IP y de utilizar a DUAL para construir y mantener la tabla de enrutamiento IP. Como se puede ver en la figura, EIGRP utiliza distintos paquetes EIGRP y mantiene vecinos, topología y tablas de enrutamiento separadas para cada protocolo de la capa de Red.
El módulo IPX EIGRP es responsable de intercambiar información de enrutamiento acerca de las redes IPX con otras rutas IPX EIGRP. IPX EIGRP y Appletalk EIGRP no están incluidos en este curso.

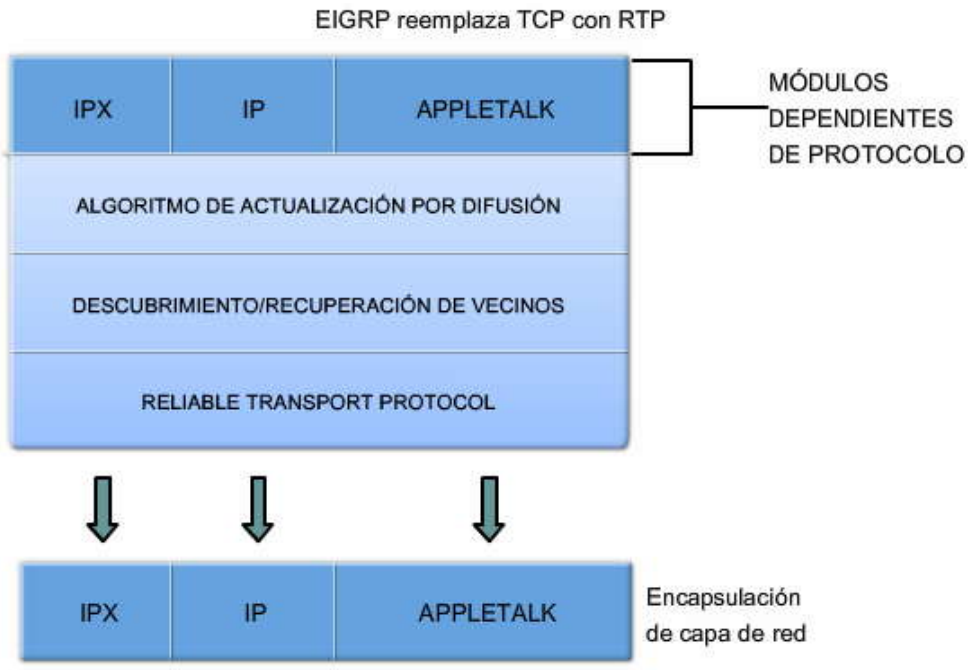



### 9.1.4 TIPOS DE PAQUETES RTP Y EIGRP.-

El Reliable Transport Protocol (RTP) es el protocolo utilizado por EIGRP para la entrega y recepción de pa quetes EIGRP. EIGRP fue diseñado como un protocolo de enrutamiento independiente de la capa de Red; por lo tanto, no puede utilizar los servicios UDP ni TCP porque IPX y Appletalk no utilizan protocolos de la suite de protocolos TCP/IP. La figura muestra conceptualmente cómo funciona RTP.

Aunque "Reliable" (confiable) forma parte de su nombre, RTP incluye la entrega confiable y la entrega no confiable de paquetes EIGRP, similar a TCP y UDP, respectivamente. RTP confiable requiere que el receptor envíe un acuse de recibo al emisor. Un paquete RTP no confiable no requiere ningún acuse de recibo.

RTP puede enviar paquetes como unicast o multicast. Los paquetes EIGRP multicast utilizan la dirección multicast reservada de 224.0.0.10



**Tipos de paquetes EIGRP**

EIGRP utiliza cinco tipos de paquetes distintos, algunos en pares.

**Haga clic en Saludo en la figura.**
EIGRP utiliza los paquetes de saludo para descubrir vecinos y para formar adyacencias con ellos. Los paquetes de saludo EIGRP son multicast y utilizan una entrega no confiable. Se analizarán los paquetes de saludo EIGRP en una sección posterior.

**Haga clic en Actualizar y en ACK en la figura.**
Los paquetes de actualización se utilizan para propagar la información de enrutamiento. A diferencia de RIP, EIGRP no envía actualizaciones periódicas. Los paquetes de actualización se envían sólo cuando es necesario. Las actualizaciones de EIGRP sólo contienen la información de enrutamiento necesaria y sólo se envían a los routers que la requieren. Los paquetes de actualización EIGRP utilizan una entrega confiable. Los paquetes de actualización se envían como multicast cuando son requeridos por múltiples routers, o como unicast cuando son requeridos por sólo un router. En la figura, debido a que los enlaces son punto a punto, las actualizaciones se envían como unicast.

**Los paquetes de acuse de recibo (ACK**) se envían a través de EIGRP cuando se utiliza una entrega confiable. RTP utiliza una entrega confiable para los paquetes EIGRP de actualización, consulta y respuesta. Los paquetes de acuse de recibo EIGRP siempre se envían como unicast no confiable. Los paquetes de acuse de recibo EIGRP utilizan la entrega no confiable.

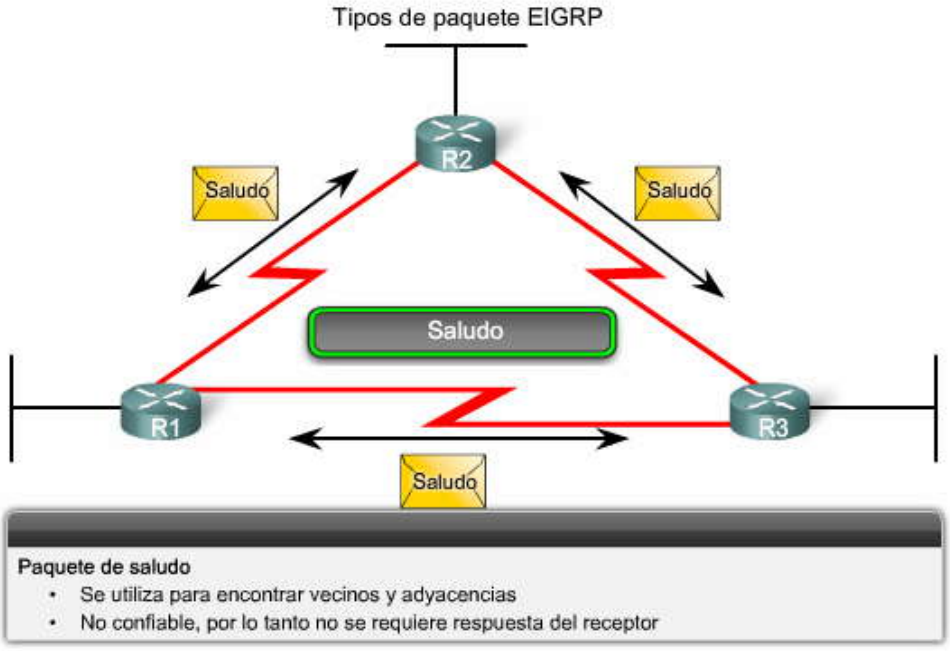
En la figura, R2 ha perdido la conectividad con la LAN conectada a su interfaz FastEthernet. R2 e nvía inmediatamente una actualización a R1 y R3 cuando determina que la ruta se encuentra caída. R1 y R3 responden con un acuse de recibo.

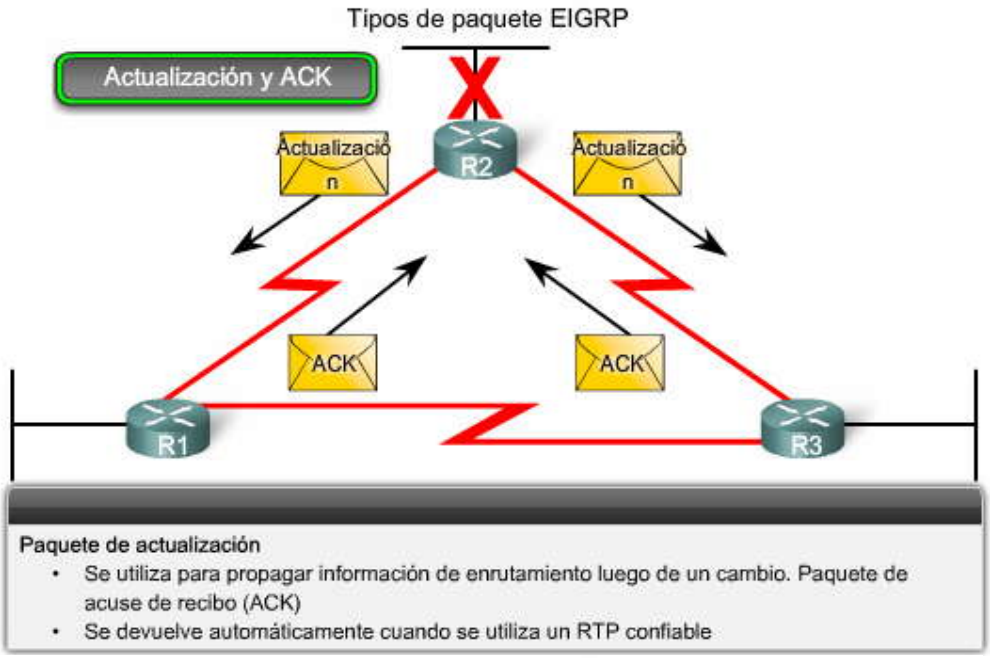
**Haga clic en Consulta y Respuesta en la figura.**
**Los paquetes de consulta y respuesta** son utilizados por DUAL cuando busca redes y otras tareas. Los paquetes de consulta y respuesta utilizan una entrega confiable. Las consultas utilizan multicast o unicast, mientras que las respuestas se envíen siempre como unicast. DUAL se analiza en una sección posterior. Los paquetes de consulta y respuesta se analizan con mayor detalle en CCNP.

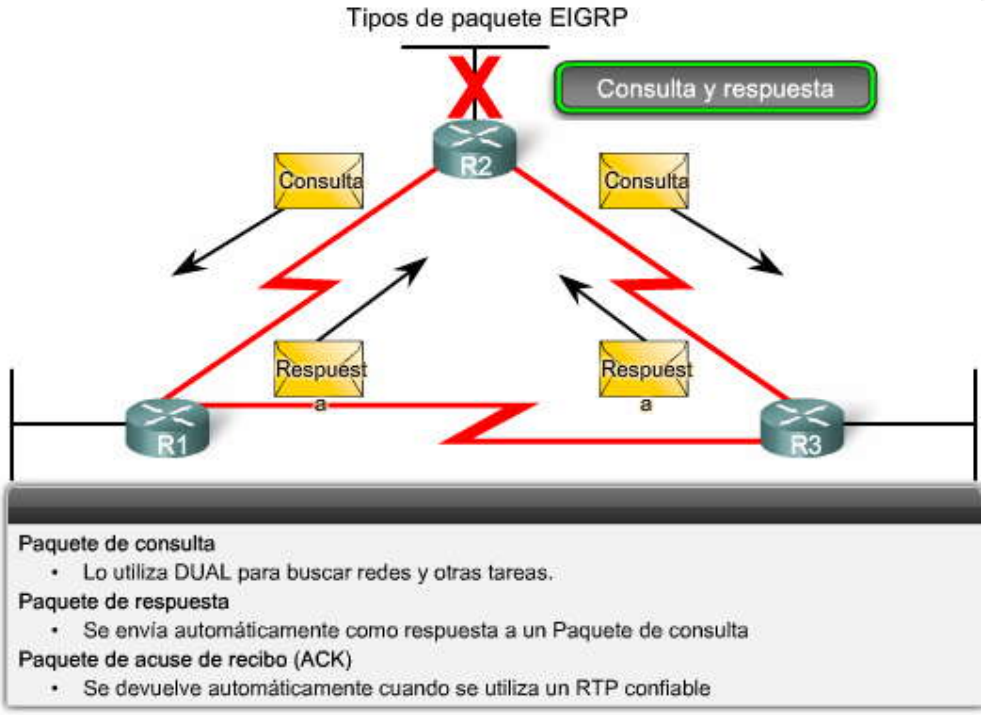
En la figura, R2 ha perdido la conectividad con LAN y envía consultas a todos los vecinos EIGRP y busca cualquier ruta posible hacia la LAN. Como las consultas utilizan una entrega confiable, el router receptor debe devolver un acuse de recibo EIGRP. (Para que el ejemplo sea simple, se omitieron los acuses de recibo en el gráfico.)

Todos los vecinos deben enviar una respuesta sin importar si tienen o no una ruta hacia la red caída. Como las re spuestas también utilizan una entrega confiable, los routers como R2, deben enviar un acuse de recibo.

Nota: Quizás se pregunte por qué R2 enviaría una consulta a una red que sabe que está caída. En realidad, sólo la interfaz conectada a la red está caída. Otro router podría estar conectado a la misma LAN. Por lo tanto, R2 consulta sobre ese router antes de retirar por completo la red de su base de datos.





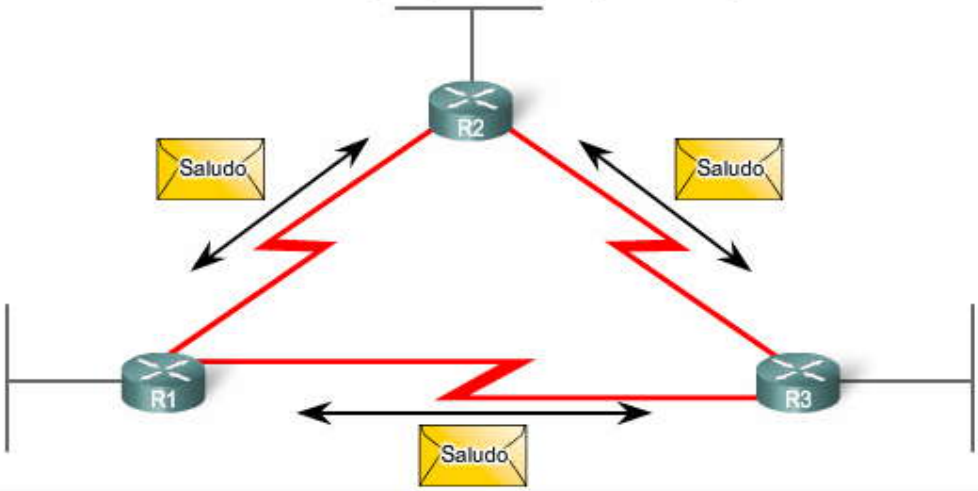

### 9.1.5 PROTOCOLO DE SALUDO.-

Antes de poder intercambiar cualquier paquete EIGRP entre los routers, EIG RP debe descubrir primero a sus vecinos. Los vecinos de EIGRP son otros routers que ejecutan EIGRP en redes conectadas directamente o compartidas.

Los routers EIGRP descubren vecinos y establecen adyacencias con los routers vecinos mediante el paquete de saludo. En la mayoría de las redes, los paquetes de saludo EIGRP se envían cada 5 segundos. En las redes de accesos múltiples sin broadcast (NBMA) y de punto múltiple, como X.25, Frame Relay e interfaces ATM con enlaces de acceso de T1 (1.544 Mbps) o más lentos, los Hello son unicast cada 60 segundos. Un router EIGRP supone que mientras reciba los paquetes de saludo de un vecino, el vecino y sus rutas permanecen viables.

El tiempo de espera le indica al router el tiempo máximo que debe esperar para recibi r el próximo Hello antes de declarar al vecino como inalcanzable. De manera predeterminada, el tiempo de espera es tres veces el intervalo de saludo, o 15 segundos en la mayoría de las redes, y 180 segundos en las redes NBMA de velocidad baja. Si el tiempo de espera expira, EIGRP declarará la ruta como desactivada y DUAL buscará una nueva ruta mediante el envío de consultas.

Intervalos de saludo y tiempos en espera por defecto para EIGRP




| Ancho de banda | Enlace de ejemplo | Intervalo de saludo por defecto | Tiempo en espera por defecto |
|---|---|---|---|
| 1544 Mbps | Frame Relay multipunto | 60 segundos | 180 segundos |
| Mayor que 1544 Mbps | T1, Ethernet | 5 segundos | 15 segundos |

**9.1.6 ACTUALIZACIONES LIMITADAS DE EIGRP.-**

EIGRP utiliza el término parcial o limitado cuando se refiere a sus paquetes de actualización. A diferencia de RIP, EIGRP no envía actualizaciones periódicas. En su lugar, EIGRP envía sus actualizaciones sólo cuando la métrica de una ruta cambia.

El término parcial significa que la actualización sólo envía información acerca de los cambios de ruta. EIGRP envía estas actualizaciones incrementales cuando el estado de un destino cambia, en lugar de enviar todos los contenidos de la tabla de enrutamiento.

El término limitado hace referencia a la propagación de las actualizaciones parciales enviadas sólo a aquellos routers que se ven afectados por el cambio. La actualización parcial se "limita" automáticamente para que sólo se actualicen los routers que necesitan la información.

Al enviar sólo la información de enrutamiento necesaria y sólo a los routers que la necesitan, EIGRP minimiza el ancho de banda requerido para enviar los paquetes EIGRP.

Actualizaciones de EIGRP

| Las actualizaciones de EIGRP son parciales y limitadas: |
|---|
| *Parcial* porque la actualización sólo incluye la información sobre los cambios de la ruta. |
| *Limitada* porque sólo recibirán la actualización aquellos routers afectados por el cambio. |

**9.1.7 DUAL: INTROIDUCCION.-**

El Algoritmo de actualización por difusión (DUAL) es el algoritmo de convergencia utilizado por EIGRP en lugar de los algoritmos Bellman-Ford o Ford Fulkerson utilizados por otros protocolos de enrutamiento por vector de distancia, como RIP. DUAL está basado en investigaciones realizadas en SRI International, mediante el uso de cálculos propuestos por primera vez por E.W. Dijkstra y C.S. Scholten. El trabajo más destacado con DUAL lo realizó J.J. Garcia-Luna-Aceves.

Los routing loops, incluso los temporarios, pueden ser extremadamente perjudiciales para el rendimiento de la red. Los protocolos de enrutamiento por vector de distancia, como RIP, impiden routing loops con temporizadores de espera y horizontes divididos. A pesar de que EIGRP utiliza ambas técnicas, las usa de manera un tanto diferentes; la forma principal en la que EIGRP impide routing loops es con el algoritmo DUAL.

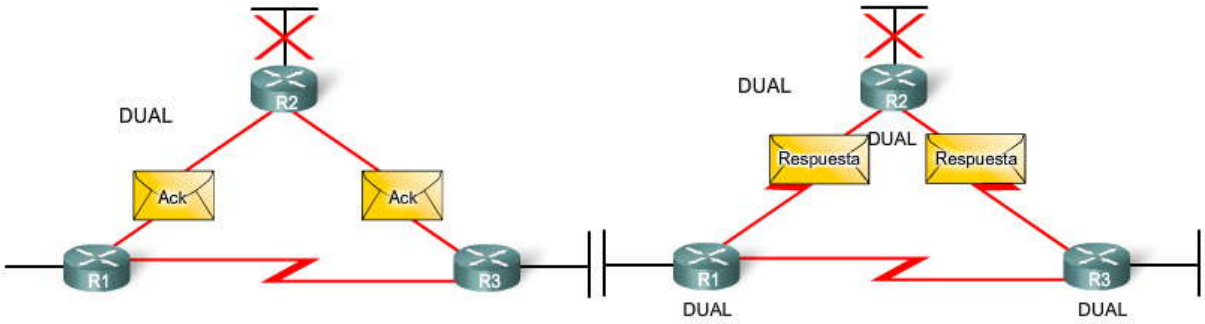
**Haga clic en Reproducir para ver el funcionamiento básico de DUAL.**

El algoritmo DUAL se utiliza para que no se produzcan bucles a cada instante, a lo largo de un cálculo de ruta. Esto permite que todos los routers involucrados en un cambio de topología se sincronicen al mismo tiempo. Los routers que no se ven afectados por los cambios en la topología no se encuentran involucrados en el recálculo. Este método proporciona a EIGRP mayor tiempo de convergencia que a otros protocolos de enrutamiento por vector de distancia.

La Máquina de Estado Finito DUAL realiza todo el proceso de decisión para todos los cálculos de ruta. En términos generales, una Máquina de Estado Finito (FSM) es un modelo de comportamiento compuesto de un número finito de estados, transiciones entre esos estados, y eventos o acciones que crean las transacciones.

FSM DUAL rastrea todas las rutas, utiliza su métrica para seleccionar rutas eficientes y sin bucles, y selecciona las rutas con la ruta de menor costo para insertarla en la tabla de enrutamiento. Se analizará FSM DUAL en mayor detalle en este capítulo.

Como el recálculo del algoritmo DUAL puede exigir mucho al procesador, es aconsejable evitar el recálculo siempre que sea posible. Por lo tanto, DUAL mantiene una lista de rutas de respaldo que ya ha determinado como sin bucles. Si la ruta principal en la tabla de enrutamiento falla, el mejor camino de respaldo se agrega de inmediato a la tabla de enrutamiento.




### 9.1.8 DISTANCIA ADMINISTRATIVA.-

Como se vio en el Capítulo 3, "Introducción a los protocolos de enrutamiento dinámicos", la distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. EIGRP tiene una distancia administrativa predeterminada de 90 para las rutas internas y de 170 para las rutas importadas desde un origen externo, como rutas por defecto. Cuando se lo compara con otros protocolos de gateway interior (IGP), EIGRP es el que IOS de Cisco prefiere porque cuenta con la distancia administrativa más baja.

Observe en la figura que EIGRP tiene un tercer valor AD, de 5, para rutas resumidas. Más adelante en este capítulo, aprenderá cómo configurar rutas EIGRP resumidas.

Distancias administrativas predeterminadas

| Origen de la ruta | Distancia administrativa |
|---|---|
| Conectado | 0 |
| Estático | 1 |
| Ruta de resumen de EIGRP | 5 |
| BGP externo | 20 |
| EIGRP interno | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EIGRP externo | 170 |
| BGP interno | 200 |

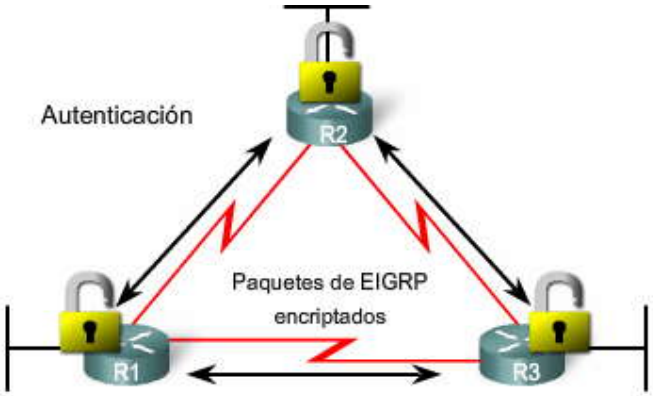
### 9.1.9 AUTENTICACION.-

Al igual que otros protocolos de enrutamiento, EIGRP puede configurarse para autenticación. RIPv2, EIGRP, OSPF, IS -IS y BGP pueden configurarse para encriptar y autenticar su información de enrutamiento.

Es aconsejable autenticar la información de enrutamiento transmitida. Esto garantiza que los routers sólo aceptarán información de enrutamiento de otros routers que estén configurados con la misma contraseña o información de autenticación.

Nota: La autenticación no encripta la tabla de enrutamiento del router.

Como se mencionó en capítulos anteriores, la configuración de protocolos de enrutamiento para utilizar la autenticación se analizará en un curso posterior.




## 9.2 CONFIGURACION BASICA DEL EIGRP.-

### 9.2.1 TOPOLOGIA DE LA RED EIGRP.-

La figura muestra la topología de capítulos anteriores, pero ahora incluye el agregado del router ISP. Observe que ambos routers, el R1 y el R2, tienen subredes que forman parte de la red con clase 172.16.0.0/16, una dirección de clase B. El hecho de que 172.16.0.0 es una dirección de clase B es sólo relevante porque EIGRP resume automáticamente en bordes con clase, de manera similar a RIP.

**Haga clic en R1, R2 y R3 para ver la configuración de inicio de cada router.**

Observe que el router ISP no existe físicamente en nuestras configuraciones. La conexión entre R2 e ISP está representada con una interfaz loopback en el router R2. Recuerde del Capítulo 7, "RIPv2", que una interfaz loopback se puede utilizar para representar una interfaz en un router que no tiene una conexión real con un enlace físico en la red. Las direcciones de loopback pueden verificarse con el comando ping y pueden incluirse en las actualizaciones de enrutamiento.

Nota: Las interfaces loopback también tienen usos específicos con algunos protocolos de enrutamiento, como veremos en el Capítulo 11, OSPF.

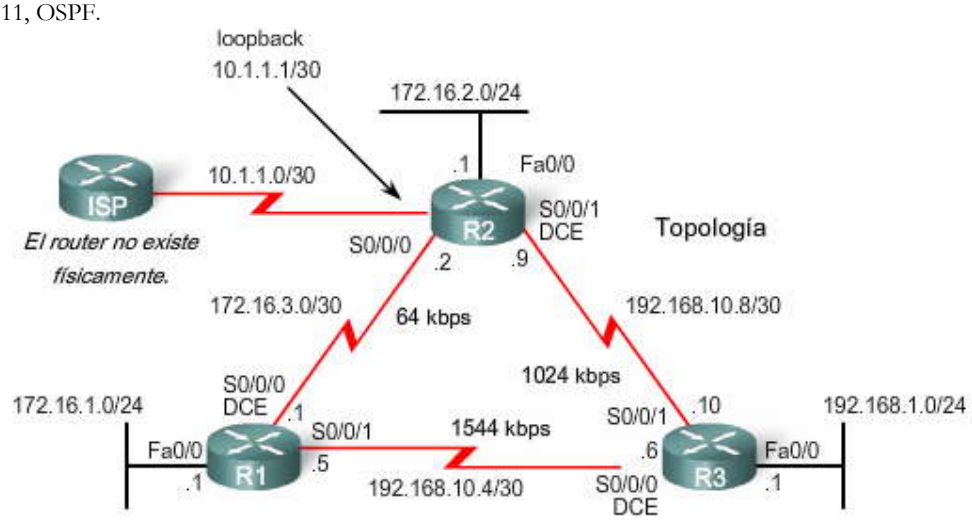


Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 172.16.1.1 | 255.255.255.0 |
| | S0/0/0 | 172.16.3.1 | 255.255.255.252 |
| | S0/0/1 | 192.168.10.5 | 255.255.255.252 |
| R2 | Fa0/0 | 172.16.2.1 | 255.255.255.0 |
| | S0/0/0 | 172.16.3.2 | 255.255.255.252 |
| | S0/0/1 | 192.168.10.9 | 255.255.255.252 |
| | Lo1 | 10.1.1.1 | 255.255.255.252 |
| R3 | Fa0/0 | 192.168.1.1 | 255.255.255.0 |
| | S0/0/0 | 192.168.10.6 | 255.255.255.252 |
| | S0/0/1 | 192.168.10.10 | 255.255.255.252 |

Configuración de inicio de R1

```
R1#show startup-config

<some output omitted>
!
hostname R1
!
interface FastEthernet0/0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 172.16.3.1 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 description Link to R3
 ip address 192.168.10.5 255.255.255.252
!
end
```

Configuración de inicio de R2

```
R2#show startup-config

<some output omitted>
!
hostname R2
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.252
 description Simulated ISP
!
interface FastEthernet0/0
 ip address 172.16.2.1 255.255.255.0
!
interface Serial0/0/0
 ip address 172.16.3.2 255.255.255.252
!
interface Serial0/0/1
 ip address 192.168.10.9 255.255.255.252
 clockrate 64000
!
end
```

Configuración de inicio de R3

```
R3#show startup-config

<some output omitted>
!
hostname R3
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.10.6 255.255.255.252
 clockrate 64000
!
interface Serial0/0/1
 ip address 192.168.10.10 255.255.255.252
!
end
```

### 9.2.2 SISTEMA AUTONOMO DE ID DE PROCESO.-

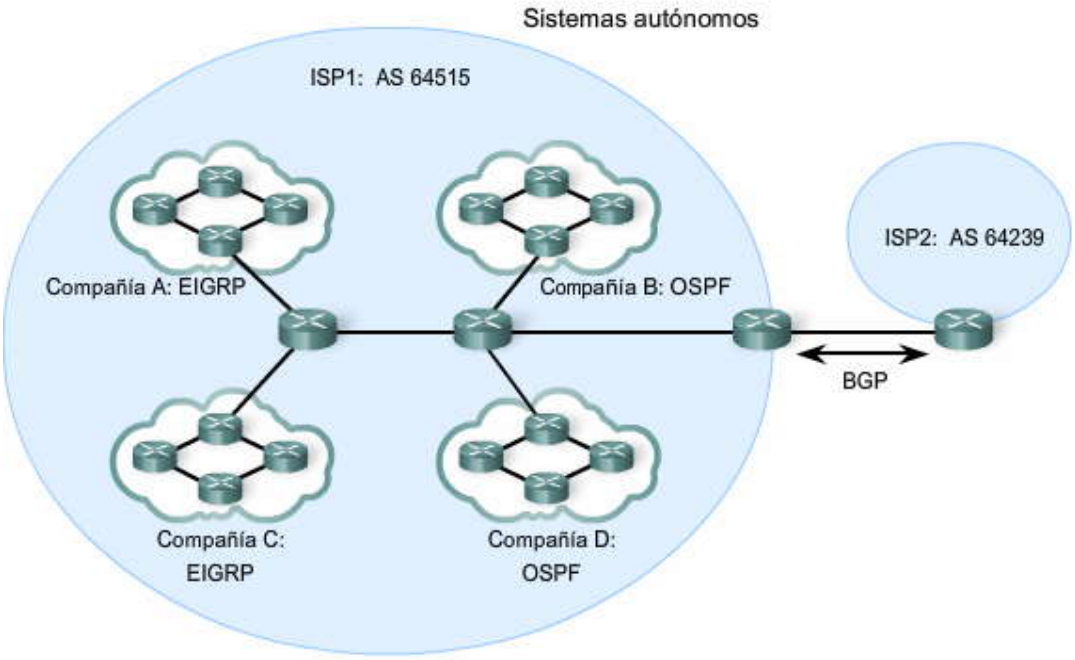
**Sistema autónomo**

Un sistema autónomo (AS) es un conjunto de redes bajo el control administrativo de una única entidad que presenta una política de enrutamiento común para Internet. En la figura, las empresas A, B, C y D se encuentran todas bajo el control administrativo de ISP1. ISP1 "presenta una política de enrutamiento común" para todas estas empresas cuando publica rutas en ISP2.

Los lineamientos para la creación, selección y registro del sistema autónomo se describen en RFC 1930. La Autoridad de números asignados de Internet (IANA) asigna números AS, la misma autoridad que asigna el espacio de dirección IP. Usted aprendió acerca de IANA y de sus registros regionales de Internet (RIRS) en un curso anterior. El RIR local es responsable de la asignación del número de AS a una entidad de su bloque de números de AS asignados. Antes del 2007, los números de AS eran números de 16 bits, que iban de 0 a 65535. En la actualidad, se asignan números de AS de 32 bits, con lo que se aumenta el número de AS disponibles a más de 4 mil millones.

¿Quién necesita un número de sistema autónomo? Por lo general los ISP (Proveedores de servicios de Internet), los proveedores de backbone de Internet y grandes instituciones que se conectan con otras entidades que también cuentan con un número de AS. Estos ISP y las grandes instituciones utilizan el Border Gateway Protocol, o BGP, del protocolo de enrutamiento de gateway exterior para propagar información de enrutamiento. BGP es el único protocolo de enrutamiento que utiliza un número de sistema autónomo real en su configuración.

La gran mayoría de las empresas e instituciones con redes IP no necesitan un número de AS porque se encuentran bajo el control de una entidad más grande, como un ISP. Estas empresas utilizan protocolos de gateway interior como RIP, EIGRP, OSPF e IS-IS para realizar el enrutamiento de paquetes dentro de sus propias redes. Son una de muchas redes independientes dentro del sistema autónomo de ISP. ISP es responsable del enrutamiento de paquetes dentro del sistema autónomo y entre otros sistemas autónomos.




**ID de proceso**

EIGRP y OSPF usan el ID de proceso para representar una instancia del protocolo de enrutamiento respectivo que se ejecuta en el router.

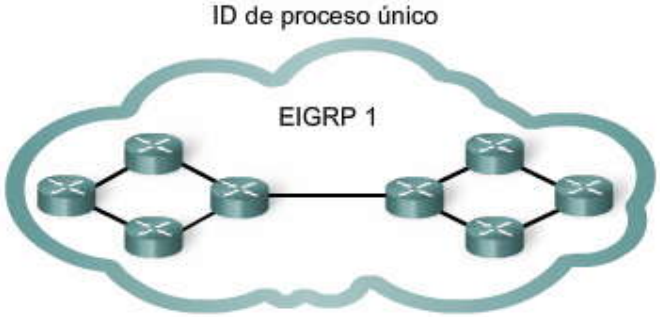
Router(config)#router eigrp autonomous-system

Aunque EIGRP hace referencia al parámetro como un número de "sistema autónomo", en realidad funciona como un ID de proceso. El número no se encuentra asociado con ningún número de sistema autónomo analizado previamente y se le puede asignar cualquier valor de 16 bits.

Router(config)#router eigrp 1

En este ejemplo, el número 1 identifica este proceso EIGRP en particular que se ejecuta en este router. Para poder establecer adyacencias de vecinos, EIGRP requiere que todos los routers del mismo dominio de enrutamiento estén configurados con el mismo ID de proceso. Por lo general, sólo se configura un único ID de proceso de cualquier protocolo de enrutamiento en un router.

Nota: RIP no utiliza ID de proceso; por lo tanto, sólo admite una única instancia de RIP. EIGRP y OSPF admiten instancias múltiples de cada protocolo de enrutamiento, aunque, por lo general, no es necesario o no se recomienda la implementación de este tipo de protocolo de enrutamiento múltiple.




```
R1(config)#router eigrp ?
  <1-65535>  Autonomous system number
R1(config)#router eigrp 1
```

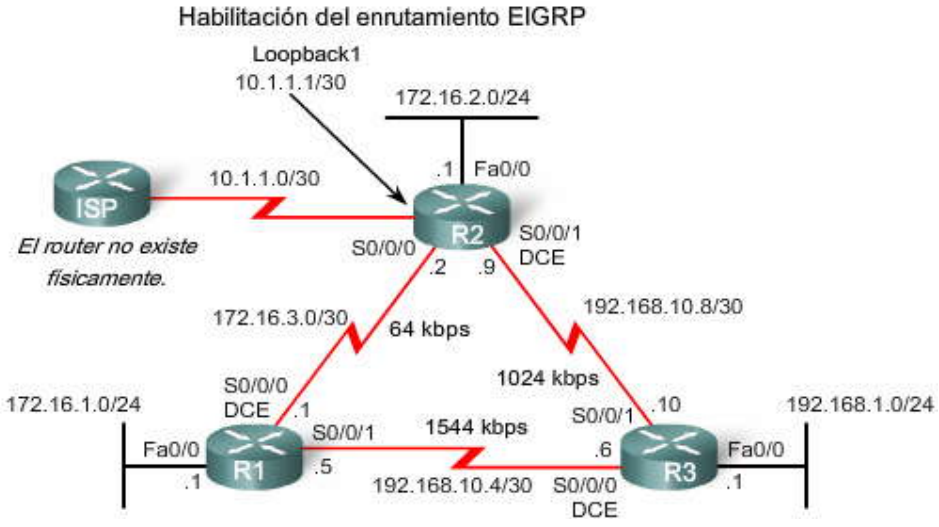
Si bien el IOS de Cisco hace referencia al parámetro router eigrp como "Número de sistema autónomo", este parámetro configura un proceso de EIGRP -un caso de ejecución de EIGRP en el router- y no se relaciona en absoluto con las configuraciones de AS (Sistema autónomo) en routers ISP.

### 9.2.3 EL COMANDO ROUTER EIGRP.-

El comando de configuración global router eigrp autonomous-system habilita a EIGRP. El parámetro del sistema autónomo es un número que el administrador de red elige entre 1 y 65535. El número elegido es el número del ID de proceso y es importante porque todos los routers en este dominio de enrutamiento EIGRP deben usar el mismo número del ID de proceso (número del sistema autónomo).

Haga clic en Resultado del router en la figura.

Como podrá ver en la topología y en el resultado del router en la figura, habilitaremos a EIGRP en los tres routers que utilizan el ID de proceso 1.



Habilitación del enrutamiento EIGRP

```
R1(config)#router eigrp 1
R1(config-router)#
```

```
R2(config)#router eigrp 1
R2(config-router)#
```

```
R3(config)#router eigrp 1
R3(config-router)#
```

### 9.2.4 COMANDOS NETWORK.-

El comando network en EIGRP tiene la misma función que en los otros protocolos de enrutamiento IGP:
Toda interfaz en este router que coincida con la dirección de red en el comando network estará habili tada para enviar y recibir actualizaciones EIGRP.
Esta red (o subred) estará incluida en las actualizaciones de enrutamiento EIGRP.

**Haga clic en Resultado del router en la figura.**

El comando network se utiliza en el modo de configuración de router.

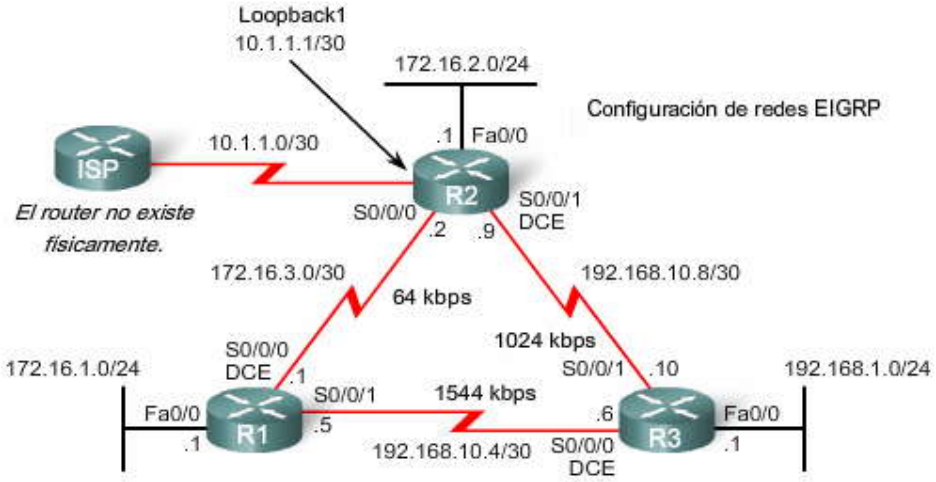
Router(config-router)#network network-address

El comando network-address es la dirección de red con clase para esta interfaz. La figura muestra los comandos de red configurados para R1 y R2. R3 se configurará en la siguiente página. En la figura, se utiliza una única opción de red con clase en R1 para incluir a las subredes 172.16.1.0/24 y 172.16.3.0/30:

R1(config-router)#network 172.16.0.0

Cuando se configura EIGRP en R2, DUAL envía un mensaje de notificación a la consola en el que indica que se ha establecido una relación de vecinos con otro router EIGRP. Esta nueva adyacencia se produce automáticamente porque R1 y R2 utilizan el mismo proceso de enrutamiento eigrp 1 y ambos routers envían en ese momento actualizaciones por la red 172.16.0.0.

R2(config-router)#network 172.16.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: El vecino 172.16.3.1 (Serial0/0) se encuentra activo: nueva adyacencia



```
R1(config)#router eigrp 1
R1(config-router)#network 172.16.0.0
R1(config-router)#network 192.168.10.0
```

```
R2(confi )#router eigrp 1
R2(config-router)#network 172.16.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency
```

**El comando network con una máscara Wildcard**

De manera predeterminada, al utilizar el comando network y una dirección de red con clase como 172.16.0.0, todas las interfaces del router que pertenecen a la dirección de red con clase estarán habilitadas para EIGRP. Sin embargo, puede haber ocasiones en las que el administrador de red no desee incluir a todas las interfaces dentro de una red al habilitar EIGRP. Para configurar a EIGRP a fin de que sólo publique subredes específicas, utilice la opción wildcard-mask con el comando network:

Router(config-router)#network network-address [wildcard-mask]

Imagine que una máscara wildcard es lo inverso a una máscara de subred. Lo inverso a una máscara de subred 255.255.255.252 es 0.0.0.3. Para calcular lo inverso a la máscara de subred, reste la máscara de subred de 255.255.255.255:

255.255.255.255
- 255.255.255.252
Reste la máscara de subred
---
0. 0. 0. 3
máscara Wildcard

Haga clic en Resultado del router en la figura.

En la figura, R2 está configurado con la subred 192.168.10.8 y la máscara wildcard 0.0.0.3.

R2(config-router)#network 192.168.10.8 0.0.0.3

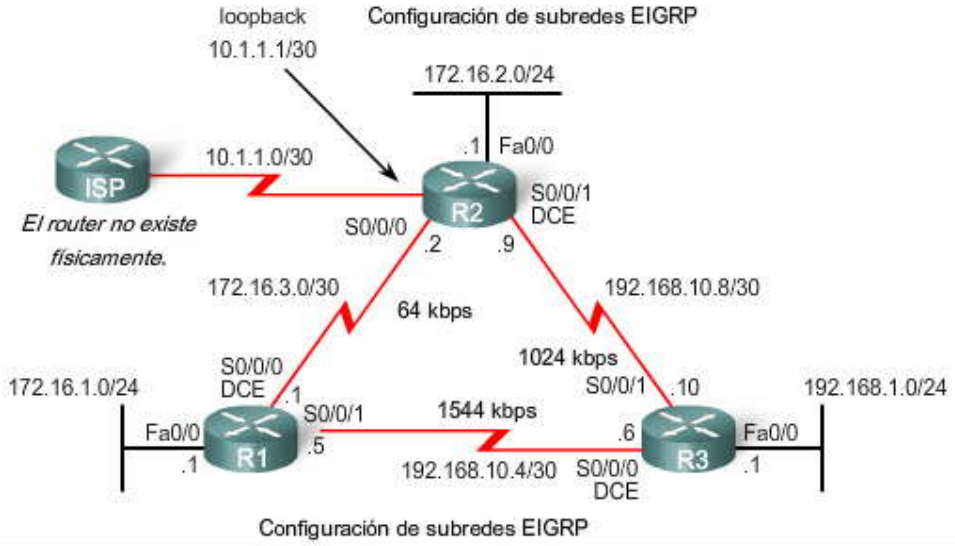
Algunas versiones de IOS también le permitirán simplemente ingresar la máscara de subred. Por ejemplo, puede ingresar lo siguiente:

R2(config-router)#network 192.168.10.8 255.255.255.252

Sin embargo, IOS luego convertirá el comando al formato de la máscara wildcard, como se puede verificar con el comando show run:

R2#show run
<some output omitted>
!
router eigrp 1
network 172.16.0.0
network 192.168.10.8 0.0.0.3
auto-summary
!

La figura también muestra la configuración para R3. Apenas se configure la red con clase 192.168.10.0, R3 establece adyacencias con ambos routers, R1 y R2.




```
R1(config)#router eigrp 1
R1(config-router)#network 172.16.0.0
R1(config-router)#network 192.168.10.0
```

```
R2(config)#router eigrp 1
R2(config-router)#network 172.16.0.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency
R2(config-router)#network 192.168.10.8 0.0.0.3
```

```
R3(config)#router eigrp 1
R3(config-router)#network 192.168.10.0
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.5 (Serial0/0/0) is up: new adjacency
R3(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 192.168.10.9 (Serial0/0/1) is up: new adjacency
R3(config-router)#network 192.168.1.0
```

### 9.2.5 VERIFICACION DE EIGRP.-

Antes de que EIGRP envíe o reciba actualizaciones, los routers deben establecer adyacencias con sus vecinos. Los routers EIGRP establecen adyacencias con los routers vecinos mediante el intercambio de paquetes de saludo EIGRP.

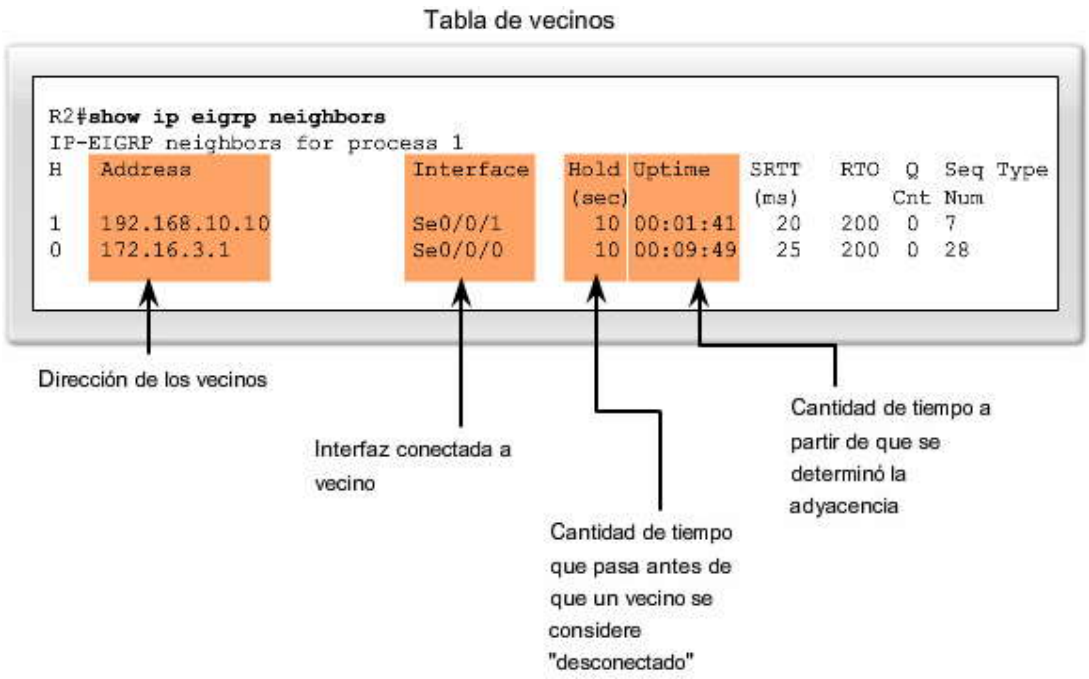
Utilice el comando show ip eigrp neighbors para ver la tabla de vecinos y verificar que EIGRP haya establecido una adyacencia con sus vecinos. Con cada router, usted debería poder ver la dirección IP del router adyacente y la interfaz que este router utiliza para alcanzar a ese vecino EIGRP. En la figura, podemos verificar que todos los routers han establecido las adyacencias necesarias. Cada router tiene dos vecinos enumerados en la tabla de vecinos.

El resultado del comando show ip eigrp neighbor incluye:

- Columna H: enumera a los vecinos en el orden en que se aprendieron.
- Dirección: dirección IP del vecino.
- Interfaz: interfaz local en la cual se recibió este paquete de saludo.
- Hold: tiempo de espera actual. Cuando se recibe un paquete de saludo, este valor se reestablece al tiempo de espera máximo para esa interfaz y luego se cuenta regresivamente hasta cero. Si se llega a cero, el vecino se considera "desactivado".
- Tiempo de actividad: cantidad de tiempo desde que este vecino se agregó a la tabla de vecinos.

- SRTT (Temporizador de ida y vuelta sin complicaciones) y RTO (Intervalo de retransmisión): utilizado por RTP para administrar paquetes EIGRP confiables. SRTT y RTO se analizan en mayor profundidad en los cursos de CCNP.
- Conteo de cola: debería ser siempre cero. Si fuera mayor que cero, entonces los paquetes EIGRP están esperando para ser enviados. El conteo de cola se analiza en mayor profundidad en los cursos de CCNP.
- Número de secuencia: utilizado para rastrear paquetes de actualización, consulta y respuesta. Los números de secuencia se analizan en mayor profundidad en los cursos de CCNP.

El comando show ip eigrp neighbors es muy útil para verificar y solucionar problemas con EIGRP. Si un vecino no se encuentra enumerado después de haber establecido las adyacencias con los vecinos del router, verifique la interfaz local para asegurarse de que se encuentre activada con el comando show ip interface brief. Si la interfaz está habilitada, intente hacer ping en la dirección IP del vecino. Si el ping falla, esto significa que la interfaz del vecino está desactivada y debe activarse. Si el ping es exitoso y EIGRP aún no ve al router como vecino, examine las siguientes configuraciones:
¿Se encuentran configurados los dos routers con el mismo ID de proceso EIGRP?
¿La red conectada directamente se encuentra incluida en las sentencias de red EIGRP?
¿El comando passive-interface está configurado para impedir paquetes de saludo EIGRP en la interfaz?




Al igual que con RIP, el comando show ip protocols se puede utilizar para verificar que EIGRP se encuentre habilitado. El comando show ip protocols muestra distintos tipos de resultados específicos de cada protocolo de enrutamiento. Examinaremos algunos de estos detalles en próximas secciones.

Haga clic en Resultado del router en la figura.

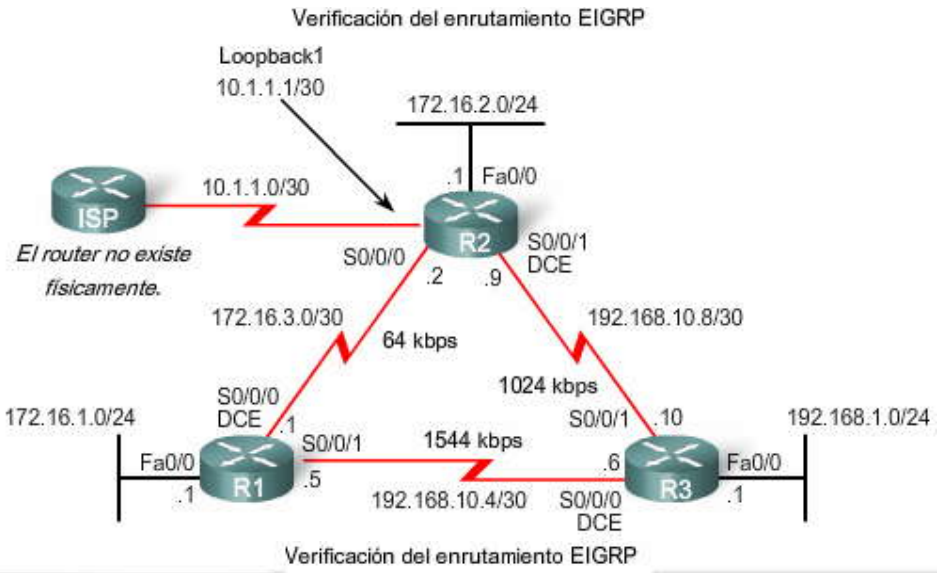
Observe que el resultado especifica el ID de proceso utilizado por EIGRP:

El protocolo de enrutamiento es "eigrp 1"

Recuerde, el ID de proceso debe ser el mismo en todos los routers para que EIGRP establezca adyacencias de vecinos y comparta información de enrutamiento.

También se muestran las distancias administrativas internas y externas de EIGRP:

Distancia: interna 90 externa 170




Verificación del enrutamiento EIGRP

```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.10.0/24 for FastEthernet0/0, Serial0/0/0
      Summarizing with metric 2169856
    172.16.0.0/16 for Serial0/0/1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)           90      00:03:29
    192.168.10.6            90      00:02:09
    Gateway         Distance      Last Update
    172.16.3.2              90      00:02:12
  Distance: internal 90 external 170
```

### 9.2.6 EXAMENES DE LA TABLA DE ENRUTAMIENTO.-

Otra manera de verificar que EIGRP y otras funciones del router se encuentran configuradas adecuadamente es examinar las tablas de enrutamiento con el comando show ip route.

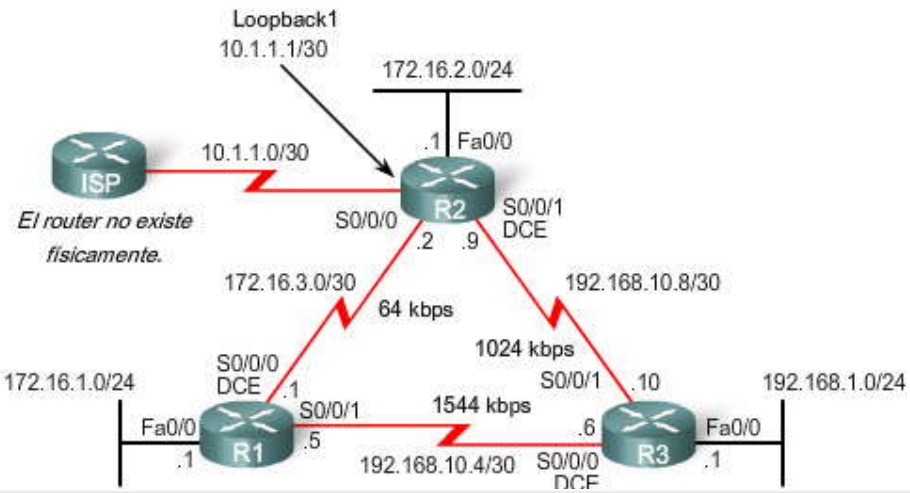
**Haga clic en R1, R2, y R3 en la figura.**

De manera predeterminada, EIGRP resume automáticamente las rutas en el borde de la red principal. Podemos deshabilitar el resumen automático con el comando no auto-summary, al igual que en RIPv2. Examinaremos estos conceptos en mayor detalle en una sección posterior.

Observe que las rutas EIGRP se denotan en la tabla de enrutamiento con una D, que significa DUAL.

Recuerde que, debido a que EIGRP es un protocolo de enrutamiento sin clase (incluye la máscara de subred en la actualización de enrutamiento), admite VLSM y CIDR. Podemos ver en la tabla de enrutamiento para R1 que la red primaria 172.16.0.0/16 se encuentra dividida en redes en forma variable con tres rutas secundarias que utilizan una máscara /24 o /30.

Topología




```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
<Output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:03:50, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/2681856] via 192.168.10.6, 00:02:43, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:10:52, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/2172416] via 172.16.3.2, 00:10:47, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:02:31, Serial0/0/1
```

```
R2#show ip route
<Output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:04:13, Null0
D       192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:03:05, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:04:07, Null0
D       172.16.1.0/24 [90/2172416] via 172.16.3.1, 00:11:11, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.1.0/24 [90/2172416] via 192.168.10.10, 00:02:54, Serial0/0/1
```

```
R3#show ip route
<Output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:03:11, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 00:03:23, Serial0/0/0
                   [90/2172416] via 192.168.10.9, 00:03:23, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Introducción de la ruta resumida Null0

La figura muestra la tabla de enrutamiento para R2 con dos entradas resaltadas. Observe que EIGRP ha incluido automáticamente una ruta resumida hacia Null0 para las redes con clase 192.168.10.0/24 y 172.16.0.0/16.

Recuerde del Capítulo 7, "RIPv2", que Null0 no es una interfaz real. Observe que las rutas resumidas se originan en Null0, esto es porque las rutas se utilizan para notificaciones. Las rutas 192.168.10.0/24 y 172.16.0.0/16 en realidad no representan ninguna ruta con la que se puedan alcanzar las redes primarias. Si un paquete no coincide con una de las rutas secundarias de nivel 2, se lo envía a la interfaz Null0. En otras palabras, si el paquete coincide con la primaria de nivel 1 (la dirección de red con clase) pero no lo hace con ninguna de las subredes, se desecha el paquete.

Nota: EIGRP automáticamente incluye una ruta resumida Null0 como ruta secundaria cuando se produce alguna de las siguientes condiciones:
Por lo menos existe una subred que se aprendió a través de EIGRP.
El resumen automático se encuentra habilitado.

Veremos que la ruta resumida null0 se retira cuando no se encuentra habilitado el resumen automático.

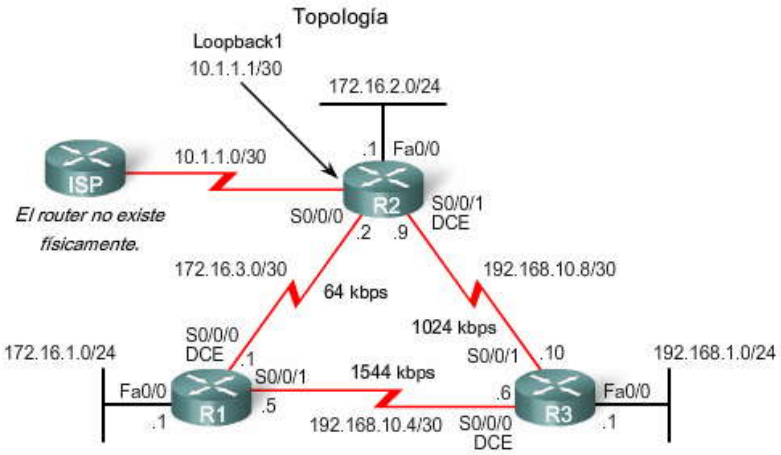



Tabla de enrutamiento R2

```
R2#show ip route
<Output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:04:13, Null0
D       192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:03:05, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:04:07, Null0
D       172.16.1.0/24 [90/2172416] via 172.16.3.1, 00:11:11, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.1.0/24 [90/2172416] via 192.168.10.10, 00:02:54, Serial0/0/1
```

**Rutas de resumen a Null0**

Tabla de enrutamiento R3

La tabla de enrutamiento para R3 muestra que R1 y R2 resumen automáticamente la red 172.16.0.0/16 y la envían como una única actualización de enrutamiento. R1 y R2 no propagan las subredes individuales debido al resumen automático. Más adelante, desconectaremos el resumen automático. Como R3 recibe dos rutas con el mismo costo para 172.16.0.0/16 de R1 y R2, ambas rutas se incluyen en la tabla de enrutamiento.

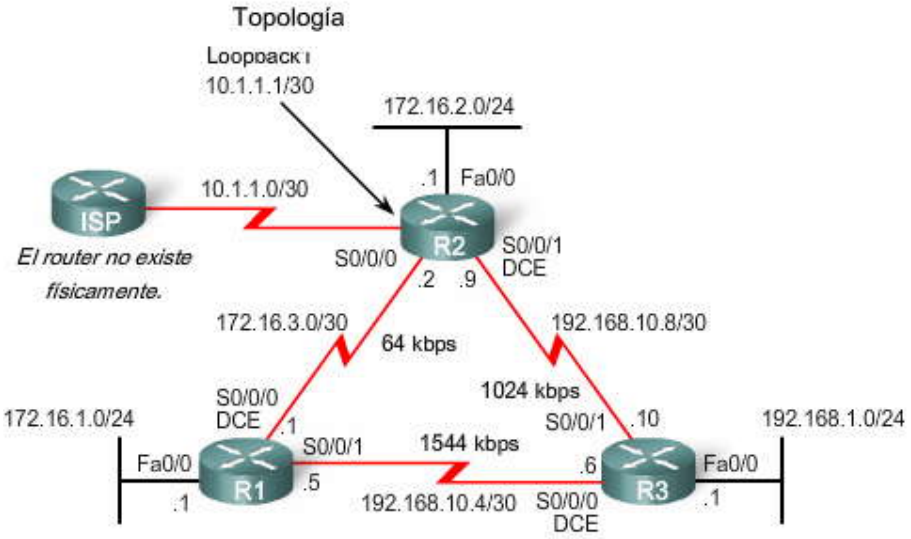



Tabla de enrutamiento R3

```
R3#show ip route
<Output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:03:11, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 00:03:23, Serial0/0/0
                   [90/2172416] via 192.168.10.9, 00:03:23, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

Rutas de igual costo a 172.16.0.0/16

## 9.3 CALCULO DE LA METRICA DEL EIGRP.-

### 9.3.1 METRICA COMPUESTA DE EIGRP Y VALORES K.-

EIGRP utiliza los siguientes valores en su métrica compuesta para calcular la ruta preferida hacia una red:

- Ancho de banda
- Retraso
- Confiabilidad
- Carga

Nota: Como se mencionó anteriormente en este capítulo, a pesar de que MTU se encuentra incluida en las actualizaciones de la tabla de enrutamiento, no es una métrica de enrutamiento que EIGRP o IGRP utilicen. De manera predetermina da, sólo se utilizan el ancho de banda y el retraso para calcular la métrica. Cisco recomienda que no se utilicen la confiabilidad ni la carga a menos que el administrador tenga una necesidad explícita de hacerlo.

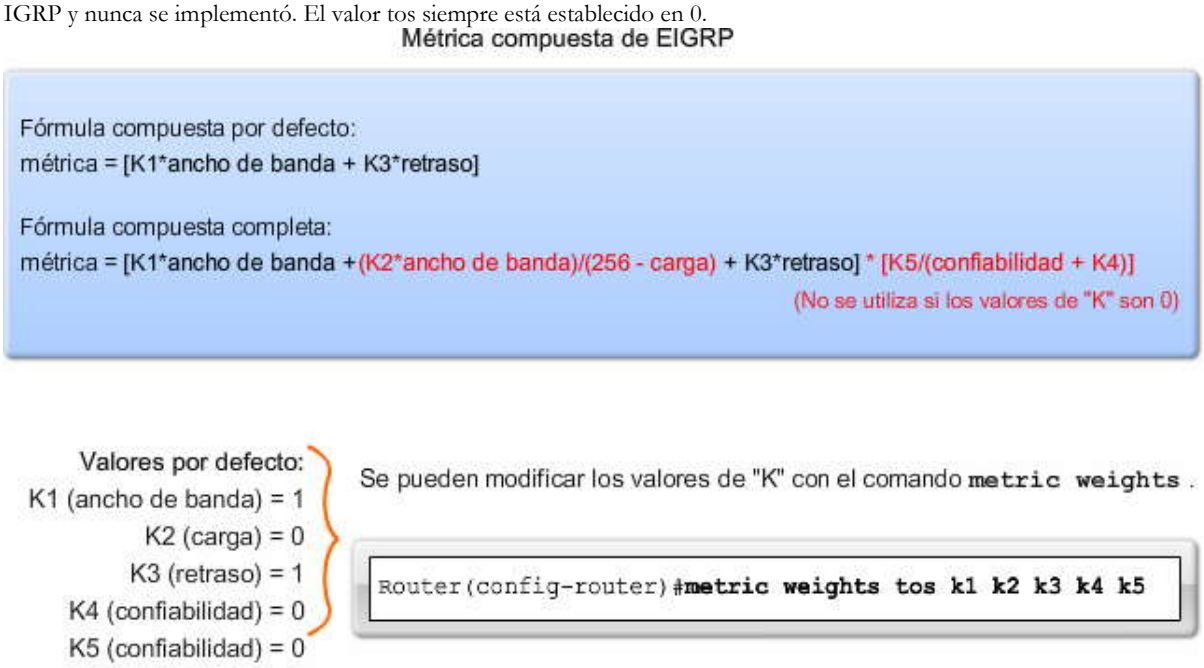
**Métrica compuesta**

La figura muestra la fórmula de la métrica compuesta que EIGRP utiliza. La fórmula consta de valores que van de K1 a K5, conocidos como pesos métricos de EIGRP. De manera predeterminada, K1 y K3 se establecen en 1, y K2, K4 y K5 se establecen en 0. El resultado consiste en que sólo el ancho de banda y los valores de retraso se utilizan en el cálculo de la métrica compuesta predeterminada.

Los valores K predeterminados pueden cambiarse con el comando del router EIGRP:

Router(config-router)#metric weights tos k1 k2 k3 k4 k5

Nota: La modificación de los pesos métricos se encuentra más allá del alcance de este curso, pero su relevancia es importante al establecer vecinos y se analizará en una sección posterior. El valor tos (Tipo de servicio) es un sobrante de IGRP y nunca se implementó. El valor tos siempre está establecido en 0.




Verificación de los valores K

El comando show ip protocols se utiliza para verificar los valores K. El resultado del comando para R1 se muestra en la figura. Observe que los valores K en R1 se encuentran establecidos en el valor predeterminado. Nuevamente, no se recomienda cambiar estos valores de los predeterminados a menos que el administrador de red tenga una muy buena razón para hacerlo.

Tabla de enrutamiento de R3

```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.10.0/24 for FastEthernet0/0, Serial0/0/0
      Summarizing with metric 2169856
    172.16.0.0/16 for Serial0/0/1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:03:29
    192.168.10.6          90      00:02:09
    Gateway         Distance      Last Update
    172.16.3.2            90      00:02:12
  Distance: internal 90 external 170
```

### 9.3.2 METRICAS DE EIGRP.-

Examen de los valores de la métrica

Ahora conoce los valores predeterminados para los valores K. Mediante el comando show interface podemos examinar los valores reales utilizados para el ancho de banda, el retraso, la confiabilidad y la carga en el cálculo de la métrica de enrutamiento.

**Haga clic en Resultado del router en la figura.**

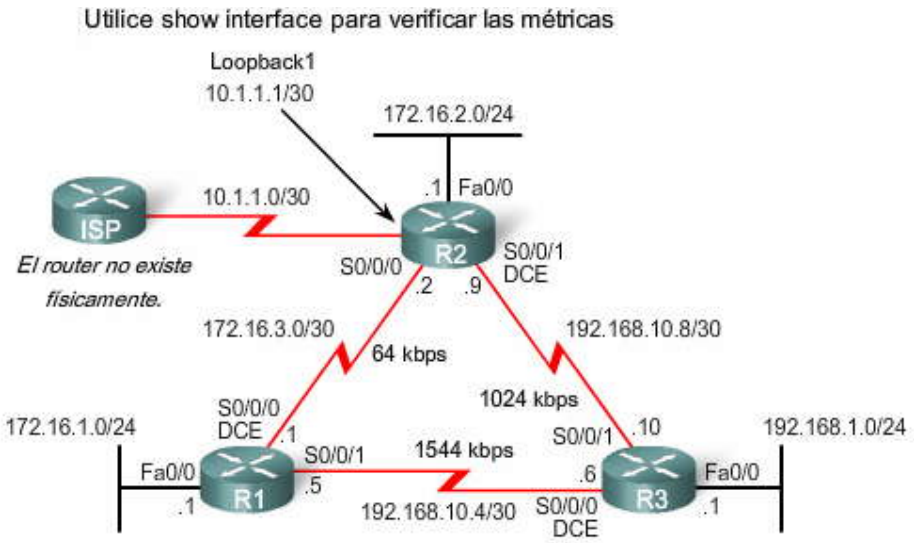
El resultado en la figura muestra los valores utilizados en la métrica compuesta para la interfaz serial 0/0/0 en R1.

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255

**Ancho de banda**

La métrica del ancho de banda (1544 Kbit) es un valor estático utilizado por algunos protocolos de enrutamiento, tales como EIGRP y OSPF, para calcular su métrica de enrutamiento. El ancho de banda se muestra en Kbit (kilobits). La mayoría de las interfaces seriales utilizan el valor de ancho de banda predeterminado de 1544 Kbit o 1 544 000 bps (1544 Mbps). Éste es el ancho de banda de una conexión T1. Sin embargo, algunas interfaces seriales utilizan otro valor de ancho de banda predeterminado. Siempre verifique el ancho de banda con el comando show interface.

El valor del ancho de banda puede reflejar o no el ancho de banda físico real de la interfaz. La modificación del valor del ancho de banda no cambia el ancho de banda real del enlace. Si el ancho de banda real del enlace es distinto del valor de ancho de banda predeterminado, entonces debe modificar el valor de ancho de banda, como veremos en una sección posterior.




Utilice show interface para verificar las métricas

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: Link to R2
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 3d22h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     112522 packets input, 7303722 bytes, 0 no buffer
     Received 40016 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     112601 packets output, 7280131 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     12 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

usec = microsegundo o 1 millonésima de segundo

**Retraso**

El retraso es la medida del tiempo que necesita un paquete para atravesar una ruta. La métrica del retraso (DLY) es un valor estático determinado en función del tipo de enlace al cual se encuentra conectada la interfaz y se expresa en microsegundos. El retraso no se mide en forma dinámica. En otras palabras, el router no registra en realidad cuánto tiempo les lleva a los paquetes llegar al destino. El valor de retraso, como el valor de ancho de banda, es un valor predeterminado que el administrador de red puede modificar.

MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255

La tabla en la figura muestra los valores de retraso predeterminados para distintas interfaces. Observe que el valor predeterminado es 20 000 microsegundos para las interfaces seriales y 100 microsegundos para las interfaces FastEthernet.

Valores de demora en microsegundos

| Medios | Retraso |
|---|---|
| 100 M ATM | 100 µs |
| Fast Ethernet | 100 µs |
| FDDI | 100 µs |
| 1HSSI | 20,000 µs |
| 16 M Token Ring | 630 µs |
| Ethernet | 1,000 µs |
| T1 (serial por defecto) | 20,000 µs |
| 512 K | 20,000 µs |
| DSO | 20,000 µs |
| 56 K | 20,000 µs |

**Confiabilidad**

Confiabilidad (confiabilidad) es la medida de probabilidad en la que fallará el enlace o con qué frecuencia el enlace experimenta errores. A diferencia del retraso, la confiabilidad se mide dinámicamente con un valor entre 0 y 255, con 1 como enlace de confiabilidad mínima y 255 como cien por ciento confiable. La confiabilidad se calcula en un promedio ponderado de 5 minutos para evitar el repentino impacto de grandes (o bajos) índices de error.

La confiabilidad se expresa como una fracción de 255; mientras mayor sea el valor, más confiable será el enlace. Por lo tanto, 255/255 sería 100 por ciento confiable, mientras que un enlace de 234/255 sería confiable en un 91,8 por ciento.

**Recuerde:** De manera predeterminada, EIGRP no utiliza la confiabilidad en su cálculo métrico.

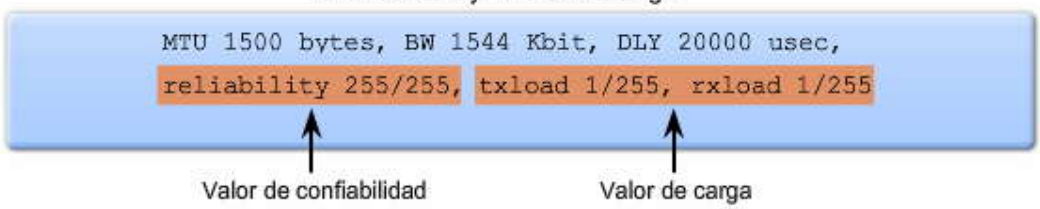
**Carga**

Carga (carga) refleja la cantidad de tráfico que utiliza el enlace. Al igual que la confiabilidad, la carga se mide dinámicamente con un valor de entre 0 y 255. Similar a la confiabilidad, la carga se expresa con una fracción de 255. Sin embargo, en este caso se prefiere un valor de carga menor porque indica menos carga en el enlace. Por lo tanto, 1/255 sería un enlace de carga mínima. 40/255 es un enlace con 16% de capacidad y 255/255 sería un enlace saturado al 100%.

La carga se muestra como un valor de carga saliente o de transmisión (txload) y un valor de carga entrante o receptor (rxload). Este valor se calcula con un promedio ponderado de 5 minutos para evitar el repentino impacto de un uso grande (o bajo) del canal.

**Recuerde:** De manera predeterminada, EIGRP no utiliza carga en sus cálculos métricos.

Confiabilidad y valores de carga




### 9.3.3 USO DEL COMANDO BANDWITH.-

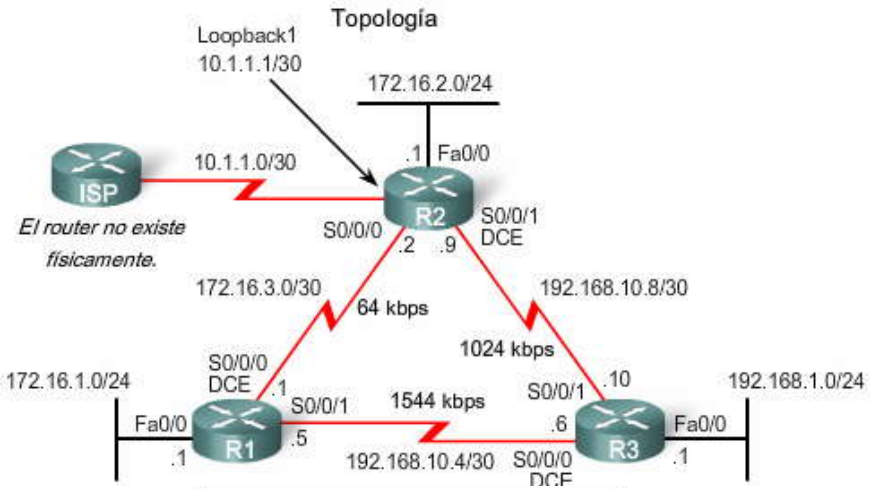
En la mayoría de los enlaces seriales, la métrica del ancho de banda será de 1544 Kbits por defecto. Debido a que EIGRP y OSPF utilizan el ancho de banda en los cálculos métricos predeterminados, un valor correcto para el ancho de banda es muy importante para la precisión de la información de enrutamiento. Pero, ¿qué sucede si el ancho de banda real del enlace no coincide con el ancho de banda predeterminado de la interfaz?

**Haga clic en Configurar ancho de banda en la figura.**

Utilice el comando de la interfaz bandwidth para modificar la métrica del ancho de banda:
Router(config-if)#bandwidth kilobits
Utilice el comando de la interfaz no bandwidth para restablecer el valor predeterminado.

En la figura, el enlace entre R1 y R2 tiene un ancho de banda de 64 kbps, y el enlace entre R2 y R3 tiene un ancho de banda de 1024 kbps. La figura muestra la configuración utilizada en los tres routers para modificar el ancho de banda en las interfaces seriales adecuadas.

**Haga clic en Verificar ancho de banda en la figura.**
Podemos verificar el cambio mediante el comando show interface. Es importante modi ficar la métrica del ancho de banda en ambos lados del enlace para garantizar el enrutamiento adecuado en ambas direcciones.
Nota: Un error común en los estudiantes nuevos en la división de redes y en IOS de Cisco es suponer que el comando bandwidth cambiará el ancho de banda físico del enlace. Según lo mencionado en la sección anterior, el comando bandwidth sólo modifica la métrica del ancho de banda utilizada por los protocolos de enrutamiento, como EIGRP y OSPF. En ocasiones, un administrador de red puede cambiar el valor del ancho de banda para tener un mayor control de la interfaz saliente elegida.




Configuración del ancho de banda

Comando bandwidth

```
R1(config)#inter s 0/0/0
R1(config-if)#bandwidth 64
```

```
R2(config)#inter s 0/0/0
R2(config-if)#bandwidth 64
R2(config)#inter s 0/0/1
R2(config-if)#bandwidth 1024
```

```
R3(config)#inter s 0/0/1
R3(config-if)#bandwidth 1024
```

Nota: El ancho de banda real del enlace entre R1 y R3 coincide con el valor por defecto para las interfaces seriales (1544 kbps).

Verificación del ancho de banda

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.16.3.2/30
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
<some output omitted>

R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
```

### 9.3.4 CALCULO DE LA METRICA DE EIGRP.-

La figura muestra la métrica compuesta utilizada por EIGRP. Al utilizar los valores predeterminados para K1 y K3, podemos simplificar este cálculo de la siguiente manera: el ancho de banda más lento (o el ancho de banda mínimo) más la suma acumulativa de todos los retrasos.

En otras palabras, al examinar los valores de ancho de banda y retraso para todas las interfaces salientes de la ruta, podemos determinar la métrica de EIGRP. Primero, determine el enlace con el ancho de banda más lento. El ancho de banda se utiliza para la porción (10,000,000/ancho de banda) * 256 de la fórmula. Luego, determine el valor de retraso para cada interfaz saliente que se dirige hacia el destino. Sume los valores de retraso y divida por 10 (suma de retrasos/10) y luego multiplique por 256 (* 256). Agregue el ancho de banda y la suma de los valores de retraso para obtener la métrica de EIGRP.

El resultado de la tabla de enrutamiento para R2 muestra que la ruta hacia 192.168.1.0/24 tiene una métrica de EIGRP de 3 014 400. Veamos exactamente cómo calculó EIGRP este valor.

Cálculo de la métrica por defecto de EIGRP

Métrica por defecto = [K1*ancho de banda + K3*retraso] * 256

Ya que K1 y K3 son ambos igual a 1, la fórmula se simplifica: ancho de banda + demora

ancho de banda = velocidad del enlace más lento de la ruta hacia el destino
retraso = suma de los retrasos de cada enlace de la ruta hacia el destino

Ancho de banda más lento: (10 000 000/kbps de ancho de banda) * 256
Más la suma de los retrasos: + (suma de retraso/10) * 256

= métrica de EIGRP

```
R2#show ip route
<output omitted>

D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:02:14, Serial0/0/1
```

**Ancho de banda**

**Haga clic en Cálculo del ancho de banda en la figura.**

Debido a que EIGRP utiliza el ancho de banda más lento en el cálculo métrico, podemos encontrar el ancho de banda más lento al examinar cada interfaz entre R2 y la red de destino 192.168.1.0. La interfaz serial 0/0/1 en R2 tiene un ancho de banda de 1024 Kbps o 1 024 000 bps. La interfaz FastEthernet 0/0 en R3 tiene un ancho de banda de 100 000 Kbps o 100 Mbps. Por lo tanto, el ancho de banda más lento es 1024 Kbps y se utiliza en el cálculo de la métrica.

EIGRP toma los valores de ancho de banda en kbps y los divide por un valor de ancho de banda de referencia de 10 000 000. Esto producirá como resultado valores de ancho de banda más elevados al recibir una métrica más baja y valores de ancho de banda más bajos al recibir una métrica más alta.

10 000 000 dividido 1024. Si el resultado no es un número entero, entonces se redondea el número. En este caso, 10 000 000 dividido 1024 es igual a 9765,625. El ,625 se descarta antes de multiplicar por 256. La porción del ancho de banda de la métrica compuesta es 2 499 840.

**Retraso**

Mediante las mismas interfaces salientes también podemos determinar el valor de retraso.

**Haga clic en Cálculo del retraso en la figura.**

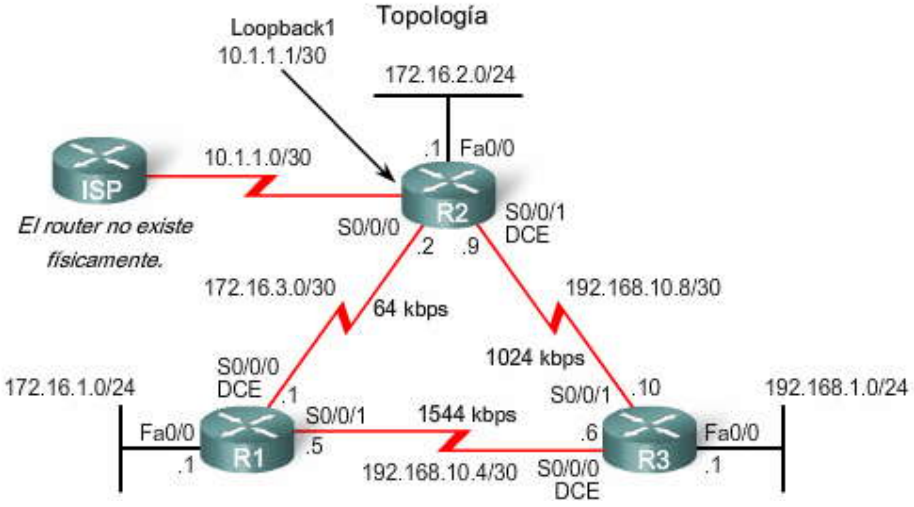
EIGRP utiliza la suma acumulativa de métricas de retraso de todas las interfaces salientes. La interfaz serial 0/0/1 en R2 tiene un retraso de 20 000 microsegundos. La interfaz FastEthernet 0/0 en R3 tiene un retraso de 100 microsegundos.

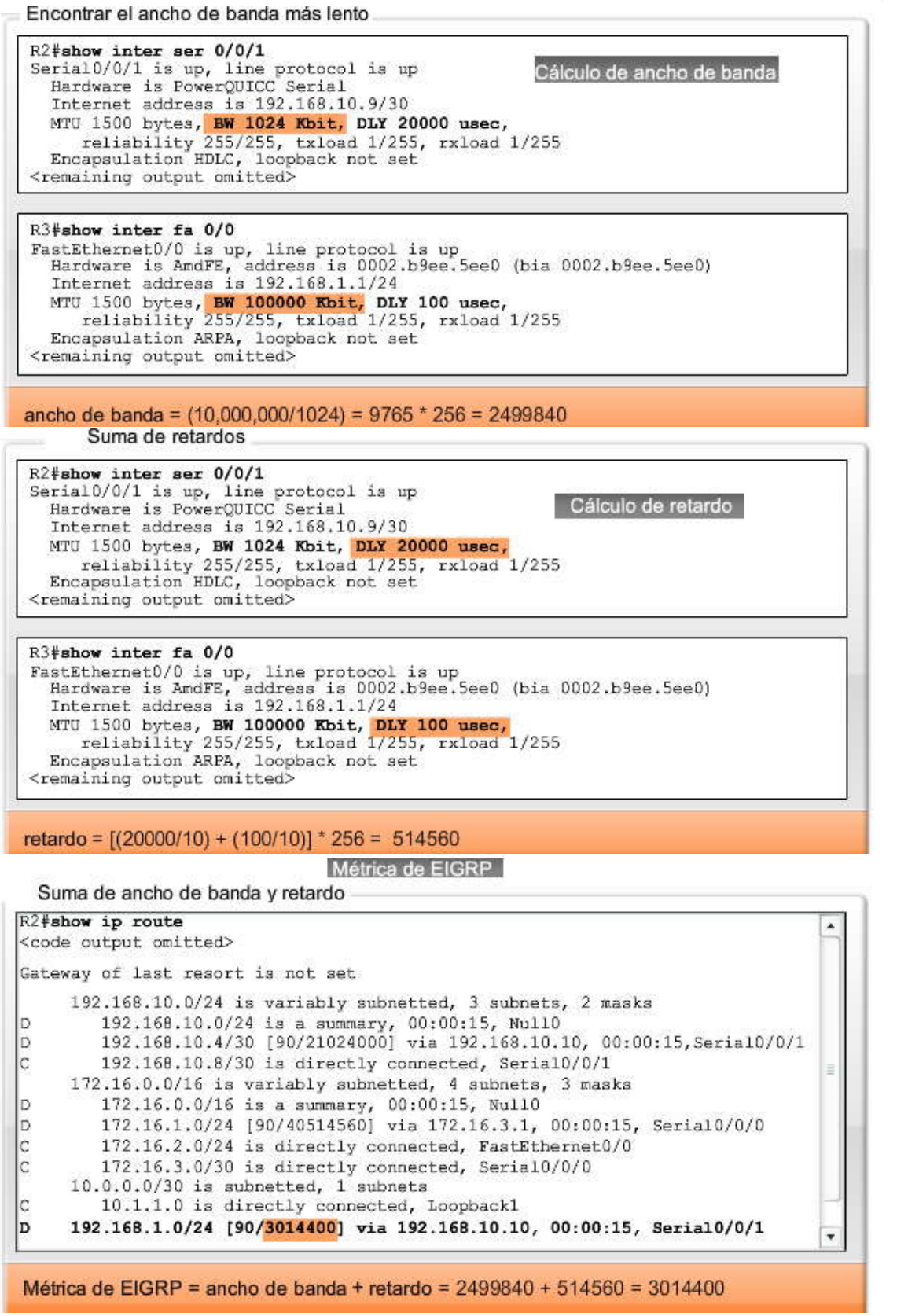
Cada valor de retraso se divide por 10 y luego se suma. 20 000/10 + 100/10 da como resultado 2010. Este resultado luego se multiplica por 256. La porción de retraso de la métrica compuesta es de 514 560.

Agregado de ancho de banda y retraso

**Haga clic en Métrica de EIGRP en la figura.**

Simplemente agregue los dos valores juntos, 2 499 840 + 514 560, para obtener la métrica de EIGRP de 3 014 400. Este valor coincide con el valor mostrado en la tabla de enrutamiento para R2. Éste es el resultado del ancho de banda más lento y de la suma de retrasos






## 9.4 DUAL.-

### 9.4.1 CONCEPTOS ACERCA DE DUAL.-

Según se mencionó en secciones anteriores, DUAL (Algoritmo de actualización por difusión) es el algoritmo utilizado por EIGRP. Esta sección analizará cómo DUAL determina el mejor camino sin bucles y las rutas de respaldo sin bucles.

DUAL utiliza varios términos que se analizarán con mayor detalle a lo largo de esta sección:
Sucesor
Distancia factible (FD)
Sucesor factible (FS)
Distancia notificada (RD) o Distancia publicada (AD)
Condición factible o Condición de factibilidad (FC)

Estos términos y conceptos se encuentran en el centro del mecanismo de DUAL para evitar bucles. Examinemos estos términos en más detalle.

Conceptos de DUAL

**DUAL proporciona:**

- Rutas sin bucles
- Rutas de respaldo sin bucles que pueden utilizarse en forma inmediata
- Convergencia rápida
- Uso mínimo del ancho de banda con actualizaciones limitadas

### 9.4.2 SUCESOR Y DISTANCIA FACTIBLE.-

Un sucesor es un router vecino que se utiliza para el reenvío de paquetes y es la ruta menos costosa hacia la red de destino. La dirección IP del sucesor se muestra en una entrada de tabla de enrutamiento justo después de la palabra via.

Distancia factible (FD) es la métrica calculada más baja para llegar a la red de destino. FD es la métrica enumerada en la entrada de la tabla de enrutamiento como el segundo número dentro de paréntesis. De la misma manera que con otros protocolos de enrutamiento también se conoce como la métrica de la ruta.

Haga clic en Resultado del router en la figura.

Al examinar la tabla de enrutamiento para R2 en la figura, podemos ver que el mejor camino de EIGRP para la red 192.168.1.0/24 es a través del router R3 y que la distancia factible es 3014400 (la misma métrica que calculamos en el último tema):

D 192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:31, Serial0/0/1

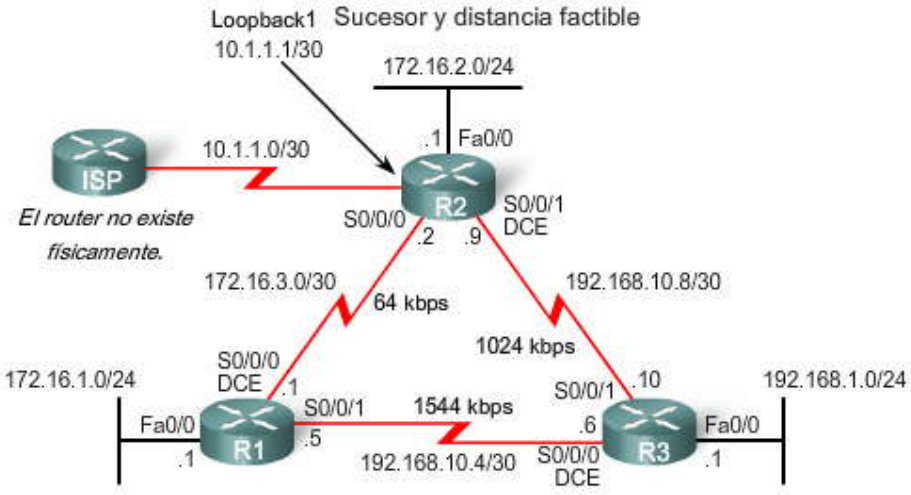
También se muestran otros sucesores y otras distancias factibles en la figura. ¿Puede responder las siguientes preguntas?

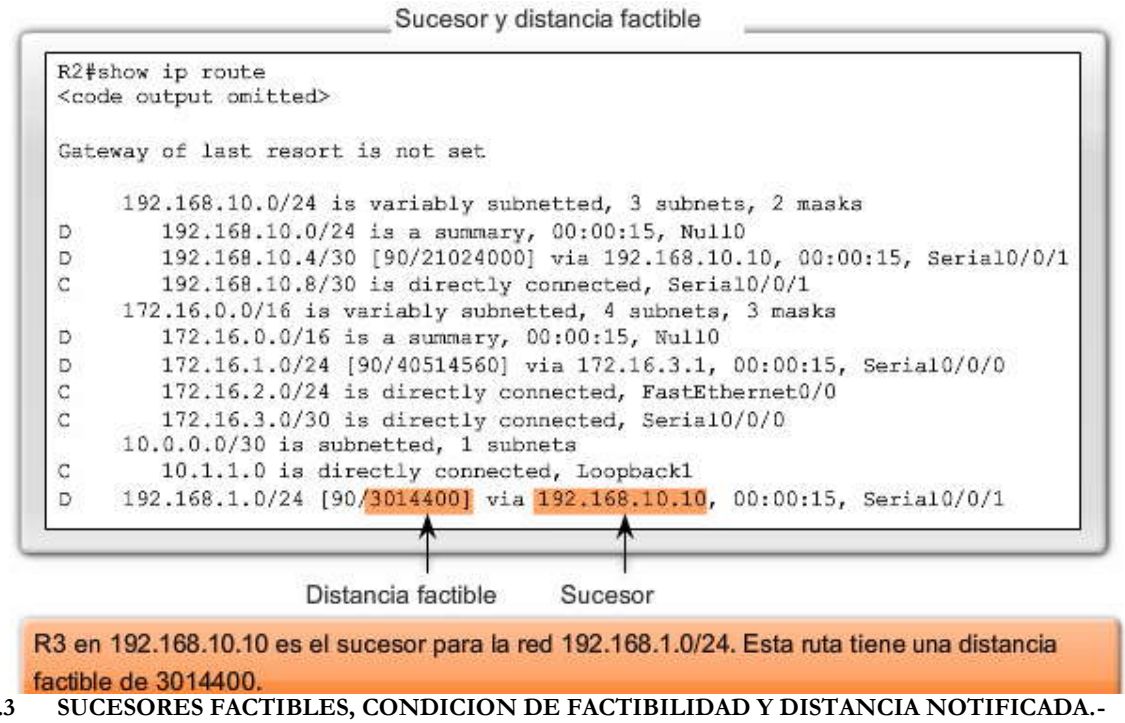
**¿Cuál es la dirección IP del sucesor para la red 172.16.1.0/24?**

Respuesta: 172.16.3.1, lo cual significa R1.

**¿Cuál es la distancia factible hacia 172.16.1.0/24?**

Respuesta: 40514560.






### 9.4.3 SUCESORES FACTIBLES, CONDICION DE FACTIBILIDAD Y DISTANCIA NOTIFICADA.-

Uno de los motivos por los cuales DUAL converge rápidamente después de un cambio en la topología es porque puede utilizar rutas de respaldo hacia otras rutas conocidas como sucesores factibles sin tener que recalcular DUAL.

**Haga clic en Sucesor factible en la figura.**

Un sucesor factible (FS) s un vecino que tiene una ruta de respaldo sin bucles hacia la mism a red que el sucesor por cumplir con la condición de factibilidad. En nuestra topología, ¿consideraría R2 a R1 como un sucesor factible para la red 192.168.1.0/24? Para poder ser un sucesor factible, R1 debe satisfacer la condición de factibilidad (FC). Ve amos que significa eso.

**Haga clic en Condición de factibilidad en la figura.**

La condición de factibilidad (FC) se cumple cuando la distancia notificada (RD) de un vecino hacia una red es menor que la distancia factible del router local hacia la misma red de destino. La distancia notificada o la distancia publicada es simplemente una distancia factible EIGRP de vecinos a la misma red de destino. La distancia notificada es la métrica que un router informa a un vecino acerca de su propio costo hacia esa red.

Si R3 es el sucesor, ¿puede el vecino R1 ser un sucesor factible para esta misma red 192.161.0/24? En otras palabras, si el enlace entre R2 y R3 falla, ¿puede utilizarse inmediatamente a R1 como una ruta de respaldo sin recálculo del algoritmo DUAL? R1 sólo puede ser un sucesor factible si cumple con la condición de factibilidad.

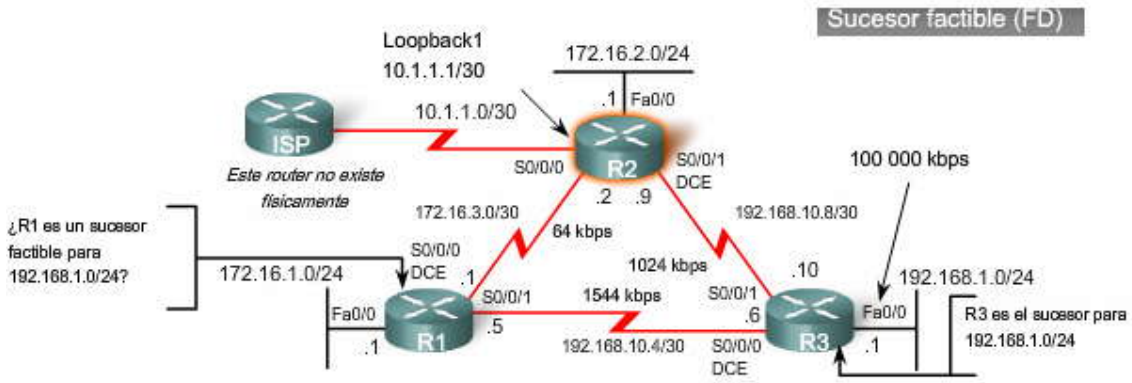
En la figura, R1 informa a R2 que su distancia factible hacia 192.168.1.0/24 es 2172416. Desde la perspectiva de R2, 2172416 es la distancia notificada de R1. Desde la perspectiva de R1, 2172416 es su distancia factible.

**Haga clic en Distancia notificada en la figura.**

R2 examina la distancia notificada (RD) 2172416 de R1. Debido a que la distancia notificada (RD) de R1 es menor que la propia distancia factible (FD) de R2, que es 3014400, R1 cumple con la condición de factibilidad. Ahora R1 es un sucesor factible para R2 hacia la red 192.168.1.0/24.

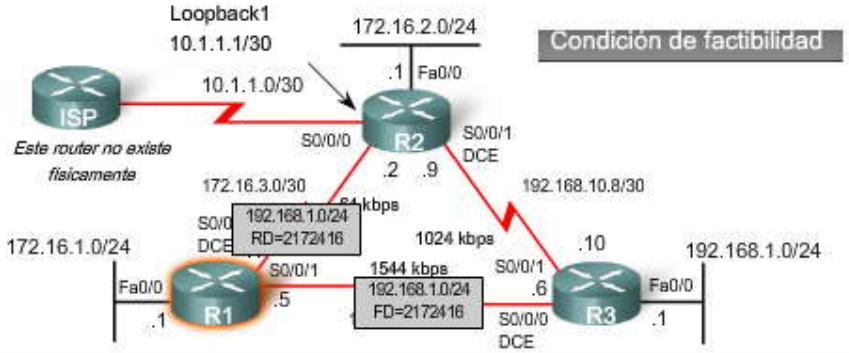
¿Por qué no es R1 el sucesor si su distancia notificada (RD) es menor que la distancia factible (FD) de R2 hacia 192.168.1.0/24? Porque el costo total para R2, su distancia factible (FD), para alcanzar 192.168.1.0/24 es mayor a través de R1 de lo que es a través de R3.

## Encontrar al sucesor factible




```
R2#show ip route
<code output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:00:15, Null0
D       192.168.10.4/30 [90/21024000] via 192.168.10.10, 00:00:15, Serial0/0/1
C       192.168.10.8/30 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:00:15, Null0
D       172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:15, Serial0/0/0
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:15, Serial0/0/1
```

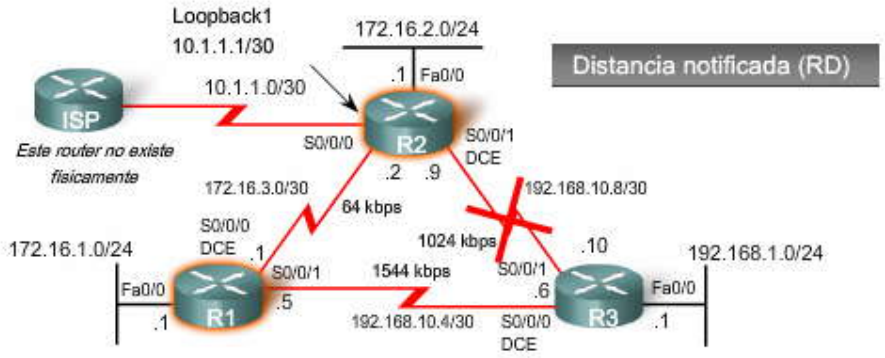
¿R1 satisface la condición de factibilidad (FC)?




```
R1#show ip route
<output omitted for brevity>

D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 01:12:26, Serial0/0/1
```

R1 notifica a R2 que su distancia factible a 192.168.1.0/24 es 2 172 416

R1 satisface la condición de factibilidad.

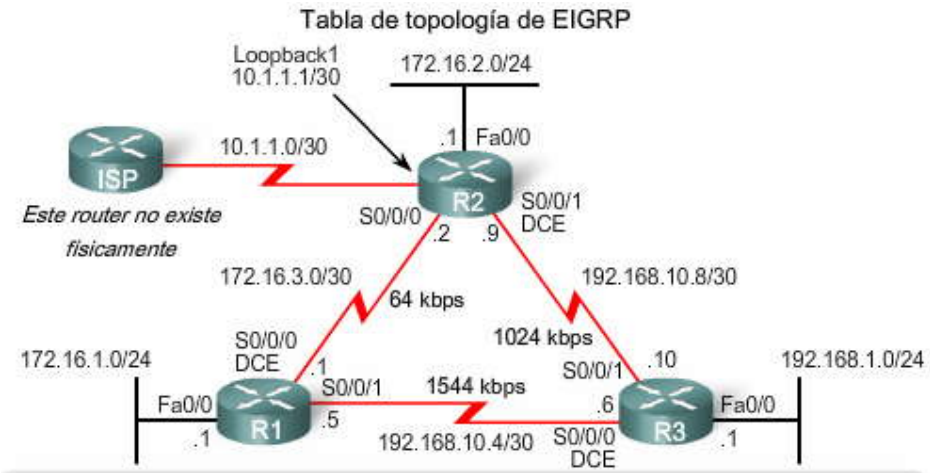



```
R1#show ip route
<output omitted for brevity>

D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 01:12:26, Serial0/0/1
```

```
R2#show ip route
<output omitted for brevity>

D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:15, Serial0/0/1
```

### 9.4.4 TABLA DE TOPOLOGIA: SUCESOR DE SUCESOR FACTIBLE.-

El router guarda el sucesor, la distancia factible y todo sucesor factible con sus distancias notificadas en su tabla de topología EIGRP o en la base de datos de topología. Como se muestra en la figura, la tabla de topología puede verse mediante el comando show ip eigrp topology. La tabla de topología enumera todos los sucesores y sucesores factibles que DUAL calculó hacia las redes de destino.




```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

<output omitted>
P 192.168.1.0/24, 1 successors, FD is 3014400
         via 192.168.10.10 (3014400/28160), Serial0/0/1
         via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/1
<output omitted>
```

Rutas para 192.168.1.0/24

Haga clic en Reproducir para ver la animación.

A continuación aparece una descripción detallada de cada parte de la tabla de topología para la red de destino 192.168.1.0/24.

La primer línea muestra:

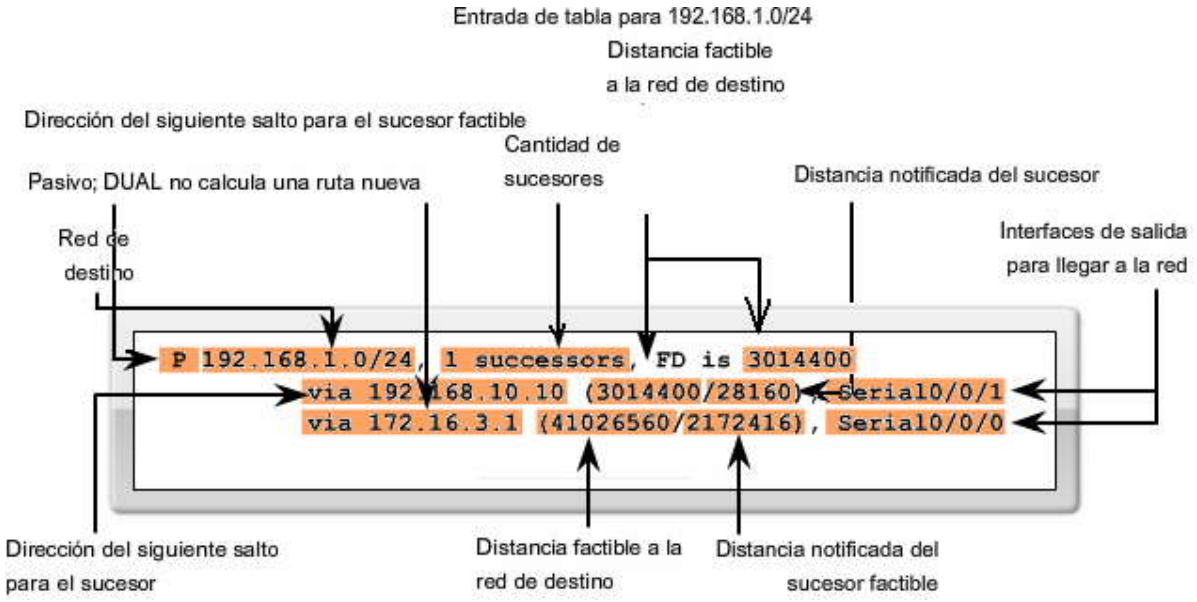
- P: Esta ruta se encuentra en estado pasivo. Cuando DUAL no se encuentra desarrollando sus cálculos por difusión para determinar una ruta para una red, la ruta se encuentra en un modo estable, conocido como el estado pasivo. Si DUAL se encuentra recalculando o buscando una nueva ruta, la ruta estará en un estado activo. Todas la rutas en la tabla de topología deberían estar en el estado pasivo para un dominio de enrutamiento estable. DUAL mostrará una A si la ruta se encuentra "Atascada en Activo", lo que significa que es un tema de resolución de problemas de CCNP.
- 192.168.1.0/24: Es la red de destino que también se encuentra en la tabla de enrutamiento.
- 1 sucesores: Muestra el número de sucesores para esta red. Si existen múltiples rutas de igual costo hacia esta red, habrá múltiples sucesores.
- FD es 3014400: Es la distancia factible, la métrica de EIGRP para llegar a la red de destino.

La primer entrada muestra al sucesor:

- via 192.168.10.10: Es la dirección de siguiente salto del sucesor factible, R3. Esta dirección se muestra en la tabla de enrutamiento.
- 3014400: Es la distancia factible hacia 192.168.1.0/24. Es la métrica que se muestra en la tabla de enrutamiento.
- 28160: Es la distancia factible hacia 192.168.1.0/24. Es la métrica que se muestra en la tabla de enrutamiento.
- Serial0/0/1: Es la interfaz saliente utilizada para alcanzar la red, también se muestra en la tabla de enrutamiento.

La segunda entrada muestra al sucesor factible, R1 (si no hay una segunda entrada, entonces no hay sucesores factibles):

- via 172.16.3.1: Es la dirección de siguiente salto del sucesor factible, R1.
- 41026560: Sería la nueva distancia factible de R2 hacia 192.168.1.0/24 si R1 fuera el nuevo sucesor.
- 2172416: Es la distancia notificada del sucesor factible o la métrica de R1 para alcanzar esta red. Este valor, RD debe ser menor que la FD actual de 3014400 para cumplir con la condición de factibilidad.
- Serial0/0/0: Es la interfaz saliente utilizada para alcanzar al sucesor factible, si este router se convierte en el sucesor.




### 9.4.5 TABLA DE TOPOLOGIA: NO HAY SUCESOR FACIBLE.-

Para continuar con nuestro aprendizaje acerca de DUAL y el uso de los sucesores y sucesores factibles, veamos la tabla de enrutamiento para R1.

**Haga clic en Tabla de enrutamiento de R1 en la figura.**

La ruta hacia 192.168.1.0/24 muestra que el sucesor es R3 via 192.168.10.6 con una distancia factible de 2172416.

D 192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:56:13, Serial0/1

Ahora examinemos la tabla de topología para ver si existe algún sucesor factible para esta ruta.

**Haga clic en Tabla de topología de R1 en la figura.**

La tabla de topología sólo muestra al sucesor 192.168.10.6. No hay sucesores factibles. Al observar la topología física real o el diagrama de red, es obvio que hay una ruta de respaldo para 192.168.1.0/24 a través de R2. ¿Por qué R2 no se encuentra enumerado como sucesor factible? R2 no es un sucesor factible porque no cumple con la condición de factibilidad.

Aunque, si observamos la topología es obvio que R2 es una ruta de respaldo, EIGRP no tiene un mapa de la topología de red. EIGRP es un protocolo de enrutamiento por vector de distancia y sólo conoce la información de la red remota a través de sus vecinos.

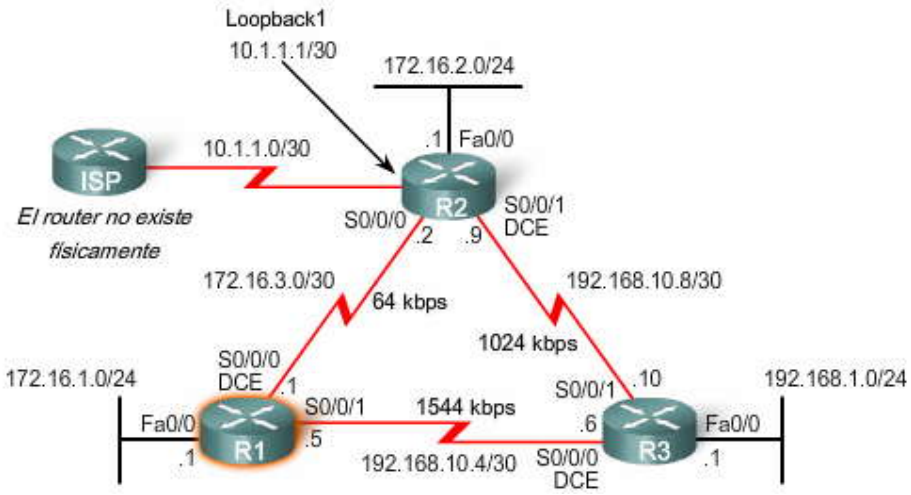
Por lo tanto, DUAL no almacena la ruta a través de R2 en la tabla de topología. Sin embargo, podemos ver todos los enlaces posibles, ya sea que satisfagan o no la condición de factibilidad, al agregar la opción [all-links] al comando show ip eigrp topology.

**Haga clic en Tabla de topología de R1 [all-links] en la figura.**

El comando show ip eigrp topology all-links muestra todas las rutas posibles hacia una red incluidos los sucesores, los sucesores factibles e incluso aquellos routers que no son sucesores factibles. La distancia factible de R1 hacia 192.168.1.0/24 es 2172416 a través del sucesor R3. Para que R2 sea considerado como sucesor factible, debe cumplir con la condición de factibilidad. La distancia factible de R2 para alcanzar a 192.168.1.0/24 debe ser menor que la distancia factible (FD) actual de R1. Como podemos ver en la figura, la distancia factible de R2 es 3014400, mayor que la distancia factible de R1 de 2172416.

Aun cuando R2 parece una ruta de respaldo viable hacia 192.168.1.0/24, R1 no tiene idea de que su ruta no es un lo op back potencial a través de sí mismo. EIGRP es un protocolo de enrutamiento por vector de distancia, sin la capacidad de ver un mapa de topología sin bucles completo de la red. El método de DUAL para garantizar que un vecino cuente con una ruta sin bucles es que la métrica del vecino debe satisfacer la condición de factibilidad. Al asegurarse que la RD del vecino es menor que la de su propia FD, el router puede suponer que este router vecino no forma parte de su propia ruta publicada, por lo tanto, siempre evita la posibilidad de un loop.

¿Significa esto que R2 no puede utilizarse si el sucesor falla? No, se puede usar a R3, pero el retraso será mayor antes de agregarlo a la tabla de enrutamiento. Antes de que esto suceda, DUAL deberá procesar más, lo cual se explica en el próximo tema.



```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:45:09, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:44:56, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:46:10, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:45:09, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:44:55, Serial0/0/1
```

Tabla de enrutamiento R1

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 2169856
        via Summary (2169856/0), Null0
P 192.168.10.4/30, 1 successors, FD is 2169856
        via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2172416
        via 192.168.10.6 (2172416/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3523840
        via 192.168.10.6 (3523840/3011840), Serial0/0/1
<output omitted>
```

Tabla de topología de R1

No hay un sucesor factible

Tabla de topología de R1 [all-links]

```
R1#show ip eigrp topology all-links
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 2169856, serno 3
        via Summary (2169856/0), Null0
        via 172.16.3.2 (41024000/3011840), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 2169856, serno 1
        via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2172416, serno 5
        via 192.168.10.6 (2172416/28160), Serial0/0/1
        via 172.16.3.2 (41026560/3014400), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3523840, serno 11
        via 192.168.10.6 (3523840/3011840), Serial0/0/1
```

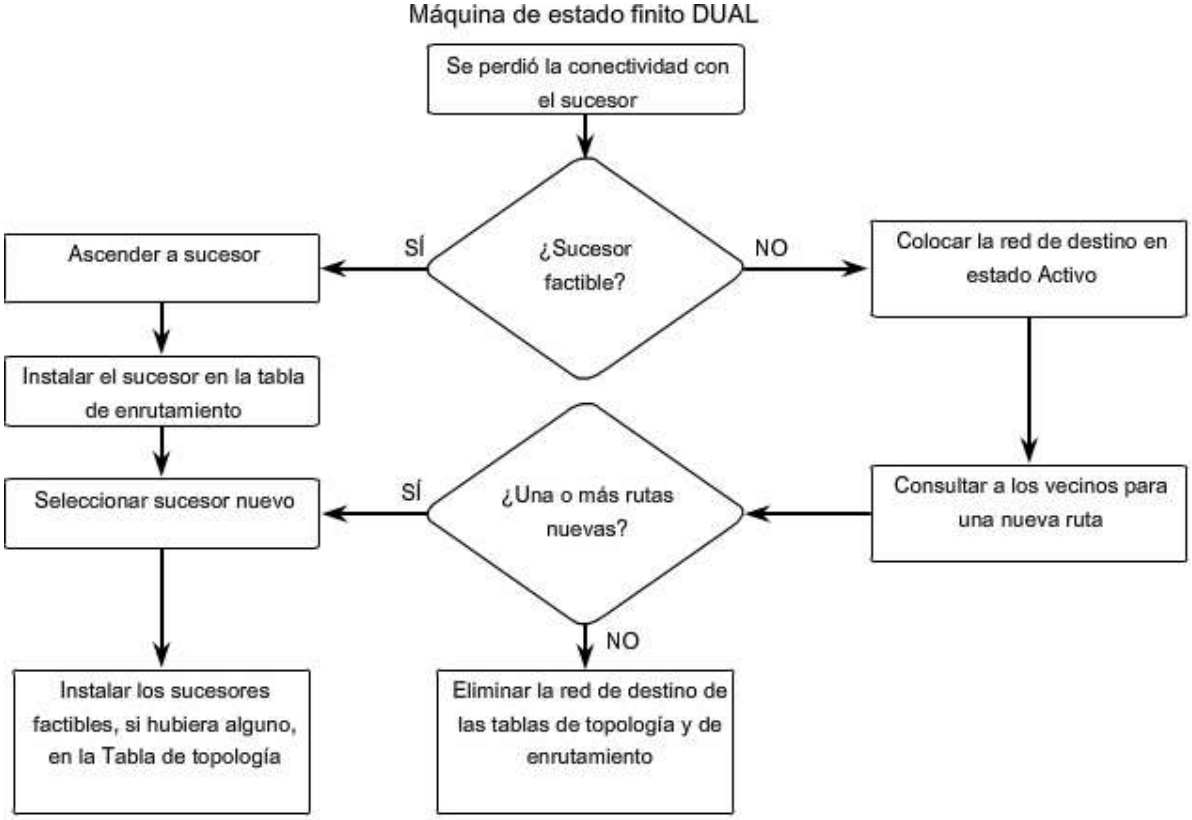
La RD desde R2 es mayor que la FD a R1.

### 9.4.6 MAQUINA DE ESTADO FINITO.-

**Máquina de Estados Finito (FSM) DUAL**

El núcleo de EIGRP son DUAL y su motor de cálculos de ruta EIGRP. El nombre real de esta tecnología es Máquina de Estados Finito (FSM) DUAL. Esta máquina de estados finitos contiene toda la lógica utilizada para calcular y comparar rutas en una red EIGRP. La figura muestra una versión simplificada de FSM DUAL.

Una máquina de estados finitos es una máquina abstracta, no un dispositivo mecánico con partes que se mueven. FSM define un conjunto de estados posibles por los que se puede pasar, qué eventos causan estos estados y qué eventos son el resultado de estos estados. Los diseñadores usan las FSM para describir de qué manera un dispositivo, programa de computador o algoritmo de enrutamiento reaccionará ante un conjunto de eventos de entrada. Las máquinas de estados finitos se encuentran más allá del alcance de este curso, sin embargo, presentamos el concepto para examinar algunos de los resultados de la máquina de estados finitos EIGRP mediante debug eigrp fsm. Utilicemos el comando para determinar qué hace DUAL cuando una ruta se elimina de la tabla de enrutamiento.




Haga clic en Tabla de topología 1 de R2 en la figura.

Recuerde de nuestro análisis previo que R2 utiliza actualmente a R3 como su sucesor para 192.168.1.0/24. Además, R2 tiene actualmente enumerado a R1 como sucesor factible. Veamos qué sucede cuando simulamos una falla de enlace entre R2 y R3.

**Haga clic en Resultado de depuración de R2 en la figura.**

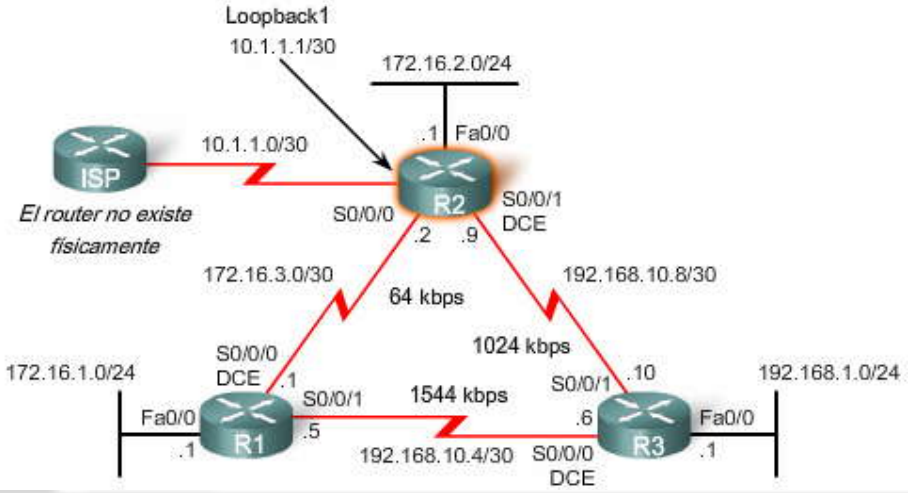
Primero, activamos la depuración de DUAL con el comando debug eigrp fsm. Luego, simulamos una falla en el enlace mediante el comando shutdown en la interfaz Serial 0/0/1 en R2.

Cuando haga esto en un router de verdad o en el Packet Tracer, observará toda la actividad que DUAL genera cuando se desactiva un enlace. R2 debe informar acerca de todos los vecinos EIGRP del enlace perdido, como así también debe actualizar su propio enrutamiento y tablas de topología. La figura en este ejemplo sólo muestra resultados de depuración seleccionados. En particular, observe que la máquina de estados finitos DUAL busca y encuentra un sucesor factible para la ruta en la tabla de topología EIGRP. El sucesor factible, R1, ahora se convierte en el sucesor y se instala en la tabla de enrutamiento como el nuevo mejor camino hacia 192.168.1.0/24.

**Haga clic en Tabla de topología 2 de R2 en la figura.**

La tabla de topología para R2 ahora muestra a R1 como sucesor y no hay sucesores factibles nuevos.

Si sigue a los routers o al Packet Tracer, asegúrese de restaurar la topología inicial reactivando la interfaz serial 0/0/1 en R2 con el comando no shutdown.



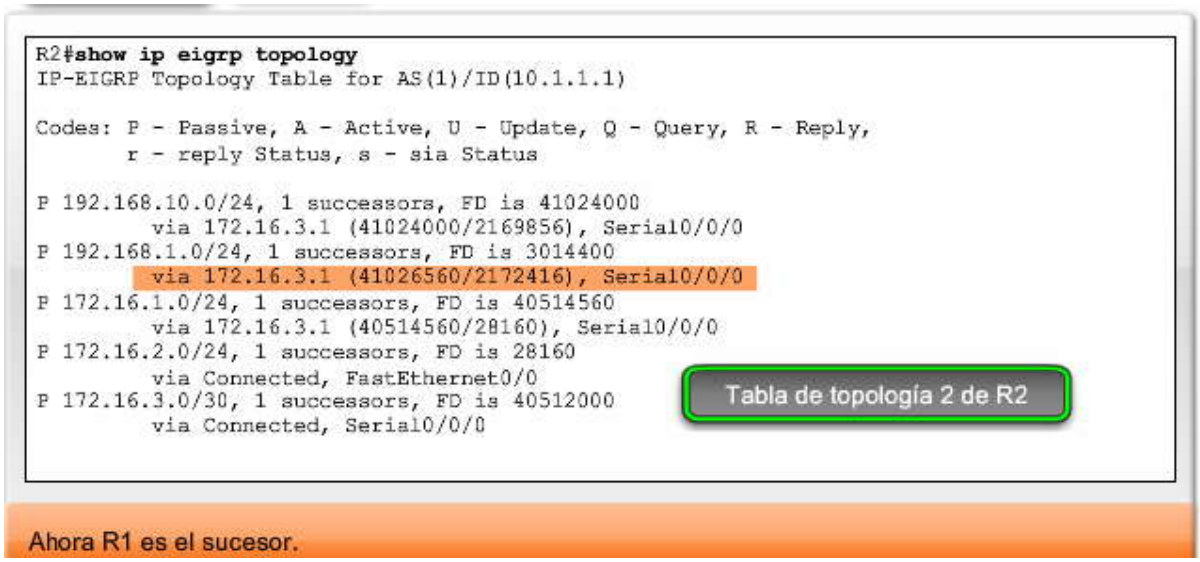

```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 3011840
         via Summary (3011840/0), Null0
         via 172.16.3.1 (41024000/2169856), Serial0/0/0
P 192.168.10.4/30, 1 successors, FD is 3523840
         via 192.168.10.10 (3523840/2169856), Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 3014400
         via 192.168.10.10 (3014400/28160), Serial0/0/1
         via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
         via Summary (28160/0), Null0
P 172.16.1.0/24, 1 successors, FD is 40514560
         via 172.16.3.1 (40514560/28160), Serial0/0/0
P 172.16.2.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
         via Connected, Serial0/0/0
```

R3 es el sucesor.

R1 es un sucesor factible.

```
R2#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#shutdown
<some debug output omitted>

DUAL: Find FS for dest 192.168.1.0/24. FD is 3014400, RD is 3014400
DUAL: 192.168.10.10 metric 4294967295/4294967295
DUAL: 172.16.3.1 metric 41026560/2172416 found Dmin is 41026560
DUAL: Removing dest 192.168.1.0/24, nexthop 192.168.10.10
DUAL: RT installed 192.168.1.0/24 via 172.16.3.1

R2(config-if)#end
R2#undebug all
All possible debugging has been turned off

R2#show ip route
<some output omitted>
D    192.168.1.0/24 [90/41026560] via 172.16.3.1, 00:08:58, Serial0/0/0
```

Resultado de debug de R2




**No hay un sucesor factible**

¿Qué sucede si la ruta del sucesor falla y no hay sucesores factibles? Recuerde, sólo porque DUAL no tenga un sucesor factible no quiere decir que no haya otra ruta hacia la red. Sólo quiere decir que DUAL no tiene una ruta de respaldo sin bucles garantizada hacia la red, por eso no se agregó a la tabla de topología como un sucesor factible. Si no hay sucesores factibles en la tabla de topología, DUAL colocará a la red en estado activo. DUAL consultará activamente a los vecinos en busca de un nuevo sucesor.

**Haga clic en Tabla de topología 1 de R1 en la figura.**

R1 utiliza actualmente a R3 como el sucesor hacia 192.168.1.0/24. Sin embargo, R1 no tiene a R2 enumerado como un sucesor factible porque R2 no satisface la condición de factibilidad. Veamos qué sucede cuando simulamos una falla de enlace entre R1 y R3.

**Haga clic en Resultado de depuración de R1 en la figura.**

Primero, activamos la depuración de DUAL con el comando debug eigrp fsm. Luego, simulamos una falla en el enlace mediante el comando shutdown en la interfaz Serial 0/0/1 en R1.

El resultado de depuración seleccionado muestra la red 192.168.1.0/24 en estado activo y se envían las consultas de EIGRP a los otros vecinos. R2 responde con una ruta hacia esta red, la cual se convierte en el nuevo sucesor y se instala en la tabla de enrutamiento.

Cuando el sucesor ya no se encuentra disponible y no hay un sucesor factible, DUAL colocará a la ruta en estado activo. DUAL enviará las consultas de EIGRP y les solicitará a otros routers una ruta hacia esta red. Los otros routers devolverán respuestas EIGRP, y le harán saber al emisor de las consultas EIGRP si tienen o no una ruta hacia la red solicitada. Si ninguna de las respuestas EIGRP tiene una ruta hacia esta red, el emisor de la consulta no tendrá una ruta hacia esta red.

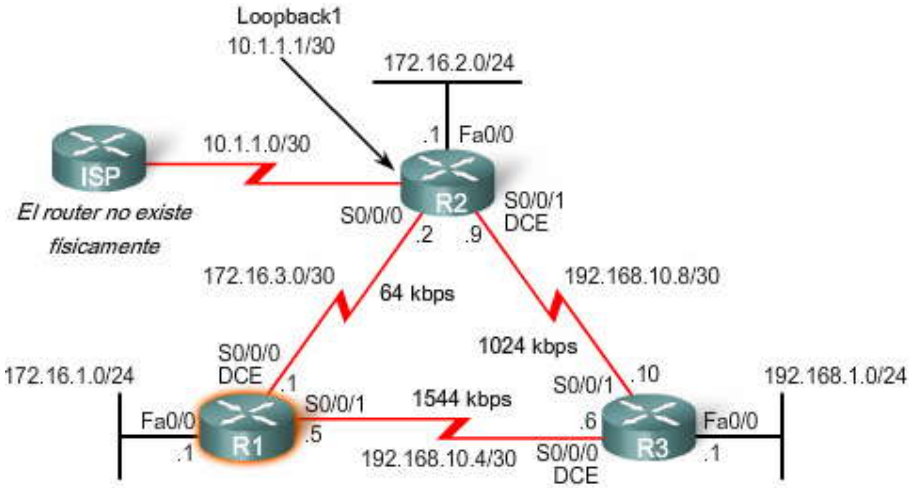
Si el emisor de las consultas EIGRP recibe respuestas EIGRP que incluyen una ruta hacia la red solicitada, la ruta preferida se agrega como nuevo sucesor y también a la tabla de enrutamiento. Este proceso llevará más tiempo que si DUAL tuviera un sucesor factible en su tabla de topología y pudiera agregar rápidamente la nueva ruta a la tabla de enrutamiento.

Nota: FSM DUAL y el proceso de consultas y respuestas se encuentra más allá del alcance de este curso .

**Haga clic en Tabla de topología 2 de R1 en la figura.**

La tabla de topología para R1 ahora muestra a R2 como el sucesor y no hay nuevos sucesores factibles.

Si sigue a los routers o al Packet Tracer, asegúrese de restaurar la topología original reactivando la interfaz serial 0/0/1 en R1 con el comando no shutdown.




```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 2169856
        via Summary (2169856/0), Null0
P 192.168.10.4/30, 1 successors, FD is 2169856
        via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2172416
        via 192.168.10.6 (2172416/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3523840
        via 192.168.10.6 (3523840/3011840), Serial0/0/1
P 172.16.0.0/16, 1 successors, FD is 28160
        via Summary (28160/0), Null0
P 172.16.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 172.16.2.0/24, 1 successors, FD is 40514560
        via 172.16.3.2 (40514560/28160), Serial0/0/0
```

Actualmente R1 utiliza a R3 como sucesor para 192.168.1.0/24.

```
R1#debug eigrp fsm
EIGRP FSM Events/Actions debugging is on
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#int s0/0/1
R1(config-if)#shutdown
<some debug output omitted>

DUAL: Find FS for dest 192.168.1.0/24. FD is 2172416, RD is 2172416
DUAL: 192.168.10.6 metric 4294967295/4294967295
DUAL: 172.16.3.2 metric 41026560/3014400 not found Dmin is 41026560
DUAL: Dest 192.168.1.0/24 entering active state.
DUAL: rcvreply: 192.168.1.0/24 via 172.16.3.2 metric 41026560/3014400
DUAL: Find FS for dest 192.168.1.0/24. FD is 4294967295, RD is 4294967295 found
DUAL: Removing dest 192.168.1.0/24, nexthop 192.168.10.6
DUAL: RT installed 192.168.1.0/24 via 172.16.3.2

R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#undebug all
All possible debugging has been turned off

R1#show ip route
<some output omitted>
```

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.0/24, 1 successors, FD is 41024000
        via 172.16.3.2 (41024000/3011840), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 41026560
        via 172.16.3.2 (41026560/3014400), Serial0/0/0
P 172.16.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 172.16.2.0/24, 1 successors, FD is 40514560
        via 172.16.3.2 (40514560/28160), Serial0/0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
        via Connected, Serial0/0/0
```

Ahora R1 muestra a R2 como sucesor y no hay nuevos sucesores factibles.

## 9.5 MAS CONFIGURACIONES EIGRP.-

### 9.5.1 LA RUTA RESUMIDA NULL0.-

El análisis de una tabla de enrutamiento que contiene rutas EIGRP puede ser confuso debido a la inclusión automática de EIGRP de las rutas resumidas Null0. En la figura, la tabla de enrutamiento R1 cuenta con dos rutas que tienen una interfaz de salida Null0. Recuerde del Capítulo 7, "RIPv2", que la interfaz Null0 es simplemente una ruta hacia ningún lado, comúnmente conocida como "cubo de bits". Por lo tanto, de manera predeterminada, EIGRP utiliza la interfaz Null0 para desechar todos los paquetes que coincidan con la ruta principal pero que no coincidan con ninguna de las rutas secundarias.

Puede pensar que si configuramos el comportamiento de enrutamiento sin clase con el comando ip classless, EIGRP no desechará ese paquete sino que continuará buscando una ruta por defecto o de superred. Sin embargo la ruta resumida Null0 es una ruta secundaria que coincidirá con todos los paquetes posibles de la ruta principal que no coinciden con otra ruta secundaria. Incluso con el comportamiento de enrutamiento sin clase, ip classless, en donde se esperaría que el proceso de búsqueda de rutas verifique la existencia de superredes y rutas por defecto, EIGRP utilizará la ruta resumida Null0 y desechará al paquete porque esta ruta coincidirá con todos los paquetes de la ruta principal que no tienen una ruta secundaria.

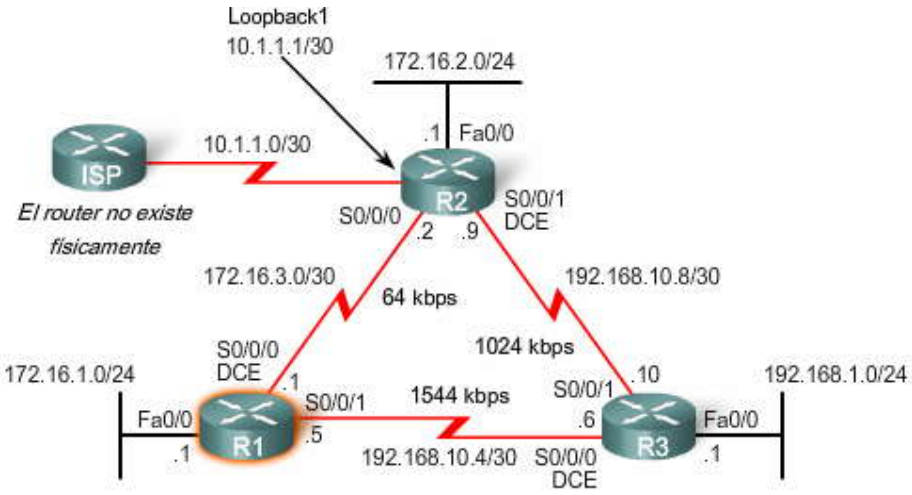
Sin importar si se está utilizando un comportamiento de enrutamiento sin clase o con clase, la ruta resumida null0 se utilizará y, por lo tanto, se denegará el uso de cualquier superred o ruta por defecto.

En la figura, R1 descartará todo paquete que coincida con la red con clase 172.16.0.0/16 principal pero que no coincida con una de las rutas secundarias 172.16.1.0/24, 172.16.2.0/24 ó 172.16.3.0/24. Por ejemplo, se descartará un paquete hacia 172.16.4.10. Incluso si se configurara una ruta por defecto, R1 igualmente descartaría el paquete porque éste coincide con la ruta resumida Null0 hacia 172.16.0.0/16.

D 172.16.0.0/16 es un resumen, 00:46:10, Null0

Nota: EIGRP automáticamente incluye una ruta resumida Null0 como ruta secundaria cuando se produce alguna de las siguientes condiciones:
Por lo menos existe una subred que se aprendió a través de EIGRP.
El resumen automático se encuentra habilitado.

Al igual que RIP, EIGRP resume automáticamente en bordes de red principales. Es posible que ya haya observado en el resultado de show run que EIGRP, de manera predeterminada, utiliza el comando auto-summary. En el próximo tema, verá que si deshabilita el resumen automático eliminará la ruta resumida Null0 y permitirá a EIGRP buscar una ruta por defecto o de superred cuando una ruta secundaria EIGRP no coincida con un paquete de destino.




```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 00:45:09, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/1
D       192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:44:56, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D       172.16.0.0/16 is a summary, 00:46:10, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/40514560] via 172.16.3.2, 00:45:09, Serial0/0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:44:55, Serial0/0/1
```

EIGRP instala una ruta de resumen Null0 para cada ruta primaria.
Se descartan los paquetes que coinciden con la ruta de resumen Null0.

### 9.5.2 DESHABILITACION DEL RESUMEN AUTOMATICO.-

Al igual que RIP, EIGRP resume automáticamente en bordes de red principales mediante el comando auto-summary en forma predeterminada. Podemos ver el resultado de esto si observamos la tabla de enrutamiento para R3.

Haga clic en Tabla de enrutamiento de R3 en la figura.

Observe que R3 no recibe rutas individuales para las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24. R1 y R2 automáticamente resumen las subredes en el borde con clase 172.16.0.0/16 cuando envían paquetes de actualización EIGRP hacia R3. El resultado es que R3 cuenta con una única ruta hacia 172.16.0.0/16 a través de R1. R1 es el sucesor por la diferencia en el ancho de banda.

D 172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:08:30, Serial0/0/0

Rápidamente puede ver que esta ruta no es la óptima. R3 enviará todos los paquetes destinados a 172.16.2.0 a través de R1. R3 no sabe que R1 tendrá que enviar después estos paquetes a través de un enlace muy lento hacia R2. La única manera en que R3 pueda detectar este ancho de banda lento es si R1 y R2 envían rutas individuales para cada una de las subredes de 172.16.0.0/16. En otras palabras, R1 y R2 deben dejar de resumir automáticamente a 172.16.0.0/16.

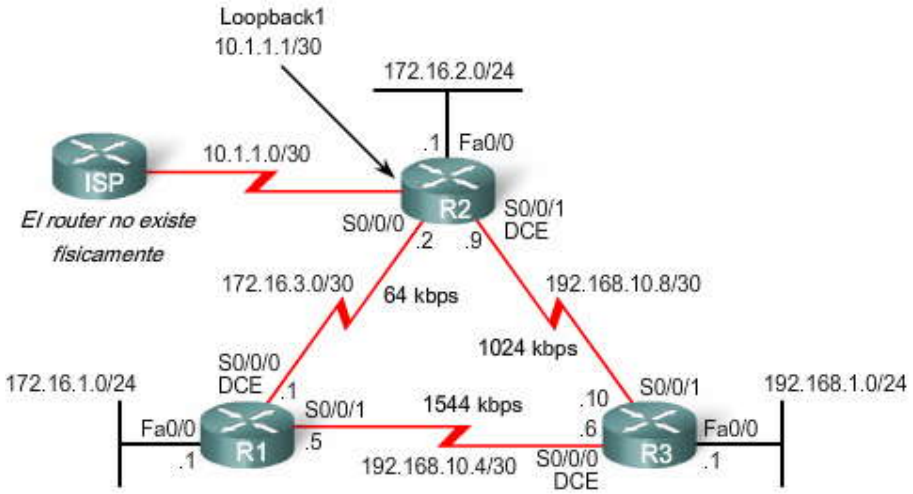
Haga clic en no auto-summary en la figura.

Como en RIPv2, se puede deshabilitar el resumen automático con el comando no auto-summary. El comando de configuración del router eigrp log-neighbor-changes se encuentra activado de manera predeterminada en algunas

implementaciones IOS. Si se encuentra activado, verá un resultado similar al mostrado para R1. DUAL desactiva todas las adyacencias de vecinos y luego las reestablece para que el efecto del comando no auto-summary se logre en su totalidad. Todos los vecinos EIGRP enviarán inmediatamente una nueva serie de actualizaciones que no se resumirá automáticamente.

Haga clic en R1, R2 y R3 en la figura.

Podemos ver en las tablas de enrutamiento de los tres routers que EIGRP se encuentra propagando subredes individuales. Observe que EIGRP ya no incluye la ruta resumida Null0, porque el resumen automático se deshabilitó con no auto-summary. Mientras el comportamiento de enrutamiento sin clase (ip classless) se encuentre en vigencia, las rutas por defecto y de superredes se utilizarán cuando no haya una coincidencia con ninguna ruta de subred.




```
R3#show ip route

     192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D       192.168.10.0/24 is a summary, 01:08:35, Null0
C       192.168.10.4/30 is directly connected, Serial0/0/0
C       192.168.10.8/30 is directly connected, Serial0/0/1
D    172.16.0.0/16 [90/2172416] via 192.168.10.5, 01:08:30, Serial0/0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

R3 utiliza la ruta subóptima a través de R1 para llegar a 172.16.2.0.

no auto-summary

```
R1#conf t
R1(config)#router eigrp 1
R1(config-router)#no auto-summary
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.3.2 (Serial0/0/0) is resync: summary
configured
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.10.6 (Serial0/0/1) is resync: summary
configured
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.3.2 (Serial0/0/0) is down: peer
restarted
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 172.16.3.2 (Serial0/0/0) is up: new adjacency
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.10.6 (Serial0/0/1) is down: peer
restarted
%DUAL-5-NBRCHANGE: IP-EIGRP(0) 1: Neighbor 192.168.10.6 (Serial0/0/1) is up: new
adjacency
```

```
R2#conf t
R2(config)#router eigrp 1
R2(config-router)#no auto-summary
```

```
R3#conf t
R3(config)#router eigrp 1
R3(config-router)#no auto-summary
```

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.4 is directly connected, Serial0/0/1
D       192.168.10.8 [90/3523840] via 192.168.10.6, 00:16:55, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:16:53, Serial0/0/1
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 00:16:52, Serial0/0/1
```

R1

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 2 subnets
D       192.168.10.4 [90/3523840] via 192.168.10.10, 00:15:44, Serial0/0/1
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.1.0/24 [90/3526400] via 192.168.10.10, 00:15:44, Serial0/0/1
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:15:44, Serial0/0/1
```

R2

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       <output omitted>

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.4 is directly connected, Serial0/0/0
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.1.0/24 [90/2172416] via 192.168.10.5, 00:00:11, Serial0/0/0
D       172.16.2.0/24 [90/3014400] via 192.168.10.9, 00:00:12, Serial0/0/1
D       172.16.3.0/30 [90/41024000] via 192.168.10.5, 00:00:12, Serial0/0/0
                      [90/41024000] via 192.168.10.9, 00:00:12, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
```

R3

Debido a que las rutas ya no se resumen automáticamente en los bordes de red principales, el enrutamiento de EIGRP y las tablas de topología también cambian.

Haga clic en R1, R2 y R3 en la figura.

Sin el resumen automático, la tabla de enrutamiento de R3 ahora incluye las tres subredes, 172.16.1 .0/24, 172.16.2.0/24 y 172.16.3.0/24. ¿Por qué tiene ahora la tabla de enrutamiento de R3 dos rutas de igual costo hacia 172.16.3.0/24? ¿El mejor camino no debería ser sólo a través de R1 con el enlace de 1544 Mbps?

Recuerde que EIGRP sólo utiliza el enlace con el ancho de banda más lento al calcular la métrica compuesta. El enlace más lento es el enlace de 64 Kbps que contiene la red 192.168.3.0/24. En este ejemplo, en enlace de 1544 Mbps y el enlace de 1021 Kbps son irrelevantes en el cálculo en lo que respecta a la métrica del ancho de banda. Como las dos rutas tienen el mismo número y tipo de interfaces salientes, los valores de retraso terminan siendo los mismos. Como resultado, la métrica de EIGRP para ambas rutas es la misma, incluso cuando la ruta a través de R1 sería en realidad la ruta "más rápida".

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.5)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.4/30, 1 successors, FD is 2169856
        via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 2172416
        via 192.168.10.6 (2172416/28160), Serial0/0/1
P 192.168.10.8/30, 1 successors, FD is 3523840
        via 192.168.10.6 (3523840/3011840), Serial0/0/1
        via 172.16.3.2 (41024000/3011840), Serial0/0/0
P 172.16.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 172.16.2.0/24, 1 successors, FD is 3526400
        via 192.168.10.6 (3526400/3014400), Serial0/0/1
        via 172.16.3.2 (40514560/28160), Serial0/0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
        via Connected, Serial0/0/0
```

```
R2#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(10.1.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.4/30, 1 successors, FD is 3523840
         via 192.168.10.10 (3523840/2169856), Serial0/0/1
         via 172.16.3.1 (41024000/2169856), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3014400
         via 192.168.10.10 (3014400/28160), Serial0/0/1
         via 172.16.3.1 (41026560/2172416), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/0/1
P 172.16.1.0/24, 1 successors, FD is 3526400
         via 192.168.10.10 (3526400/2172416), Serial0/0/1
         via 172.16.3.1 (40514560/28160), Serial0/0/0
P 172.16.2.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
         via Connected, Serial0/0/0
```

```
R3#show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.10.10)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.10.4/30, 1 successors, FD is 2169856
         via Connected, Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 28160
         via Connected, FastEthernet0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
         via Connected, Serial0/0/1
P 172.16.1.0/24, 1 successors, FD is 2172416
         via 192.168.10.5 (2172416/28160), Serial0/0/0
P 172.16.2.0/24, 1 successors, FD is 3014400
         via 192.168.10.9 (3014400/28160), Serial0/0/1
P 172.16.3.0/30, 2 successors, FD is 41024000
         via 192.168.10.9 (41024000/40512000), Serial0/0/1
         via 192.168.10.5 (41024000/40512000), Serial0/0/0
```

### 9.5.3 RESUMEN MANUAL.-

EIGRP puede configurarse para que resuma rutas, ya sea que se encuentre habilitado el resumen automático (auto-summary) o no. Debido a que EIGRP es un protocolo de enrutamiento sin clase e incluye la máscara de subred en las actualizaciones de enrutamiento, el resumen manual puede incluir rutas de superredes. Recuerde, una superred es una agregación de múltiples direcciones de redes principales con clase.

Haga clic en Nuevas LAN de R3 en la figura.

Supongamos que agregáramos dos redes más al router R3 mediante las interfaces loopback: 192.168.2.0/24 y 192.168.3.0/24. También configuramos redes en el proceso de enrutamiento EIGRP de R3 con comandos network para que R3 propague estas redes hacia otros routers.

Haga clic en Tablas de enrutamiento 1 en la figura.

Para verificar que R3 envió paquetes de actualización EIGRP hacia R1 y R2, revisamos las tablas de enrutamiento. En la figura, sólo se muestran las rutas pertinentes. Las tablas de enrutamiento de R1 y R2 muestran estas redes adicionales en sus tablas de enrutamiento: 192.168.2.0/24 y 192.168.3.0/24. En lugar de enviar tres redes por separado, R3 resume las redes 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24 como una única ruta.

Haga clic en Ruta resumida de R3 en la figura.

Determinación de la ruta EIGRP resumida

Primero determinemos cuál sería el resumen de estas tres rutas mediante el mismo método que utilizamos para determinar las rutas estáticas de resumen:

1. Escriba en binario las redes que desea resumir.

2. Si desea encontrar la máscara de subred para el resumen, comience con el bit que se encuentra más a la izquierda.

3. Vaya hacia la derecha y busque todos los bits que coincidan consecutivamente.

4. Cuando encuentre una columna de bits que no coincida, deténgase. Se encuentra en el límite de resumen.

5. Ahora, cuente el número de los bits que se encuentran más hacia la izquierda que coincidan, que en nuestro ejemplo es 22. Este número será su máscara de subred para la ruta resumida: /22 ó 255.255.252.0

6. Para encontrar la dirección de red para el resumen, copie los 22 bits que coinciden y agregue a todos los bits 0 al final para obtener 32 bits.

El resultado es la dirección de red resumida y la máscara para 192.168.0.0/22.

Configuración del resumen manual de EIGRP

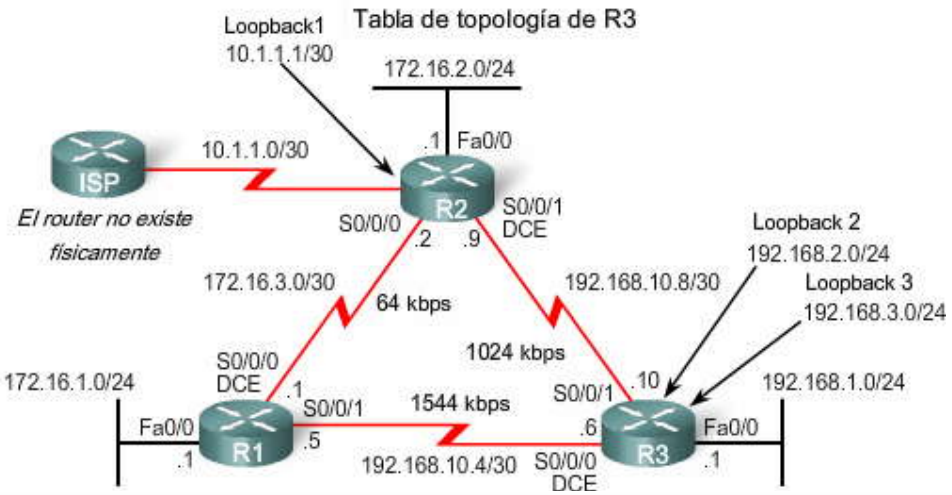
Para establecer el resumen manual de EIGRP en todas las interfaces que envían paquetes EIGRP, utilice el siguiente comando de interfaz:

Router(config-if)#ip summary-address eigrpas-number network-address subnet-mask

Como R3 tiene dos vecinos EIGRP, el resumen manual de EIGRP se configura en Serial 0/0/0 y Serial 0/0/1.

Haga clic en Tablas de enrutamiento 2 en la figura.

Las tablas de enrutamiento de R1 y R2 ahora no incluyen las redes individuales 192.168.1.0/24, 192.168.2.0/24 ni 192.168.3.0/24. En su lugar, muestran una única ruta resumida de 192.168.0.0/22. Como aprendió en el Capítulo 2, "Enrutamiento estático", las rutas resumidas disminuyen el número de rutas totales en las tablas de enrutamiento, lo cual hace más eficiente el proceso de búsqueda en la tabla de enrutamiento. Las rutas resumidas también requieren menor utilización de ancho de banda para las actualizaciones de enrutamiento porque se puede enviar una sola ruta en lugar de múltiples rutas individuales.




```
R3(config)#inter loopback 2
R3(config-if)#ip address 192.168.2.1 255.255.255.0
R3(config-if)#interface loopback 3
R3(config-if)#ip address 192.168.3.1 255.255.255.0
R3(config-if)#router eigrp 1
R3(config-router)#network 192.168.2.0
R3(config-router)#network 192.168.3.0
```

Nuevas LAN de R3

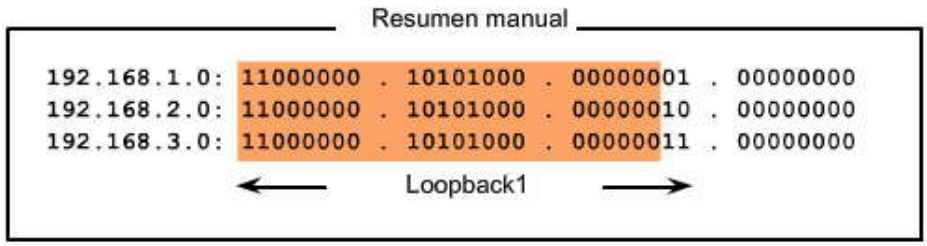
Se agregan dos LAN simuladas a R3 mediante interfaces de loopback.
Luego se configuran las redes como parte del proceso de EIGRP.

Rutas de R1 y R2 para 192.168

Tablas de enrutamiento 1

```
R1#show ip route
<output limited to 192.168 routes>

Gateway of last resort is not set

D    192.168.1.0/24 [90/2172416] via 192.168.10.6, 02:07:38, Serial0/0/1
D    192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:00:34, Serial0/0/1
D    192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:00:18, Serial0/0/1
```

```
R2#show ip route
<output limited to 192.168 routes>

Gateway of last resort is not set

D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 02:08:50, Serial0/0/1
D    192.168.2.0/24 [90/3139840] via 192.168.10.10, 00:01:46, Serial0/0/1
D    192.168.3.0/24 [90/3139840] via 192.168.10.10, 00:01:30, Serial0/0/1
```




Loopback 2

Ruta resumida de R3

```
R3(config)#interface serial 0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
```

Configurar la ruta de resumen en todas las interfaces que envían paquetes EIGRP.

Tablas de enrutamiento de R1 y R2

```
R1#show ip route
<output omitted>
Gateway of last resort is not set

 192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.4 is directly connected, Serial0/0/1
D       192.168.10.8 [90/3523840] via 192.168.10.6, 00:01:34, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/3526400] via 192.168.10.6, 00:01:12, Serial0/0/1
C       172.16.3.0/30 is directly connected, Serial0/0/0
D    192.168.0.0/22 [90/2172416] via 192.168.10.6, 00:01:11, Serial0/0/1
```

Tablas de enrutamiento 2

```
R2#show ip route
<output omitted>

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 2 subnets
D       192.168.10.4 [90/3523840] via 192.168.10.10, 00:00:23, Serial0/0/1
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.1.0/24 [90/3526400] via 192.168.10.10, 00:00:23, Serial0/0/1
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
D    192.168.0.0/22 [90/3014400] via 192.168.10.10, 00:00:23, Serial0/0/1
```

Rutas de resumen manual

### 9.5.4 RUTA POR DEFECTO EIGRP.-

Haga clic en Configuración estática predeterminada de R2.

El uso de una ruta estática hacia 0.0.0.0/0 como ruta por defecto no depende de ningún protocolo de enrutamiento. La ruta estática por defecto "quad zero" se puede utilizar con cualquier protocolo de enrutamiento actualmente admitido. La ruta estática por defecto generalmente se configura en el router que tiene una conexión con una red fuera del dominio de enrutamiento EIGRP, por ejemplo, con un ISP.

EIGRP requiere el uso del comando redistribute static para que incluya esta ruta estática por defecto con sus actualizaciones de enrutamiento EIGRP. El comando redistribute static le dice a EIGRP que incluya esta ruta estática en sus actualizaciones EIGRP de otros routers. Esta figura muestra la configuración de la ruta estática por defecto y del comando redistribute static en el router R2.

Nota: La ruta estática por defecto utiliza la interfaz de salida de Loopback1. Esto se realiza porque el router ISP en nuestra topología no existe físicamente. Al utilizar una interfaz loopback, podemos simular una conexión con otro router.

Haga clic en R1, R2 y R3 en la figura.

Las tablas de enrutamiento ahora muestran una ruta estática por defecto y ahora se establece un gateway de último recurso.

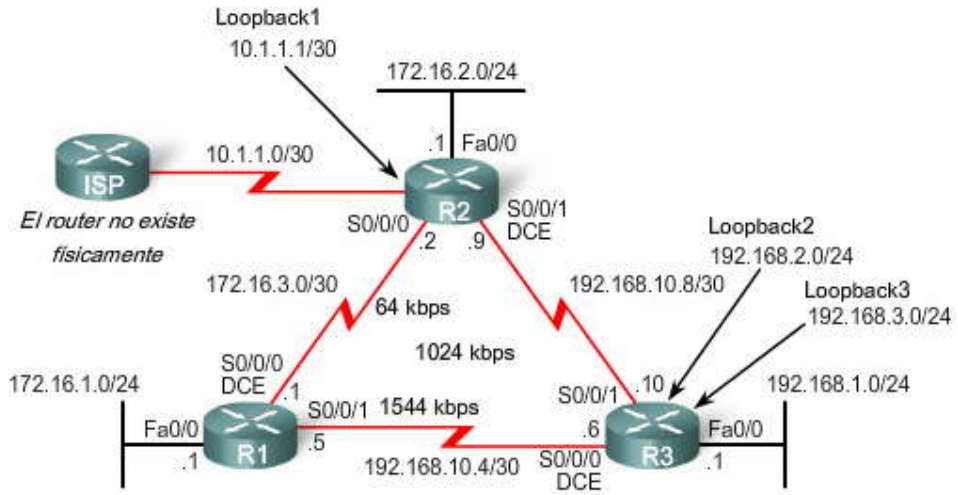
En las tablas de enrutamiento para R1 y R3, observe el origen de enrutamiento y la distancia administrativa para la nueva ruta estática por defecto. La entrada para la ruta estática por defecto en R1 es la siguiente:

D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:01:08, Serial0/1
D: Esta ruta estática se obtuvo de una actualización de enrutamiento EIGRP.
*: La ruta es un candidato para una ruta por defecto.
EX: La ruta es una ruta EIGRP externa, en este caso una ruta estática externa al dominio de enrutamiento EIGRP.
170: Ésta es la distancia administrativa de una ruta EIGRP externa.

Las rutas por defecto proporcionan una ruta predeterminada para salir del dominio de enrutamiento y, al igual que las rutas resumidas, minimizan el número de entradas en la tabla de enrutamiento.

Nota: Existe otro método para propagar una ruta por defecto en EIGRP, mediante el comando ip default-network. Para obtener más información acerca de este comando consulte:

http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094374.shtml




Configuración estática por defecto de R2

```
R2(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
R2(config)#router eigrp 1
R2(config-router)#redistribute static
```

R1

```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.10.6 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.4 is directly connected, Serial0/0/1
D       192.168.10.8 [90/3523840] via 192.168.10.6, 01:06:01, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       172.16.1.0/24 is directly connected, FastEthernet0/0
D       172.16.2.0/24 [90/3526400] via 192.168.10.6, 01:05:39, Serial0/0/1
C       172.16.3.0/30 is directly connected, Serial0/0/0
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:02:14, Serial0/0/1
D    192.168.0.0/22 [90/2172416] via 192.168.10.6, 01:05:38, Serial0/0/1
```

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 2 subnets
D       192.168.10.4 [90/3523840] via 192.168.10.10, 01:03:26, Serial0/0/1
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.1.0/24 [90/3526400] via 192.168.10.10, 01:03:26, Serial0/0/1
C       172.16.2.0/24 is directly connected, FastEthernet0/0
C       172.16.3.0/30 is directly connected, Serial0/0/0
     10.0.0.0/30 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
S*   0.0.0.0/0 is directly connected, Loopback1
D    192.168.0.0/22 [90/3014400] via 192.168.10.10, 01:03:26, Serial0/0/1
```

R2

```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.10.9 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 2 subnets
C       192.168.10.4 is directly connected, Serial0/0/0
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D       172.16.1.0/24 [90/2172416] via 192.168.10.5, 01:04:48, Serial0/0/0
D       172.16.2.0/24 [90/3014400] via 192.168.10.9, 01:04:50, Serial0/0/1
D       172.16.3.0/30 [90/41024000] via 192.168.10.5, 01:04:50, Serial0/0/0
                      [90/41024000] via 192.168.10.9, 01:04:50, Serial0/0/1
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Loopback2
C    192.168.3.0/24 is directly connected, Loopback3
D*EX 0.0.0.0/0 [170/3139840] via 192.168.10.9, 00:01:25, Serial0/0/1
D    192.168.0.0/22 is a summary, 01:04:48, Null0
```

R3

### 9.5.5 AJUSTE DE EIGRP.-

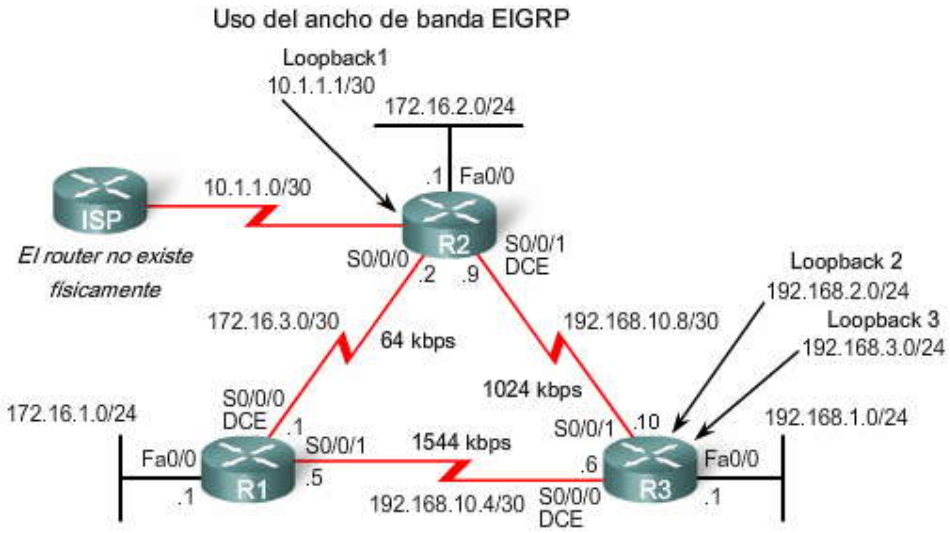
Los dos últimos temas de este capítulo analizan dos maneras fundamentales de ajustar las operaciones de EIGRP. Primero, analizaremos la utilización del ancho de banda de EIGRP. Luego, analizaremos cómo cambiar el saludo predeterminado y los valores de tiempo de espera.

**Utilización del ancho de banda de EIGRP**

De manera predeterminada, EIGRP sólo utilizará hasta 50% del ancho de banda de una interfaz para información EIGRP. Esto impide que el proceso EIGRP utilice en exceso los enlaces y que no permita suficiente ancho de banda para el enrutamiento de tráfico normal. El comando ip bandwidth-percent eigrp puede utilizarse para configurar el porcentaje del ancho de banda que EIGRP puede utilizar en una interfaz.

Router(config-if)#ip bandwidth-percent eigrp as-number percent

En la figura, R1 y R2 comparten un enlace muy lento de 64 kbps. La configuración que limita qué cantidad de ancho de banda EIGRP utiliza se muestra junto con el comando bandwidth. El comando ip bandwidth-percent eigrp utiliza la cantidad de ancho de banda configurada (o el ancho de banda predeterminado) al calcular el porcentaje que EIGRP puede utilizar. En nuestro ejemplo, limitamos a EIGRP a no más de un 50% del ancho de banda del enlace. Por lo tanto, EIGRP nunca utilizará más de 32 kbps del ancho de banda del enlace para el tráfico de paquetes EIGRP.




Uso del ancho de banda EIGRP

```
R1(config)#interface serial 0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#ip bandwidth-percent eigrp 1 50
```

```
R2(config)#interface serial 0/0/0
R2(config-if)#bandwidth 64
R2(config-if)#ip bandwidth-percent eigrp 1 50
```

Configuración de intervalos de saludo y tiempos de espera

Los intervalos de saludo y los tiempos de espera se configuran por interfaz y no tienen que coincidir con otros routers EIGRP para establecer adyacencias. El comando para configurar un intervalo de saludo distinto es:

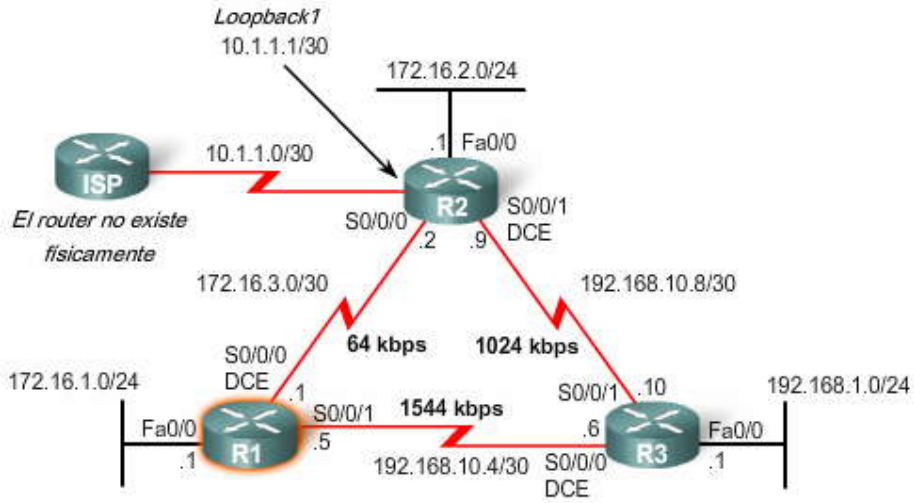
Router(config-if)#ip hello-interval eigrp as-number seconds

Si cambia el intervalo de saludo, asegúrese de cambiar también el tiempo de espera a un valor igual o superior al intervalo de saludo. De lo contrario, la adyacencia de vecinos se desactivará después que haya terminado el tiempo de espera y ant es del próximo intervalo de saludo. El comando para configurar un tiempo de espera distinto es:

Router(config-if)#ip hold-time eigrp as-number seconds

El valor segundos para los intervalos de saludo y de tiempo de espera puede variar de 1 a 65 535. Este rango indica que el usuario puede establecer el intervalo de saludo en un valor mayor que 18 horas, el cual puede ser adecuado para un enlace dial-up muy costoso. Sin embargo, en la figura configuramos a R1 y R2 para que usen un intervalo de saludo de 60 s egundos y un tiempo de espera de 180 segundos. La forma no puede usarse en ambos comandos para restaurar los valores predeterminados.

Configuración de intervalos de saludo y tiempos de espera




Configuración de intervalos de saludo y tiempos de espera

```
R1(config)#int s0/0/0
R1(config-if)#ip hello-interval eigrp 1 60
R1(config-if)#ip hold-time eigrp 1 180
R1(config-if)#end
```

```
R2(config)#int s0/0/0
R2(config-if)#ip hello-interval eigrp 1 60
R2(config-if)#ip hold-time eigrp 1 180
R2(config-if)#end
```

# CAPITULO X – "PROCOLOS DE ENRUTAMIENTO DE ESTADO DE ENLACE"

## 10.0 INTRODUCCION DEL CAPITULO.-

### 10.0.1 INTRODUCCIÓN DEL CAPITULO.-

En el Capítulo 3, "Introducción a los protocolos de enrutamiento dinámico", ilustramos la diferencia entre el enrutamiento por vector de distancia y de estado de enlace con una analogía. La analogía menciona que los protocolos de enrutamiento por vector de distancia son semejantes a la utilización de carteles de carretera para guiarse en el camino hasta un destino; sólo le brindan información acerca de la distancia y la dirección. Sin embargo, los protocolos de enrutamiento de estado de enlace son semejantes a la utilización de un mapa. Con un mapa, puede ver todas las posibles rutas y determinar su propia ruta preferida.

Los protocolos de enrutamiento por vector de distancia son semejantes a los carteles de carretera debido a que los routers deben tomar decisiones de rutas preferidas conforme a una distancia o métrica a una red. Del mismo modo que los viajeros confían en que el cartel de carretera indique en forma precisa la distancia hasta el próximo pueblo, un router vector distancia confía en que otro router publique la verdadera distancia hacia la red de destino.

Los protocolos de enrutamiento de estado de enlace tienen un enfoque diferente. Los protocolos de enrutamiento de estado de enlace son más similares a los mapas de carretera ya que crean un mapa topológico de la red y cada router utiliza dicho mapa para determinar la ruta más corta hacia cada red. De la misma manera en que se utiliza un mapa para buscar la ruta hacia otro pueblo, los routers de estado de enlace utilizan un mapa para determinar la ruta preferida para alcanzar otro destino.

Los routers que ejecutan un protocolo de enrutamiento de estado de enlace envían información acerca del estado de sus enlaces a otros routers en el dominio de enrutamiento. El estado de dichos enlaces hace referencia a sus redes conectadas directamente e incluye información acerca del tipo de red y los routers vecinos en dichas redes; de allí el nombre protocolo de enrutamiento de estado de enlace.

El objetivo final es que cada router reciba toda la información de estado de enlace acerca de todos los demás routers en el área de enrutamiento. Con esta información de estado de enlace, cada router puede crear su propio mapa topológico de la red y calcular independientemente la ruta más corta hacia cada red.

Este capítulo presenta los conceptos de los protocolos de enrutamiento de estado de enlace. En el Capítulo 11, aplicaremos dichos conceptos a OSPF.

**En este capítulo, aprenderá a:**

- Describir las características y los conceptos básicos de los protocolos de enrutamiento de estado de enlace.
- Enumerar los beneficios y requerimientos de los protocolos de enrutamiento de estado de enlace.

## 10.1 ENRUTAMIENTO DE ESTADO DE ENLACE.-

### 10.1.1 PROCOLO DE ENRUTAMIENTO DE ESTADO DE ENLACE.-

A los protocolos de enrutamiento de estado de enlace también se los conoce como protocolos de shortest path first y se desarrollan en torno del algoritmo shortest path first (SPF) de Edsger Dijkstra. El algoritmo SPF se analizará con mayor detalle en una sección posterior.

Los protocolos de enrutamiento de estado de enlace IP se muestran en la figura:

- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

Los protocolos de enrutamiento de estado de enlace son conocidos por presentar una complejidad bastante mayor que sus vectores de distancia equivalentes. Sin embargo, la funcionalidad y configuración básicas de los protocolos de enrutamiento de estado de enlace no son complejas en absoluto. Incluso el mismo algoritmo puede comprenderse fácilmente, como podrá ver en el siguiente tema. Las operaciones OSPF básicas pueden configurarse con un comando router ospf process-id y una sentencia de red, similar a otros protocolos de enrutamiento como RIP y EIGRP.

Nota: OSPF se analiza en el Capitulo 11 e IS-IS se analiza en CCNP. También hay protocolos de enrutamiento de estado de enlace para las redes que no son IP. Éstos incluyen DNA de fase V de DEC y el NetWare Link Services Protocol (NLSP) de Novell, que no forman parte del plan de estudios de CCNA ni CCNP.

Clasificación de los protocolos de enrutamiento

| | Protocolos de gateway interiores | | | Protocolos de Gateway Exterior |
|---|---|---|---|---|
| | Protocolos de enrutamiento por vector de distancia | | Protocolos de enrutamiento de estado de enlace | Vector de ruta |
| Con clase | **RIP** | IGRP | | EGP |
| Sin clase | **RIPv2** | **EIGRP** | **OSPFv2** IS-IS | BGPv4 |
| IPv6 | RIPng | **EIGRP** para IPv6 | OSPFv3 **IS-IS** para IPv6 | **BGPv4** para IPv6 |

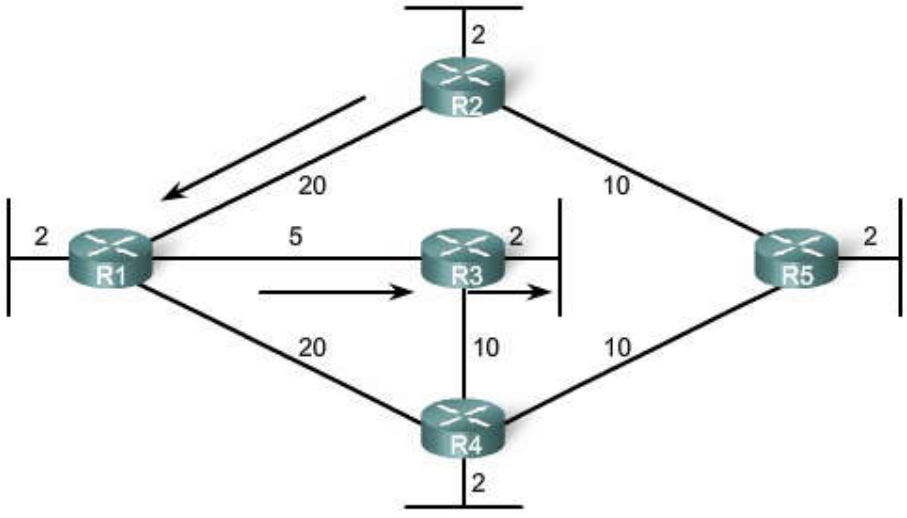
El currículum se concentra en los protocolos de enrutamiento escritos en negrita.

### 10.1.2 INTRODUCCION AL ALGORITMO SPF.-

Al algoritmo de Dijkstra se lo llama comúnmente algoritmo shortest path first (SPF). Este algoritmo acumula costos a lo largo de cada ruta, desde el origen hasta el destino. Si bien al algoritmo de Dijkstra se conoce como el algoritmo shortest path first, éste es de hecho el objetivo de cada algoritmo de enrutamiento.

En la figura, cada ruta se rotula con un valor arbitrario para el costo. El costo de la ruta más corta para que R2 envíe paquetes a la LAN conectada a R3 es 27. Observe que este costo no es 27 para que todos los routers alcancen la LAN conectada a R3. Cada router determina su propio costo hacia cada destino en la topología. En otros términos, cada router calcula el algoritmo SPF y determina el costo desde su propia perspectiva. Esto se volverá más evidente más adelante en este capítulo.

Shortest path first del algoritmo de Dijkstra




Ruta más corta para que el host en la LAN del R2 alcance al host en la LAN de R3:
R2 a R1 (20) + R1 a R3 (5) + R3 a LAN (2) = 27

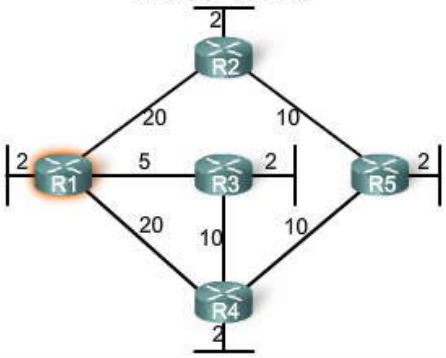
**Haga clic en R1 en la figura.**

Para R1, la ruta más corta hacia cada LAN, junto con el costo, se muestra en la tabla. La ruta más corta no es necesariamente la ruta con la menor cantidad de saltos. Por ejemplo, observe la ruta hacia la LAN R5. Podría pensar que R1 realizará el envío directamente a R4 en lugar de R3. Sin embargo, el costo para llegar a R4 directamente (22) es más alto que el costo para llegar a R4 a través de R3 (17).

**Continúe haciendo clic en R2, hasta llegar a R5 en la figura.**

Observe la ruta más corta para que cada router alcance cada una de las LAN, como se muestra en las tablas.

Introducción al algoritmo SPF
Árbol SPF para R1

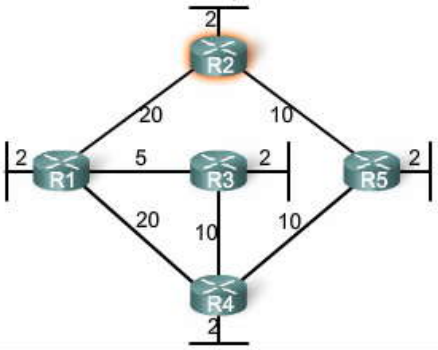



| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R2 | R1 a R2 | 22 |
| LAN de R3 | R1 a R3 | 7 |
| LAN de R4 | R1 a R3 a R4 | 17 |
| LAN de R5 | R1 a R3 a R4 a R5 | 27 |

R1 R2 R3 R4 R5

Haga clic para ver el árbol SPF y las rutas para cada router.

Introducción al algoritmo SPF
Árbol SPF para R2

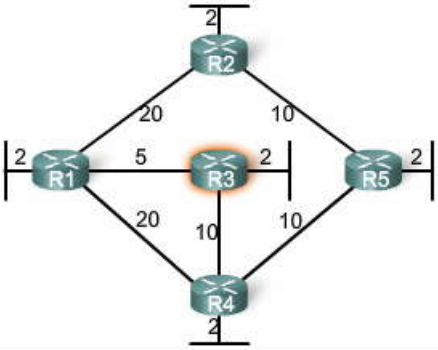



| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R1 | R2 a R1 | 22 |
| LAN de R3 | R2 a R1 a R3 | 27 |
| LAN de R4 | R2 a R5 a R4 | 22 |
| LAN de R5 | R2 a R5 | 12 |

R1 R2 R3 R4 R5

Haga clic para ver el árbol SPF y las rutas para cada router.

Introducción al algoritmo SPF
Árbol SPF para R3

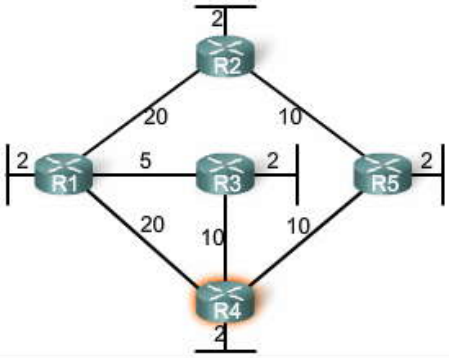



| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R1 | R3 a R1 | 7 |
| LAN de R2 | R3 a R1 a R2 | 27 |
| LAN de R4 | R3 a R4 | 12 |
| LAN de R5 | R3 a R4 a R5 | 22 |

R1 R2 R3 R4 R5

Haga clic para ver el árbol SPF y las rutas para cada router.

Introducción al algoritmo SPF
Árbol SPF para R4

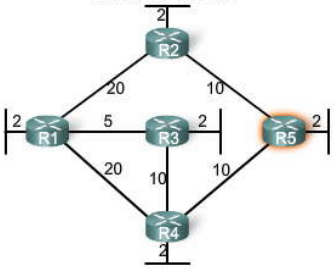



| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R1 | R4 a R3 a R1 | 17 |
| LAN de R2 | R4 a R5 a R2 | 22 |
| LAN de R3 | R4 a R3 | 12 |
| LAN de R5 | R4 a R5 | 12 |

R1 R2 R3 R4 R5

Haga clic para ver el árbol SPF y las rutas para cada router.

Introducción al algoritmo SPF
Árbol SPF para R5




| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R1 | R5 a R4 a R3 a R1 | 27 |
| LAN de R2 | R5 a R2 | 12 |
| LAN de R3 | R5 a R4 a R3 | 22 |
| LAN de R4 | R5 a R4 | 12 |

R1 R2 R3 R4 R5

Haga clic para ver el árbol SPF y las rutas para cada router.

### 10.1.3 PROCESO DE ENRUTAMIENTO DE ESTADO DE ENLACE.-

Por lo tanto, ¿de qué manera exactamente funciona un protocolo de enrutamiento de estado de enlace? Todos los routers de nuestra topología completarán el siguiente proceso genérico de enrutamiento de estado de enlace para alcanzar un estado de convergencia:

1. **Cada router aprende sobre sus propios enlaces, sus propias redes conectadas directamente**. Esto se realiza al detectar que una interfaz se encuentra en estado up.

2. **Cada router es responsable de reunirse con sus vecinos en redes conectadas directamente**. En forma similar a EIGRP, los routers de estado de enlace lo realizan intercambiando paquetes de saludo con otros routers de estado de enlace en redes conectadas directamente.

3. **Cada router crea un Paquete de estado de enlace (LSP) que incluye el estado de cada enlace conectado directamente.** Esto se realiza registrando toda la información pertinente acerca de cada vecino, que incluye el ID de vecino, el tipo de enlace y el ancho de banda.

4. **Cada router satura con el LSP a todos los vecinos, que luego almacenan todos los LSP recibidos en una base de datos**. Los vecinos luego saturan con los LSP a sus vecinos hasta que todos los routers del área hayan recibido los LSP. Cada router almacena una copia de cada LSP recibido por parte de sus vecinos en una base de datos local.

5. **Cada router utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino**. En forma similar a tener un mapa de carretera, el router tiene ahora un mapa completo de todos los destinos de la topología y las rutas para alcanzarlos. El algoritmo SPF se utiliza para construir el mapa de la topología y determinar el mejor camino hacia cada red.

Analizaremos este proceso con mayor detalle en los siguientes temas.

Proceso de enrutamiento de estado de enlace

**Proceso de enrutamiento de estado de enlace**

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
3. Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.
4. Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.
5. Cada router utiliza la base de datos para construir un mapa topológico completo y calcula la mejor ruta para cada red de destino.

### 10.1.4 CONOCIMIENTOS SOBRE REDES CONECTADAS DIRECTAMENTE.-

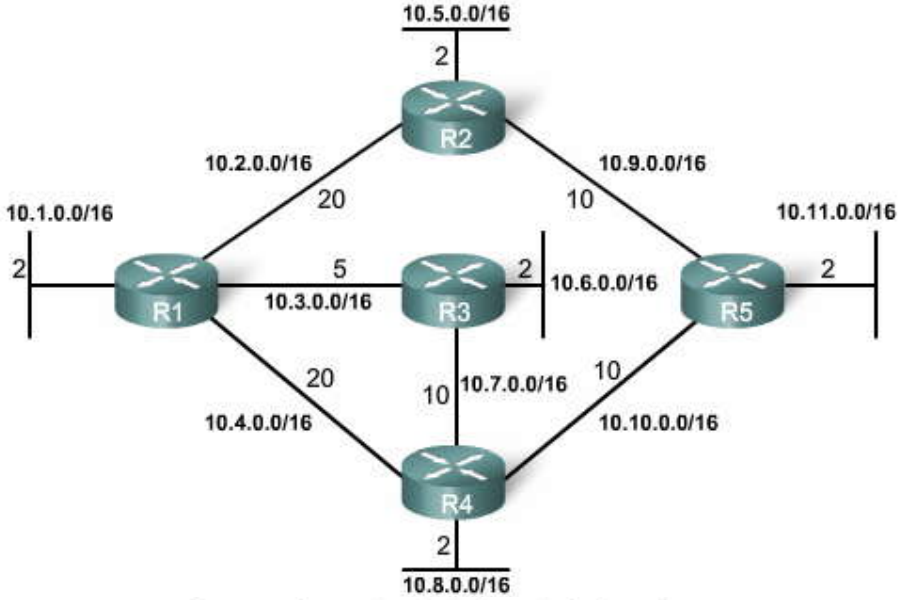
**Haga clic en Proceso del enrutamiento de estado de enlace en la figura.**

La topología muestra ahora las direcciones de red para cada enlace. **Cada router aprende sobre sus propios enlaces, sus propias redes directamente conectadas del mismo modo que se analizó en el Capítulo 1**, "Introducción al enrutamiento y envío de paquetes". Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz se vuelve parte de esa red.

**Haga clic en R1 en la figura.**

Cuando configura y activa correctamente las interfaces, el router aprende sobre sus propias redes conectadas directamente. Independientemente de los protocolos de enrutamiento utilizados, dichas redes conectadas directamente ahora forman parte de la tabla de enrutamiento. A los fines de nuestro análisis, nos concentraremos en el proceso de enrutamiento de estado de enlace desde la perspectiva de R1.

Proceso de enrutamiento de estado de enlace

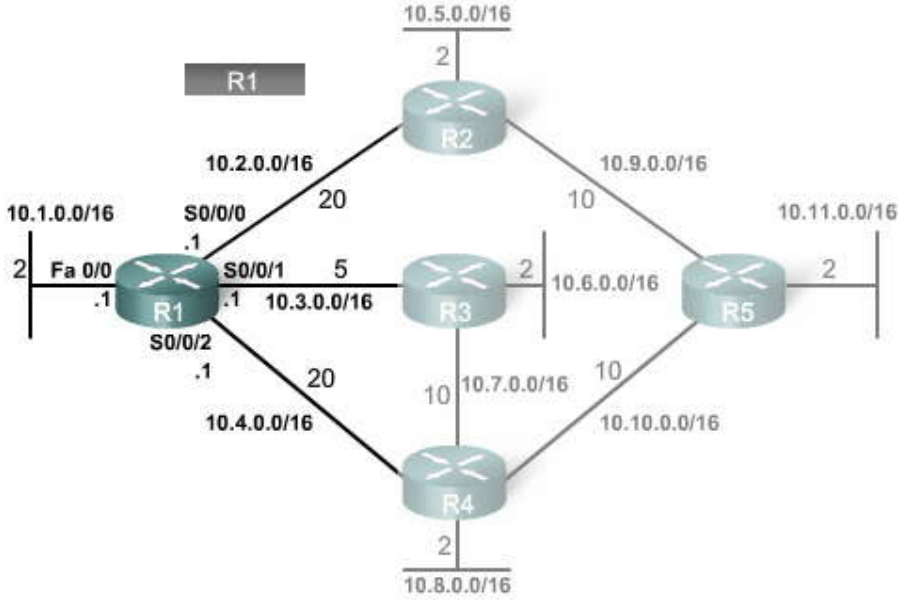



Proceso de enrutamiento de estado de enlace

## Proceso de enrutamiento de estado de enlace

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
3. Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.
4. Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.
5. Cada router utiliza la base de datos para construir un mapa topológico completo y calcula la mejor ruta para cada red de destino.

Proceso de enrutamiento de estado de enlace



**Enlace**

Con los protocolos de enrutamiento de estado de enlace, un enlace es una interfaz en un router. Como ocurre con los protocolos por vector de distancia y las rutas estáticas, la interfaz debe configurarse adecuadamente con una dirección IP y una máscara de subred, y el enlace debe encontrarse en estado activo antes de que el protocolo de enrutamiento de estado de enlace pueda aprender acerca de un enlace. Asimismo, como ocurre con los protocolos por vector de distancia, la interfaz debe incluirse en una de las sentencias de red antes de que ésta pueda participar en el proceso de enrutamiento de estado de enlace.

La figura muestra a R1 conectado a cuatro redes conectadas directamente:

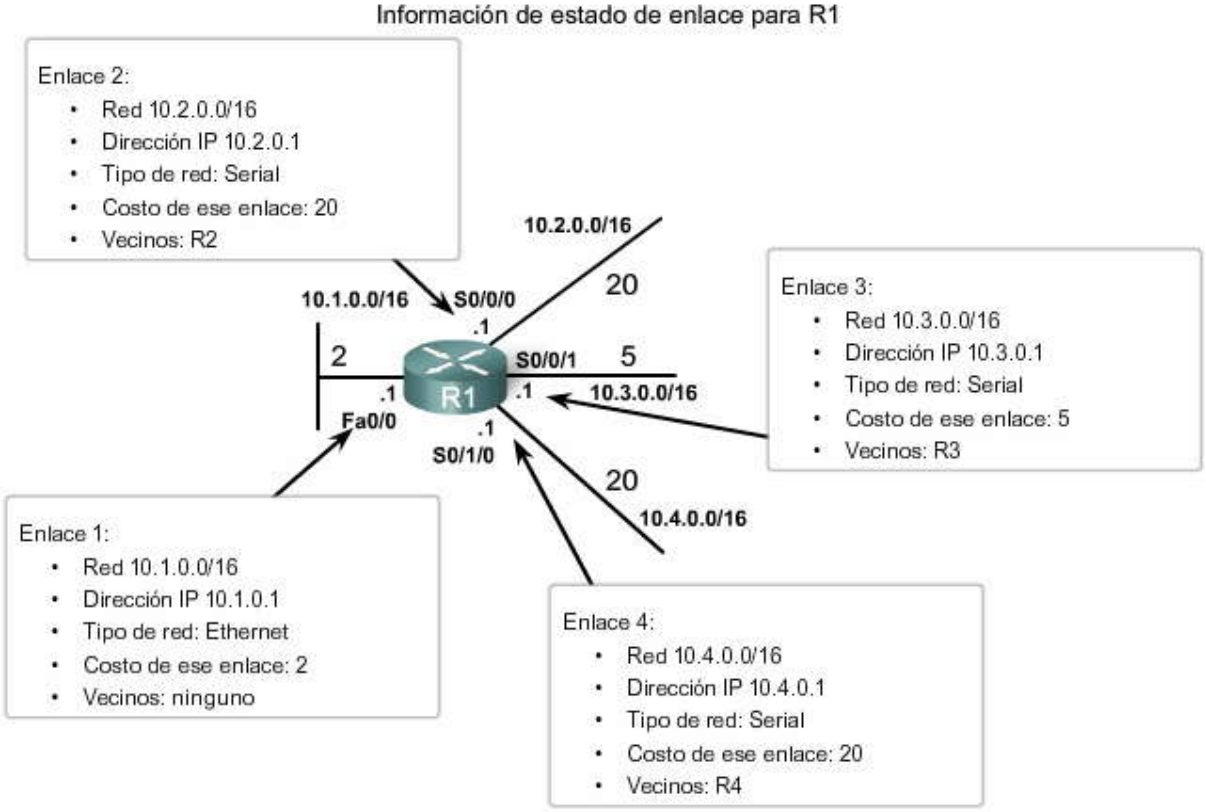
- La interfaz FastEthernet 0/0 se encuentra en la red 10.1.0.0/16
- La red Serial 0/0/0 se encuentra en la red 10.2.0.0/16
- La red Serial 0/0/1 se encuentra en la red 10.3.0.0/16
- La red Serial 0/0/2 se encuentra en la red 10.4.0.0/16

**Estado de enlace**

La información sobre el estado de aquellos enlaces se conoce como estados de enlace. Como podrá ver en la figura, esta información incluye:

- La dirección IP de la interfaz y la máscara de subred.
- El tipo de red, como Ethernet (broadcast) o enlace serial punto a punto.
- El costo de dicho enlace.
- Cualquier router vecino en dicho enlace.

**Nota:** Veremos que la implementación de OSPF realizada por Cisco especifica el costo del enlace, la métrica de enrutamiento de OSPF, como el ancho de banda de la interfaz saliente. Sin embargo, a los fines del presente capítulo, utilizamos valores de costo arbitrarios para simplificar nuestra demostración.

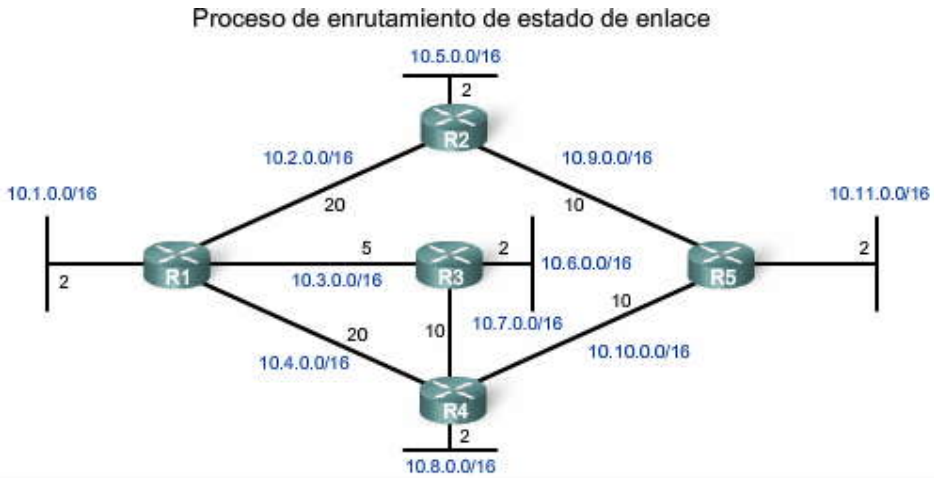


### 10.1.5 ENVIO DE PAQUETES DE SALUDO A LOS VECINOS.-

El segundo paso en el proceso de enrutamiento de estado de enlace consiste en lo siguiente:

Cada router es responsable de reunirse con sus vecinos en redes conectadas directamente.

Los routers con protocolos de enrutamiento de estado de enlace utilizan un protocolo de saludo para descubrir cualquier vecino en sus enlaces. Un vecino es cualquier otro router habilitado con el mismo protoc olo de enrutamiento de estado de enlace.



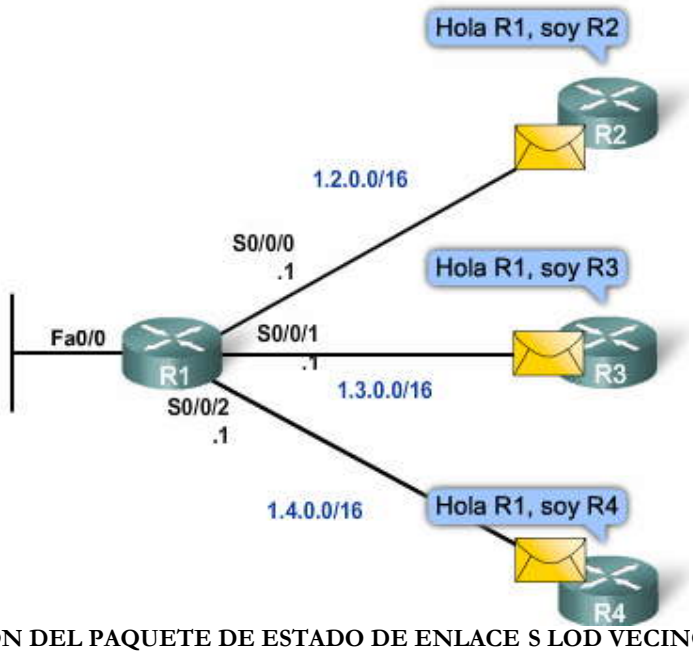

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. *Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.*
3. Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.
4. Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.
5. Cada router utiliza la base de datos para construir un mapa topológico completo y calcula la mejor ruta para cada red de destino.

**Haga clic en Reproducir para ver la animación.**

R1 envía paquetes de saludo a sus enlaces (interfaces) para detectar la presencia de vecinos. R2, R3 y R4 responden al paquete de saludo con sus propios paquetes de saludo debido a que dichos routers están configurados con el mismo protocolo de enrutamiento de estado de enlace. No hay vecinos fuera de la interfaz FastEthernet 0/0. Debido a que R1 no recibe un Saludo en esta interfaz, no continuará con los pasos del proceso de enrutamiento de estado de enlace para el enlace FastEthernet 0/0.

En forma similar a los paquetes de saludo de EIGRP, cuando dos routers de estado de enlace notan que son vecinos, forman una adyacencia. Dichos paquetes de saludo pequeños contin úan intercambiándose entre dos vecinos adyacentes que cumplen la función de "mensaje de actividad" para supervisar el estado del vecino. Si un router deja de recibir paquetes de saludo por parte de un vecino, dicho vecino se considera inalcanzable y se rom pe la adyacencia. En la figura, R1 forma una adyacencia con los tres routers.

Detección de vecinos—Paquetes de saludo




**10.1.6 CONSTRUCCION DEL PAQUETE DE ESTADO DE ENLACE S LOD VECINOS.-**
**Haga clic en Proceso del enrutamiento de estado de enlace en la figura.**

Nos encontramos ahora en el tercer paso del proceso del enrutamiento de estado de enlace:

**Cada router crea un paquete de estado de enlace (LSP) que incluye el estado de cada enlace conectado directamente.**

**Haga clic en R1 en la figura.**

Una vez que un router establece sus adyacencias, puede crear sus propios paquetes de estado de enlace (LSP), los cuales incluyen la información de estado de enlace de sus enlaces. Una versión simplificada de los LSP de R1 es:

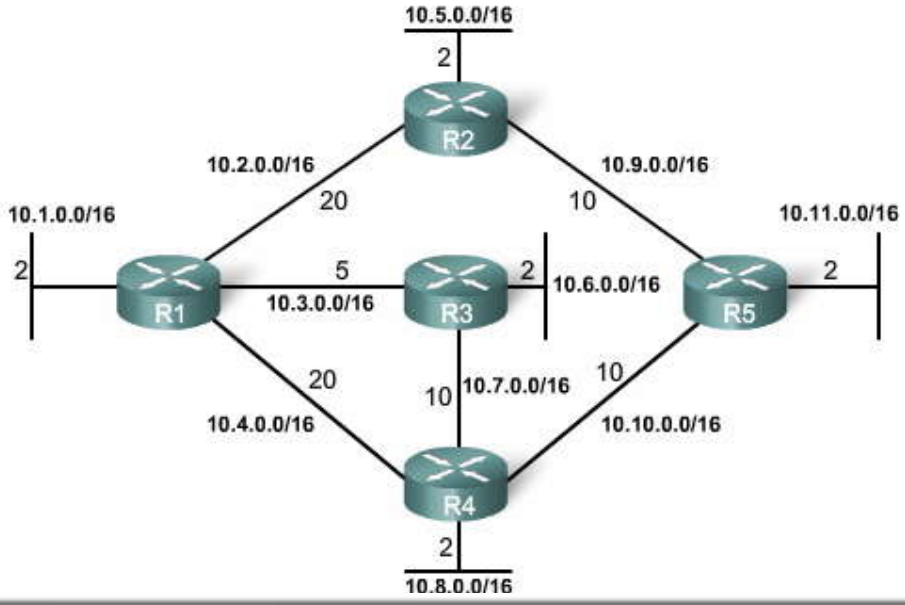
1. R1; Ethernet network 10.1.0.0/16; Cost 2

2. R1 -> R2; Serial point-to-point network; 10.2.0.0/16; Cost 20

3. R1 -> R3; Serial point-to-point network; 10.3.0.0/16; Cost 5

4. R1 -> R4; Serial point-to-point network; 10.4.0.0/16; Cost 20

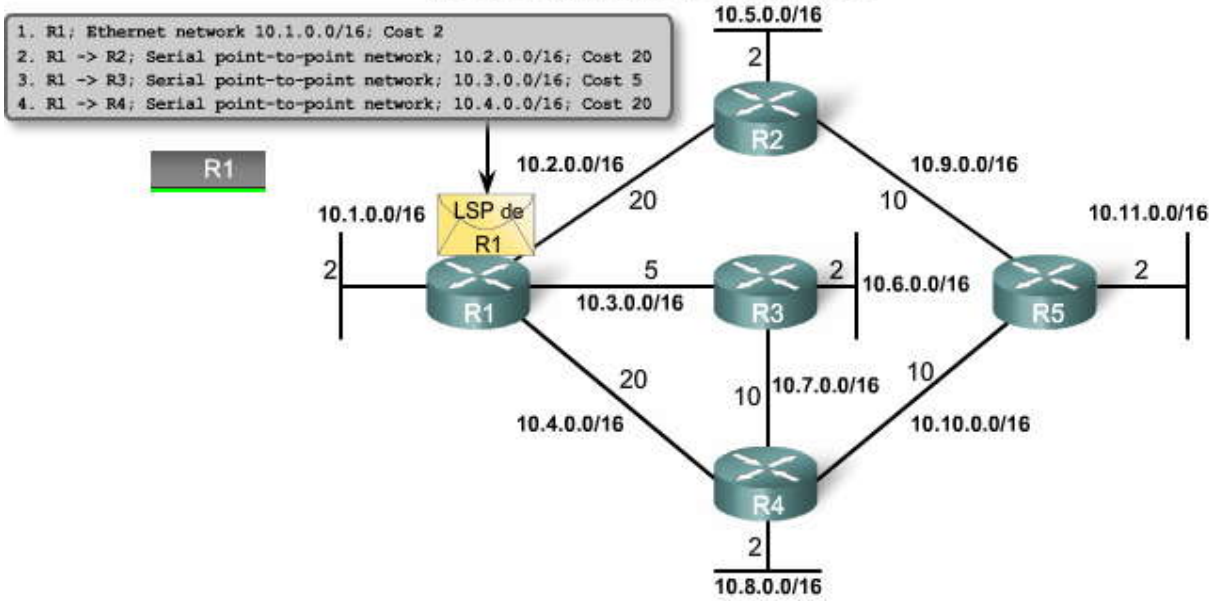
Proceso de enrutamiento de estado de enlace




## Proceso de enrutamiento de estado de enlace

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
3. *Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.*
4. Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.
5. Cada router utiliza la base de datos para construir un mapa topológico completo y computa la mejor ruta para cada red de destino.

Proceso de enrutamiento de estado de enlace

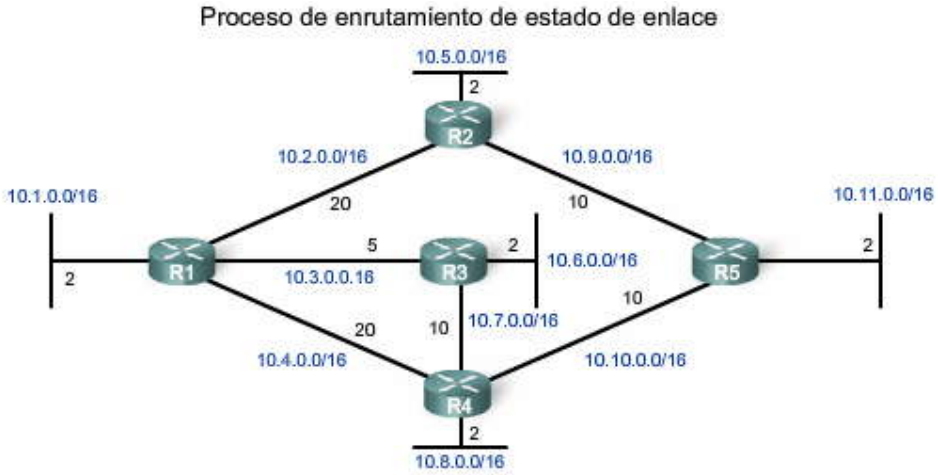


### 10.1.7 SATURACION DE PAQUETES DE ESTADO DE ENLACE A LOS VECINOS.-

Como se muestra en la figura, el cuarto paso en el proceso de enrutamiento de estado de enlace consiste en lo siguiente:

Cada router inunda el LSP a todos los vecinos, que luego almacenan todos los LSP recibidos en una base de datos.

Cada router inunda con su información de estado de enlace a todos los demás routers de estado de enlace en el área de enrutamiento. Siempre que un router recibe un LSP de un router vecino, envía de inmediato dicho LSP a todas las demás interfaces, excepto la interfaz que recibió el LSP. Este proceso crea un efecto de saturación de los LSP desde todos los routers a través del área de enrutamiento.




**Proceso de enrutamiento de estado de enlace**

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
3. Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.
4. *Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.*
5. Cada router utiliza la base de datos para construir un mapa topológico completo y calcula la mejor ruta para cada red de destino.

**Haga clic en Reproducir para ver la animación.**

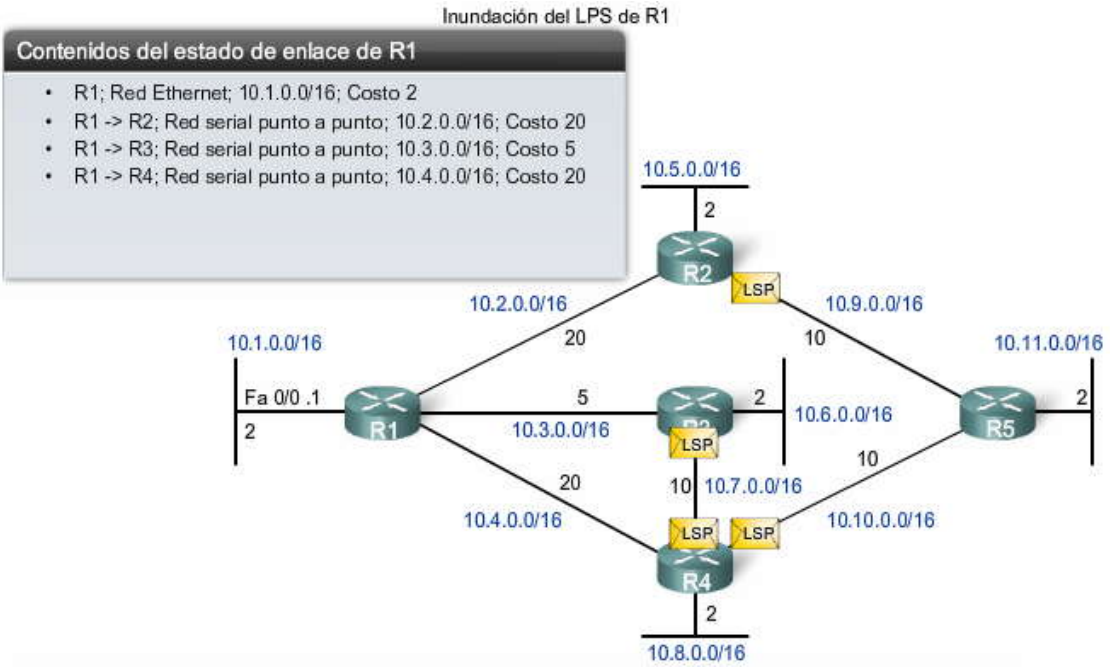
Como podrá ver en la animación, la inundación de los LSP se produce prácticamente de inmediato una vez recibidos, sin ningún cálculo intermedio. A diferencia de los protocolos de enrutamiento por vector de distancia que primero deben ejecutar el algoritmo Bellman-Ford para procesar las actualizaciones de enrutamiento antes de enviarlas a los demás routers, los protocolos de enrutamiento de estado de enlace calculan el algoritmo SPF después de completar la saturación. Como consecuencia, los protocolos de enrutamiento de estado de enlace alcanzan la convergencia mucho más rápido que los protocolos de enrutamiento por vector de distancia.

Recuerde que los LSP no necesitan enviarse periódicamente. Un LSP sólo necesita enviarse:

- durante la puesta en marcha inicial del router o del proceso del protocolo de enrutamiento en dicho router
- cuando hay un cambio en la topología, incluido un enlace que se desactiva o activa, o una adyacencia de vecinos que se establece o se rompe

Además de la información de estado de enlace, se incluye información adicional en el LSP, como los números de secuencia y la información de antigüedad, para ayudar a administrar el proceso de saturación. Cada router utiliza esta información para determinar si ya recibió el LSP de otro router o si el LSP tiene información más nueva que la contenida en la base de datos de estado de enlace. Este proceso permite que un router conserve sólo la información más actual en su base de datos de estado de enlace.

**Nota:** La forma en que se utilizan los números de secuencia y la información de antigüedad se encuentra más allá del alcance de este plan de estudios. Podrá encontrar información adicional en Routing TCP/IP por Jeff Doyle.

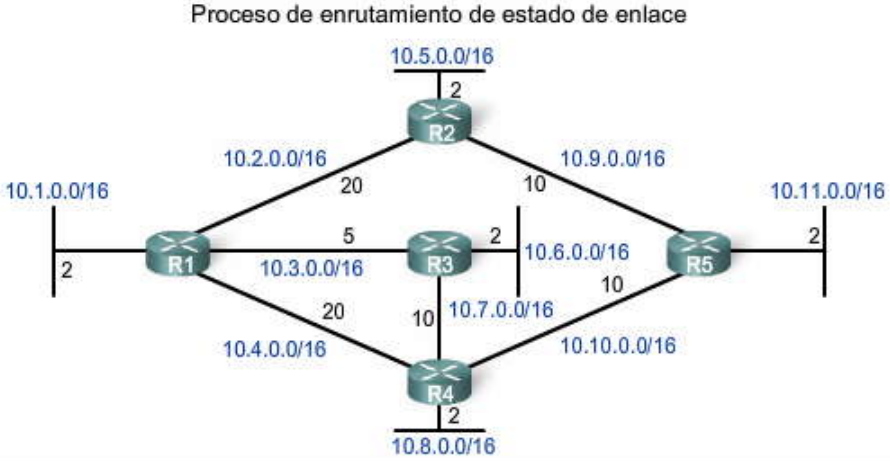



### 10.1.8 CONSTRUCCION DE UN A BASE DE DATOS DE ESTADO DE ENLACE.-

El paso final en el proceso de enrutamiento de estado de enlace consiste en lo siguiente:

Cada router utiliza la base de datos para construir una mapa completo de la topología y calcule el mejor camino para cada red de destino.

Después de que cada router haya propagado sus propios LSP con el proceso de saturación de estado de enlace, cada router tendrá luego un LSP proveniente de cada router de estado de enlace en el área de enrutamiento. Dichos LSP se almacenan en la base de datos de estado de enlace. Cada router en el área de enrutamiento puede ahora usar el algoritmo SPF para construir los árboles SPF que vio anteriormente.




**Proceso de enrutamiento de estado de enlace**

1. Cada router aprende de cada una de sus propias redes conectadas directamente.
2. Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
3. Cada router crea un Paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.
4. Cada router inunda el LSP hacia todos sus vecinos, quienes luego almacenan en una base de datos todos los LSP recibidos.
5. *Cada router utiliza la base de datos para construir un mapa topológico completo y calcula la mejor ruta para cada red de destino.*

Observemos la base de datos de estado de enlace para R1, así como el árbol SPF que se obtiene del cálculo del algoritmo SPF.

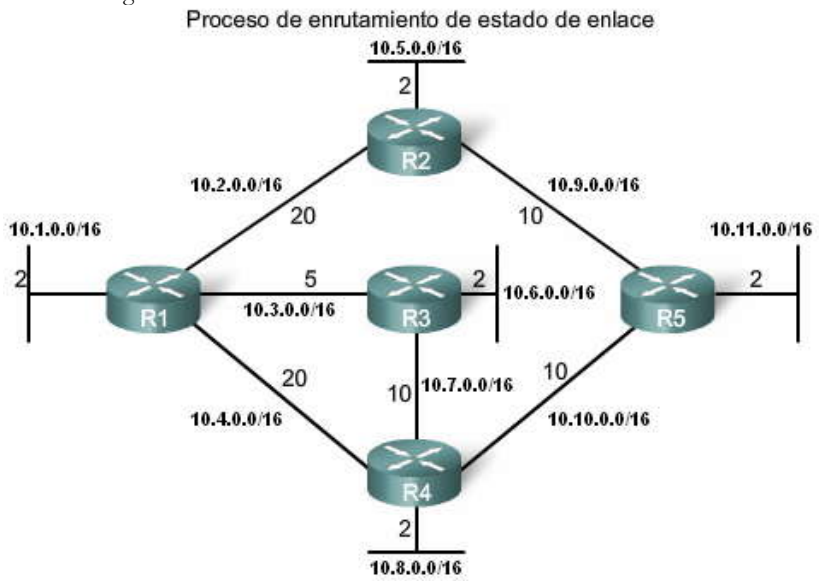
**Haga clic en Base de datos de estado de enlace de R1 en la figura.**

Como resultado del proceso de saturación, el router R1 aprendió la información de estado de enlace para cada router de esta área de enrutamiento. La figura muestra la información de estado de enlace que R1 recibió y almacenó en su base de datos de estado de enlace. Observe que R1 también incluye su propia información de e stado de enlace en la base de datos de estado de enlace.

**Haga clic en Árbol SPF de R1 en la figura.**

Con una base de datos de estado de enlace completa, R1 ahora puede utilizar la base de datos y el algoritmo shortest path first (SPF) para calcular la ruta preferida o la ruta más corta para cada red. En la figura, observe que R1 no utiliza la ruta entre sí mismo y R4 para alcanzar cualquier LAN en la topología, incluida la LAN conectada a R4. La ruta a través de R3 tiene un costo inferior. Asimismo, R1 no utiliza la ruta entre R2 y R5 para llegar a R5. La ruta a través de R3 tiene un costo inferior. Cada router en la topología determina la ruta más corta desde su propia perspectiva.

**Nota**: La base de datos de estado de enlace y el árbol SPF aún incluirán las redes conectadas directamente, los enlaces que se encuentran sombreados en el gráfico.




Proceso de enrutamiento de estado de enlace

**Base de datos de estado de enlace de R1**

LSP de R2:
- Conectado al vecino R1 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R5 en la red 10.9.0.0/16, costo de 10
- Posee una red 10.5.0.0/16, costo de 2

Base de datos de estado de enlace R1

LSP de R3:
- Conectado al vecino R1 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.7.0.0/16, costo de 10
- Posee una red 10.6.0.0/16, costo de 2

LSP de R4:
- Conectado al vecino R1 en la red 10.4.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.7.0.0/16, costo de 10
- Conectado al vecino R5 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.8.0.0/16, costo de 2

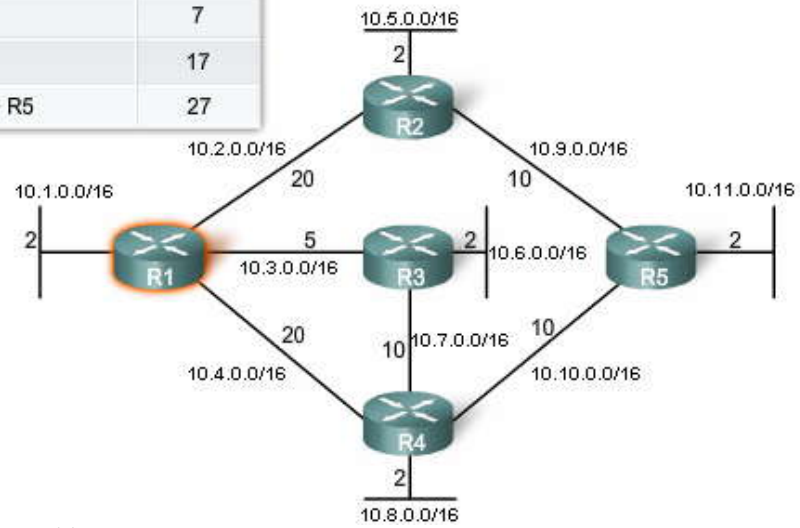
LSP de R5:
- Conectado al vecino R2 en la red 10.9.0.0/16, costo de 10
- Conectado al vecino R4 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.11.0.0/16, costo de 2

Estados de enlace del R1:
- Conectado al vecino R2 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.4.0.0/16, costo de 20
- Posee una red 10.1.0.0/16, costo de 2

Proceso de enrutamiento de estado de enlace

| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R2 | R1 -> R2 | 22 |
| LAN de R3 | R1 -> R3 | 7 |
| LAN de R4 | R1 -> R3 -> R4 | 17 |
| LAN de R5 | R1 -> R3 -> R4 -> R5 | 27 |

Árbol SPF de R1




### 10.1.9 ARBOL SHORTEST PATH FIRST(SPF).-

**Construcción del árbol SPF**

Examinemos con mayor detalle la manera en que R1 construye su árbol SPF. La topología actual de R1 sólo incluye a sus vecinos. Sin embargo, al utilizar la información de estado de enlace proveniente de todos los demás routers, R1 puede ahora comenzar a construir un árbol SPF ubicándose en la raíz de éste.

Nota: El proceso que se describe en esta sección es sólo una forma conceptual del algoritmo SPF y del árbol SPF como una ayuda para volverlo más comprensible.

**Haga clic en LSP de R2 en la figura.**

El algoritmo SPF comienza con el procesamiento de la siguiente información de LSP proveniente de R2:

1. Conectado al R1 vecino en la red 10.2.0.0/16, costo de 20

2. Conectado al R5 vecino en la red 10.9.0.0/16, costo de 10

3. Tiene una red 10.5.0.0/16, costo de 2

R1 puede ignorar el primer LSP debido a que R1 ya sabe que está conectado a R2 en la red 10.2.0.0/16 con un costo de 20. R1 puede utilizar el segundo LSP y crear un enlace desde R2 hasta otro router, R5, con la red 10.9.0.0/16 y un costo de 10. Esta información se agrega al árbol SPF. Al utilizar el tercer LSP, R1 detectó que R2 tiene una red 10.5.0.0/16 con un costo de 2 y sin vecinos. Este enlace se agrega al árbol SPF de R1.

**Haga clic en LSP de R3 en la figura.**

El algoritmo SPF ahora procesa los LSP de R3:

1. Conectado al R1 vecino en la red 10.3.0.0/16, costo de 5

2. Conectado al R4 vecino en la red 10.7.0.0/16, costo de 10

3. Tiene una red 10.6.0.0/16, costo de 2

R1 puede ignorar el primer LSP debido a que R1 ya sabe que está conectado a R3 en la red 10.3.0.0/16 con un costo de 5. R1 puede utilizar el segundo LSP y crear un enlace desde R3 hasta el router R4, con la red 10.7.0.0/16 y un costo de 10. Esta información se agrega al árbol SPF. Al utilizar el tercer LSP, R1 detectó que R3 tiene una red 10.6.0.0/16 con un costo de 2 y sin vecinos. Este enlace se agrega al árbol SPF de R1.

**Haga clic en LSP de R4 en la figura.**

El algoritmo SPF procesa ahora los LSP de R4:

1. Conectado al R1 vecino en la red 10.4.0.0/16, costo de 20

2. Conectado al R3 vecino en la red 10.7.0.0/16, costo de 10

3. Conectado al R5 vecino en la red 10.10.0.0/16, costo de 10

4. Tiene una red 10.8.0.0/16, costo de 2

R1 puede ignorar el primer LSP debido a que R1 ya sabe que está conectado al R4 en la red 10.4.0.0/16 con un costo de 20. R1 también puede ignorar el segundo LSP debido a que SPF ya detectó la red 10.6.0.0/16 con un costo de 10 de R3.

Sin embargo, R1 puede utilizar el tercer LSP para crear un enlace desde R4 hasta el router R5, con la red 10.10.0.0/16 y un costo de 10. Esta información se agrega al árbol SPF. Al utilizar el cuarto LSP, R1 detectó que R4 tiene una red 10.8.0.0/16 con un costo de 2 y sin vecinos. Este enlace se agrega al árbol SPF de R1.

**Haga clic en LSP de R5 en la figura.**

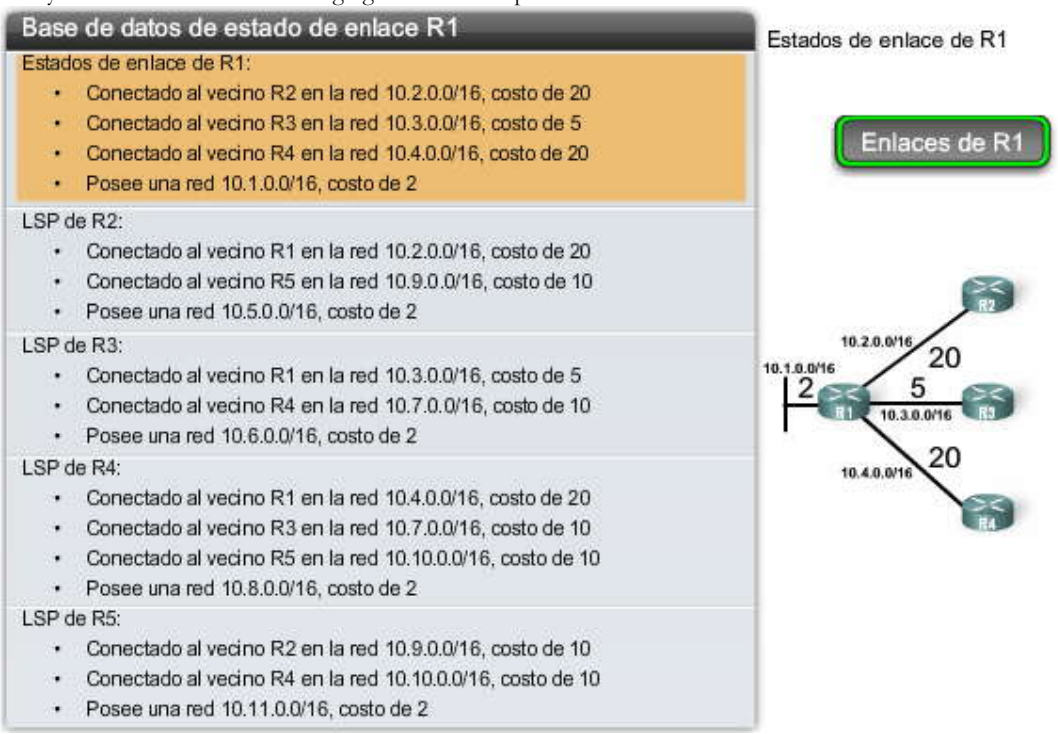
El algoritmo SPF procesa ahora los LSP de R5:

1. Conectado al R2 vecino en la red 10.9.0.0/16, costo de 10

2. Conectado al R4 vecino en la red 10.10.0.0/16, costo de 10

3. Tiene una red 10.11.0.0/16, costo de 2

R1 puede ignorar los primeros dos LSP (para las redes 10.9.0.0/16 y 10.10.0.0/16), debido a que SPF ya detectó estos enlaces y los agregó al árbol SPF. R1 puede procesar el tercer LSP y detectar que R5 tiene una red 10.11.0.0/16 con un costo de 2 y sin vecinos. Este enlace se agrega al árbol SPF para R1.



## Base de datos de estado de enlace R1

Estados de enlace de R1:

- Conectado al vecino R2 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.4.0.0/16, costo de 20
- Posee una red 10.1.0.0/16, costo de 2

LSP de R2:

- Conectado al vecino R1 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R5 en la red 10.9.0.0/16, costo de 10
- Posee una red 10.5.0.0/16, costo de 2

LSP de R3:

- Conectado al vecino R1 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.7.0.0/16, costo de 10
- Posee una red 10.6.0.0/16, costo de 2

LSP de R4:

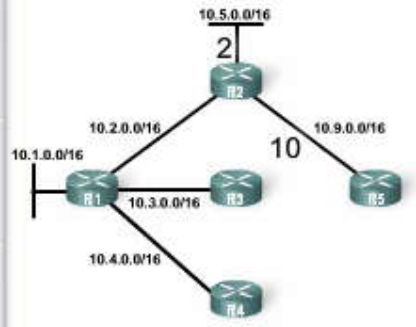
- Conectado al vecino R1 en la red 10.4.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.7.0.0/16, costo de 10
- Conectado al vecino R5 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.8.0.0/16, costo de 2

LSP de R5:

- Conectado al vecino R2 en la red 10.9.0.0/16, costo de 10
- Conectado al vecino R4 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.11.0.0/16, costo de 2

Procesamiento de los LPS de R2

LSP de R2




## Base de datos de estado de enlace R1

Estados de enlace de R1:

- Conectado al vecino R2 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.4.0.0/16, costo de 20
- Posee una red 10.1.0.0/16, costo de 2

LSP de R2:

- Conectado al vecino R1 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R5 en la red 10.9.0.0/16, costo de 10
- Posee una red 10.5.0.0/16, costo de 2

LSP de R3:

- Conectado al vecino R1 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.7.0.0/16, costo de 10
- Posee una red 10.6.0.0/16, costo de 2

LSP de R4:

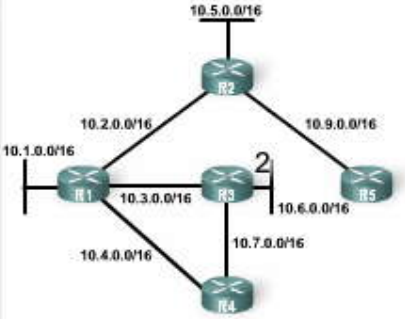
- Conectado al vecino R1 en la red 10.4.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.7.0.0/16, costo de 10
- Conectado al vecino R5 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.8.0.0/16, costo de 2

LSP de R5:

- Conectado al vecino R2 en la red 10.9.0.0/16, costo de 10
- Conectado al vecino R4 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.11.0.0/16, costo de 2

Procesamiento de los LPS de R3

LSP de R3



**Base de datos de estado de enlace R1**

Estados de enlace de R1:
- Conectado al vecino R2 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.4.0.0/16, costo de 20
- Posee una red 10.1.0.0/16, costo de 2

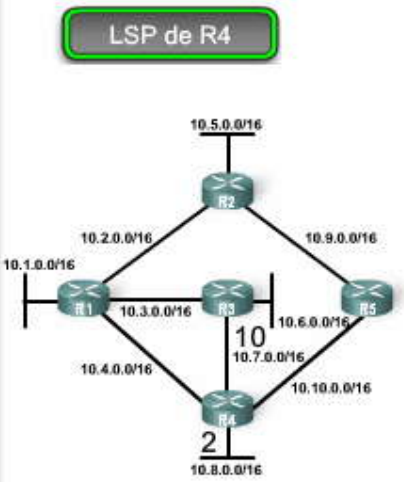
LSP de R2:
- Conectado al vecino R1 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R5 en la red 10.9.0.0/16, costo de 10
- Posee una red 10.5.0.0/16, costo de 2

LSP de R3:
- Conectado al vecino R1 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.7.0.0/16, costo de 10
- Posee una red 10.6.0.0/16, costo de 2

LSP de R4:
- Conectado al vecino R1 en la red 10.4.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.7.0.0/16, costo de 10
- Conectado al vecino R5 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.8.0.0/16, costo de 2

LSP de R5:
- Conectado al vecino R2 en la red 10.9.0.0/16, costo de 10
- Conectado al vecino R4 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.11.0.0/16, costo de 2

Procesamiento de los LPS de R4




**Base de datos de estado de enlace R1**

Estados de enlace de R1:
- Conectado al vecino R2 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.4.0.0/16, costo de 20
- Posee una red 10.1.0.0/16, costo de 2

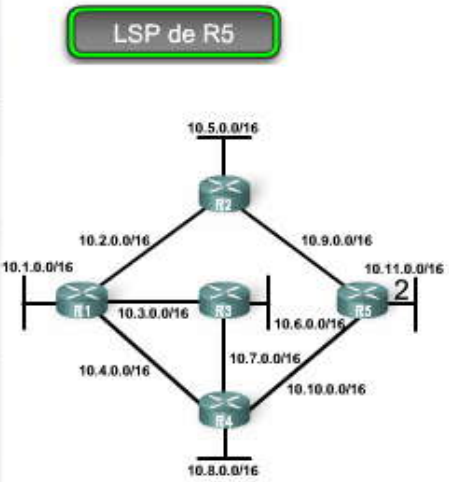
LSP de R2:
- Conectado al vecino R1 en la red 10.2.0.0/16, costo de 20
- Conectado al vecino R5 en la red 10.9.0.0/16, costo de 10
- Posee una red 10.5.0.0/16, costo de 2

LSP de R3:
- Conectado al vecino R1 en la red 10.3.0.0/16, costo de 5
- Conectado al vecino R4 en la red 10.7.0.0/16, costo de 10
- Posee una red 10.6.0.0/16, costo de 2

LSP de R4:
- Conectado al vecino R1 en la red 10.4.0.0/16, costo de 20
- Conectado al vecino R3 en la red 10.7.0.0/16, costo de 10
- Conectado al vecino R5 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.8.0.0/16, costo de 2

LSP de R5:
- Conectado al vecino R2 en la red 10.9.0.0/16, costo de 10
- Conectado al vecino R4 en la red 10.10.0.0/16, costo de 10
- Posee una red 10.11.0.0/16, costo de 2

Procesamiento de los LPS de R5



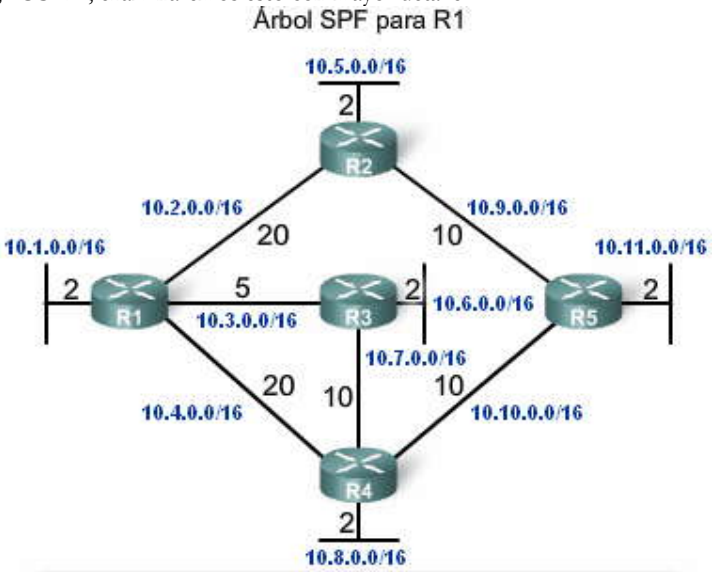

**Determinación de la ruta más corta**

Debido a que todos los LSP se procesaron con el algoritmo SPF, R1 construyó ahora el árbol SPF completo. Los enlaces 10.4.0.0/16 y 10.9.0.0/16 no se utilizan para alcanzar otras redes debido a que existen rutas más cortas o de menor costo. Sin embargo, dichas redes aún forman parte del árbol SPF y se utilizan para alcanzar dispositivos en dichas redes.

Nota: El algoritmo SPF real determina la ruta más corta al construir el árbol SPF. Hemos hecho esto en dos pasos para simplificar la comprensión del algoritmo.

La figura muestra el árbol SPF para R1. Al utilizar este árbol, los resultados del algoritmo SPF indican la ruta más corta hacia cada red. Si bien en la tabla se muestran únicamente las LAN, SPF también puede utilizarse para determinar la ruta más corta hacia cada red de enlace WAN. En este caso, R1 determina que la ruta más corta para cada red es:

Red 10.5.0.0/16 via serial 0/0/0 de R2 al costo de 22
Red 10.6.0.0/16 via serial 0/0/1 de R3 al costo de 7
Red 10.7.0.0/16 via serial 0/0/1 de R3 al costo de 15
Red 10.8.0.0/16 via serial 0/0/1 de R3 al costo de 17
Red 10.9.0.0/16 via serial 0/0/0 de R2 al costo de 30
Red 10.10.0.0/16 via serial 0/0/1 de R3 al costo de 25
Red 10.11.0.0/16 via serial 0/0/1 de R3 al costo de 27
Cada router construye su propio árbol SPF independientemente de todos los demás routers. Pa ra garantizar el enrutamiento adecuado, las bases de datos de estado de enlace utilizadas para construir dichos árboles deben ser idénticas en todos los routers. En el Capítulo 11, "OSFP", examinaremos esto con mayor detalle.

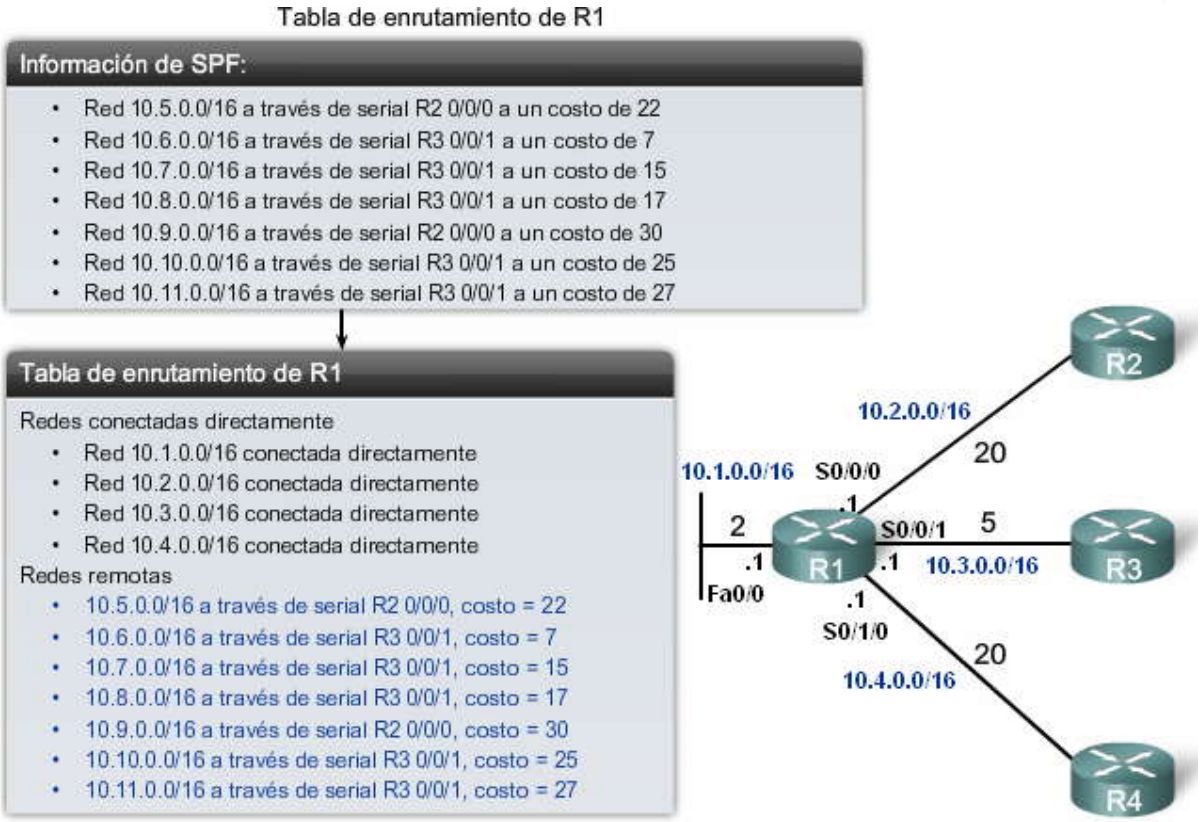



| Destino | Ruta más corta | Costo |
|---|---|---|
| LAN de R2 | R1 a R2 | 22 |
| LAN de R3 | R1 a R3 | 7 |
| LAN de R4 | R1 a R3 a R4 | 17 |
| LAN de R5 | R1 a R3 a R4 a R5 | 27 |

**Generación de una tabla de enrutamiento desde el árbol SPF**

Al utilizar la información de la ruta más corta determinada por el algoritmo SPF, dichas rutas ahora pueden agregarse a la tabla de enrutamiento. Puede ver en la figura la forma en que se agregaron ahora las siguientes rutas a la tabla de enrutamiento de R1:
10.5.0.0/16 via Serial 0/0/0 de R2, costo = 22
10.6.0.0/16 via Serial 0/0/1 de R3, costo = 7
10.7.0.0/16 via Serial 0/0/1 de R3, costo = 15
10.8.0.0/16 via Serial 0/0/1 de R3, costo = 17
10.9.0.0/16 via Serial 0/0/0 de R2, costo = 30
10.10.0.0/16 via Serial 0/0/1 de R3, costo = 25
10.11.0.0/16 via Serial 0/0/1 de R3, costo = 27

La tabla de enrutamiento también incluirá todas las redes conectadas directamente y las rutas provenientes de cualquier otro origen, tales como las rutas estáticas. Los paquetes se reenviarán ahora según dichas entradas en la tabla de enrutamiento.




## 10.2 IMPLEMENTACION DE PROTOCOLOS DE ENRUAMIENTO DE ESTADO DE ENLACE.-

### 10.2.1 VENTAJAS DE UN PRODUCTO DE ENRUTAMIENTO DE ESTADO DE ENLACE.-

Las siguientes son algunas ventajas de los protocolos de enrutamiento de estado de enlace comparados con los protocolos de enrutamiento por vector de distancia.

**Crean un mapa topológico**

Los protocolos de enrutamiento de estado de enlace crean un mapa topológico o árbol SPF de la topología de red. Los protocolos de enrutamiento por vector de distancia no tienen un mapa topológico de la red. Los routers que implementan un protocolo de enrutamiento por vector de distancia sólo tienen una lista de redes, que incluye el costo (distancia) y routers del siguiente salto (dirección) a dichas redes. Debido a que los protocolos de enrutamiento de estado de enlace intercambian estados de enlace, el algoritmo SPF puede crear un árbol SPF de la red. Al utilizar el árbol SPF, cada router puede determinar en forma independiente la ruta más corta a cada red.

**Convergencia rápida**

Al recibir un Paquete de estado de enlace (LSP), los protocolos de enrutamiento de estado de enlace saturan de inmediato con el LSP todas las interfaces excepto la interfaz desde la que se recibió el LSP. Un router que utiliza un protocolo de enrutamiento por vector de distancia necesita procesar cada actualización de enrutamiento y actualizar su tabla de enrutamiento antes de saturarlas a otras interfaces, incluso con updates disparados. Se obtiene una convergencia más rápida para los protocolos de enrutamiento de estado de enlace. EIGRP es una excepción notable.

**Actualizaciones desencadenadas por eventos**

Después de la saturación inicial de los LSP, los protocolos de enrutamiento de estado de enlace sólo envían un LSP cuando hay un cambio en la topología. El LSP sólo incluye la información relacionada con el enlace afectado. A diferencia de algunos protocolos de enrutamiento por vector de distancia, los protocolos de enrutamiento de estado de enlace no envían actualizaciones periódicas.

Nota: Los routers OSPF realizan la saturación de sus propios estados de enlace cada 30 minutos. Esto se conoce como actualización reiterada y se analiza en el capítulo siguiente. Asimismo, no todos los protocolos de enrutamiento por vector de distancia envían actualizaciones periódicas. RIP e IGRP envían actualizaciones periódicas; sin embargo, EIGRP no lo hace.

**Diseño jerárquico**

Los protocolos de enrutamiento de estado de enlace, como OSPF e IS-IS utilizan el concepto de áreas. Las áreas múltiples crean un diseño jerárquico para redes y permiten una mejor agregación de ruta (resumen) y el aislamiento de los problemas de enrutamiento dentro del área. Los OSPF de áreas múltiples e IS-IS se analizan más adelante en CCNP.

Ventajas de los protocolos de enrutamiento de estado de enlace

**Ventajas de los protocolos de enrutamiento de estado de enlace**

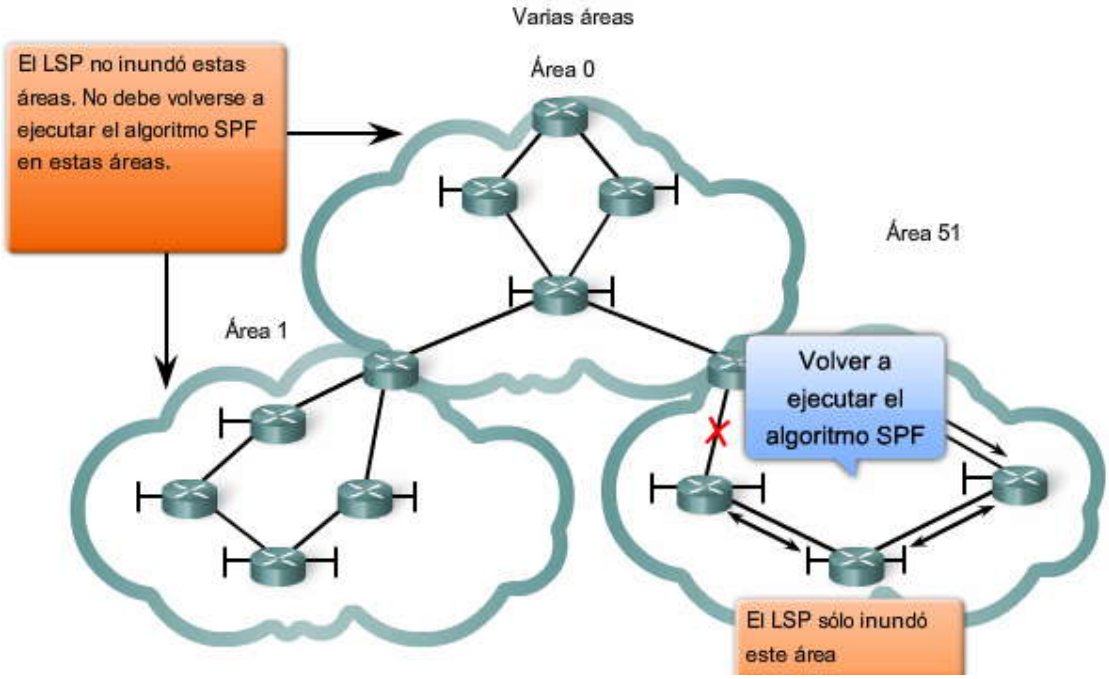
- Cada router crea su propio mapa topológico de la red para determinar la ruta más corta.
- La saturación inmediata de los LSP logra una convergencia más rápida.
- Sólo se envían LSP cuando se produce un cambio en la topología y éstos únicamente contienen la información relacionada con tal cambio.
- Diseño jerárquico utilizado cuando se implementan varias áreas.

### 10.2.2 REQUERIMIENTOS DE UN PRODUCTOS DESTADO DE ENLACE.-

Los protocolos de enrutamiento de estado de enlace modernos están diseñados para minimizar los efectos en la memoria, el CPU y el ancho de banda. La utilización y configuración de áreas múltiples puede reducir el tamaño de las bases de datos de estado de enlace. Las áreas múltiples también pueden limitar el grado de saturación de información de estado de enlace en un dominio de enrutamiento y enviar los LSP sólo a aquellos routers que los necesitan.

Por ejemplo, cuando hay un cambio en la topología, sólo aquellos routers del área afectada reciben el LSP y ejecutan el algoritmo SPF. Esto puede ayudar a aislar un enlace inestable en un área específica en el dominio de enru tamiento. En la figura, hay tres dominios de enrutamiento independientes: Área 1, Área 0 y Área 51. Si una red en el Área 51 se desactiva, el LSP con la información sobre este enlace desactivado se satura sólo a otros routers en tal área. Únicamente los ro uters del Área 51 necesitan actualizar sus bases de datos de estado de enlace, volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar sus tablas de enrutamiento. Los routers de otras áreas notarán que esta ruta está desactivada pero esto se realizará con un tipo de paquete de estado de enlace que no los obliga a volver a ejecutar sus algoritmos SPF. Los routers de otras áreas pueden actualizar sus tablas de enrutamiento directamente.

Nota: Las áreas múltiples con OSPF e IS-IS se analizan más adelante en CCNP.




**Requerimientos de memoria**

Los protocolos de enrutamiento de estado de enlace normalmente requieren más memoria, más procesamiento de CPU y, en ocasiones, un mayor ancho de banda que los protocolos de enrutamiento por vector de di stancia. Los requerimientos de memoria responden a la utilización de bases de datos de estado de enlace y la creación del árbol SPF.

**Requerimientos de procesamiento**

Los protocolos de estado de enlace también pueden requerir un mayor procesamiento de CPU que los protocolos de enrutamiento por vector de distancia. El algoritmo SPF requiere un mayor tiempo de CPU que los algoritmos de vector de distancia, como Bellman-Ford, ya que los protocolos de estado de enlace crean un mapa completo de la topología.

**Requerimientos de ancho de banda**

La saturación de paquetes de estado de enlace puede ejercer un impacto negativo en el ancho de banda disponible en una red. Si bien esto sólo debería ocurrir durante la puesta en marcha inicial de los routers, también podría ser un problema en redes inestables.

Requerimientos de los protocolos de enrutamiento de estado de enlace


### 10.2.3 COMPARACION DE PROTOCOLOS DE ENRUTAMIENTO DE ESTADO DE ENLACE.-

En la actualidad, se utilizan dos protocolos de enrutamiento de estado de enlace para realizar el enrutamiento de IP:
Open Shortest Path First (OSPF)
Intermediate System-to-Intermediate System (IS-IS)

**OSPF**

OSPF fue diseñado por el grupo de trabajo de OSPF: IETF (Grupo de trabajo de ingeniería de Internet), que aún hoy existe. El desarrollo de OSPF comenzó en 1987 y actualmente hay dos versiones en uso:
OSPFv2: OSPF para redes IPv4 (RFC 1247 y RFC 2328)
OSPFv3: OSPF para redes IPv6 (RFC 2740)

La mayor parte del trabajo en OSPF lo realizó John Moy, autor de la mayoría de los RFC sobre OSPF. Su libro, OSPF, Anatomy of an Internet Routing Protocol ofrece una interesante perspectiva sobre el desarrollo de OSPF.

Nota: OSPF se analiza en el siguiente capítulo. OSPF de áreas múltiples y OSPFv3 se analizan en CCNP.

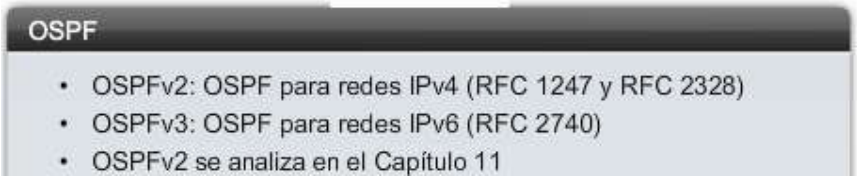
**IS-IS**

IS-IS fue diseñado por ISO (Organización Internacional para la Estandarización) y se describe en ISO 10589. DEC (Digital Equipment Corporation) desarrolló la primera representación de este protocolo de enrutamiento que se conoce como DECnet de fase V. Radia Perlman fue la principal diseñadora del protocolo de enrutamiento IS-IS.

IS-IS se diseñó originalmente para el suite de protocolo de OSI y no para el suite de protocolo de TCP/IP. Más adelante, IS-IS integrado, o IS-IS doble, incluyó la compatibilidad con redes IP. Si bien se conoció a IS-IS como el protocolo de enrutamiento más utilizado por proveedores e ISP, se están comenzando a utilizar más redes IS-IS corporativas.

OSPF e IS-IS presentan varias similitudes y diferencias. Existen diversas posturas a favor de OSPF y a favor de IS-IS que analizan y debaten las ventajas de un protocolo de enrutamiento frente al otro. Ambos protocolos de enrutamiento brindan la funcionalidad de enrutamiento necesaria. Podrá aprender más acerca de IS-IS y OSPF en CCNP y comenzar a realizar su propia determinación sobre si un protocolo es más provechoso que el otro.

OSPF e IS-IS




**Resumen**

A los protocolos de enrutamiento de estado de enlace también se los conoce como protocolos shortest path first y se desarrollan en torno al algoritmo shortest path first (SPF) de Edsger Dijkstra. Hay dos protocolos de enrutamiento de estado de enlace para IP: OSPF (Open Shortest Path First) e IS-IS (Intermediate-System-to-Intermediate-System).

El proceso de estado de enlace puede resumirse de la siguiente manera:

1. Cada router detecta sus propias redes conectadas directamente.

2. Cada router es responsable de "saludar" a sus vecinos en las redes conectadas directamente.

3. Cada router crea un Paquete de estado de enlace (LSP) que incluye el estado de cada enlace directamente conectado.

4. Cada router satura con el LSP a todos los vecinos, que luego almacenan todos los LSP recibidos en una base de datos.

5. Cada router utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino para cada red de destino.

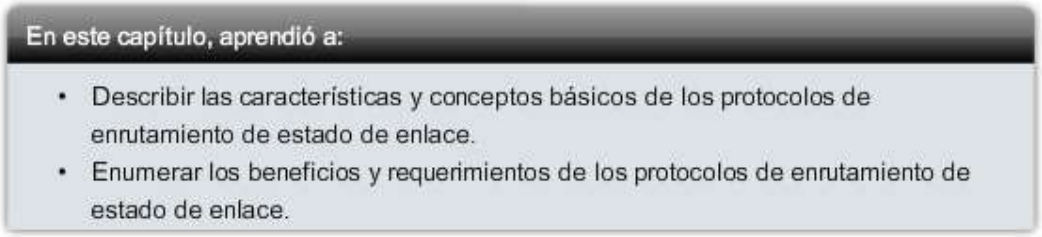
Un enlace es una interfaz en el router. Un estado de enlace es la información sobre dicha interfaz, incluida su dirección IP y máscara de subred, el tipo de red, el costo asociado con el enlace y todo router vecino en dicho enlace.

Cada router determina sus propios estados de enlace y satura con la información a todos los demás routers del área. Como consecuencia, cada router crea una base de datos de estado de enlace (LSDB) que incluye la información de estado de enlace de todos los demás routers. Cada router tendrá LSDB idénticas. Con la información de LSDB, cada router ejecutará el algoritmo SPF. El algoritmo creará un árbol SPF, con el router en la raíz del árbol. A medida que cada enlace se conecta a los demás enlaces, se crea el árbol SPF. Una vez que el árbol SPF se completa, el router puede determinar por su cuenta el mejor camino a cada red del árbol. Esta información sobre el mejor camino luego se almacena en la tabla de enrutamiento del router.

Los protocolos de enrutamiento de estado de enlace crean un mapa de la topología local de la red que permite a cada router determinar el mejor camino para una red determinada. Se envía un nuevo LSP únicamente cuando hay un cambio en la topología. Cuando se agrega, retira o modifica un enlace, el router saturará con el nuevo LSP a todos los demás routers. Cuando un router recibe el nuevo LSP, éste actualizará su LSDB, volverá a ejecutar el algoritmo SPF, creará un nuevo árbol SPF y actualizará su tabla de enrutamiento.

Los protocolos de enrutamiento de estado de enlace tienden a presentar un tiempo de convergencia menor que los protocolos de enrutamiento por vector de distancia. EIGRP es una excepción notable. Sin embargo, los protocolos de enrutamiento de estado de enlace exigen más requerimientos de memoria y procesamiento. Esto normalmente no representa un problema con los nuevos routers de la actualidad.

En el próximo y último capítulo de este curso, aprenderá acerca del protocolo de enrutamiento de estado de enlace, OSPF.



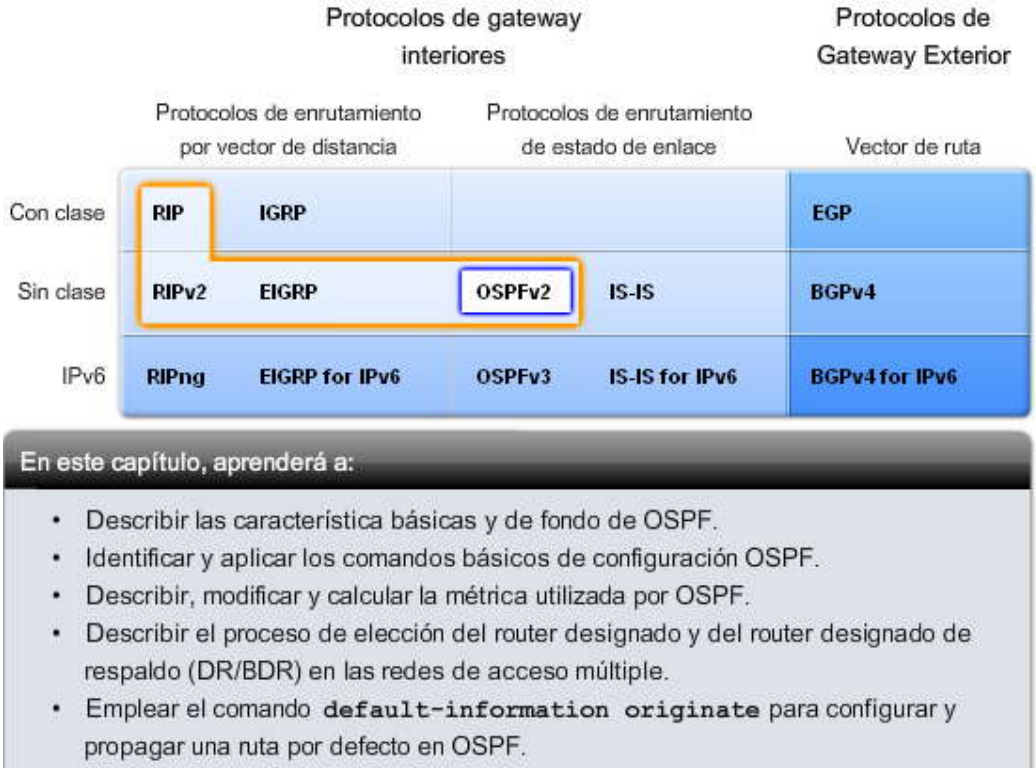
# CAPITULO XI – "OSPF"

## 11.0 INTRODUCCION DEL CAPITULO.-

### 11.0.1 INTRODUCCIÓN DEL CAPITULO.-

Open Shortest Path First (OSPF) es un protocolo de enrutamiento de estado de enlace desarrollado como reemplazo del protocolo de enrutamiento por vector de distancia: RIP. RIP constituyó un protocolo de enrutamiento aceptable en los comienzos del networking y de Internet; sin embargo, su dependencia en el conteo de saltos como la única medida para elegir el mejor camino rápidamente se volvió inaceptable en redes mayores que necesitan una solución de enrutamiento más sólida. OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. RFC 2328 define la métrica OSPF como un valor arbitrario llamado costo. El IOS de Cisco utiliza el ancho de banda como la métrica de costo de OSPF.

Las principales ventajas de OSPF frente a RIP son su rápida convergencia y escalabilidad a implementaciones de redes mucho mayores. En este capítulo final del curso de Conceptos y protocolos y de enrutamiento, aprenderá sobre implementaciones y configuraciones de OSPF básicas de área única. Las configuraciones y conceptos de OSPF más complejos se reservan para los cursos de nivel CCNP.




## 11.1 INTROCCION AL OPSF.-

### 11.1.1 INFORMACION BASICA DEL OSPF.-

El desarrollo inicial de OSPF comenzó en 1987 por parte del grupo de trabajo de OSPF, el Grupo de trabajo de ingeniería de Internet (IETF). En aquel momento, Internet constituía fundamentalmente una red académica y de investigación financiada por el gobierno de los EE. UU.

Coloque el cursor sobre las fechas en la figura Cronograma de desarrollo de OSPF para ver los eventos relacionados.

En 1989, la especificación para OSPFv1 se publicó en RFC 1131. Había dos implementaciones desarrolladas: una para ejecutar en routers y otra para ejecutar en estaciones de trabajo UNIX. La última implementación se convirtió luego en un proceso UNIX generalizado y conocido como GATED. OSPFv1 fue un protocolo de enrutamiento experimental y nunca se implementó.

En 1991, John Moy introdujo OSPFv2 en RFC 1247. OSPFv2 ofrecía significativas mejoras técnicas con respecto a OSPFv1. Al mismo tiempo, ISO trabajaba en un protocolo de enrutamiento de estado de enlace propio, Intermediate System-to-Intermediate System (IS-IS). Lógicamente, IETF eligió OSPF como su IGP (Interior Gateway Protocol) recomendado.

En 1998, la especificación OSPFv2 se actualizó en RFC 2328 y representa la RFC actual para OSPF.

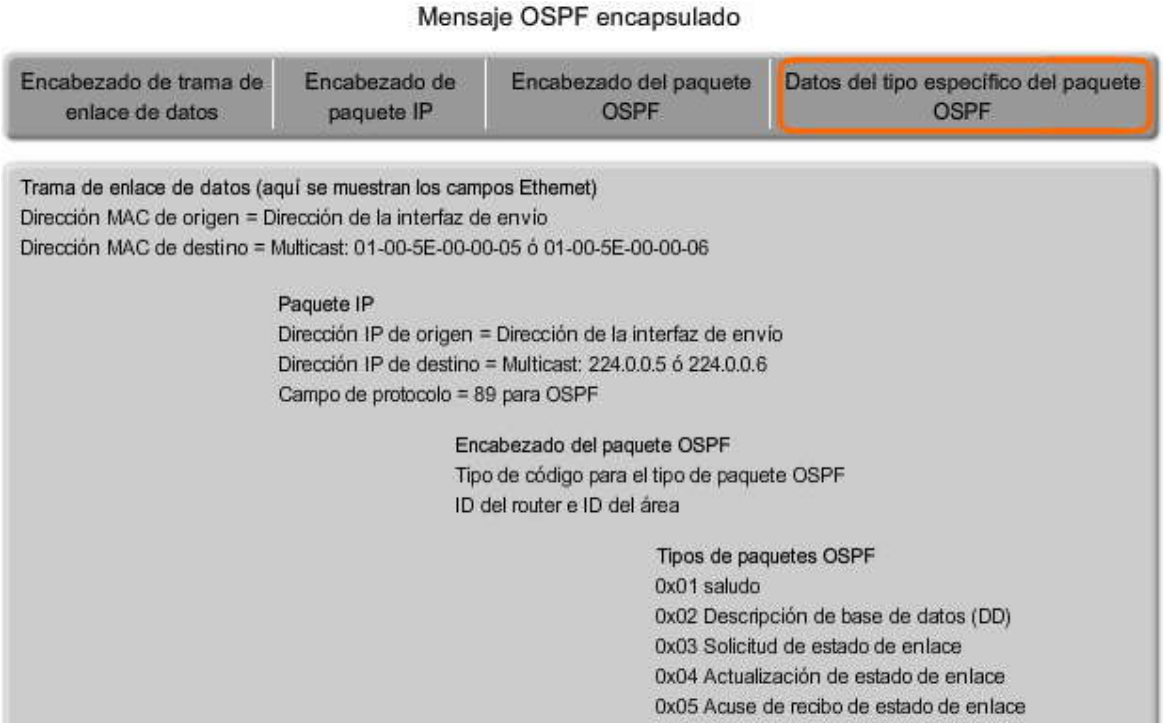
Nota: En 1999, OSPFv3 para IPv6 se publicó en RFC 2740. John Moy, Rob Coltun y Dennis Ferguson de sarrollaron RFC 2740. OSPFv3 se analiza en CCNP.


### 11.1.2 ENCAPSULACION DE MENSAJES OSPF.-

La porción de datos de un mensaje OSPF se encapsula en un paquete. Este campo de datos puede incluir uno de cinco tipos de paquetes OSPF. Cada tipo de paquete se analiza brevemente en el próximo tema.

Coloque el cursor sobre los campos en la figura Mensaje de OSPF encapsulado para ver el proceso de encapsulación.

El encabezado del paquete OSPF se incluye con cada paquete OSPF, independientemente de su tipo. El encabezado del paquete OSPF y los datos específicos según el tipo de paquete específico se encapsulan luego en un paquete IP. En el encabezado del paquete IP, el campo Protocolo se establece en 89 para indicar el OSPF y la dirección de destino se establece para una de dos direcciones multicast: 224.0.0.5 ó 224.0.0.6. Si el paquete OSPF se encapsula en una trama de Ethernet, la dirección MAC de destino es también una dirección multicast: 01-00-5E-00-00-05 ó 01-00-5E-00-00-06.




### 11.1.3 TIPOS DE PAQUETES OSPF.-

En el capítulo anterior, presentamos Paquetes de estado de enlace (LSP). La figura muestra los cinco tipos diferentes de LSP de OSPF. Cada paquete cumple una función específica en el proceso de enrutamiento de OSPF:

1. Saludo: los paquetes de saludo se utilizan para establecer y mantener la adyacencia con otros routers OSPF. El protocolo de saludo se analiza en detalle en el próximo tema.

2. DBD: el paquete de Descripción de bases de datos (DBD) incluye una lista abreviada de la base de datos de estado de enlace del router emisor y lo utilizan los routers receptores para comparar con la base de datos de estado de enlace local.

3. LSR: los routers receptores pueden luego solicitar más información acerca de una entrada en la DBD enviando una Solicitud de estado de enlace (LSR).

4. LSU: los paquetes de Actualización de estado de enlace (LSU) se utilizan para responder las LSR y para anunciar nueva información. Las LSU contienen siete tipos diferentes de Notificaciones de estado de enlace (LSA). Las LSU y LSA se analizan brevemente en un tema posterior.

5. LSAck: cuando se recibe una LSU, el router envía un Acuse de recibo de estado de enlace (LSAck) para confirmar la recepción de LSU.

Tipos de paquete OSPF

| Tipo | Nombre del paquete | Descripción |
|---|---|---|
| 1 | Saludo | Descubre los vecinos y construye adyacencias entre ellos |
| 2 | Descripción de la base de datos (DBD) | Controla la sincronización de la base de datos entre routers |
| 3 | Solicitud de estado de enlace (LSR) | Solicita registros específicos de estado de enlace de router a router |
| 4 | Actualización de estado de enlace (LSU) | Envía los registros de estado de enlace específicamente solicitados |
| 5 | Acuse de recibo de estado de enlace (LSAck) | Reconoce los demás tipos de paquetes |

### 11.1.4 PROTOCOLO DE SALUDO.-

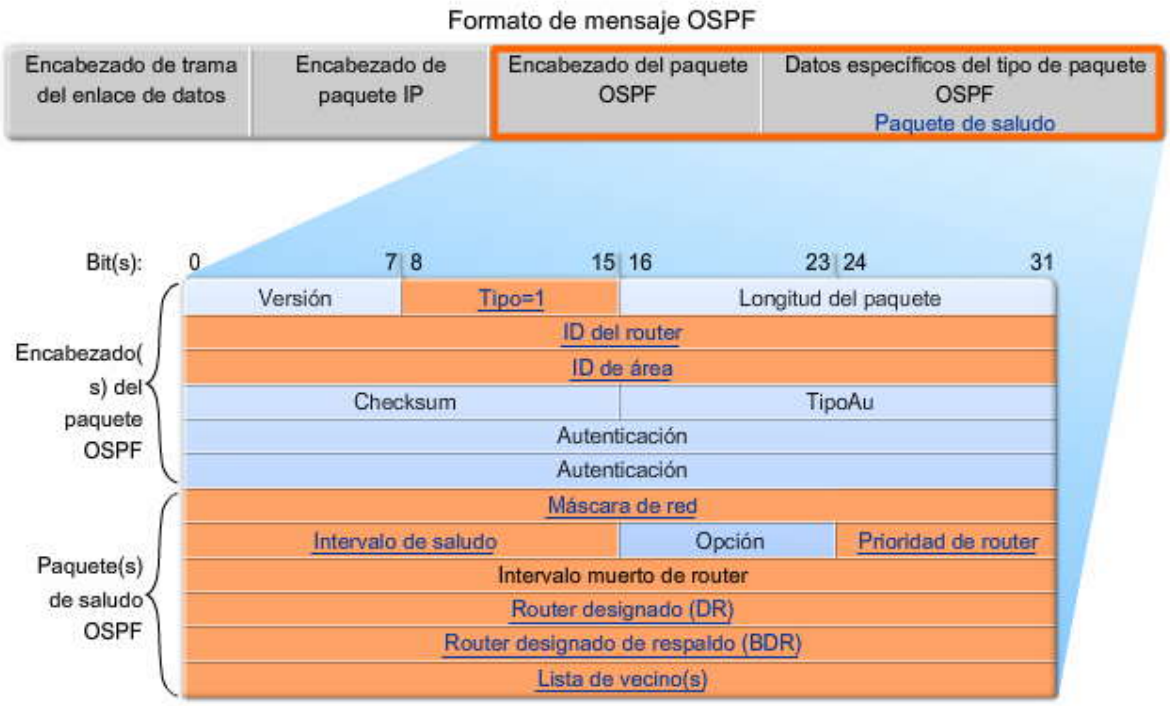
La figura muestra el encabezado del paquete OSPF y el paquete de saludo. Los campos sombreados en color azul se analizarán en mayor detalle más adelante en el capítulo. Por el momento, nos enfocaremos en los usos del paquete de saludo.

El paquete OSPF Tipo 1 es el paquete de saludo OSPF. Los paquetes de saludo se utilizan para:

Descubrir vecinos OSPF y establecer adyacencias de vecinos.
Publicar parámetros en los que dos routers deben acordar convertirse en vecinos.
Elegir el Router designado (DR) y el Router designado de respaldo (BDR) en redes de accesos múltiples, como Ethernet y Frame Relay.

Los campos importantes que se muestran en la figura incluyen:

Tipo: Tipo de paquete OSPF: Saludo (1), DD (2), Solicitud LS (3), Actualización LS (4), ACK LS (5)
ID del Router: ID del router de origen
ID del área: área en la que se originó el paquete
Máscara de red: máscara de subred asociada con la interfaz emisora
Intervalo de saludo: cantidad de segundos entre los paquetes de saludo del router emisor
Prioridad del router: utilizado en la elección de DR/BDR (se analizará más adelante)
Router designado (DR): ID del router del DR, si existe
Router designado de respaldo (BDR): ID del router del BDR, si existe
Lista de vecinos: enumera la ID del router OSPF de los routers vecinos




**Establecimiento de vecinos**

Antes de que un router OSPF pueda saturar a otros routers con sus estados de enlace, primero debe determinar si existe algún otro vecino OSPF en alguno de sus enlaces. En la figura, los routers OSPF envían paquetes de saludo a todas las interfaces habilitadas con OSPF para determinar si hay vecinos en dichos enlaces. La información en el saludo de OSPF incluye la ID del router OSPF del router que envía el paquete de saludo (la ID del router se analiza más adelante en el capítulo). La recepción de un paquete de saludo OSPF en una interfaz confirma a un router la presencia de otro router OSPF en dicho enlace. OSPF luego establece la adyacencia con el vecino. Por ejemplo, en la figura, R1 establecerá adyacencias con R2 y R3.

**Intervalos muerto y de saludo de OSPF**

Antes de que dos routers puedan formar una adyacencia de vecinos OSPF, éstos deben estar de acuerdo con respecto a tres valores: Intervalo de saludo, intervalo muerto y tipo de red. El intervalo de saludo de OSPF indica la frecuencia con que un router OSPF transmite sus paquetes de saludo. De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos multiacceso y punto a punto, y cada 30 segundos en segmentos multiacceso sin broadcast (NBMA) (Frame Relay, X.25, ATM).

En la mayoría de los casos, los paquetes de saludo OSPF se envían como multicast a una dirección reservada para ALLSPFRouters en 224.0.0.5. La utilización de una dirección multicast permite a un dispositivo ignorar el paquete si la interfaz no está habilitada para aceptar paquetes OSPF. Esto ahorra tiempo de procesamiento de CPU en los dispositivos que no son OSPF.

El intervalo muerto es el período, expresado en segundos, que el router esperará para recibir un paquete de saludo antes de declarar al vecino "desactivado". Cisco utiliza en forma predeterminada cuatro veces el intervalo de Hello. En el caso de los segmentos multiacceso y punto a punto, dicho período es de 40 segundos. En el caso de las redes NBMA, el intervalo muerto es de 120 segundos.

Si el intervalo muerto expira antes de que los routers reciban un paquete de saludo, OSPF retirará a dicho vecino de su base de datos de estado de enlace. El router satura con la información de estado de enlace acerca del vecino "desactivado" desde todas las interfaces habilitadas con OSPF.

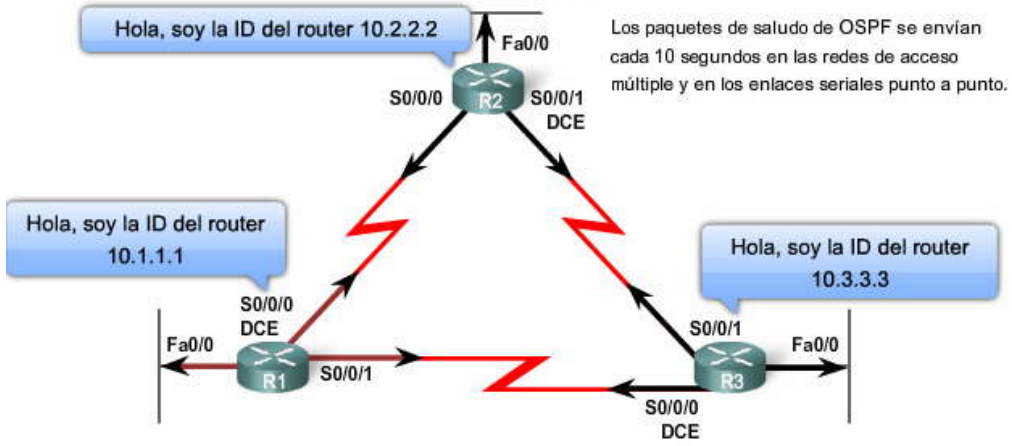
Los tipos de redes se analizan más adelante en el capítulo.

**Selección de DR y BDR**

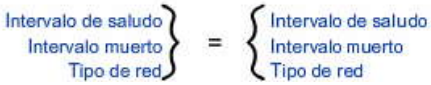
Para reducir la cantidad de tráfico de OSPF en redes de accesos múltiples, OSPF selecciona un Router designado (DR) y un Router designado de respaldo (BDR). El DR es responsable de actualizar todos los demás routers OSPF (llamados

DROthers) cuando ocurre un cambio en la red de accesos múltiples. El BDR supervisa al DR y reemplaza a DR si el DR actual falla.
En la figura, R1, R2 y R3 están conectados a través de enlaces punto a punto. Por lo tanto, no ocurre la elección de DR/BDR. La selección y los procesos de DR/BDR se analizarán en un tema posterior y se cambiará la topología por una red de accesos múltiples.
Nota: El paquete de saludo se analiza en mayor detalle en CCNP junto con los otros tipos de paquetes OSPF.

El protocolo de saludo




Coincidencia de valores de interfaz para dos routers para formar una adyacencia




### 11.1.5 ACTUALIZACIONES DE ESTADO DE ENLACE DE OSPF.-

Las actualizaciones de estado de enlace (LSU) son los paquetes utilizados para las actualizaciones de enrutamiento OSPF. Un paquete LSU puede incluir diez tipos diferentes de Notificaciones de estado de enlace (LSA), como se muestra en la figura. La diferencia entre los términos Actualización de estado de enlace (LSU) y Notificación de estado de enlace (LSA) en ocasiones puede ser confusa. A veces, dichos términos pueden utilizarse indistintamente. Una LSU incluye una o varias LSA y cualquiera de los dos términos puede usarse para hacer referencia a la información de estado de enlace propagada por los routers OSPF.
Nota: Los diferentes tipos de LSA se analizan en CCNP.

Las LSU contienen notificaciones de estado de enlace (LSA)

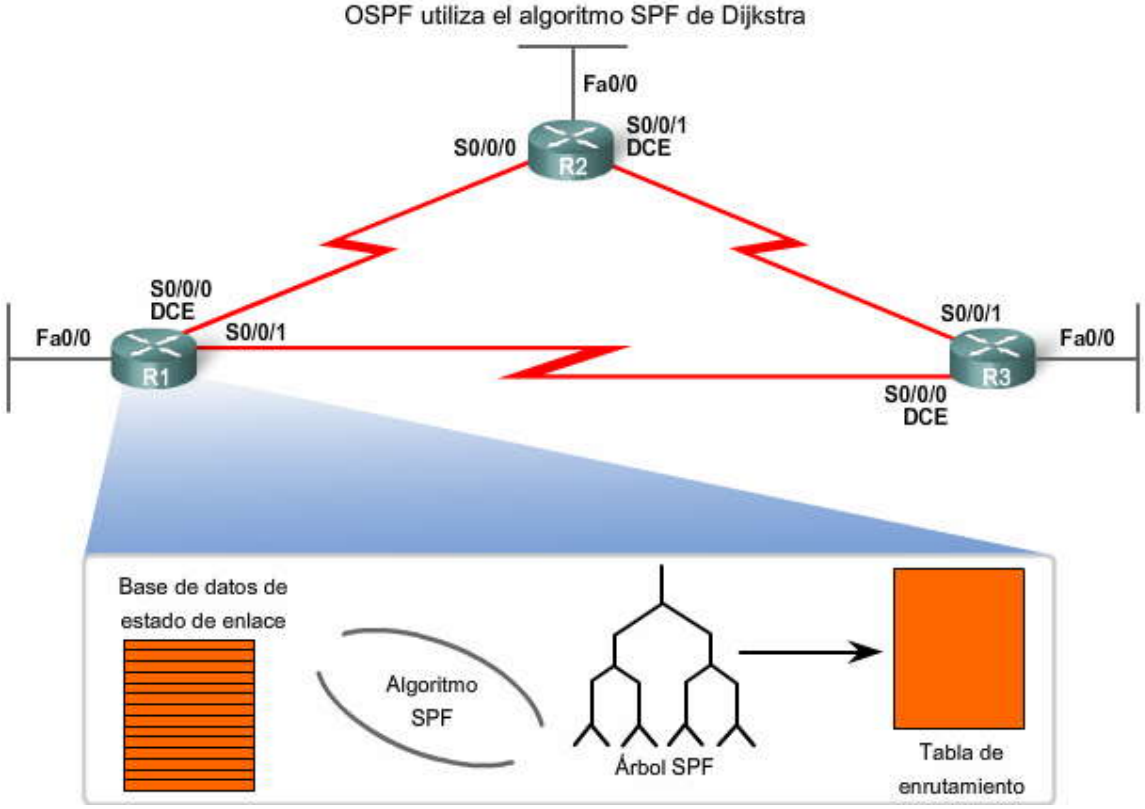
| Tipo | Nombre del paquete | Descripción |
|---|---|---|
| 1 | Saludo | Descubre los vecinos y construye adyacencias entre ellos |
| 2 | DBD | Controla la sincronización de la base de datos entre routers |
| 3 | LSR | Solicita registros específicos de estado de enlace de router a router |
| 4 | LSU | Envía los registros de estado de enlace específicamente solicitados |
| 5 | LSAck | Reconoce los demás tipos de paquetes |

- Las siglas LSA y LSU con frecuencia se utilizan indistintamente.
- Una LSU contiene una o más LSA.
- Las LSA contienen información de ruta para las redes de destino.
- La información específica de LSA se analiza en CCNP.

| Tipo de LSA | Descripción |
|---|---|
| 1 | LSA de router |
| 2 | LSA de red |
| 3 ó 4 | LSA de resumen |
| 5 | LSA externos del sistema autónomo |
| 6 | LSA de OSPF multicast |
| 7 | Definido para áreas no tan llenas |
| 8 | Atributos externos de LSA para Border Gatway Protocol (BGP) |
| 9, 10, 11 | LSA opacas |

### 11.1.6 ALGORITMO OSPF.-

Cada router OSPF mantiene una base de datos de estado de enlace que contiene las LSA recibidas por parte de todos los demás routers. Una vez que un router recibió todas las LAS y creó su base de datos de estado de enlace local, OSPF utiliza el algoritmo shortest path first (SPF) de Dijkstra para crear un árbol SPF. El árbol SPF luego se utiliza para completar la tabla de enrutamiento IP con las mejores rutas para cada red.




### 11.1.7 DISTANCIA ADMINISTRATIVA.-

Como se vio en el Capítulo 3, "Introducción al enrutamiento dinámico", la distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110. Como puede ver en la figura, al compararlo con otros protocolos de gateway interiores (IGP), se prefiere a OSPF con respecto a IS-IS y RIP.

Distancias administrativas predeterminadas

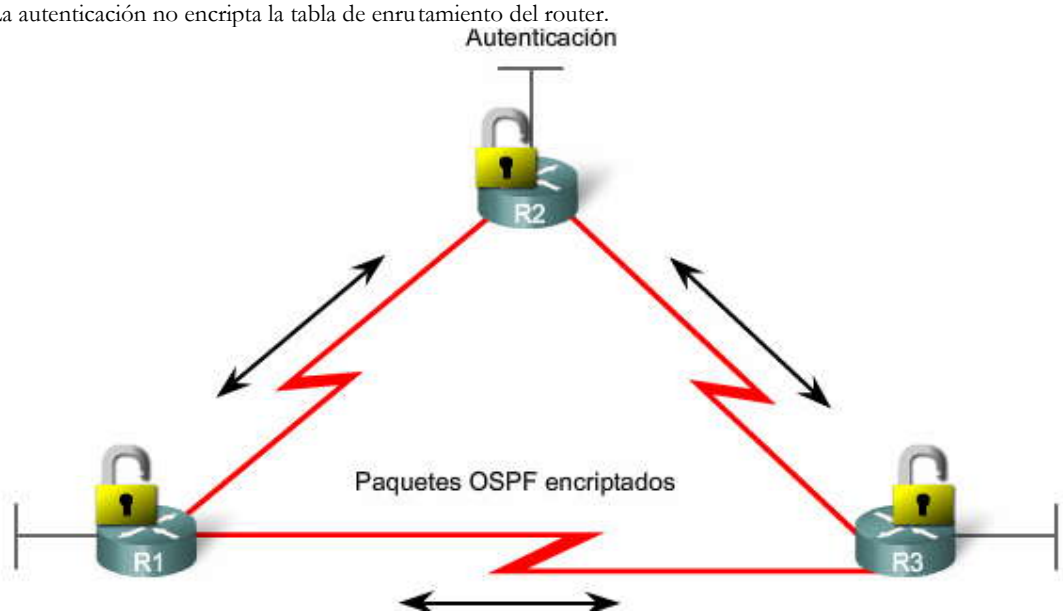
| Origen de la ruta | Distancia administrativa |
|---|---|
| Conectado | 0 |
| Estático | 1 |
| Ruta de resumen de EIGRP | 5 |
| BGP externo | 20 |
| EIGRP interno | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| EIGRP externo | 170 |
| BGP interno | 200 |

### 11.1.8 AUTENTICACION.-

Como se mencionó en capítulos anteriores, la configuración de protocolos de enrutamiento para utilizar la autenticación se analizará en un curso posterior. Al igual que otros protocolos de enrutamiento, OSPF puede configurarse para autenticación.

Es aconsejable autenticar la información de enrutamiento transmitida. RIPv2, EIGRP, OSPF, IS-IS y BGP pueden configurarse para encriptar y autenticar su información de enrutamiento. Esto garantiza que los routers sólo aceptarán información de enrutamiento de otros routers que estén configurados con la misma contraseña o información de autenticación.

Nota: La autenticación no encripta la tabla de enrutamiento del router.




## 11.2 CONFIGURACCION OSPF BASICA.-

### 11.2.1 TOPOLOGIA DE LABORATORIO.-

La figura muestra la topología para este capítulo. Observe que el esquema de direccionamiento no es contiguo. OSPF es un protocolo de enrutamiento sin clase. Por lo tanto, configuraremos la máscara como parte de nuestra configuración OSPF. Como sabe, al hacerlo se solucionará el problema del direccionamiento no contiguo. También observe que en esta topología hay tres enlaces seriales de varios anchos de banda y cada router tiene múltiples rutas para cada red remota.

**Haga clic en Direccionamiento para revisar las direcciones IP.**
**Haga clic en R1, R2 y R3 para revisar la configuración de inicio de cada router.**

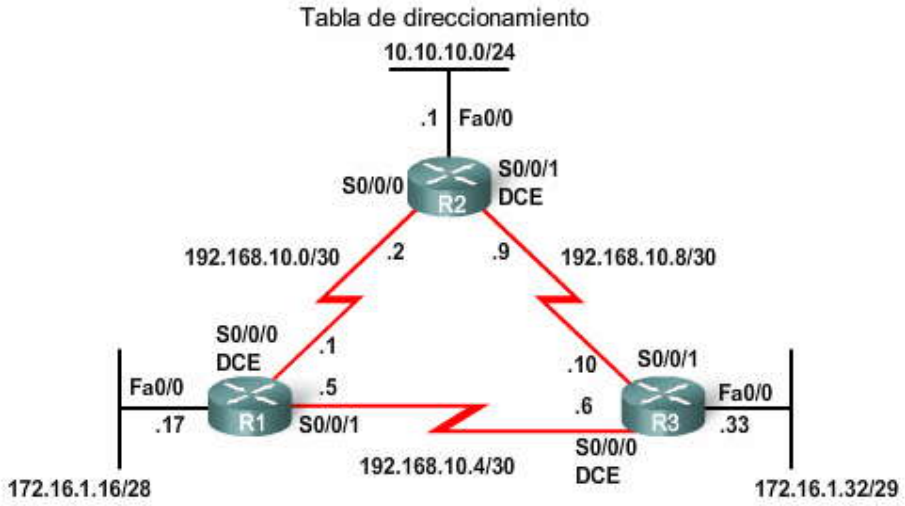


Tabla de direccionamiento

| Dispositivo | Interfaz | Dirección IP | Máscara de subred |
|---|---|---|---|
| R1 | Fa0/0 | 172.16.1.17 | 255.255.255.240 |
| | S0/0/0 | 192.168.10.1 | 255.255.255.252 |
| | S0/0/1 | 192.168.10.5 | 255.255.255.252 |
| R2 | Fa0/0 | 10.10.10.1 | 255.255.255.0 |
| | S0/0/0 | 192.168.10.2 | 255.255.255.252 |
| | S0/0/1 | 192.168.10.9 | 255.255.255.252 |
| R3 | Fa0/0 | 172.16.1.33 | 255.255.255.248 |
| | S0/0/0 | 192.168.10.6 | 255.255.255.252 |
| | S0/0/1 | 192.168.10.10 | 255.255.255.252 |

Configuración inicial de R1

```
R1#show startup-config

Current configuration : 1344 bytes
!
<some output omitted>
!
hostname R1
!
!
!
interface FastEthernet0/0
 description R1 LAN
 ip address 172.16.1.17 255.255.255.240
!
interface Serial0/0/0
 description Link to R2
 ip address 192.168.10.1 255.255.255.252
 clock rate 64000
!
```

Configuración inicial de R2

```
R2#show startup-config

Current configuration : 1343 bytes
!
<some output omitted>
!
hostname R2
!
!
!
interface FastEthernet0/0
 description R2 LAN
 ip address 10.10.10.1 255.255.255.0
!
interface Serial0/0/0
 description Link to R1
 ip address 192.168.10.2 255.255.255.252
!
interface Serial0/0/1
```

Configuración inicial de R3

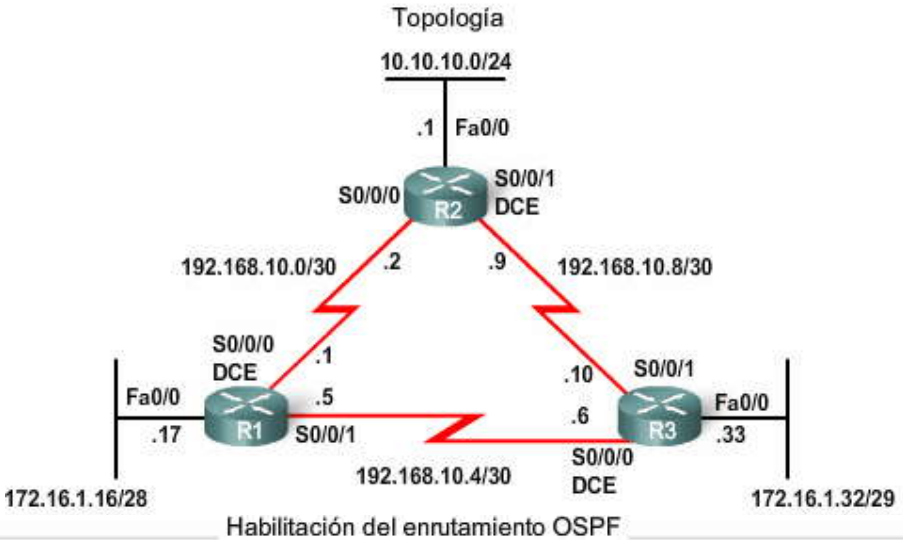
```
R3#show startup-config

Current configuration : 1342 bytes
!
<some output omitted>
!
hostname R3
!
interface FastEthernet0/0
 description R3 LAN
 ip address 172.16.1.33 255.255.255.248
!
interface Serial0/0/0
 description Link to R1
 ip address 192.168.10.6 255.255.255.252
 clockrate 64000
!
interface Serial0/0/1
```

### 11.2.2 COMANDO ROUTER OSPF.-

OSPF se habilita con el comando de configuración global router ospf process-id. El comando process-id es un número entre 1 y 65535 elegido por el administrador de red. El comando process-id es significativo a nivel local, lo que implica que no necesita coincidir con otros routers OSPF para establecer adyacencias con dichos vecinos. Esto difiere de EIGRP. La ID del proceso EIGRP o el número de sistema autónomo sí necesita coincidir con dos vecinos EIGRP para volverse adyacente.

En nuestra topología, habilitaremos OSPF en los tres routers que utilizan la misma ID de proceso de 1. Utilizamos la misma ID de proceso simplemente por cuestiones de uniformidad.

R1(config)#router ospf 1
R1(config-router)#




Habilitación del enrutamiento OSPF

```
R1(config)#router ospf 1
R1(config-router)#
```

```
R2(config)#router ospf 1
R2(config-router)#
```

```
R3(config)#router ospf 1
R3(config-router)#
```

### 11.2.3 COMANDO NETWORK.-

El comando network utilizado con OSPF tiene la misma función que cuando se utiliza con otros protocolos de enrutamiento IGP:

Cualquier interfaz en un router que coincida con la dirección de red en el comando network estará habilitada para enviar y recibir paquetes OSPF.
Esta red (o subred) estará incluida en las actualizaciones de enrutamiento OSPF.

El comando network se utiliza en el modo de configuración de router.

Router(config-router)#network network-address wildcard-mask area area-id

El comando network de OSPF utiliza una combinación de network-address y wildcard-mask similar a la que puede utilizar EIGRP. Sin embargo, a diferencia de EIGRP, OSPF requiere la máscara wildcard. La dirección de red junto con la máscara wildcard se utiliza para especificar la interfaz o rango de interfaces que se habilitarán para OSPF con el comando network.

Al igual que con EIGRP, la máscara wildcard puede configurarse en forma inversa a una máscara de subred. Por ejemplo, la interfaz FastEthernet 0/0 de R1 se encuentra en la red 172.16.1.16/28. La máscara de subred para esta interfaz es /28 ó 255.255.255.240. Lo inverso a la máscara de subred es la máscara wildcard.

Nota: Al igual que EIGRP, algunas versiones de IOS simplemente le permiten ingresar la máscara de subred en lugar de la máscara wildcard. Luego, IOS convierte la máscara de subred al formato de la máscara wildcard.

255.255.255.255

- 255.255.255.240 Reste la máscara de subred

---

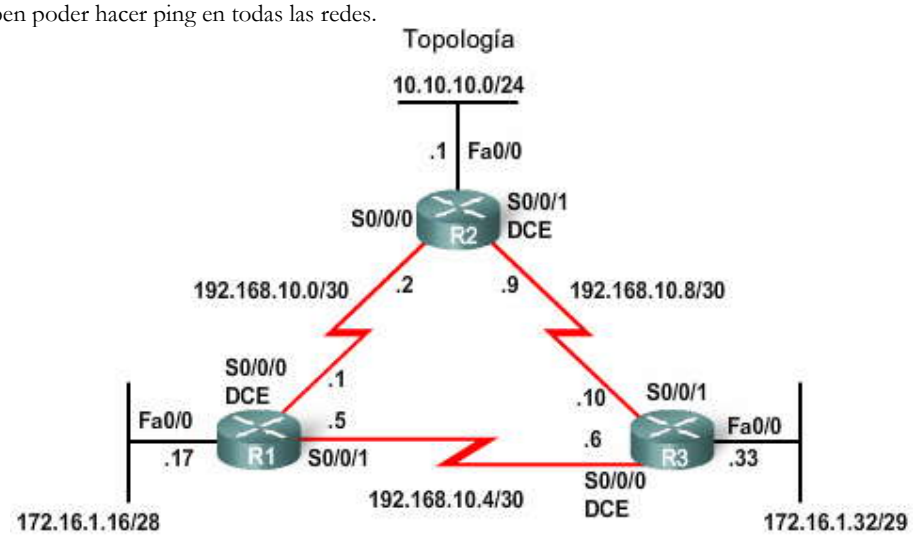
0. 0. 0. 15 Máscara wildcard

El área area-id hace referencia al área OSPF. Un área OSPF es un grupo de routers que comparte la información de estado de enlace. Todos los routers OSPF en la misma área deben tener la misma información de estado de enlace en sus bases de datos de estado de enlace. Esto se logra a través de la saturación por parte de los routers de todos los demás routers en el área con sus estados de enlace individuales. En este capítulo, configuraremos todos los routers OSPF dentro de un área única. Esto se conoce como OSPF de área única.

Una red OSPF también puede configurarse como áreas múltiples. Existen varias ventajas en la configuración de redes OSPF amplias como áreas múltiples, incluidas las bases de datos de estado de enlace más pequeñas y la capacidad de aislar problemas de redes inestables dentro de un área. El OSPF de áreas múltiples se desarrolla en CCNP.

Cuando todos los routers se encuentran dentro de la misma área OSPF, deben configurarse los comandos network con la misma area-id en todos los routers. Si bien puede usarse cualquier area-id, es aconsejable utilizar un area-id de 0 con OSPF de área única. Esta convención facilita la posterior configuración de la red como áreas OSPF múltiples en las que área 0 se convierte en el área de backbone.

La figura muestra los comandos network para los tres routers y habilita OSPF en todas las interfaces. En este punto, todos los routers deben poder hacer ping en todas las redes.



Configuración de subredes de OSPF

```
R1(config)#router ospf 1
R1(config-router)#network 172.16.1.16 0.0.0.15 area 0
R1(config-router)#network 192.168.10.0 0.0.0.3 area 0
R1(config-router)#network 192.168.10.4 0.0.0.3 area 0
```

```
R2(config)#router ospf 1
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#network 192.168.10.0 0.0.0.3 area 0
R2(config-router)#network 192.168.10.8 0.0.0.3 area 0
```

```
R3(config)#router ospf 1
R3(config-router)#network 172.16.1.32 0.0.0.7 area 0
R3(config-router)#network 192.168.10.4 0.0.0.3 area 0
R3(config-router)#network 192.168.10.8 0.0.0.3 area 0
```

### 11.2.4 ID DEL ROUTER OSPF.-

Determinación de la ID del router

La ID del router OSPF se utiliza para identificar en forma exclusiva cada router en el dominio de enrutamiento OSPF. La ID de un router es simplemente una dirección IP. Los routers de Cisco obtienen la ID del router conforme a tres criterios y con la siguiente prioridad:

1. Utilizar la dirección IP configurada con el comando router-id de OSPF.

2. Si router-id no está configurado, el router elige la dirección IP más alta de cualquiera de sus interfaces loopback.

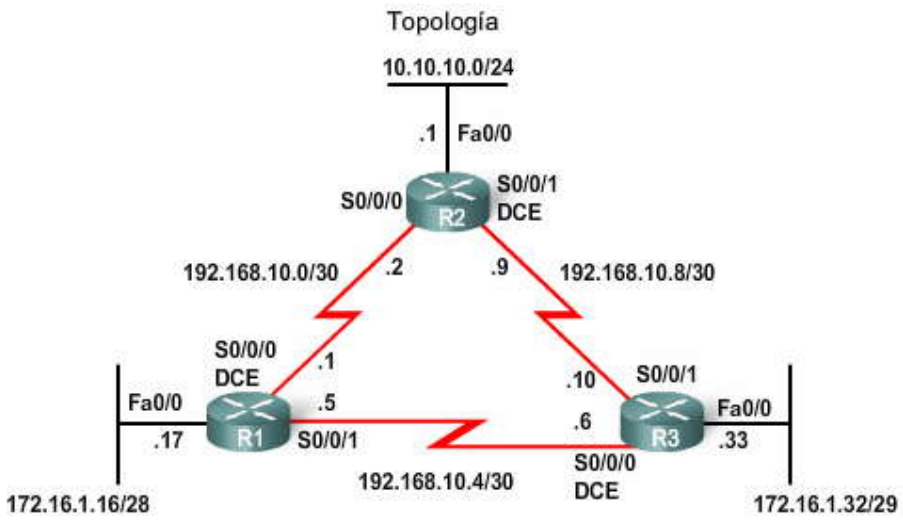
3. Si no hay ninguna interfaz loopback configurada, el router elige la dirección IP activa más alta de cualquiera de sus interfaces físicas.

Dirección IP activa más alta

Si un router OSPF se configura con el comando router-id de OSPF y no hay interfaces loopback configuradas, la ID del router OSPF será la dirección IP activa más alta de cualquiera de sus interfaces. La interfaz no necesita estar habilitada para OSPF, lo que significa que no necesita estar incluida en uno de los comandos network de OSPF. Sin embargo, la interfaz debe estar activa, debe encontrarse en estado up.

Haga clic en el botón Topología en la figura.

Con los criterios descritos anteriormente, ¿puede determinar las ID del router para R1, R2 y R3? La respuesta se encuentra en la próxima página.



## Determinación de la ID del router

**La ID del router se determina en el siguiente orden:**

1. Utilice la dirección IP configurada con el comando router-id de OSPF.
2. Si la id el router no está configurada, el router elige direcciones IP más altas de cualquiera de sus interfaces loopback.
3. Si no está configurada ninguna interfaz loopback, el router elige la dirección IP activa más alta de alguna de sus interfaces físicas.

Verificación de la ID del router

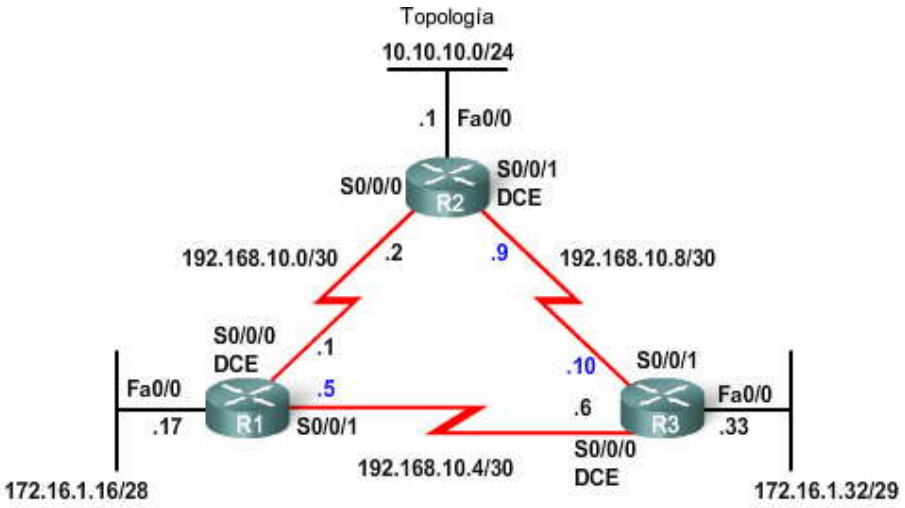
Debido a que no hemos configurado las ID del router ni las interfaces loopback en nuestros tres routers, la ID del route r para cada router está determinada por el tercer criterio de la lista: la dirección IP activa más alta en cualquiera de las interfaces físicas del router. Como se muestra en la figura, la ID del router para cada router es:

R1: 192.168.10.5, que es mayor que 172.16.1.17 ó 192.168.10.1

R2: 192.168.10.9, que es mayor que 10.10.10.1 ó 192.168.10.2

R3: 192.168.10.10, que es mayor que 172.16.1.33 ó 192.168.10.6

Un comando que puede utilizar para verificar la ID del router actual es show ip protocols. Algunas ver siones de IOS no muestran la ID del router como se muestra en la figura. En dichos casos, utilice los comandos show ip ospf o show ip ospf interface para verificar la ID del router.




Verificación de ID de router con `show ip protocols`

```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

```
R2#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.9
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

```
R3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.10.10
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

**Dirección de loopback**

Si no se utilizó el comando router-id de OSPF y están configuradas las interfaces loopback, OSPF elegirá la dirección IP más alta de cualquiera de sus interfaces loopback. Una dirección de loopback es una interfaz virtual y se encuentra en estado up en forma automática cuando está configurada. El usuario ya conoce los comandos para configurar una interfaz loopback:

Router(config)#interface loopback number
Router(config-if)#ip address ip-address subnet-mask

**Haga clic en el botón Topología en la figura.**

En esta topología, los tres routers se configuraron con direcciones de loopback para representar las ID del router OSPF. La ventaja de utilizar una interfaz loopback es que, a diferencia de las interfaces físicas, ésta no puede fallar. No hay cables ni dispositivos adyacentes reales de los que dependa la interfaz loopback para encontrarse en estado up. Por lo tanto, la utilización de una dirección de loopback para la ID del router ofrece estabilidad al proceso OSPF. Debido a que el comando router-id de OSPF que se analiza a continuación, se agregó recientemente a IOS, es más común encontrar direcciones de loopback utilizadas para configurar las ID del router OSPF.

**Comando router-id de OSPF**

El comando router-id de OSPF se introdujo en IOS 12.0(T) y tiene prioridad sobre direcciones IP físicas y de loopback en la determinación de la ID del router. La sintaxis de comando es:

Router(config)#router ospf process-id
Router(config-router)#router-id ip-address

**Modificación de la ID del router**

La ID del router se selecciona cuando se configura OSPF con su primer comando network de OSPF. Si el comando router-id de OSPF o la dirección de loopback se configuran después del comando network de OSPF, la ID del router se obtendrá de la interfaz con la dirección IP activa más alta.

La ID del router puede modificarse con la dirección IP de un comando router-id de OSPF subsiguiente, volviendo a cargar el router o utilizando el siguiente comando:

Router#clear ip ospf process

Nota: La modificación de la ID de un router con una nueva dirección IP física o de loopback puede requerir la recarga del router.

**ID duplicadas del router**

Cuando dos routers tienen la misma ID de router en un OSPF, es posible que el enrutamiento de dominio no funcione correctamente. Si la ID del router es la misma en dos routers vecinos, es posible que no se realice el establecimiento de vecinos. Cuando se producen ID duplicadas del router OSPF, IOS mostrará un mensaje similar al siguiente:

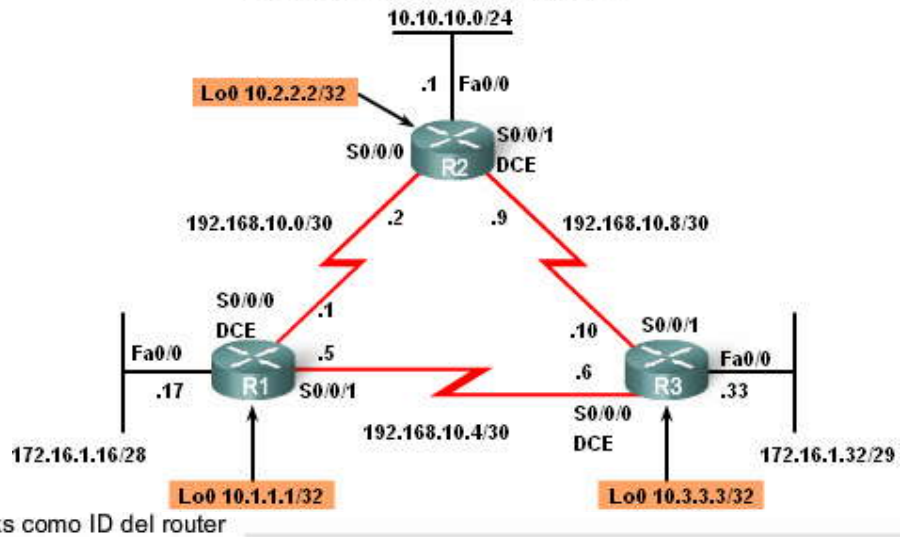
%OSPF-4-DUP_RTRID1: Detección de router con ID duplicadas

Para corregir este problema, configure todos los routers para que tengan una ID del router OSPF única.

**Haga clic en Nuevas ID del router en la figura.**

Debido a que algunas versiones de IOS no admiten el comando router-id, utilizaremos el método de dirección de loopback para asignar las ID del router. Una dirección IP de una interfaz loopback por lo general sólo reemplazará a una ID del router OSPF actual mediante la recarga del router. En la figura, se recargaron los routers. El comando show ip protocols se utiliza para verificar que cada router esté utilizando la dirección de loopback para cada ID del router.

Topología con interfaces loopback




Loopbacks como ID del router

```
R1(config)#interface loopback 0
R1(config-if)#ip add 10.1.1.1 255.255.255.255
```

```
R2(config)#interface loopback 0
R2(config-if)#ip add 10.2.2.2 255.255.255.255
```

```
R3(config)#interface loopback 0
R3(config-if)#ip add 10.3.3.3 255.255.255.255
```

Verificación de la nueva ID del router

```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

```
R2#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

```
R3#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
<output omitted>
```

### 11.2.5 VERIFICACION DE OSPF.-

El comando show ip ospf neighbor puede utilizarse para verificar las relaciones de vecinos OSPF y solucionar sus problemas. Este comando muestra el siguiente resultado para cada vecino:

- ID de vecino: la ID del router vecino.
- Pri: la prioridad OSPF de la interfaz. Esto se analiza en una sección posterior.
- Estado: el estado OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen bases de datos de estado de enlace de OSPF idénticas. Los estados OSPF se analizan en CCNP.

- Tiempo muerto: la cantidad de tiempo restante que el router esperará para recibir un paquete de saludo OSPF por parte del vecino antes de declararlo desactivado. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
- Dirección: la dirección IP de la interfaz del vecino a la que está conectada directamente el router.
- Interfaz: la interfaz donde este router formó adyacencia con el vecino.

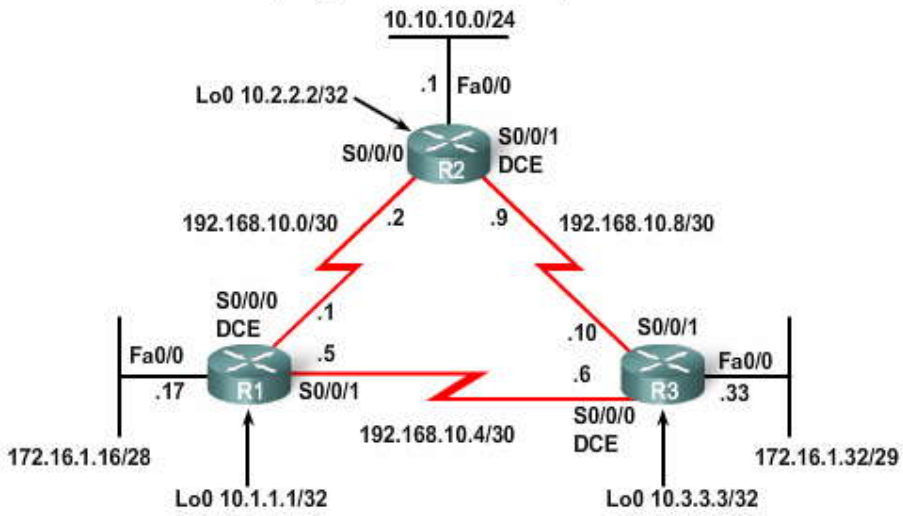
Al resolver problemas de redes OSPF, el comando show ip ospf neighbor puede utilizarse para verificar que el router formó adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o si no muestra el estado FULL, los dos routers no formaron una adyacencia OSPF. Si dos routers no establecieron adyacencia, no se intercambiará la información de estado de enlace. Las bases de datos de estado de enlace incompletas pueden crear árboles SPF y tablas de enrutamiento imprecisos. Es posible que no existan rutas a las redes de destino o que no representen la ruta más óptima.

Nota: En el caso de redes de accesos múltiples, como Ethernet, dos routers adyacentes pueden mostrar sus estados como 2WAY. Esto se analizará en una sección posterior.

Es posible que dos routers no formen adyacencia OSPF si:

Las máscaras de subred no coinciden, esto hace que los routers se encuentren en redes separadas.
Los temporizadores muerto y de saludo de OSPF no coinciden.
Los tipos de redes OSPF no coinciden.
Hay un comando network de OSPF faltante o incorrecto.

Topología con interfaces loopback




Verificación de adyacencia vecina

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          1   FULL/  -        00:00:30    192.168.10.6    Serial0/0/1
10.2.2.2          1   FULL/  -        00:00:33    192.168.10.2    Serial0/0/0
```

```
R2#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          1   FULL/  -        00:00:36    192.168.10.10   Serial0/0/1
10.1.1.1          1   FULL/  -        00:00:37    192.168.10.1    Serial0/0/0
```

```
R3#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.2.2.2          1   FULL/  -        00:00:34    192.168.10.9    Serial0/0/1
10.1.1.1          1   FULL/  -        00:00:38    192.168.10.5    Serial0/0/0
```

Otros poderosos comandos de resolución de problemas de OSPF incluyen:

show ip protocols
show ip ospf
show ip ospf interface

Como se muestra en la figura, el comando show ip protocols representa una manera rápida de verificar información de configuración vital de OSPF, incluida la ID del proceso OSPF, la ID del router, las redes que el router publica, los vecinos de quienes el router recibe actualizaciones y la distancia administrativa predeterminada, que es de 110 para OSPF.

Haga clic en show ip ospf en la figura.

El comando show ip ospf también puede utilizarse para examinar la ID del proceso OSPF y la ID del router. Asimismo, este comando muestra la información del área OSPF, así como la última vez que se calculó el algoritmo SPF. Como puede ver en el resultado de ejemplo, OSPF es un protocolo de enrutamiento muy estable. El único evento relacionado con OSPF en el que tuvo participación R1 durante las últimas 11 horas y media es el envío de paquetes de saludo a sus vecinos.

Nota: La información adicional que muestra el comando show ip ospf se analiza en los cursos CCNP.

El resultado del comando incluye información importante del algoritmo SPF que incluye el retraso en el programa SPF:

El retraso en el programa SPF inicial es de 5000 milisegundos
El tiempo en espera mínimo entre dos SPF consecutivos es de 10 000 milisegundos
El tiempo de espera máximo entre dos SPF consecutivos es de 10 000 milisegundos

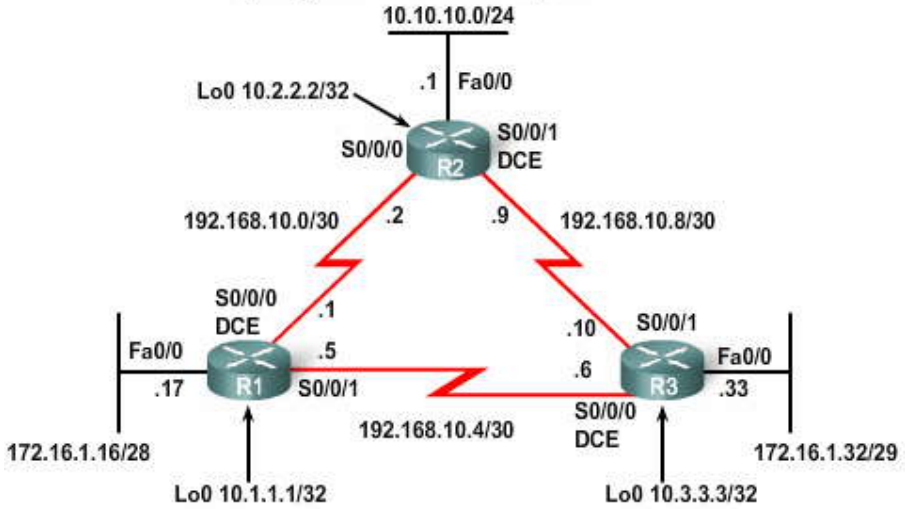
Cada vez que un router recibe nueva información acerca de la topología (adición, eliminación o modificación de un enlace), el router debe volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar la tabla de enrutamiento. El algoritmo SPF representa una gran exigencia para el CPU y el tiempo que le toma realizar los cál culos depende del tamaño del área. El tamaño de un área se mide por la cantidad de routers y el tamaño de la base de datos de estado de enlace.

A una red que alterna entre un estado up y down se la denomina enlace inestable. Un enlace inestable puede pro vocar que los routers OSPF de un área vuelvan a calcular constantemente el algoritmo SPF, lo que evita la convergencia adecuada. Para minimizar este problema, el router espera 5 segundos (5000 milisegundos) después de recibir una LSU antes de ejecutar el algoritmo SPF. Esto se conoce como retraso en el programa SPF. Para evitar que un router ejecute el algoritmo SPF constantemente, existe un tiempo en espera adicional de 10 segundos (10000 milisegundos). El router espera 10 segundos después de ejecutar el algoritmo SPF antes de volver a ejecutarlo nuevamente.

Haga clic en show ip ospf interface en la figura.

La forma más rápida de verificar los intervalos muerto y de saludo es utilizar el comando show ip ospf interface. Como se muestra en la figura, al agregar el nombre y el número de la interfaz al comando aparece el resultado para una interfaz específica. Dichos intervalos se incluyen en los paquetes de saludo OSPF enviados entre vecinos. OSPF puede tener diferentes intervalos muerto y de saludo en varias interfaces; sin embargo, para que los routers OSPF se conviertan en vecinos, sus intervalos muertos y de saludo de OSPF deben ser idénticos. Por ejemplo, en la figura, R1 utiliza un intervalo de saludo de 10 y un intervalo muerto de 40 en la interfaz Serial 0/0/0. R2 también debe usar los mismos intervalos en su interfaz Serial 0/0/0; de lo contrario, los dos routers no formarán una adyacencia.

Topología con interfaces loopback




El comando **show ip protocols**

```
R1#show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 10.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.16 0.0.0.15 area 0
    192.168.10.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    10.2.2.2              110      11:29:29
    10.3.3.3              110      11:29:29
  Distance: (default is 110)
```

El comando **show ip ospf**

```
R1#show ip ospf
 <some output omitted>
 Routing Process "ospf 1" with ID 10.1.1.1
 Start time: 00:00:19.540, Time elapsed: 11:31:15.776
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 Area BACKBONE(0)
        Number of interfaces in this area is 3
        Area has no authentication
        SPF algorithm last executed 11:30:31.628 ago
        SPF algorithm executed 5 times
        Area ranges are
        <output omitted>
```

El comando **show ip ospf interface**

```
R1#show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.2.2.2
  Suppress hello for 0 neighbor(s)
```

### 11.2.6 EXAMEN DE LA TABLA DE ENRUTAMIENTO.-

Como sabe, la manera más rápida de verificar la convergencia de OSPF es observar la tabla de enrutamiento para cada router en la topología.

**Haga clic en R1, R2 y R3 en la figura para ver el resultado de show ip route.**

El comando show ip route puede utilizarse para verificar si dicho OSPF envía y recibe rutas a través de OSPF. La O al inicio de cada ruta indica que el origen de la ruta es OSPF. La tabla de enrutamiento y OSPF se examinarán más detenidamente en la siguiente sección. Sin embargo, el usuario debería distinguir inmediatamente dos diferencias visibles en la tabla de enrutamiento de OSPF en comparación con las tablas de enrutamiento que se vieron en los capítulos anteriores. Primero, observe que cada router tiene cuatro redes conectadas directamente, ya que la interfaz loopback se cuenta como una cuarta red. Dichas interfaces loopback no se publican en OSPF. Por lo tanto, cada router enumera siete redes conocidas. Además, a diferencia de RIPv2 y EIGRP, OSPF no realiza un resumen automático en los bordes de la red principal. OSPF es esencialmente sin clase.

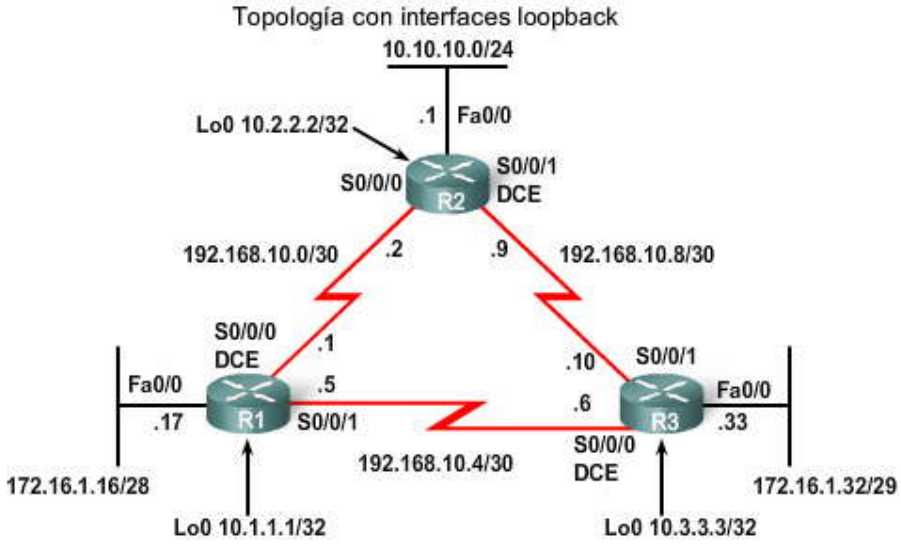



Tabla de enrutamiento de R1

```
R1#show ip route

Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/128] via 192.168.10.2, 14:27:57, Serial0/0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/65] via 192.168.10.6, 14:27:57, Serial0/0/1
C       172.16.1.16/28 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.10.10.0/24 [110/65] via 192.168.10.2, 14:27:57, Serial0/0/0
C       10.1.1.1/32 is directly connected, Loopback0
```

Tabla de enrutamiento de R2

```
R2#show ip route

Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
O       192.168.10.4 [110/128] via 192.168.10.1, 14:31:18, Serial0/0/0
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/65] via 192.168.10.10, 14:31:18, Serial0/0/1
O       172.16.1.16/28 [110/65] via 192.168.10.1, 14:31:18, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.2.2.2/32 is directly connected, Loopback0
C       10.10.10.0/24 is directly connected, FastEthernet0/0
```

Tabla de enrutamiento de R3

```
R3#show ip route

Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

Gateway of last resort is not set

     192.168.10.0/30 is subnetted, 3 subnets
O       192.168.10.0 [110/845] via 192.168.10.9, 14:31:52, Serial0/0/1
                     [110/845] via 192.168.10.5, 14:31:52, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0
C       192.168.10.8 is directly connected, Serial0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.32/29 is directly connected, FastEthernet0/0
O       172.16.1.16/28 [110/782] via 192.168.10.5, 14:31:52, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.3.3.3/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/782] via 192.168.10.9, 14:31:52, Serial0/0/1
```

**11.3 METRICA DEL OSPF.-**

La métrica del OSPF se denomina costo. En RFC 2328: "Un costo se asocia con el resultado de cada interfaz de router. Dicho costo está configurado por el administrador del sistema. Cuanto más bajo sea el costo, más probabilidad hay d e que la interfaz sea utilizada para enviar tráfico de datos."

Observe que RFC 2328 no especifica los valores que deben utilizarse para determinar el costo.

**El IOS de Cisco utiliza los anchos de banda acumulados de las interfaces de salida desde el route r hasta la red de destino como valor del costo.** En cada router, el costo de una interfaz se calcula en 10 a la octava potencia dividido por el ancho de banda en bps. Esto se conoce como ancho de banda de referencia. La división de 10 a la octava potencia p or el ancho de banda de la interfaz se realiza para que las interfaces con mayores valores de ancho de banda tengan un costo calculado inferior. Recuerde, en las métricas de enrutamiento, la ruta de inferior costo es la ruta preferida (por ejemplo, con RIP, 3 saltos es mejor que 10 saltos). La figura muestra los costos predeterminados de OSPF para varios tipos de interfaces.

**Ancho de banda de referencia**

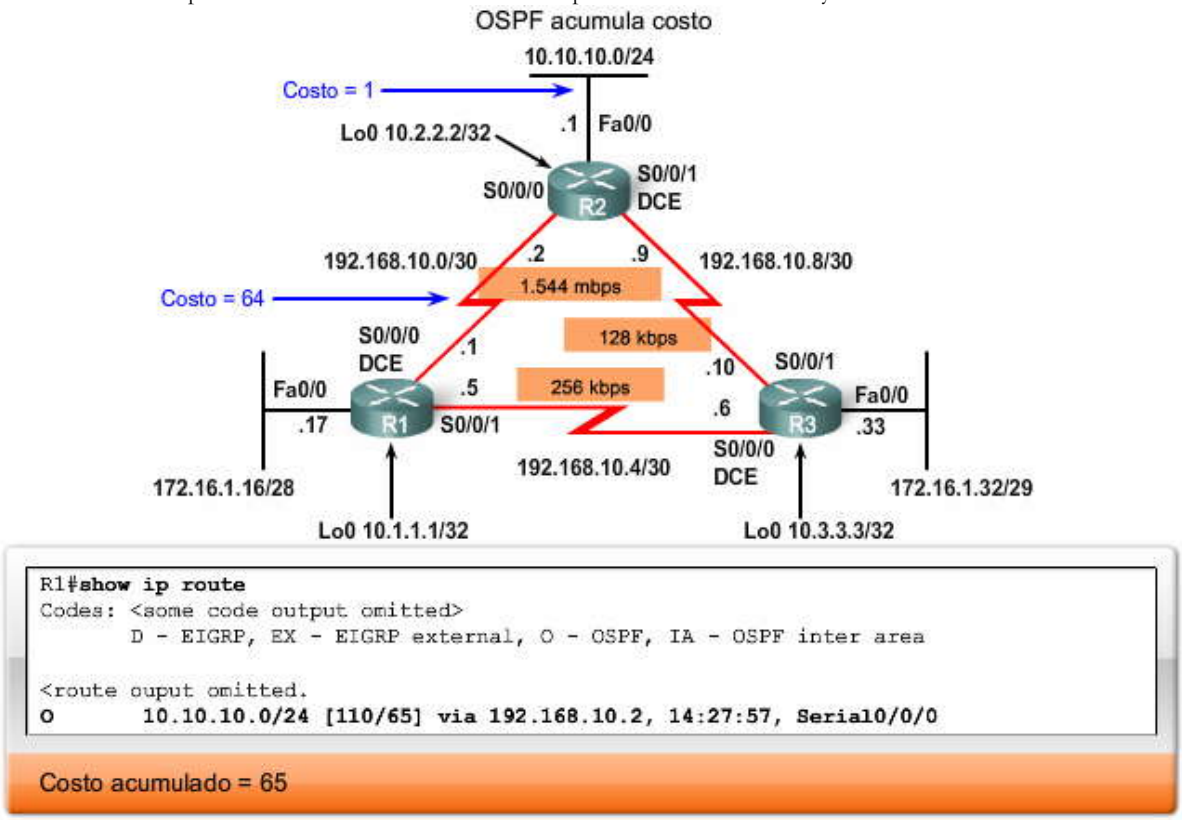
El ancho de banda de referencia predeterminado es de 10 a la octava potencia, 100 000 000 bps o 100 Mbps. Esto da como resultado interfaces con un ancho de banda de 100 Mbps y más con el mismo costo de OSPF de 1. El ancho de banda de referencia puede modificarse para adaptarse a redes con enlaces más rápidos que 100 000 000 bps (100 Mbps) con el comando auto-cost reference-bandwidth de OSPF. Cuando este comando es necesario, se recomienda su utilización en todos los routers para que la métrica de enrutamiento de OSPF se mantenga uniforme.

Valores de costo OSPF de Cisco

| Tipo de interfaz | $10^8$/ bps = Costo |
|---|---|
| Fast Ethernet y más rápida | $10^8$/100 000 000 bps = 1 |
| Ethernet | $10^8$/10 000 000 bps = 10 |
| E1 | $10^8$/2 048 000 bps = 48 |
| T1 | $10^8$/1 544 000 bps = 64 |
| 128 kbps | $10^8$/128 000 bps = 781 |
| 64 kbps | $10^8$/64 000 bps = 1562 |
| 56 kbps | $10^8$/56 000 bps = 1785 |

**OSPF acumula costos**

El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino. Por ejemplo, en la figura, la tabla de enrutamiento en R1 muestra un costo de 65 para alcanzar la red 10.10.10.0/24 en R2. Debido a que 10.10.10.0/24 está conectada a la interfaz FastEthernet, R2 asigna el valor de 1 como costo para 10.10.10.0/24. R1 luego agrega el valor del costo adicional de 64 para enviar datos a través del enlace T1 predeterminado entre R1 y R2.




**Ancho de banda predeterminado en interfaces seriales**

Es posible que recuerde del Capítulo 9, "EIGRP", que puede utilizar el comando show interface para ver el valor del ancho de banda utilizado para una interfaz. En los routers de Cisco, el valor del ancho de banda predeterminado de varias interfaces seriales es T1 (1 544 Mbps). Sin embargo, algunas interfaces seriales pueden tener el valor predeterminado de 128 kbps. Por lo tanto, nunca suponga que OSPF utiliza un valor de ancho de banda particular. Verifique siempre el valor predeterminado con el comando show interface.

Recuerde, este valor de ancho de banda no afecta realmente la velocidad del enlace; lo utilizan ciertos protocolos de enrutamiento para calcular la métrica de enrutamiento. Muy probablemente, en las interfaces seriales la velocidad real del enlace es diferente del ancho de banda predeterminado. Es importante que el valor de ancho de banda refleje la velocidad real del enlace para que la tabla de enrutamiento tenga información precisa del mejor camino. Por ejemplo, el usuario puede estar pagando a su proveedor de servicios únicamente por una conexión T1 fraccional, un cuarto de la conexión T1

completa (384 kbps). Sin embargo, a los fines del protocolo de enrutamiento, IOS supone el valor de ancho de banda de T1 a pesar de que la interfaz en realidad sólo envía y recibe un cuarto de una conexión T1 completa (384 kbps).

La figura muestra el resultado de la interfaz Serial 0/0/0 en R1. La topología también refleja ahora el ancho de banda real del enlace entre los routers. Observe que el valor de ancho de banda predeterminado en el resultado del comando para R1 es 1544 kbps. Sin embargo, el ancho de banda real de este enlace es 64 kbps. Esto significa que el router tiene información de enrutamiento que no refleja en forma precisa la topología de red.

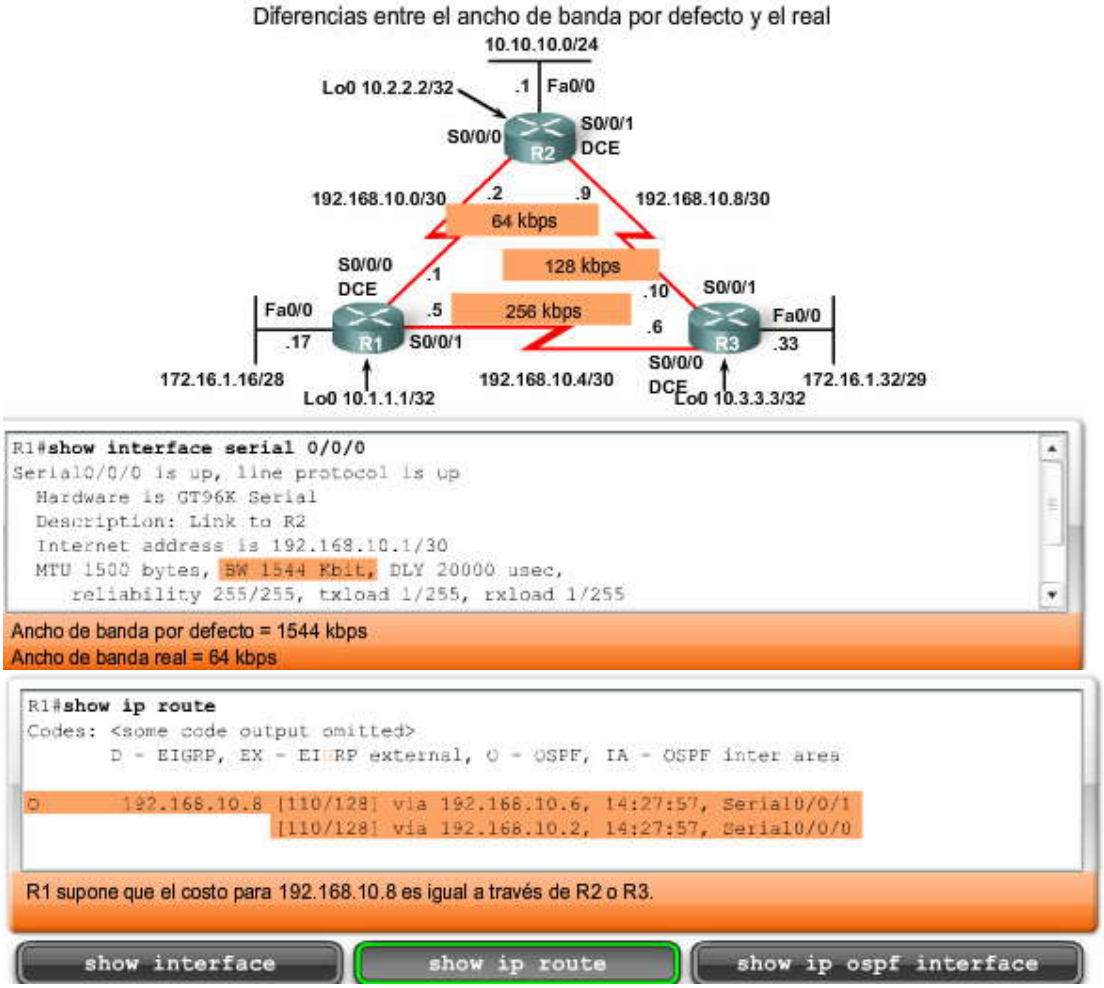
**Haga clic en show ip routeen la figura.**

La figura muestra la tabla de enrutamiento para R1. R1 considera que sus dos interfaces seriales están conectadas a enlaces de T1 a pesar de que uno de sus enlaces es de 64 kbps y el otro de 256 kbps. Esto provoca que la tabla de enrutamiento de R1 tenga dos rutas de igual costo hacia la red 192.168.8.0/30, donde Serial 0/0/1 es realmente el mejor camino.

O 192.168.10.8 [110/128] via 192.168.10.6, 00:03:41, Serial0/0/1
[110/128] via 192.168.10.2, 00:03:41, Serial0/0/0

**Haga clic en show ip ospf interface en la figura.**

El costo OSPF calculado de una interfaz puede verificarse con el comando show ip ospf interface. En la figura, podemos verificar que R1 verdaderamente asigna un costo de 64 a la interfaz Serial 0/0/0. Si bien el usuario puede pensar que éste es el costo correcto, ya que esta interfaz está conectada a un enlace de 64 kbps, recuerde que el costo deriva de la fórmula de costo. El costo de un enlace de 64 kbps es 1562 (100 000 000/64 000). El valor mostrado de 64 corresponde al costo de un enlace T1. En el siguiente tema, aprenderá la manera de modificar el costo de todos los enlaces de la topología.



```
R1#show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  <output omitted>
```

El valor del costo OSPF de 64 no es lo mismo que 64 kbps.
El valor del costo OSPF de un enlace 64 kbps es 1562.

show interface | show ip route | show ip ospf interface

### 11.3.1 METRICA DEL OSPF.-

### 11.3.2 MODIFICACION DEL COSTO DEL ENLACE.-

Cuando la interfaz serial no está funcionando realmente a la velocidad predeterminada de T1, la interfaz requiere una modificación manual. Ambos lados del enlace deben configurarse para tener el mismo valor. Tanto el comando de interfaz bandwidth como el comando de interfaz ip ospf cost logran este fin, un valor preciso que OSPF utilizará p ara determinar el mejor camino.

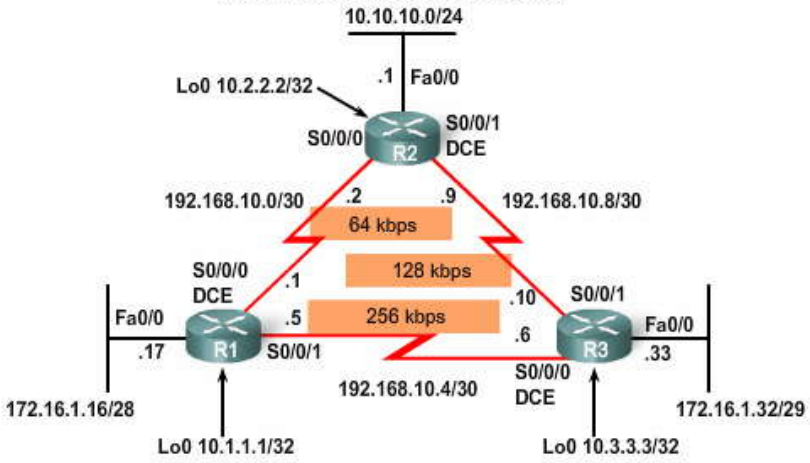
Comando bandwidth

El comando bandwidth se utiliza para modificar el valor del ancho de banda utilizado por IOS en el cálculo de la métrica de costo de OSPF. La sintaxis del comando interface es la misma sintaxis que aprendió en el Capítulo 9, "EIGRP":

Router(config-if)#bandwidth bandwidth-kbps

La figura muestra los comandos bandwidth utilizados para modificar los costos de todas las interfaces seriales de la topología. En el caso de R1, el comando show ip ospf interface muestra que el costo del enlace Serial 0/0/0 es ahora 1562, el resultado del cálculo de costo OSPF de Cisco de 100 000 000/64 000.

Topología con interfaces loopback




Comando bandwidth

```
R1(config)#inter serial 0/0/0
R1(config-if)#bandwidth 64
R1(config-if)#inter serial 0/0/1
R1(config-if)#bandwidth 256
R1(config-if)#end
R1#show ip ospf interface serial 0/0/0
Serial0/0 is up, line protocol is up
  Internet Address 192.168.10.1/30, Area 0
  Process ID 1, Router ID 10.1.1.1, Network Type POINT_TO_POINT, Cost: 1562
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  <output omitted>
```

$10^8 / 64{,}000 \text{ bps} = 1562$

```
R2(config)#inter serial 0/0/0
R2(config-if)#bandwidth 64
R2(config-if)#inter serial 0/0/1
R2(config-if)#bandwidth 128
```

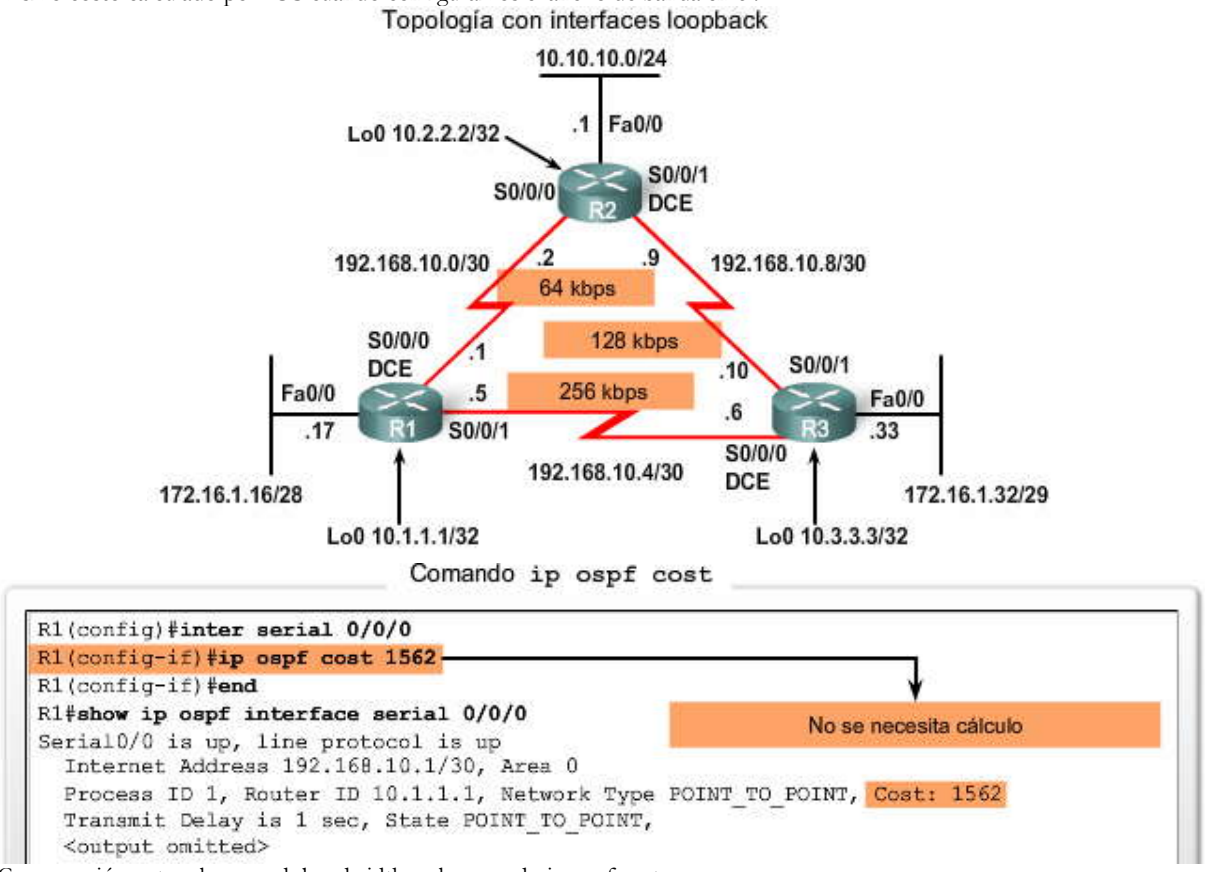
```
R3(config)#inter serial 0/0/0
R3(config-if)#bandwidth 256
R3(config-if)#inter serial 0/0/1
R3(config-if)#bandwidth 128
```

Comando ip ospf cost

Un método alternativo a la utilización del comando bandwidth es utilizar el comando ip ospf cost, que le permite especificar directamente el costo de una interfaz. Por ejemplo, en R1 podríamos configurar Serial 0/0/0 con el siguiente comando:

R1(config)#interface serial 0/0/0
R1(config-if)#ip ospf cost 1562

Ciertamente, esto no cambiará el resultado del comando show ip ospf interface, que aún muestra el costo de 1562. Éste es el mismo costo calculado por IOS cuando configuramos el ancho de banda en 64.



Comparación entre el comandobandwidth y el comando ip ospf cost

El comando ip ospf cost es útil en entornos de varios fabricantes, donde los routers que no son de Cisco utilizan una métrica diferente del ancho de banda para calcular los costos de OSPF. La principal diferencia entre los dos comandos es que el comando bandwidth utiliza el resultado del cálculo de costo para determinar el costo del enlace. El comando ip ospf cost evita este cálculo al establecer directamente el costo del enlace en un valor específico.

La figura muestra las dos alternativas que pueden utilizarse al modificar los costos de los enlaces seriales en la topología. El lado derecho de la figura muestra los comandos ip ospf cost equivalentes a los comandos bandwidth de la izquierda.

Comandos equivalentes

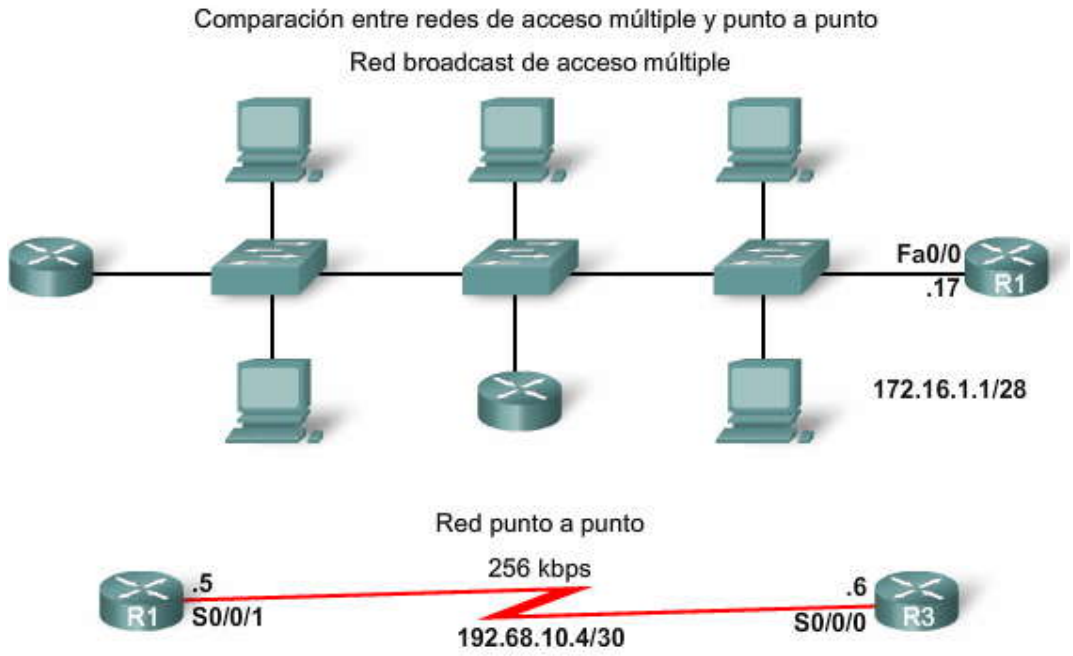
| Comandos **bandwidth** | | Comandos **ip ospf cost** |
|---|---|---|
| **Router R1**<br>R1(config)#**interface serial 0/0/0**<br>R1(config-if)#**bandwidth 64** | = | **Router R1**<br>R1(config)#**interface serial 0/0/0**<br>R1(config-if)#**ip ospf cost 1562** |
| R1(config)#**interface serial 0/0/1**<br>R1(config-if)#**bandwidth 256** | = | R1(config)#**interface serial 0/0/1**<br>R1(config-if)#**ip ospf cost 390** |
| **Router R2**<br>R2(config)#**interface serial 0/0/0**<br>R2(config-if)#**bandwidth 64** | = | **Router R2**<br>R2(config)#**interface serial 0/0/0**<br>R2(config-if)#**ip ospf cost 1562** |
| R2(config)#**interface serial 0/0/1**<br>R2(config-if)#**bandwidth 128** | = | R2(config)#**interface serial 0/0/1**<br>R2(config-if)#**ip ospf cost 781** |
| **Router R3**<br>R3(config)#**interface serial 0/0/0**<br>R3(config-if)#**bandwidth 256** | = | **Router R3**<br>R3(config)#**interface serial 0/0/0**<br>R3(config-if)#**ip ospf cost 390** |
| R3(config)#**interface serial 0/0/1**<br>R3(config-if)#**bandwidth 128** | = | R3(config)#**interface serial 0/0/0**<br>R3(config-if)#**ip ospf cost 781** |

## 11.4 OSPF Y REDES DE ACCESOS MULTIPLES.-

### 11.4.1 DESAFIOS EN REDES DE ACCESOS MULTIPLES.-

Una red de accesos múltiples es una red con más de dos dispositivos en los mismos medios compartidos. En el sector superior de la figura, la LAN Ethernet conectada a R1 se extiende para mostrar los posibles dispositivos que pueden conectarse a la red 172.16.1.16/28. Las LAN Ethernet son un ejemplo de una red broadcast de accesos múltiples. Son redes broadcast ya que todos los dispositivos de la red ven todas las tramas. Son redes de accesos múltiples ya que puede haber gran cantidad de hosts, impresoras, routers y demás dispositivos que formen parte de la misma red.

Por el contrario, en una red punto a punto sólo hay dos dispositivos en la red, uno en cada extremo. El enlace WAN entre R1 y R3 es un ejemplo de enlace punto a punto. El sector inferior de la figura muestra el enla ce punto a punto entre R1 y R3.




OSPF define cinco tipos de redes:

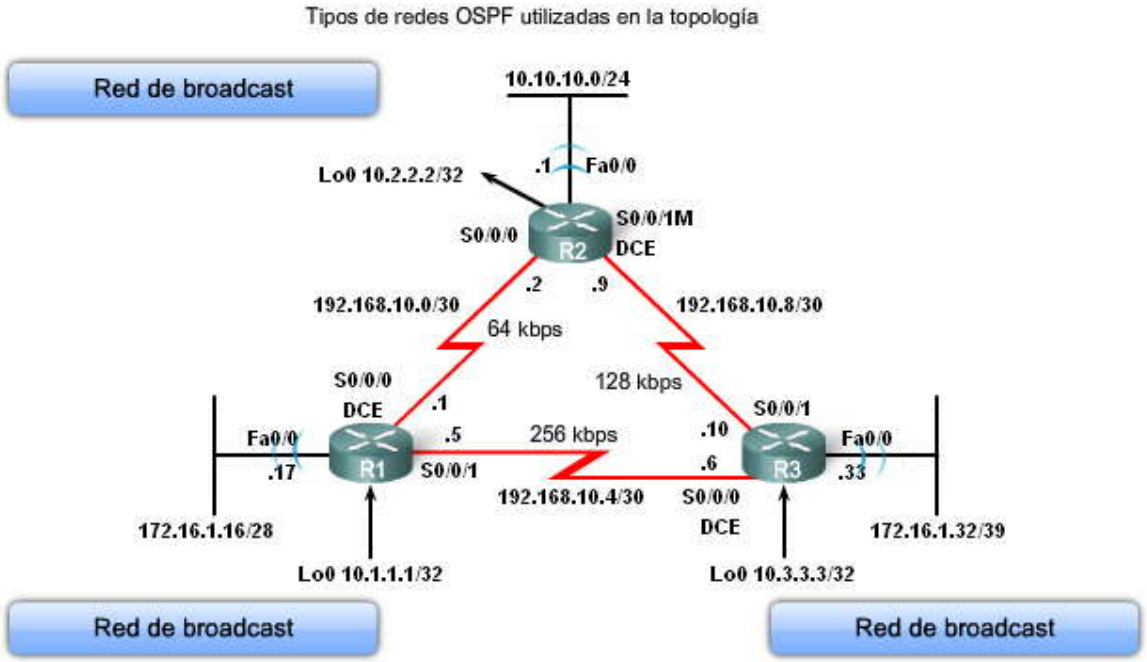
Punto a punto

Broadcast de accesos múltiples
Multiacceso sin broadcast (NBMA)
Punto a multipunto
Enlaces virtuales

Las redes NBMA y punto a multipunto incluyen redes Frame Relay, ATM y X.25. Las redes NBMA se analizan en otro curso de CCNA. Las redes punto a multipunto se analizan en CCNP. Los enlaces virtuales son un tipo especial de enlace que puede usarse en un OSPF de áreas múltiples. Los enlaces virtuales de OSPF se analizan en CCNP.

Haga clic en Reproducir para ver la animación.

La animación muestra que la topología utiliza redes punto a punto y broadcast.




Las redes de accesos múltiples pueden crear dos desafíos para OSPF en relación con la saturación de las LSA:

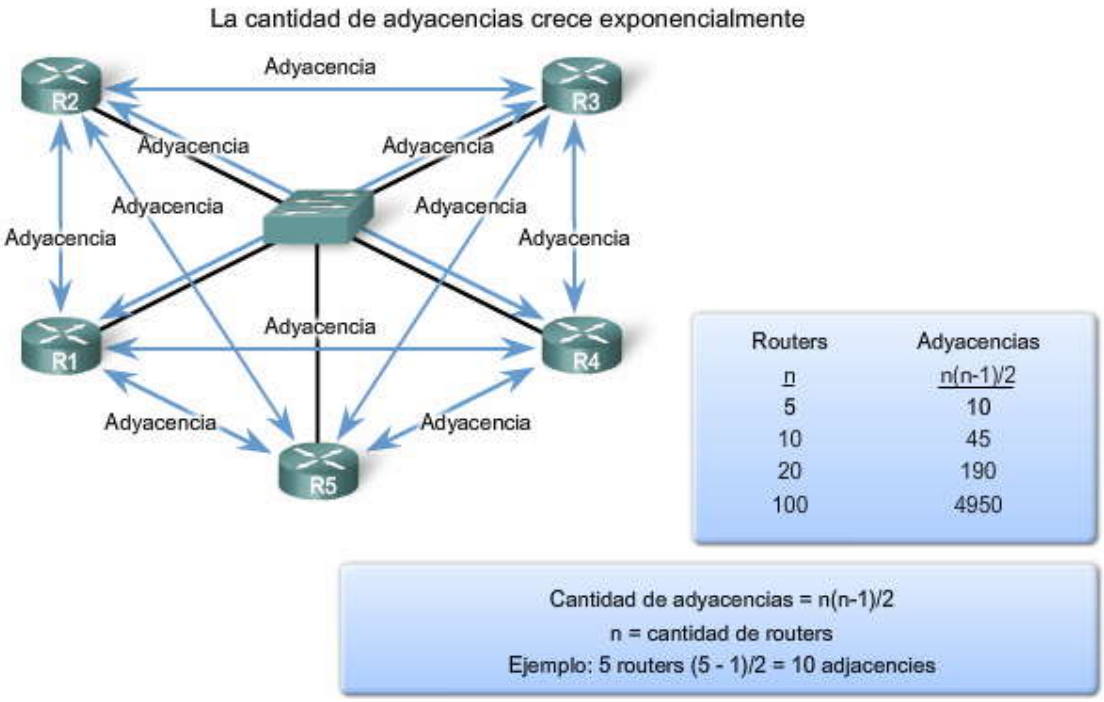
1. Creación de adyacencias múltiples, una adyacencia para cada par de routers.

2. Saturación extensa de las LSA (Notificaciones de estado de enlace).

**Adyacencias múltiples**

La creación de una adyacencia entre cada par de routers en una red creará una cantidad innecesaria de adyacencias. Esto llevará al paso de una cantidad excesiva de LSA entre routers de la misma red.

Para comprender el problema con las adyacencias múltiples, necesitamos estudiar una fórmula. Para cualquier cantidad de routers (designada como n) en una red de accesos múltiples, habrá n ( n - 1 ) / 2 adyacencias. La figura muestra una topología simple de cinco routers, los cuales están conectados a la misma red Ethernet de accesos múltiples. Sin ningún tipo de mecanismo para reducir la cantidad de adyacencias, estos routers en forma colectiva formarán 10 adyacencias: 5 ( 5 - 1 ) / 2 = 10. Si bien esto puede no parecer demasiado, a medida que se agregan routers a la red, la cantidad de adyacencias aumenta significativamente. Si bien los 5 routers de la figura sólo necesitarán 10 adyacencias, podrá ver que 10 routers requerirán 45 adyacencias. ¡Veinte routers requerirán 190 adyacencias!




**Saturación de las LSA**

Recuerde del Capitulo 10, "Protocolos de enrutamiento de estado de enlace", que los routers de estado de enlace saturan sus paquetes de estado de enlace al inicializarse OSPF o cuando hay un cambio en la topología.

**Haga clic en Reproducir para ver la animación de un escenario de saturación de LSA.**

En una red de accesos múltiples, esta saturación puede volverse excesiva. En la animación, R2 envía una LSA. Este evento hace que cada router también envíe una LSA. En la animación no se muestran los acuses de recibo requeridos enviados para cada LSA recibida. Si cada router en una red de accesos múltiples tuviera que saturar y reconocer todas las LSA recibidas a todos los demás routers en la misma red de accesos múltiples, el tráfico de la red se volvería bastante caótico.

Para ilustrar este punto, imagine que se encuentra en un cuarto con una gran cantidad de personas. ¿Qué sucedería si todos tuvieran que presentarse ante los demás en forma individual? Cada persona no sólo tendría que decir a los demás su nombre, sino que además cada vez que una persona aprenda el nombre de otra, ésta última tendría que decirlo a las demás personas que se encuentran en el cuarto, una persona por vez. Como podrá ver, ¡este proceso conduce al caos!

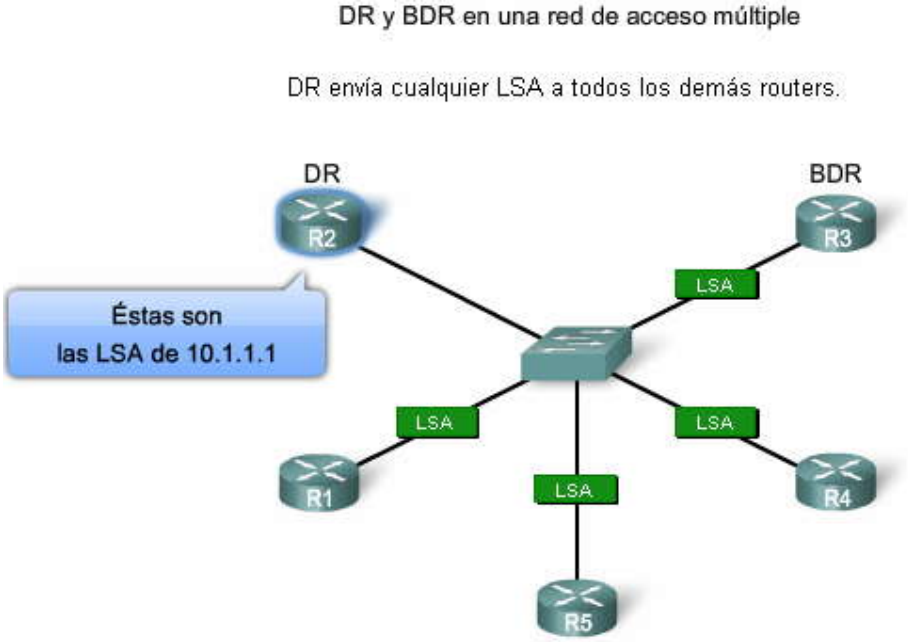

**Solución: Router designado**

La solución para administrar la cantidad de adyacencias y la saturación de las LSA en una red de accesos múltiples es el Router designado (DR). Continuando con nuestro ejemplo anterior, esta solución es igual a elegir a alguien del cuarto para que aprenda los nombres de todos y luego los pronuncie ante todos en el cuarto al mismo tiempo.

En las redes de accesos múltiples, OSPF elige un Router designado (DR) para que represente el punto de recolección y distribución de las LSA enviadas y recibidas. También se elige un Router designado de respaldo (BDR) en caso de que falle el Router designado. Todos los demás routers se convierten en DROthers (esto indica un router que no es DR ni BDR).

**Haga clic en Reproducir para ver la animación del rol del DR.**

Los routers de una red de accesos múltiples eligen un DR y un BDR. Los DROthers sólo forman adyacencias completas con el DR y el BDR en la red. Esto significa que en lugar de saturar las LSA a todos los routers en la red, los DROthers sólo envían sus LSA al DR y al BDR con la dirección multicast 24.0.0.6 (ALLDRouters - All DR routers). En la animación, R1 envía las LSA al DR. El BDR también escucha. El DR es responsable de reenviar todas las LSA desde R1 hasta todos los demás routers. El DR utiliza la dirección multicast 224.0.0.5 (AllSPFRouters - All OSPF routers). El resultado final es que sólo hay un router que realiza la saturación completa de todas las LSA en la red de accesos múltiples.



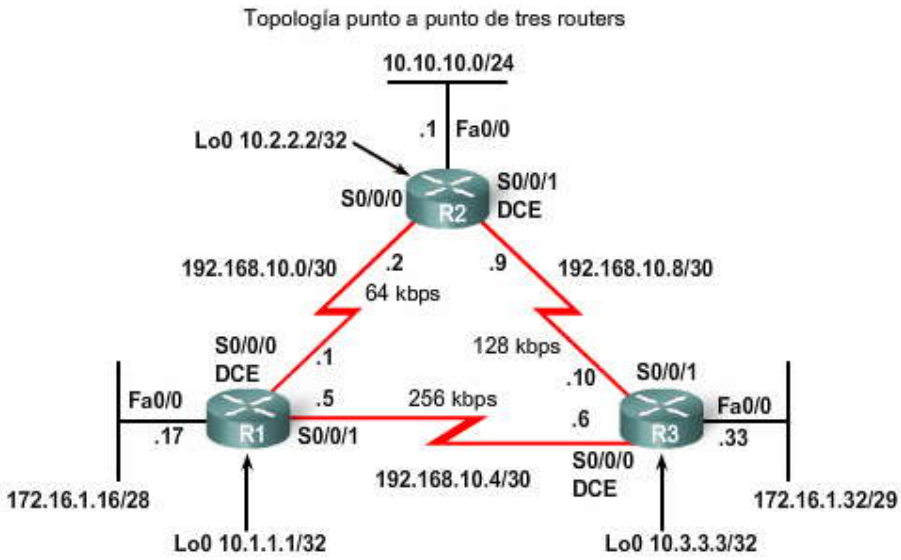

### 11.4.2 PROCESO DE ELECCION DE DR/BDR.-

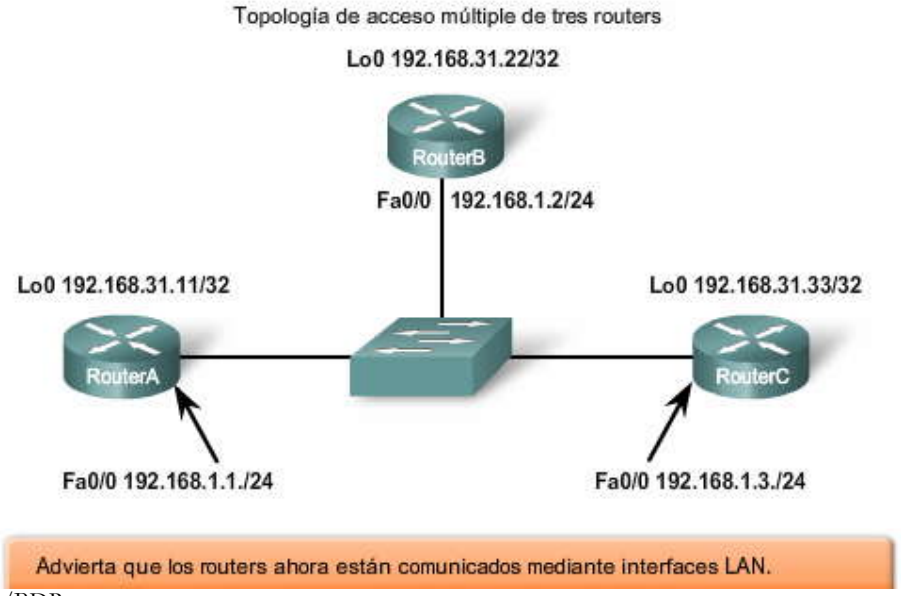
**Cambio de topología**

Las elecciones de DR/BDR no se presentan en las redes punto a punto. Por lo tanto, en una topología estándar de tres routers, R1, R2 y R3 no necesitan elegir un DR ni un BDR, ya que los enlaces entre estos routers no son redes de accesos múltiples.

**Haga clic en Topología de accesos múltiples en la figura.**

Para el resto de la discusión del DR y BDR, utilizaremos la topología de accesos múltiples que muestra la figura. Los nombres de los routers son diferentes, únicamente para enfatizar que esta topología no es la misma topología de tres routers que hemos utilizado hasta aquí. Regresaremos a nuestra topología del capítulo luego de la discusión sobre el proceso de elección de DR/BDR. En esta nueva topología, tenemos tres routers que comparten una red Ethernet de accesos múltiples común, 192.168.1.0/24. Cada router está configurado con una dirección IP en la interfaz Fast Ethernet y una dirección de loopback para la ID del router.




Advierta que los routers ahora están comunicados mediante interfaces LAN.

Elección de DR/BDR

¿Cómo se eligen el DR y el BDR? Se aplican los siguientes criterios:

1. DR: Router con la prioridad más alta de interfaz OSPF.

2. BDR: Router con la segunda prioridad más alta de interfaz OSPF.

3. Si las prioridades de la interfaz OSPF son iguales, la ID del router más alta se utiliza para desempatar.

En este ejemplo, la prioridad de interfaz OSPF predeterminada es 1. Como consecuencia, en base a los criterios de selección enumerados anteriormente, la ID del router OSPF se utiliza para elegir el DR y el BDR. Como podrá ver, el RouterC se convierte en el DR y el RouterB, con la segunda ID del router más alta, se convierte en el BDR. Debido a que el RouterA no se elige como DR ni BDR, se convierte en DROther.

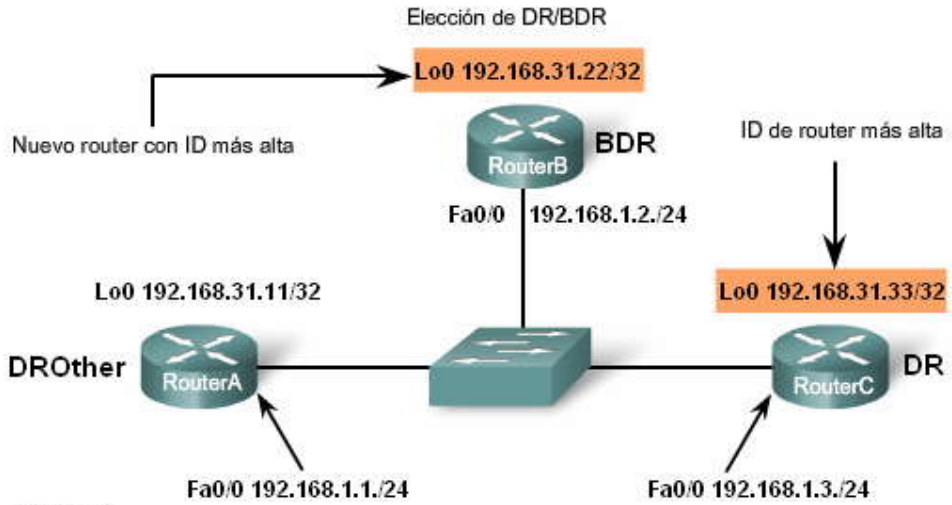
Los DROthers sólo forman adyacencias FULL con el DR y el BDR; sin embargo, aún forman una adyacencia de vecinos con cualquier DROther que se una a la red. Esto significa que todos los routers DROther en la red de accesos múltiples aún reciben paquetes de saludo por parte de todos los demás routers DROther. De esta manera, éstos conocen a todos los routers de la red. Cuando dos routers DROther forman una adyacencia de vecinos, el estado de vecino se muestra como 2WAY. Los diferentes estados de vecino se analizan en CCNP.

Haga clic en show ip ospf neighbor en la figura.

El resultado del comando en la figura muestra la adyacencia de vecinos de cada router en la red de accesos múltiples. Observe en el caso del RouterA que éste muestra que DR es el RouterC con la ID de router 192.168.31.33 y que BDR es el RouterB con la ID de router 192.168.31.22.

Haga clic en show ip ospf interface en la figura.

Debido a que el RouterA muestra a sus vecinos como DR y BDR, el RouterA es un DROther. Esto puede verificarse con el comando show ip ospf interface fastethernet 0/0 en el RouterA, como se muestra en la figura. Este comando mostrará el estado DR, BDR o DROTHER de este router, junto con la ID del router de DR y BDR en esta red de accesos múltiples.




Elección de DR/BDR

```
RouterA#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.31.33     1   FULL/DR         00:00:39    192.168.1.3     FastEthernet0/0
192.168.31.22     1   FULL/BDR        00:00:36    192.168.1.2     FastEthernet0/0
```

```
RouterB#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.31.33     1   FULL/DR         00:00:34    192.168.1.3     FastEthernet0/0
192.168.31.11     1   FULL/DROTHER    00:00:38    192.168.1.1     FastEthernet0/0
```

```
RouterC#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.31.22     1   FULL/BDR        00:00:35    192.168.1.2     FastEthernet0
192.168.31.11     1   FULL/DROTHER    00:00:32    192.168.1.1     FastEthernet0
```

La prioridad es igual en el valor por defecto de 1.

Elección de DR/BDR

```
RouterA#show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  Backup Designated router (ID) 192.168.31.22, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.31.22  (Backup Designated Router)
    Adjacent with neighbor 192.168.31.33  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

**Elección de temporización de DR/BDR**

El proceso de elección de DR y BDR se lleva a cabo tan pronto como el primer router con una interfaz OSPF habilitada se activa en la red de accesos múltiples. Esto puede suceder cuando se encienden los routers o cuando se configura el comando network de OSPF para dicha interfaz. El proceso de elección sólo toma unos pocos segundos. Si todos los routers de la red de accesos múltiples no finalizaron el inicio, es posible que un router con una ID de router más baja se convierta en DR. Podría ser un router de extremo inferior que tarde menos tiempo en iniciar.

Cuando se elige el DR, éste continúa como DR hasta que se presente alguna de las siguientes condiciones:

El DR falla.
El proceso OSPF en el DR falla.
La interfaz de accesos múltiples en el DR falla.

En la figura, una X roja indica una o más de dichas fallas.

Haga clic en Falla de DR en la figura.

Si DR falla, BDR asume el rol de DR y se lleva a cabo una elección para seleccionar un nuevo BDR. En la figura, el RouterC falla y el anterior BDR, el RouterB, se convierte en DR. El único otro router disponible para convertirse en BDR es el RouterA.

Haga clic en Nuevo router en la figura.

RouterD se une a la red. Si un nuevo router ingresa en la red después de que se hayan elegido el DR y el BDR, éste no se convertirá en DR ni en BDR, aunque cuente con una prioridad de interfaz OSPF o una ID del router mayor que la del DR o BDR actual. El nuevo router puede elegirse como el BDR si falla el DR o BDR actual. Si el DR actual falla, el BDR se convertirá en el DR, y el nuevo router puede elegirse como el BDR. Luego de que el nuevo router se convierte en BDR, si el DR falla, el nuevo router router se convertirá en DR. El DR y BDR actuales deben fallar antes de que el nuevo router pueda elegirse como DR o BDR.

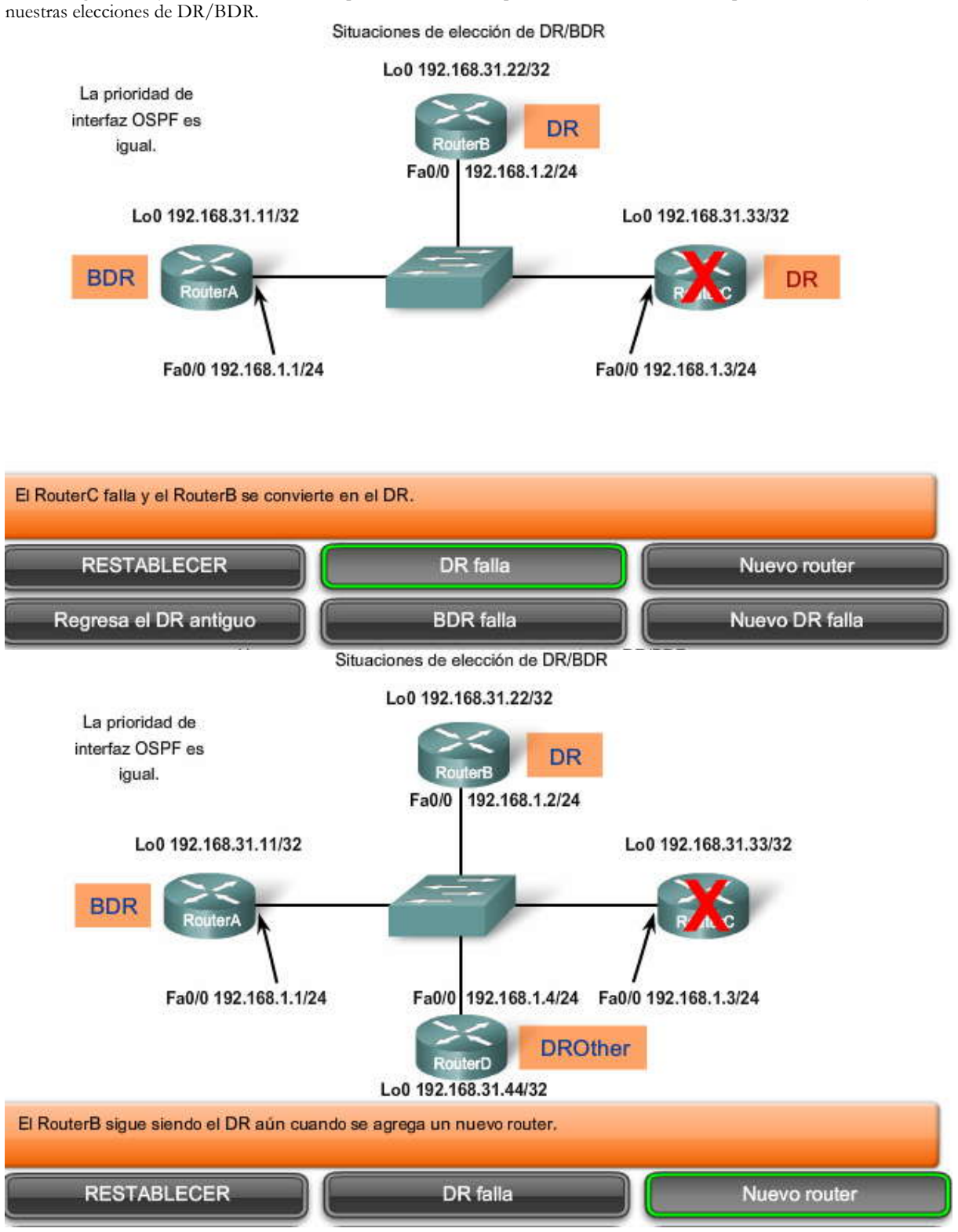
Haga clic en Regreso del antiguo DR en la figura.

Un DR antiguo no recupera el estado de DR si regresa a la red. En la figura, el RouterC se reinició y se convierte en DROther a pesar de que su ID de router, 192.168.31.33, es mayor que la del DR y del BDR actuales.

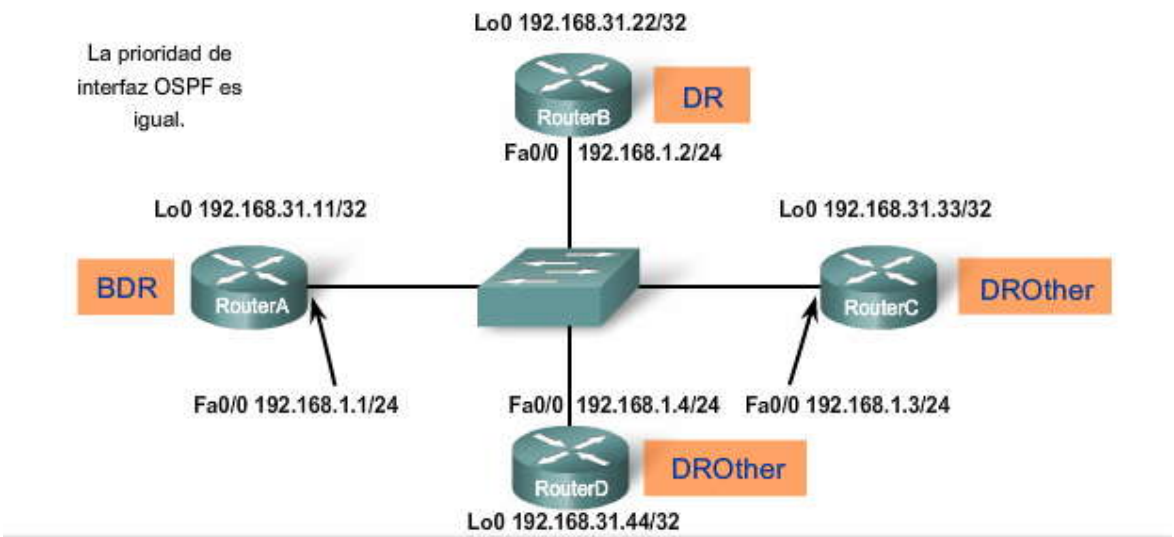
Haga clic en Falla de BDR en la figura.

Si BDR falla, se lleva a cabo una elección entre los DRothers para ver cuál router será el nuevo BDR. En la figura, el router BDR falla. Se lleva a cabo una elección entre el RouterC y el RouterD. El RouterD gana la elección con una ID de router más alta.

Haga clic en Falla del nuevo DR en la figura.
En la figura, RouterB falla. Debido a que el RouterD es el BDR actual, éste cambia a DR. El RouterC se convierte en BDR. Por lo tanto, ¿cómo se asegura el usuario de que los routers que desea que sean DR y BDR ganen la elección? Sin una configuración adicional, la solución es:
Primero inicie el DR, luego el BDR y luego el resto de los routers, o
Desconecte la interfaz de todos los routers, luego no shutdown en el DR, el BDR y luego el resto de los routers.
Sin embargo, como ya debe haber deducido, podemos cambiar la prioridad de la interfaz OSPF para controlar mejor nuestras elecciones de DR/BDR.



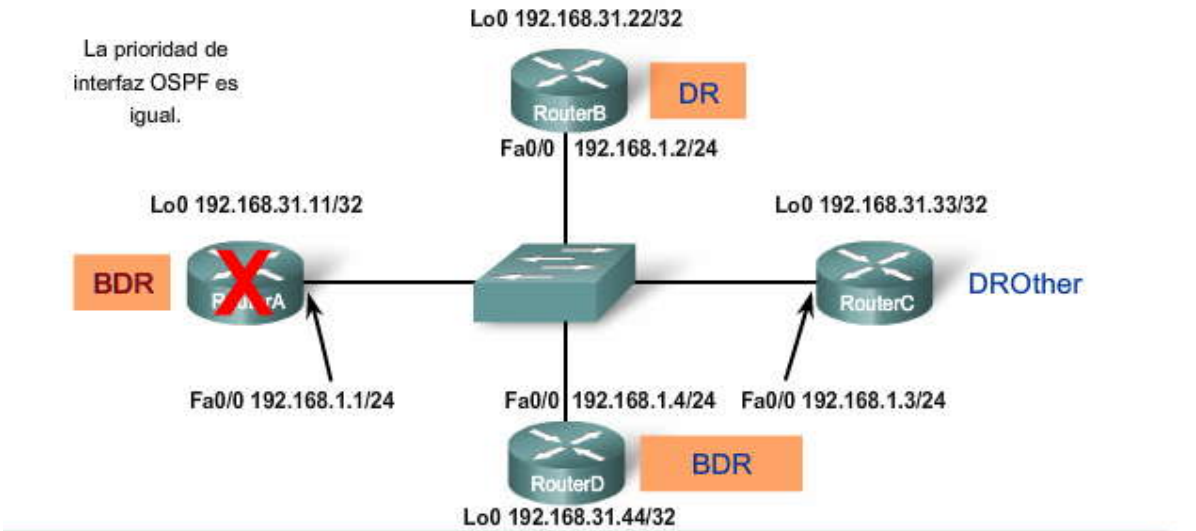
Situaciones de elección de DR/BDR




El RouterB sigue siendo el DR aún cuando el DR anterior regresa.

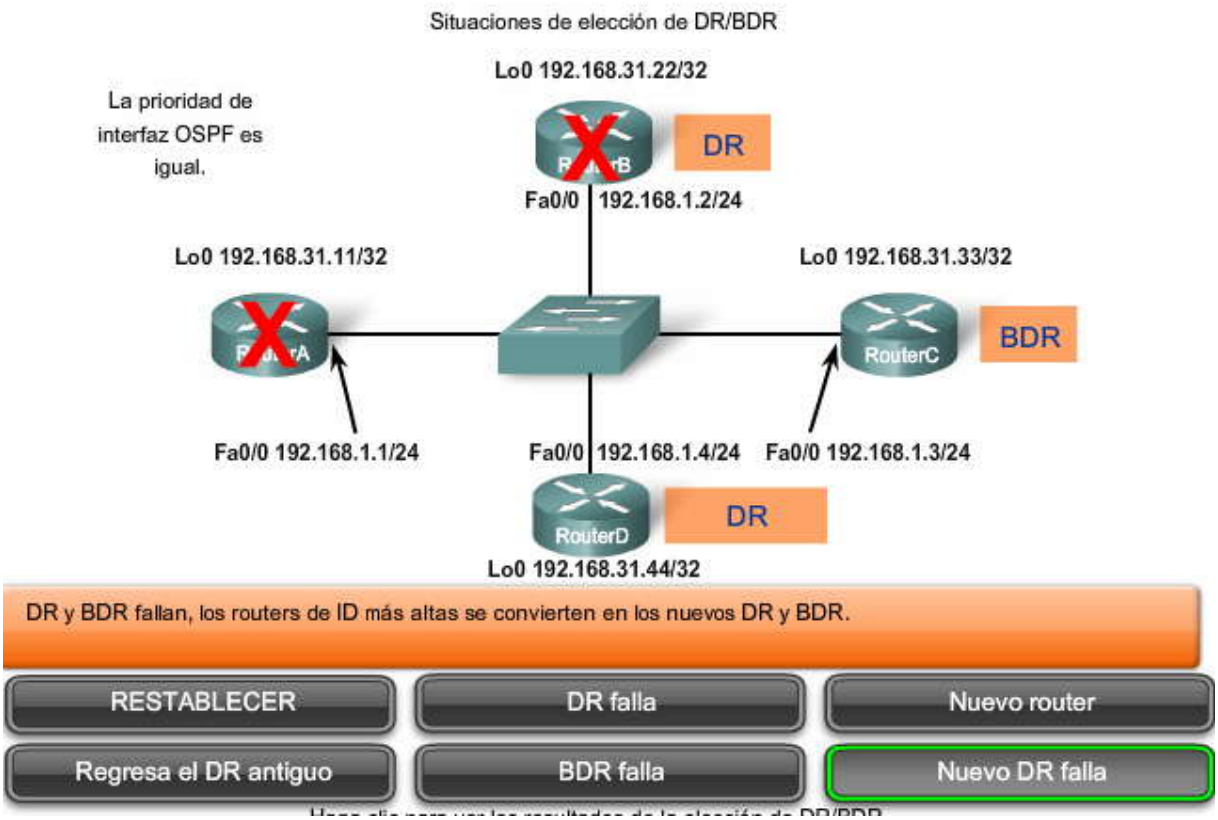
| | | |
|---|---|---|
| RESTABLECER | DR falla | Nuevo router |
| Regresa el DR antiguo | BDR falla | Nuevo DR falla |

Situaciones de elección de DR/BDR




BDR falla, el router de ID más alta entre DROthers se convierte en el nuevo BDR.

| | | |
|---|---|---|
| RESTABLECER | DR falla | Nuevo router |
| Regresa el DR antiguo | BDR falla | Nuevo DR falla |




### 11.4.3 PRIORIDAD DE INTERFAZ OSPF.-

Debido a que DR se convierte en el punto central de recolección y distribución de las LSA, es importante que este router tenga suficiente capacidad de memoria y CPU para cumplir con la responsabilidad. En vez de confiar en la ID del router para decidir cuáles routers se elegirán como DR y BDR, es mejor controlar la elección de dichos routers con el comando ip ospf priority interface.

Router(config-if)#ip ospf priority {0 - 255}

En nuestra discusión anterior, la prioridad OSPF era igual. Esto se debe a que, de manera predeterminada, el valor de prioridad es 1 para todas las interfaces del router. Por lo tanto, la ID del router determina el DR y el BDR. Sin embargo, si cambia el valor predeterminado de 1 por un valor mayor, el router con la prioridad más alta se convertirá en DR y el router con la segunda prioridad más alta se convertirá en BDR. Un valor de 0 hace que el router no sea elegible para convertirse en DR ni en BDR.

Debido a que las prioridades son un valor específico según la interfaz, suministran un mejor control de las redes de accesos múltiples de OSPF. También permiten a un a router ser DR en una red y DROther en otra.

Haga clic enshow ip ospf interface en la figura.

Para simplificar nuestro análisis, retiramos el RouterD de la topología. La prioridad de interfaz OSPF puede verse a través del comando show ip ospf interface. En la figura, podemos verificar que la prioridad en el RouterA se encuentra en el valor predeterminado de 1.

Haga clic en Modificar prioridad en la figura.

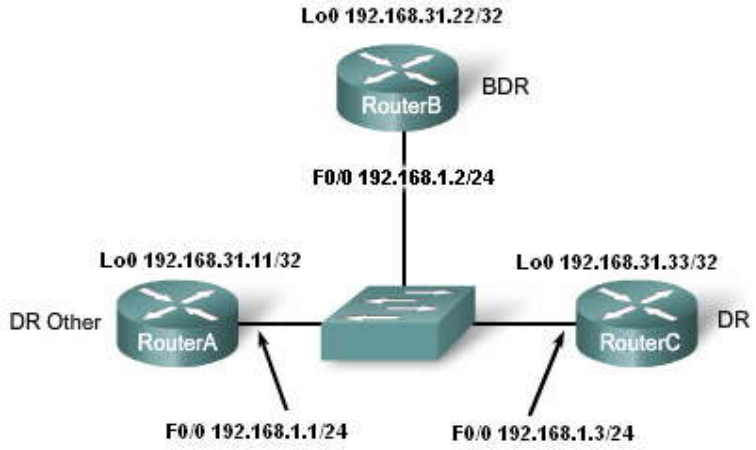
La figura muestra las prioridades de interfaz OSPF del RouterA y el RouterB modificadas para que el RouterA con la prioridad más alta se convierta en DR y el RouterB se convierta en BDR. La prioridad de interfaz OSPF del Ro uterC continúa en el valor predeterminado 1.

Haga clic en Forzar elección en la figura.

Después de ejecutar shutdown y no shutdown en las interfaces FastEthernet 0/0 de los tres routers, vemos el resultado del cambio de las prioridades de interfaz OSPF. El comando show ip ospf neighbor en el RouterC ahora muestra que el RouterA (ID del router 192.168.31.11) es el DR con la prioridad más alta de interfaz OSPF de 200 y el RouterB (ID del

router 192.168.31.22) es aún el BDR, con la segunda prioridad más alta de interfaz OSPF de 100. Observe que el resultado show ip ospf neighbor del RouterA no muestra un DR, ya que el RouterA es el DR real en esta red.

Topología de acceso múltiple




Cambio de prioridad de interfaz OSPF

```
RouterA#show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.31.33, Interface address 192.168.1.3
  Backup Designated router (ID) 192.168.31.22, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.31.22  (Backup Designated Router)
    Adjacent with neighbor 192.168.31.33  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

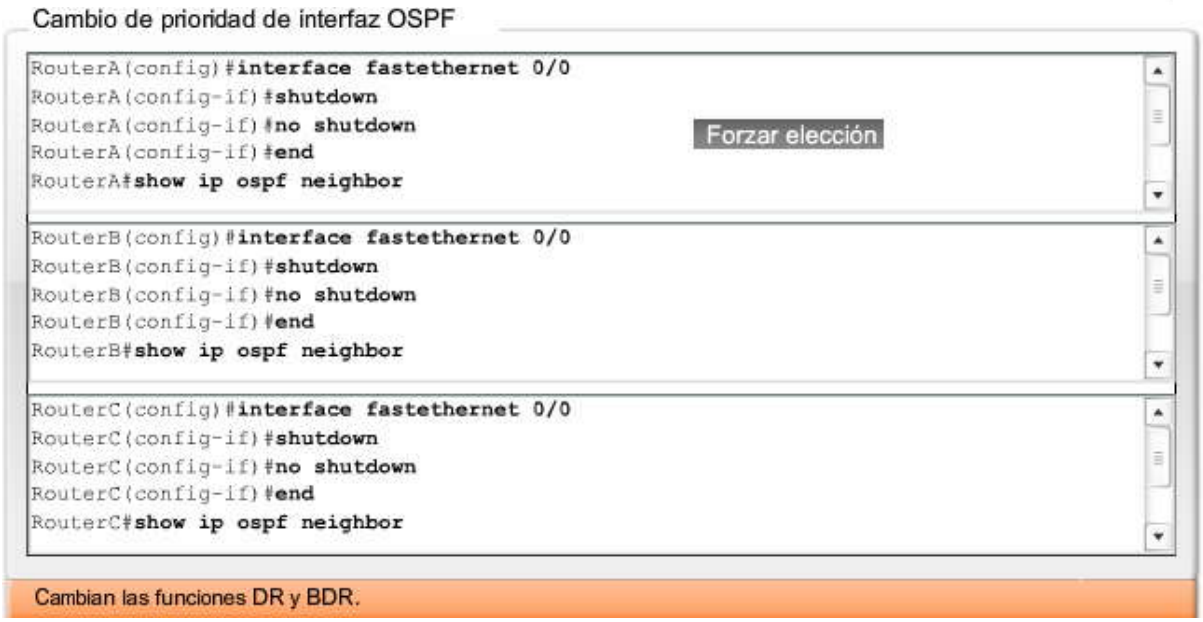
Actualmente todos los routers tienen la prioridad de interfaz OSPF por defecto de 1.

Cambio de prioridad de interfaz OSPF

```
RouterA(config)#interface fastethernet 0/0
RouterA(config-if)#ip ospf priority 200
```

Modificar prioridad

```
RouterB(config)#interface fastethernet 0/0
RouterB(config-if)#ip ospf priority 100
```




**11.5 MAS CONFIGURACION DEL OSPF.-**

**11.5.1 RESTRIBUCION DE UNA RUTA OSPF POR DEFECTO.-**

Topología

Regresemos a la topología anterior, que ahora incluye un nuevo enlace a ISP. Al igual que con RIP y EIGRP, el router conectado a Internet se utiliza para propagar una ruta por defecto a otros routers en el dominio de enrutamiento OSPF. A este router se lo denomina en ocasiones router de borde, entrada o gateway. Sin embargo, en la terminología OSPF, el router ubicado entre un dominio de enrutamiento OSPF y una red que no es OSPF se denomina Autonomous System Boundary Router (ASBR). En esta topología, Loopback1 (Lo1) representa un enlace a una red que no es OSPF. No configuraremos la red 172.30.1.1/30 como parte del proceso de enrutamiento OSPF.

Haga clic en Configuración estática predeterminada de R1 en la figura.

La figura muestra el ASBR (R1) configurado con la dirección IP de Loopback1 y el reenvío de tráfico de la ruta estática por defecto al router ISP:

R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1

Nota: La ruta estática por defecto utiliza el loopback como una interfaz de salida ya que el router ISP en esta topología no existe físicamente. Al utilizar una interfaz loopback, podemos simular la conexión a otro router.

Al igual que RIP, OSPF requiere el uso del comando default-information originate para publicar la 0.0.0.0/0 ruta estática por defecto a los demás routers del área. Si no se utiliza el comando default-information originate, la ruta por defecto "quad-zero" no se propagará a los demás routers del área OSPF.

La sintaxis del comando es:

R1(config-router)#default-information originate

Haga clic en R1, R2 y R3 en la figura.

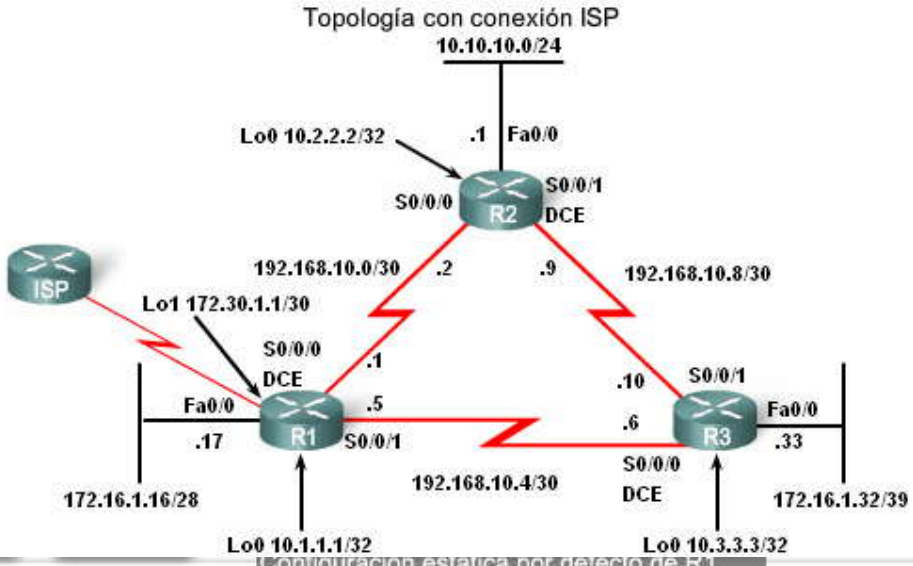
R1, R2 y R3 ahora presentan un "gateway de último recurso" establecido en la tabla de enrutamiento. Observe la ruta por defecto en R2 y R3 con el OSPF de origen de enrutamiento, pero con el código adicional, E2. Para R2, la ruta es:

O*E2 0.0.0.0/0 [110/1] via 192.168.10.10, 00:05:34, Serial0/0/1

E2 denota que esta ruta es una ruta OSPF externa Tipo 2.

Las rutas OSPF externas se encuentran en una de las dos siguientes categorías: External Type 1 (Externa Tipo 1, E1) o External Type 2 (Externa Tipo 2, E2). La diferencia entre las dos radica en el modo en que se calcula el costo de OSPF de la ruta en cada router. OSPF acumula costo para una ruta E1, ya que la ruta se propaga a través del área OSPF. Este proceso es idéntico a los cálculos de costo para las rutas internas normales de OSPF. Sin embargo, el costo de una ruta E2 es

siempre el costo externo, independientemente del costo interior para alcanzar dicha ruta. En esta topología, debido a que la ruta por defecto tiene un costo externo de 1 en el router R1, R2 y R3 también muestran un costo de 1 para la ruta por defecto E2. Las rutas E2 con un costo de 1 constituyen la configuración OSPF predeterminada. El cambio de dichos valores predeterminados, así como la información adicional acerca de las rutas externas, se analiza en CCNP.




Configuración estática por defecto de R1

```
R1(config)#interface loopback 1
R1(config-if)#ip add 172.30.1.1 255.255.255.252
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 1
R1(config)#router ospf 1
R1(config-router)#default-information originate
```

```
R1#show ip route
Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/1171] via 192.168.10.6, 00:00:58, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/391] via 192.168.10.6, 00:00:58, Serial0/0/1
C       172.16.1.16/28 is directly connected, FastEthernet0/0
     172.30.0.0/30 is subnetted, 1 subnets
C       172.30.1.0 is directly connected, Loopback1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.10.10.0/24 [110/1172] via 192.168.10.6, 00:00:58, Serial0/0/1
C       10.1.1.1/32 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Loopback1
```

R1

```
R2#show ip route
Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 192.168.10.10 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
O       192.168.10.4 [110/1171] via 192.168.10.10, 00:00:25, Serial0/0/1
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/782] via 192.168.10.10, 00:00:25, Serial0/0/1
O       172.16.1.16/28 [110/1172] via 192.168.10.10, 00:00:25, Serial0/0/1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.2.2.2/32 is directly connected, Loopback0
C       10.10.10.0/24 is directly connected, FastEthernet0/0
O*E2     0.0.0.0/0 [110/1] via 192.168.10.10, 00:00:13, Serial0/0/1
```

R2

```
R3#show ip route
Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 192.168.10.10 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
O       192.168.10.0 [110/1952] via 192.168.10.5, 00:00:38, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/0
C       192.168.10.8 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.32/29 is directly connected, FastEthernet0/0
O       172.16.1.16/28 [110/391] via 192.168.10.5, 00:00:38, Serial0/0/0
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.3.3.3/32 is directly connected, Loopback0
O       10.10.10.0/24 [110/782] via 192.168.10.9, 00:00:38, Serial0/0/1
O*E2     0.0.0.0/0 [110/1] via 192.168.10.5, 00:00:27, Serial0/0/0
```

R3

**11.5.2 AJUSTE DE OSPF.-**

Ancho de banda de referencia

Como debe recordar, el costo OSPF de Cisco utiliza el ancho de banda acumulado. El valor del ancho de banda de cada interfaz se calcula con 100 000 000/ancho de banda. Al ancho de banda de referencia se lo conoce como 100 000 000 ó 10 a la octava potencia.

Por lo tanto, 100 000 000 es el ancho de banda predeterminado de referencia cuando el ancho de banda real se convierte en una métrica de costo. Como se vio en estudios anteriores, ahora contamos con velocidades de enlace mucho más rápidas que las velocidades de Fast Ethernet, que incluyen Gigabit Ethernet y 10GigE. Al utilizar un ancho de banda de referencia de 100 000 000 se obtienen interfaces con valores de ancho de banda de 100 Mbps y mayores con el mismo costo OSPF de 1.

Para obtener cálculos de costo más precisos, puede ser necesario ajustar el valor del ancho de banda de referencia. El ancho de banda de referencia puede modificarse para adaptarse a dichos enlaces más rápidos mediante un comando OSPF auto-cost reference-bandwidth. Cuando este comando sea necesario, úselo en todos los routers para que la métrica de enrutamiento de OSPF se mantenga uniforme.

R1(config-router)#auto-cost reference-bandwidth ?
1-4294967 El ancho de banda de referencia en términos de Mbits por segundo

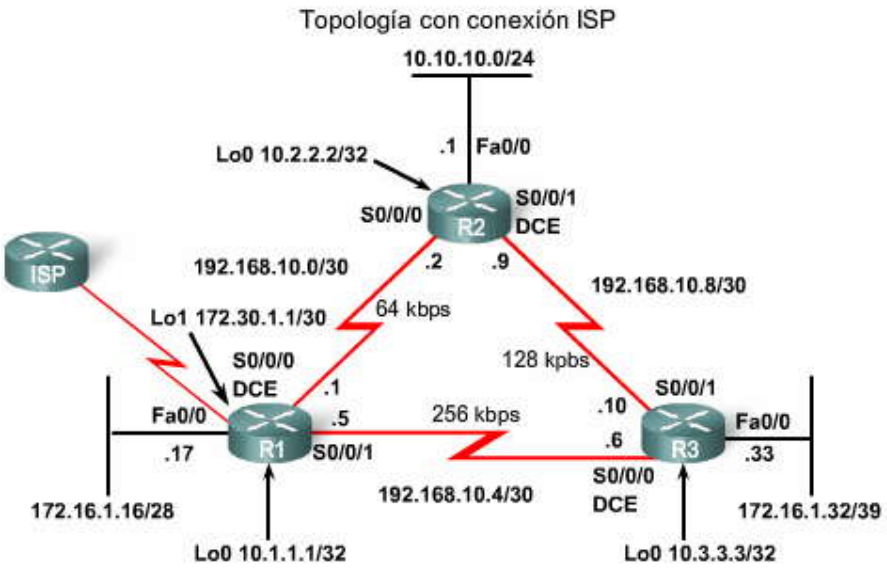
Observe que el valor se expresa en Mbps. Por lo tanto, el valor predeterminado es equivalente a 100. Para aumentarlo a velocidades de 10GigE, necesitará cambiar el ancho de banda de referencia a 10000.

R1(config-router)#auto-cost reference-bandwidth 10000

Nuevamente, asegúrese de configurar este comando en todos los routers en el dominio de enrutamiento OSPF. IOS también puede recordárselo, como se muestra en la figura.

Haga clic en R1 antes y R1 después en la figura.

La tabla de enrutamiento de R1 muestra el cambio en la métrica de costo de OSPF. Observe que los valores presentan valores de costo mucho mayores para las rutas OSPF. Por ejemplo, en R1 antes, el costo para 10.10.10.0/24 es 1172. Después de configurar un nuevo ancho de banda de referencia, el costo para la misma ruta es ahora 65635.




Cambio del ancho de banda de referencia

```
R1(config-if)#router ospf 1
R1(config-router)#auto-cost reference-bandwidth ?
  <1-4294967>  The reference bandwidth in terms of Mbits per second

R1(config-router)#auto-cost reference-bandwidth  10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers
```

```
R2(config-if)#router ospf 1
R2(config-router)#auto-cost reference-bandwidth  10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

```
R3(config-if)#router ospf 1
R3(config-router)#auto-cost reference-bandwidth  10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
```

```
R1#show ip route
Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [110/1171] via 192.168.10.6, 00:00:58, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/391] via 192.168.10.6, 00:00:58, Serial0/0/1
C       172.16.1.16/28 is directly connected, FastEthernet0/0
     172.30.0.0/30 is subnetted, 1 subnets
C       172.30.1.0 is directly connected, Loopback1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.10.10.0/24 [110/1172] via 192.168.10.6, 00:00:58, Serial0/0/1
C       10.1.1.1/32 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Loopback1
```

R1 antes

```
R1#show ip route
Codes: <some code output omitted>
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     192.168.10.0/30 is subnetted, 3 subnets
C       192.168.10.0 is directly connected, Serial0/0/0
C       192.168.10.4 is directly connected, Serial0/0/1
O       192.168.10.8 [100/117187] via 192.168.10.6, 00:01:33, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
O       172.16.1.32/29 [110/39162] via 192.168.10.6, 00:01:33, Serial0/0/1
C       172.16.1.16/28 is directly connected, FastEthernet0/0
     172.30.0.0/30 is subnetted, 1 subnets
C       172.30.1.0 is directly connected, Loopback1
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O       10.10.10.0/24 [110/117287] via 192.168.10.6, 00:01:33, Serial0/0/0
C       10.1.1.1/32 is directly connected, Loopback0
S*   0.0.0.0/0 is directly connected, Loopback1
```

R1 después

Modificación de intervalos OSPF
Haga clic en Vecinos de R1 1 en la figura.

El comando show ip ospf neighbor en R1 verifica que R1 sea adyacente a R2 y R3. Observe en el resultado que el Tiempo muerto cuenta regresivamente a partir de los 40 segundos. De manera predeterminada, este valor se actualiza cada 10 segundos cuando R1 recibe un saludo del vecino.

Puede ser aconsejable cambiar los temporizadores OSPF para que los routers detecten las fallas de red en menor tiempo. Si bien al hacerlo se aumentará el tráfico, en ocasiones se necesita una convergencia rápida que compense el tráfico adicional.

Los intervalos muertos y de saludo de OSPF pueden modificarse manualmente con los siguientes comandos de interfaz:

Router(config-if)#ip ospf hello-intervalseconds
Router(config-if)#ip ospf dead-intervalseconds

Haga clic en Modificar temporizadores de R1 en la figura.

La figura muestra los intervalos muerto y de saludo modificados a 5 y 20 segundos, respectivamente, en la interfaz Serial 0/0/0 para R1. Inmediatamente después de cambiar el intervalo de saludo, el IOS de Cisco modifica automáticamente el intervalo muerto a un valor equivalente a cuatro veces el intervalo de saludo. Sin embargo, siempre es aconsejable modificar explícitamente el temporizador en lugar de depender de la función automática de IOS para que las modificaciones se documenten en la configuración.

Después de 20 segundos, expira el Temporizador muerto en R1. R1 y R2 pierden adyacencia. Sólo modificamos los valores en un lado del enlace serial entre R1 y R2.

%OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down: El te mporizador muerto expiró

Haga clic en Vecinos de R1 2 en la figura.

Recuerde, los intervalos muerto y de saludo de OSPF deben ser equivalentes entre vecinos. Puede verificar la pérdida de adyacencia con el comando show ip ospf neighbor en R1. Observe que el vecino 10.2.2.2 ya no se encuentra presente. Sin embargo, 10.3.3.3 o R3 aún es un vecino. Los temporizadores establecidos en Serial 0/0/0 no afectan la adyacencia de vecinos con R3.

Haga clic en Temporizadores de R2 en la figura.

Los intervalos muerto y de saludo incompatibles pueden verificarse en R2 con el comando show ip ospf interface serial 0/0/0. Los valores de intervalos en R2, ID del router 10.2.2.2, aún están establecidos con un intervalo de saludo de 10 segundos y un intervalo muerto de 40 segundos.

Haga clic en Modificar temporizadores de R2 en la figura.

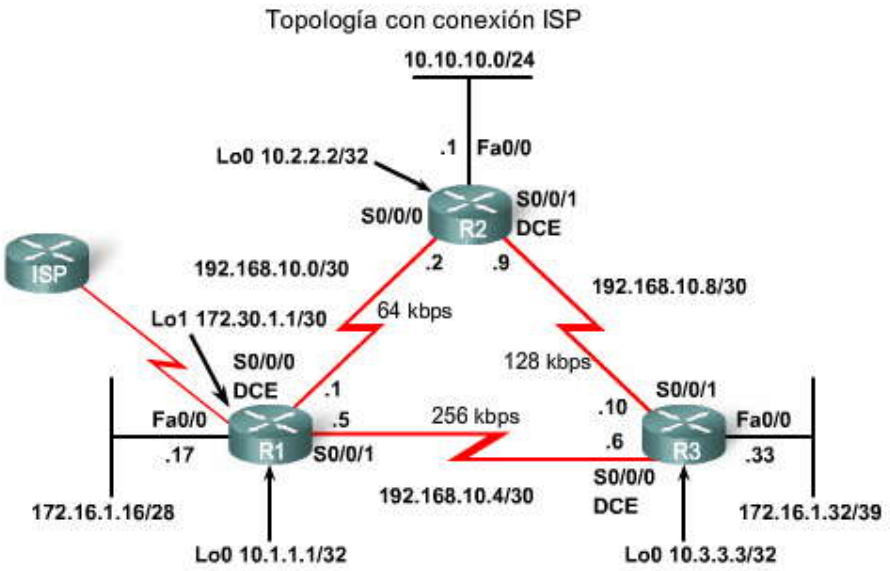
Para restaurar la adyacencia entre R1 y R2, modifique los intervalos muerto y de saludo en la interfaz Serial 0/0/0 en R2 para hacer coincidir los intervalos de la interfaz Serial 0/0/0 en R1. IOS muestra un mensaje que indica que se estableció la adyacencia con un estado FULL.

14:22:27: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0 from LOADING to FULL, Loading Done

Haga clic en Vecinos de R1 3 en la figura.

Verifique que se restaure la adyacencia de vecinos con el comando show ip ospf neighbor en R1. Observe que el Tiempo muerto para Serial 0/0/0 es ahora muy inferior, ya que cuenta regresivamente a partir de los 20 segundos en lugar de los 40 segundos predeterminados. Serial 0/0/1 aún funciona con los temporizadores predeterminados.

Nota: OSPF requiere que los intervalos muerto y de saludo coincidan entre dos routers para que sean adyacentes. Esto es distinto de EIGRP, donde los temporizadores de saludo y de espera no necesita n coincidir para que dos routers formen una adyacencia EIGRP.



## Modificación de temporizadores

R1 Vecinos 1

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          0   FULL/  -        00:00:35    192.168.10.6    Serial0/0/1
10.2.2.2          0   FULL/  -        00:00:36    192.168.10.2    Serial0/0/0
```

## Modificación de temporizadores

Modificar temporizadores R1

```
R1(config)#interface serial 0/0/0
R1(config-if)#ip ospf hello-interval 5
R1(config-if)#ip ospf dead-interval 20
R1(config-if)#end

<Wait 20 seconds for IOS message>

%OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Dead timer expired
```

## Modificación de temporizadores

R1 Vecinos 2

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          0   FULL/  -        00:00:35    192.168.10.6    Serial0/0/1
```

## Modificación de temporizadores

Temporizadores R2

```
R2#show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 192.168.10.2/30, Area 0
  Process ID 1, Router ID 10.2.2.2, Network Type POINT_TO_POINT, Cost: 65535
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:09
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

## Modificación de temporizadores

Modificar temporizadores R2

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip ospf hello-interval 5
R2(config-if)#ip ospf dead-interval 20
R2(config-if)#end
%OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading
Done
```

## Modificación de temporizadores

R1 Vecinos 3

```
R1#show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.3.3.3          0   FULL/  -        00:00:36    192.168.10.6    Serial0/0/1
10.2.2.2          0   FULL/  -        00:00:17    192.168.10.2    Serial0/0/0
```