

## Capítulo 1: Introducción a escalamiento de redes 1.0.1.1 Introducción

A medida que una empresa crece, también aumentan sus requisitos de red. Las empresas dependen de la infraestructura de red para proporcionar servicios esenciales. Las interrupciones de la red pueden provocar pérdidas de ganancias y de clientes. Los diseñadores de redes deben diseñar y armar una red empresarial que sea escalable y de alta disponibilidad.

En este capítulo, se presentan estrategias que se pueden utilizar para diseñar sistemáticamente una red de alta funcionalidad, como el modelo de diseño de red jerárquico y la arquitectura empresarial de Cisco, y las selecciones adecuadas de dispositivos. Los objetivos del diseño de red son limitar el número de dispositivos que se ven afectados por la falla de un solo dispositivo de red, proporcionar un plan y un camino de crecimiento y crear una red confiable.

**Después de completar este capítulo, podrá hacer lo siguiente:**

- Describir el uso de la red jerárquica en una pequeña empresa.
- Describir las recomendaciones para diseñar una red escalable.
- Seleccionar las características adecuadas de hardware del switch para que admita los requisitos de las redes de pequeñas o medianas empresas.
- Describir los tipos de routers disponibles para las redes de pequeñas o medianas empresas.
- Configurar los parámetros básicos en un dispositivo con IOS de Cisco.

## Capítulo 1: Introducción a escalamiento de redes 1.0.1.2 Actividad de clase: Red por diseño

### **Red por diseño**

Su empleador está por abrir una nueva sucursal.

A usted lo reubicaron en la sucursal como administrador de red, donde se encargará de diseñar y mantener la red de la nueva sucursal.

Los administradores de red en las otras sucursales utilizaron el modelo jerárquico de tres capas de Cisco para diseñar sus redes. Decide utilizar el mismo enfoque.

A fin de tener una idea de lo que puede aportar el uso del modelo jerárquico para mejorar el proceso de diseño, investiga el tema.

### [Actividad de clase: Red por diseño](#)



El modelo jerárquico de tres capas de Cisco puede contribuir a que el diseño de la red se vuelva una tarea un poco más sencilla.

Ca

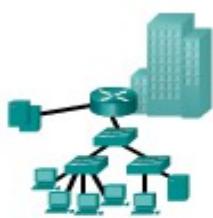
#### pítulo 1: Introducción a escalamiento de redes 1.1.1.1 La necesidad de escalar la red

Las empresas recurren cada vez más a su infraestructura de red para proporcionar servicios de misión crítica. A medida que las empresas crecen y evolucionan, contratan más empleados, abren sucursales y se expanden a los mercados globales. Estos cambios afectan directamente los requisitos de la red. Un entorno comercial de gran tamaño que cuenta con muchos usuarios, ubicaciones y sistemas se conoce como “empresa”. La red que se utiliza para respaldar las actividades comerciales de la empresa se denomina red empresarial.

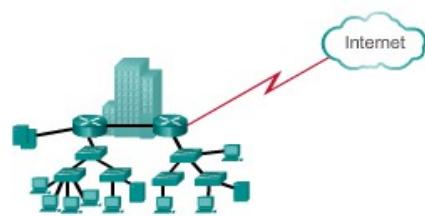
Haga clic en el botón Reproducir de la ilustración para ver una animación de cómo una red pequeña se convierte en una red empresarial.

Una red empresarial debe admitir el intercambio de diversos tipos de tráfico de red, entre ellos archivos de datos, correo electrónico, telefonía IP y aplicaciones de video para varias unidades empresariales. Todas las redes empresariales deben cumplir los siguientes requisitos:

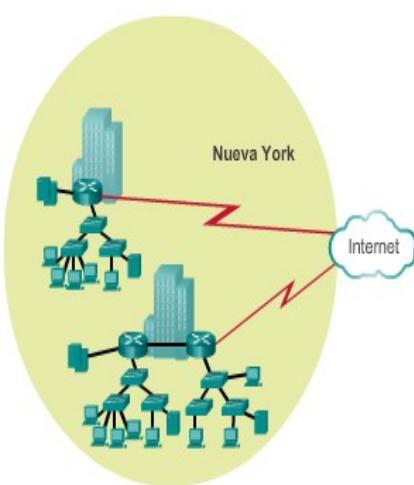
- Admitir aplicaciones fundamentales.
- Admitir el tráfico de redes convergentes.
- Admitir las diversas necesidades comerciales.
- Proporcionar un control administrativo centralizado.



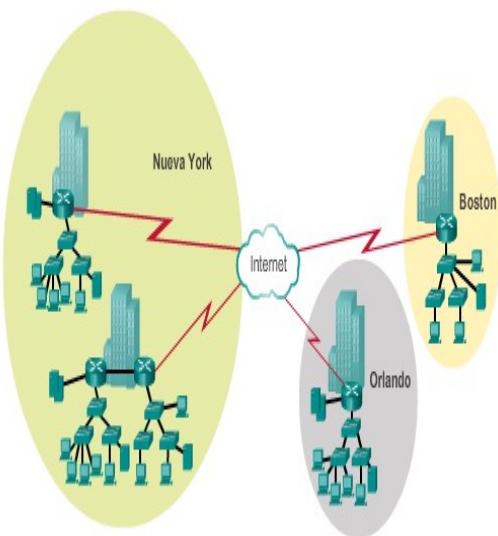
Una empresa pequeña con una única ubicación.



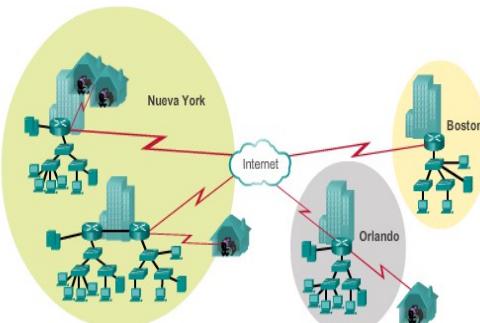
La empresa aumenta su cantidad de empleados.



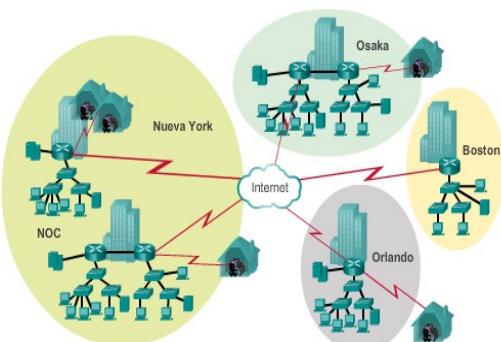
La empresa crece y crea varias sucursales en la misma ciudad.



La empresa crece y se expande a varias ciudades.



La empresa contrata empleados a distancia.



La empresa centraliza la administración de la red en un centro de operaciones de red (NOC, Network Operations Center).

Capítulo 1: Introducción a escalamiento de redes 1.1.1.2 Dispositivos comerciales para empresas

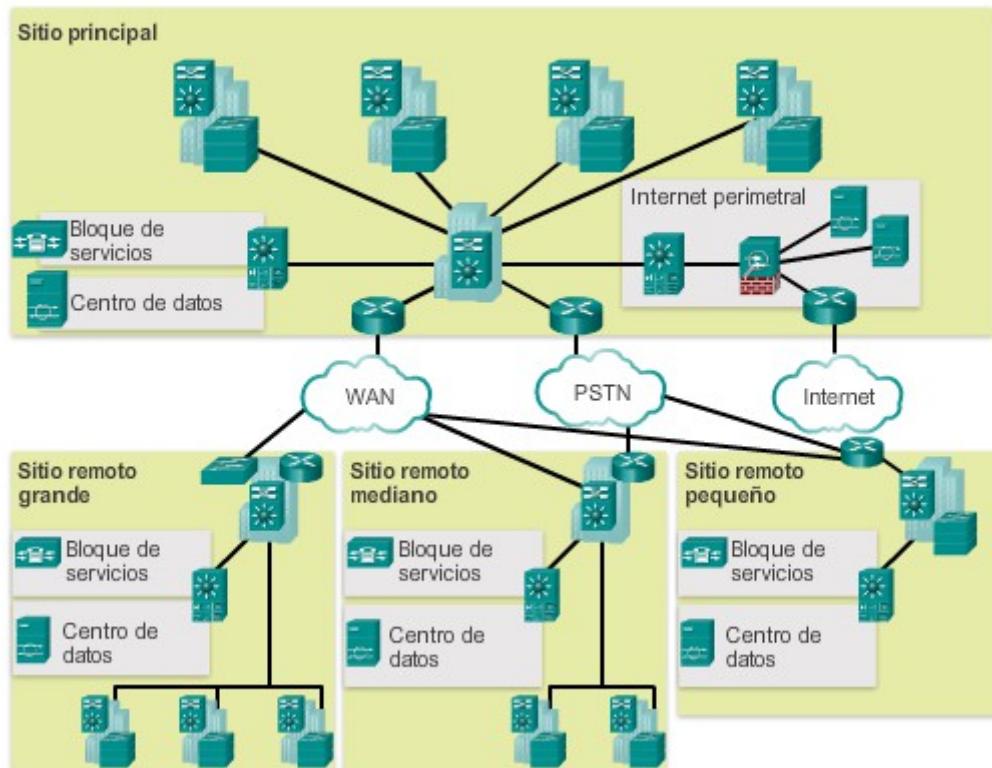
Los usuarios esperan que las redes empresariales, como la que se muestra en la ilustración, estén activas el 99,999% del tiempo. Las interrupciones que se producen en las redes empresariales impiden que las empresas lleven a cabo sus actividades normales, lo que puede provocar pérdidas de ganancias, de clientes, de datos y de oportunidades.

Para alcanzar este nivel de confiabilidad, se suelen instalar equipos de tecnología avanzada de clase empresarial en la red empresarial. Los equipos empresariales, diseñados y fabricados para cumplir con estándares más estrictos que los dispositivos más económicos, transportan un gran volumen de tráfico de red.

Los equipos de alta tecnología están diseñados para ser confiables, con características como fuentes de alimentación redundantes y capacidad de migración en caso de fallos. La capacidad de conmutación por falla es la habilidad que posee un dispositivo para pasar de un módulo, un servicio o un dispositivo que no funciona a uno que sí lo hace sin interrumpir el servicio o con una interrupción mínima.

La adquisición e instalación de equipos empresariales de alta tecnología no elimina la necesidad de diseñar correctamente la red.

**Diseño de una red empresarial grande**



Capítulo 1: Introducción a escalamiento de redes 1.1.1.3 Diseño jerárquico de la red

Para optimizar el ancho de banda en una red empresarial, la red debe estar organizada para que el tráfico se mantenga en el nivel local y no se propague innecesariamente a otras partes de la red. El uso del modelo de diseño jerárquico de tres capas ayuda a organizar la red.

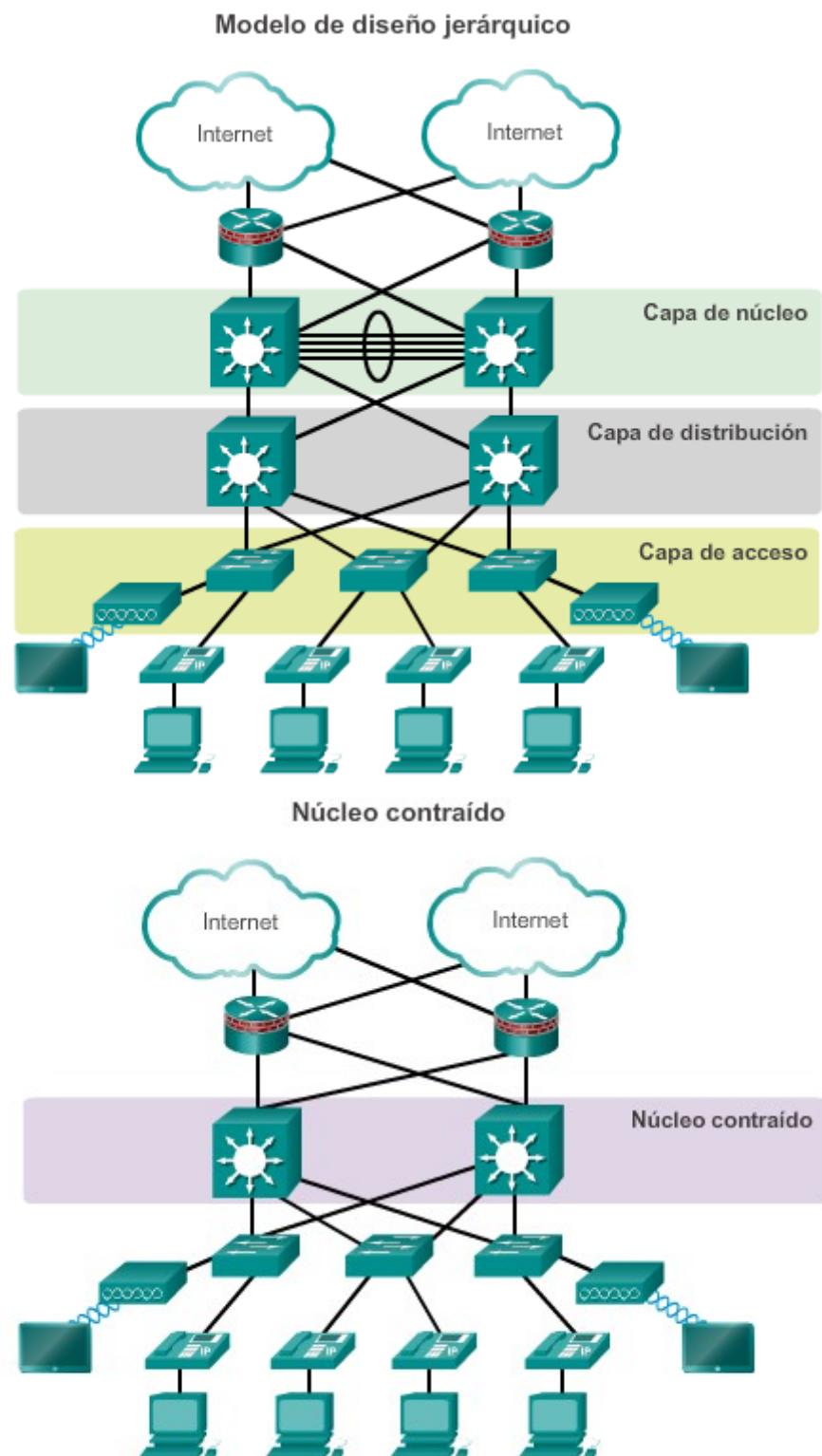
Como se muestra en la figura 1, en este modelo se divide la funcionalidad de la red en tres capas diferentes.

- Capa de acceso
- Capa de distribución
- Capa de núcleo

Cada capa está diseñada para cumplir funciones específicas.

La capa de acceso proporciona conectividad a los usuarios. La capa de distribución se utiliza para enviar el tráfico de una red local a otra. Por último, la capa de núcleo representa una capa troncal de alta velocidad entre las redes dispersas. El tráfico de los usuarios se inicia en la capa de acceso y pasa por las demás capas si se necesita utilizar la funcionalidad de esas capas.

Aunque el modelo jerárquico consta de tres capas, es posible que en algunas redes empresariales pequeñas se implemente un diseño jerárquico de dos niveles. Como se muestra en la figura 2, en un diseño jerárquico de dos niveles, las capas de núcleo y de distribución se combinan en una, lo que reduce el costo y la complejidad.



#### Capítulo 1: Introducción a escalamiento de redes 1.1.1.4 Arquitectura empresarial de Cisco

La arquitectura empresarial de Cisco divide la red en componentes funcionales, al tiempo que mantiene las capas de núcleo, de distribución y de acceso. Como se muestra en la ilustración, los principales módulos de la arquitectura empresarial de Cisco incluyen lo siguiente:

- Campus empresarial
- Perímetro empresarial
- Perímetro del proveedor de servicios
- Remoto

### **Campus empresarial**

El módulo de campus empresarial está compuesto por toda la infraestructura del campus e incluye las capas de acceso, de distribución y de núcleo. El módulo de capa de acceso incluye switches de capa 2 o de capa 3 para proporcionar la densidad de puertos requerida. En este módulo, se produce la implementación de las VLAN y los enlaces troncales a la capa de distribución del edificio. La redundancia a los switches de distribución del edificio es importante. El módulo de capa de distribución agrega acceso al edificio mediante dispositivos de capa 3. En el módulo de capa de distribución, se llevan acabo el routing, el control de acceso y la QoS. El módulo de capa de núcleo proporciona una interconectividad de alta velocidad entre los módulos de la capa de distribución, las granjas de servidores de los centros de datos y el perímetro empresarial. En este módulo, el eje central del diseño es la redundancia, la convergencia rápida y la tolerancia a fallas.

Además de estos módulos, el campus empresarial puede incluir otros submódulos, como los siguientes:

- **Módulo de centro de datos y granja de servidores:** esta área proporciona conectividad de alta velocidad y protección para los servidores. Es de suma importancia proporcionar seguridad, redundancia y tolerancia a fallas. Los sistemas de administración de red controlan el rendimiento mediante el monitoreo de la disponibilidad de los dispositivos y la red.
- **Módulo de servicios:** esta área proporciona acceso a todos los servicios, como los servicios de telefonía IP, los servicios de controlador inalámbrico y los servicios unificados.

### **Perímetro empresarial**

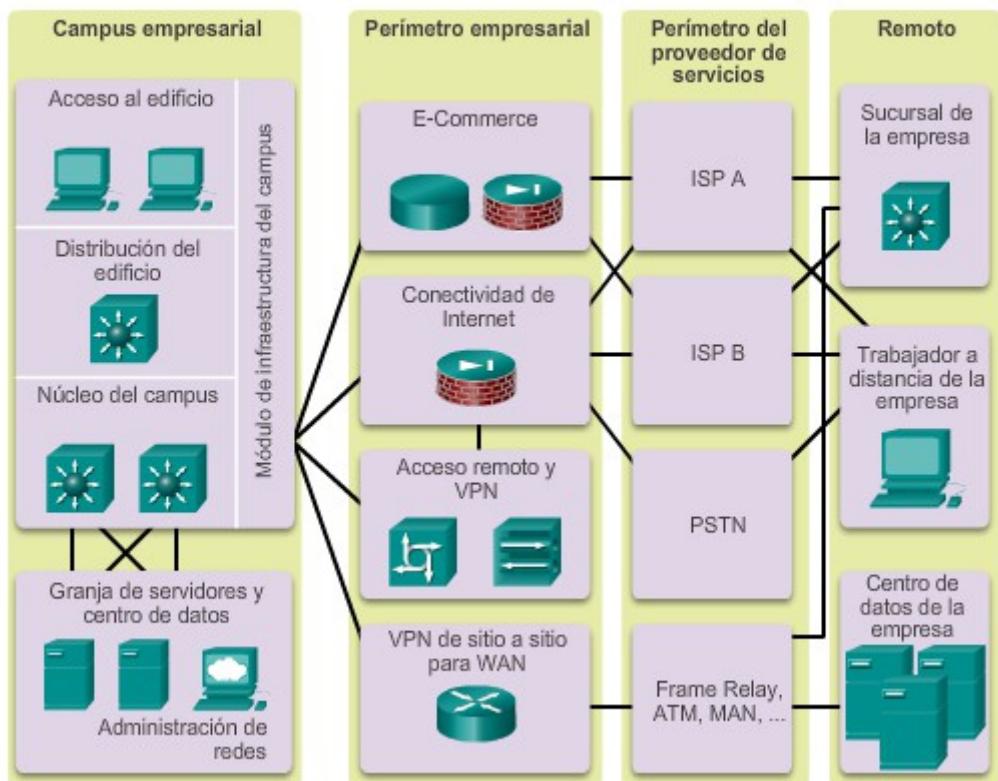
El módulo de perímetro empresarial está compuesto por los módulos de Internet, VPN y WAN que conectan la empresa a la red del proveedor de servicios. Este módulo extiende los servicios de la empresa a sitios remotos y permite que la empresa utilice recursos de Internet y de socios. Proporciona QoS, refuerzo de políticas, niveles de servicio y seguridad.

### **Perímetro del proveedor de servicios**

El módulo de perímetro del proveedor de servicios proporciona servicios de Internet, de red pública de telefonía conmutada (PSTN) y WAN.

El modelo de red empresarial compuesta (ECNM) pasa a través de un dispositivo de extremo. Este es el momento en el que los paquetes se pueden analizar y se puede tomar la decisión de si se debe permitir el ingreso de estos a la red empresarial. Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) también se pueden configurar en el perímetro empresarial para brindar protección contra actividades malintencionadas.

## Arquitectura empresarial



### Capítulo 1: Introducción a escalamiento de redes 1.1.1.5 Dominios de fallas

Una red bien diseñada no solo controla el tráfico, sino que además limita el tamaño de los dominios de fallas. Un dominio de fallas es el área de la red que se ve afectada cuando un dispositivo o un servicio de red esenciales experimentan problemas.

La función del dispositivo que inicialmente falla determina el impacto del dominio de fallas. Por ejemplo, un switch que funciona mal en un segmento de red normalmente afecta solo a los hosts de ese segmento. Sin embargo, si la falla se presenta en el router que conecta este segmento con otros segmentos, el impacto es mucho mayor.

El uso de enlaces redundantes y equipos confiables de alta tecnología minimizan las posibilidades de interrupciones de los servicios de la red. Si los dominios de fallas son más pequeños, se reduce el impacto de las fallas sobre la productividad de la empresa. Además, simplifican el proceso de resolución de problemas, lo que reduce el tiempo de inactividad para todos los usuarios.

En la ilustración, haga clic en cada dispositivo de red para ver el dominio de fallas relacionado.

### **Limitación del tamaño de los dominios de fallas**

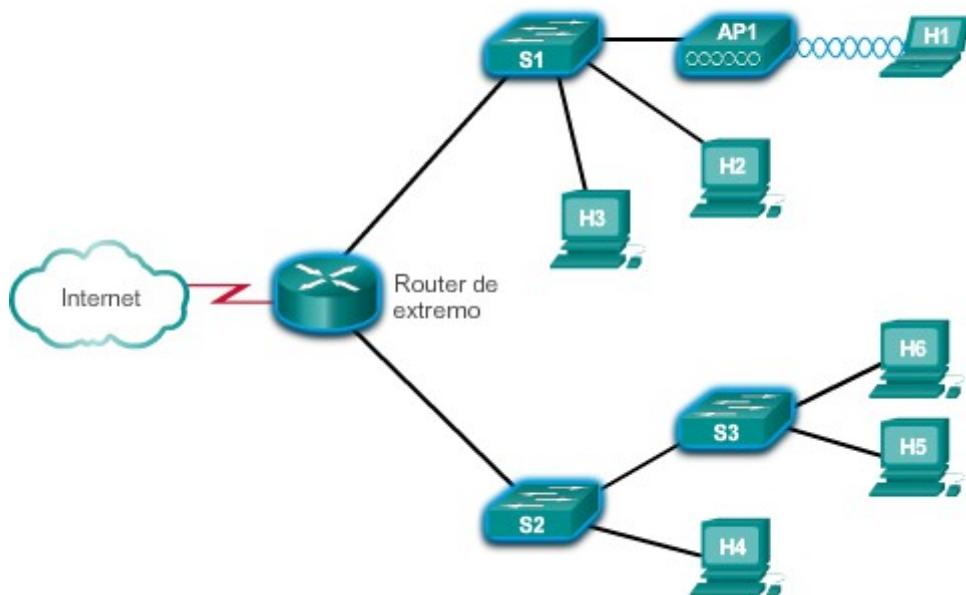
Dado que una falla en la capa de núcleo de una red puede tener un gran impacto, el diseñador de red suele enfocarse en los esfuerzos para prevenir fallas. Estos esfuerzos pueden suponer un gran incremento del costo de implementación de la red. En el modelo de diseño jerárquico, es más fácil y, generalmente, más económico controlar el tamaño de un dominio de fallas en la capa de distribución. En esta capa, los errores de la red se pueden contener en un área más pequeña, de manera que se vean afectados menos usuarios. Cuando se utilizan dispositivos de

capa 3 en la capa de distribución, cada router funciona como gateway para un número limitado de usuarios de la capa de acceso.

### Implementación de un bloque de switches

Los routers, o los switches multicapa, generalmente se implementan de a pares, y los switches de capa de acceso se dividen en partes iguales entre ellos. A esta configuración se la denomina “bloque de switches de edificio” o “de departamento”. Cada bloque de switches funciona de manera independiente. Como resultado, la falla de un único dispositivo no desactiva la red. Ni siquiera la falla de todo un bloque de switches afecta a un gran número de usuarios finales.

Dominios de fallas



Capítulo 1: Introducción a escalamiento de redes 1.1.1.6 Actividad: Identificar los módulos de la arquitectura empresarial de Cisco

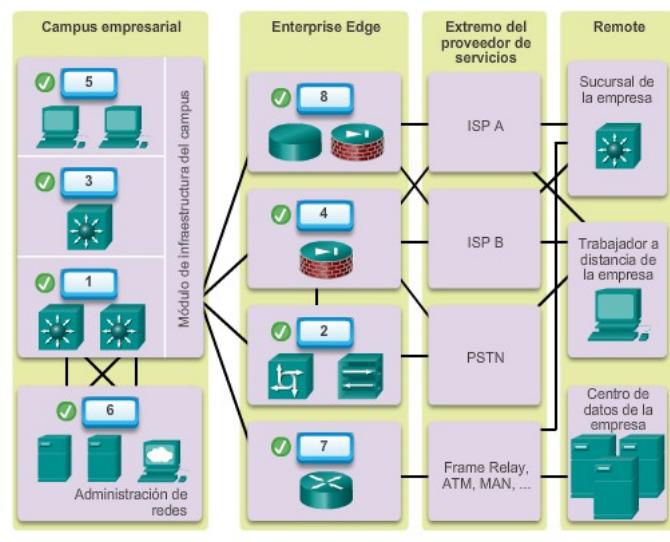
**Actividad: Identificar los módulos de la arquitectura empresarial de Cisco**

Arrastre el número que se encuentra junto al nombre de cada módulo de la arquitectura empresarial de Cisco hasta la ubicación correcta en el gráfico proporcionado.

- 1 Núcleo del campus
- 2 Acceso remoto y VPN
- 3 Distribución del edificio
- 4 Conectividad de Internet
- 5 Acceso al edificio
- 6 Granja de servidores y centro de datos
- 7 WAN de sitio a sitio
- 8 E-Commerce

**Verificar**

**Restablecer**



### Capítulo 1: Introducción a escalamiento de redes 1.1.2.1 Diseño que admite la escalabilidad

Para admitir una red empresarial, el diseñador de red debe desarrollar una estrategia que permita que la red esté disponible y se pueda escalar fácil y eficazmente. En una estrategia de diseño básico de red, se incluyen las siguientes recomendaciones:

- Utilice equipo modular expansible o de dispositivos agrupados que puedan actualizarse fácilmente para incrementar las capacidades. Se pueden agregar módulos de dispositivos a los equipos existentes para admitir nuevos dispositivos y características sin necesidad de actualizaciones de equipos a gran escala. Algunos dispositivos se pueden integrar en un clúster para que funcionen como un solo dispositivo, a fin de simplificar la administración y la configuración.
- Diseñe la red jerárquica para que incluya módulos que se puedan agregar, actualizar y modificar según sea necesario, sin afectar el diseño de otras áreas funcionales de la red. Por ejemplo, cree una capa de acceso independiente que se pueda expandir sin afectar las capas de distribución y de núcleo de la red de campus.
- Cree una estrategia de direcciones IPv4 o IPv6 que sea jerárquica. Si el direccionamiento IPv4 se planifica meticulosamente, se evita la necesidad de volver a direccionar la red para admitir usuarios y servicios adicionales.
- Elija routers o switches de capas múltiples para limitar la difusión y filtrar otro tipo de tráfico no deseado en la red. Utilice dispositivos de capa 3 para filtrar y reducir el tráfico al núcleo de la red.

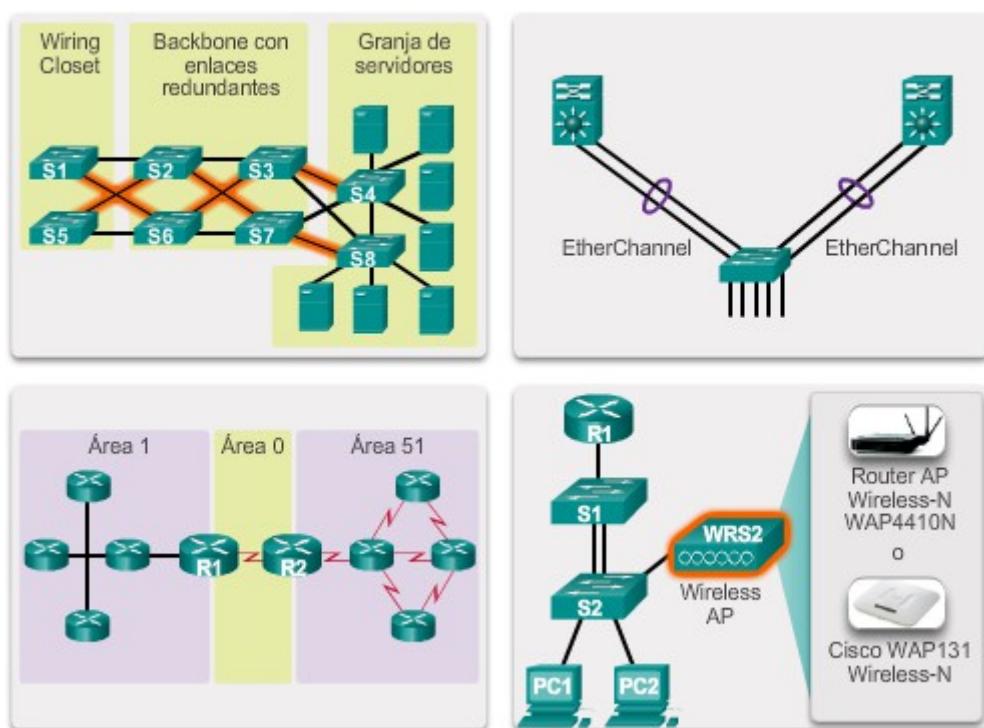
Como se muestra en la ilustración, los requisitos de diseño de red más avanzado incluyen lo siguiente:

- La implementación de enlaces redundantes en la red, entre los dispositivos esenciales y los dispositivos de capa de acceso y de capa de núcleo.
- La implementación de varios enlaces entre los equipos, ya sea con agregación de enlaces (EtherChannel) o con balanceo de carga de mismo costo para aumentar el ancho de banda. La combinación de varios enlaces Ethernet en una única configuración con

balanceo de carga de EtherChannel aumenta el ancho de banda disponible. Las implementaciones de EtherChannel se pueden utilizar cuando, por restricciones de presupuesto, no se pueden adquirir interfaces de alta velocidad o tendidos de fibra óptica.

- La Implementación de conectividad inalámbrica para permitir movilidad y expansión.
- El uso de un protocolo de routing escalable y la implementación de características dentro de ese protocolo para aislar las actualizaciones de routing y minimizar el tamaño de la tabla de routing.

### Diseño que admite la escalabilidad



### Capítulo 1: Introducción a escalamiento de redes 1.1.2.2 Planificación para la redundancia

#### Implementación de la redundancia

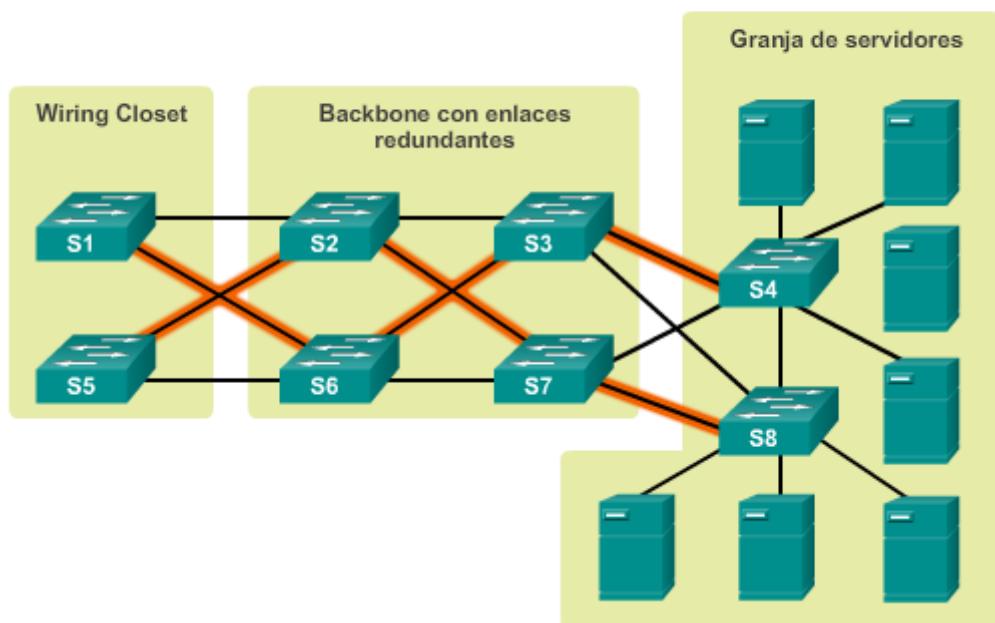
Para la mayoría de las organizaciones, la disponibilidad de la red es fundamental para satisfacer las necesidades empresariales. La redundancia es una parte importante del diseño de la red para prevenir interrupciones de los servicios de la red al minimizar la posibilidad de un punto único de falla. Un método para implementar la redundancia consiste en instalar equipos duplicados y proporcionar servicios de comutación por falla para los dispositivos esenciales.

Otro método para implementar la redundancia es mediante rutas redundantes, como se muestra en la ilustración. Las rutas redundantes ofrecen rutas físicas alternativas para que los datos atraviesen la red. En una red conmutada, las rutas redundantes admiten una alta disponibilidad. Sin embargo, debido al funcionamiento de los switches, es posible que las rutas redundantes en una red Ethernet conmutada causen bucles lógicos en la capa 2. Por esta razón, se necesita el protocolo de árbol de expansión (STP).

El protocolo STP permite la redundancia necesaria para proporcionar confiabilidad, pero elimina los bucles de switching. Para hacerlo, proporciona un mecanismo para deshabilitar rutas redundantes en una red conmutada hasta que la ruta se vuelva necesaria, por ejemplo, cuando ocurre una falla. Es un protocolo de estándares abiertos, que se utiliza en un entorno de conmutación para crear una topología lógica sin bucles.

En el capítulo “Redundancia de LAN”, se describen más detalles acerca de la redundancia LAN y el funcionamiento de STP.

### Redundancia de LAN



[Capítulo 1: Introducción a escalamiento de redes 1.1.2.3 Aumento del ancho de banda](#)

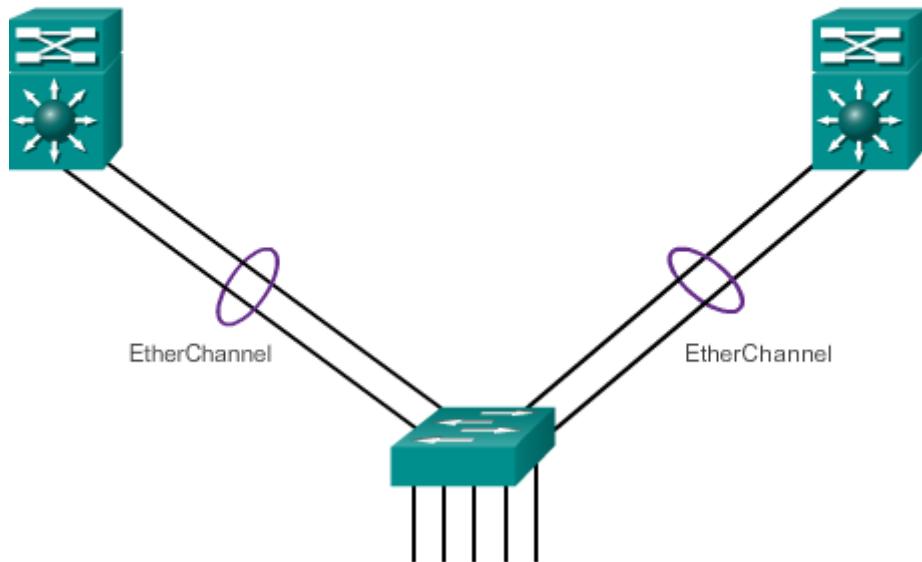
#### Implementación de EtherChannel

En el diseño de red jerárquico, es posible que algunos enlaces entre los switches de acceso y distribución necesiten procesar una mayor cantidad de tráfico que otros enlaces. A medida que el tráfico de varios enlaces converge en un único enlace de salida, es posible que en dicho enlace se produzca un cuello de botella. La agregación de enlaces permite que el administrador aumente el ancho de banda entre los dispositivos mediante la creación de un enlace lógico compuesto de varios enlaces físicos. Como se muestra en la ilustración, EtherChannel es una forma de agregación de enlaces que se utiliza en las redes conmutadas.

EtherChannel utiliza los puertos de switch existentes, por lo tanto, no es necesario incurrir en gastos adicionales para actualizar el enlace a una conexión más veloz y costosa. El enlace EtherChannel se ve como un enlace lógico que utiliza una interfaz EtherChannel. La mayoría de las tareas de configuración se realizan en la interfaz EtherChannel en lugar de en cada puerto individual, lo que asegura la coherencia de configuración en todos los enlaces. Por último, la configuración de EtherChannel aprovecha el balanceo de carga entre los enlaces que forman parte del mismo EtherChannel y, según la plataforma de hardware, se pueden implementar uno o más métodos de balanceo de carga.

En el capítulo “Agregación de enlaces”, se detallan el funcionamiento y la configuración de EtherChannel.

### Ventajas de EtherChannel



#### Capítulo 1: Introducción a escalamiento de redes 1.1.2.4 Expansión de la capa de acceso

##### **Implementación de la conectividad inalámbrica**

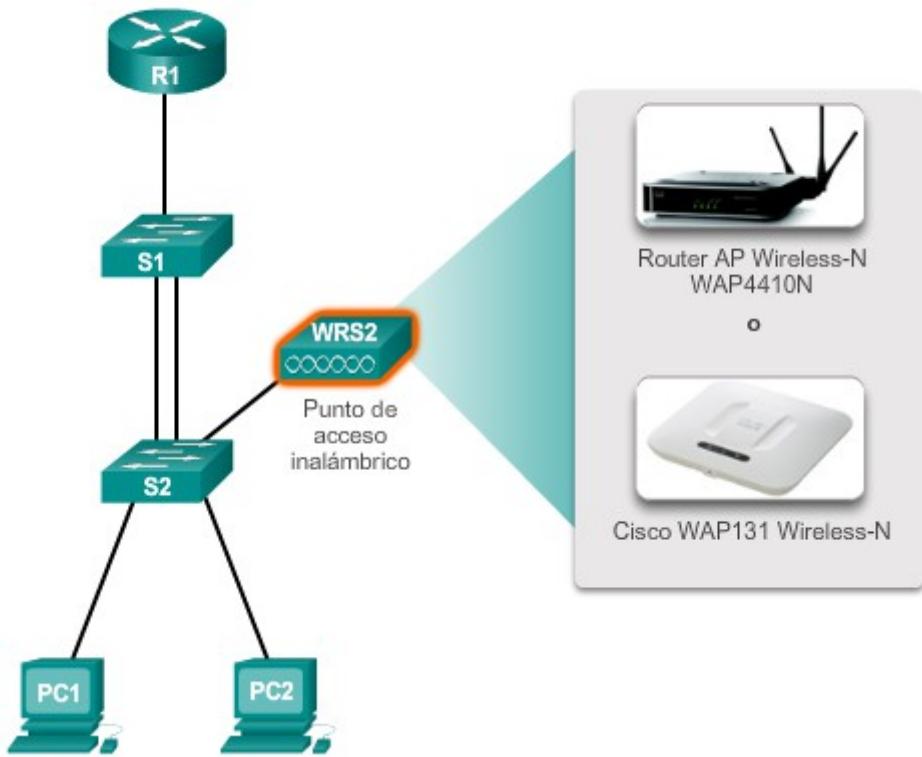
La red debe estar diseñada para poder expandir el acceso a la red para las personas y los dispositivos, según sea necesario. Para la extensión de la conectividad de la capa de acceso, cada vez es más importante la conectividad inalámbrica. La provisión de conectividad inalámbrica proporciona muchas ventajas, como un aumento de la flexibilidad, una reducción de costos y la capacidad de crecer y adaptarse a los requisitos cambiantes de las redes y las empresas.

Para comunicarse de forma inalámbrica, los terminales requieren una NIC inalámbrica que incorpore un transmisor o un receptor de radio y el controlador de software necesario para que funcione. Como se muestra en la ilustración, también se necesita un router inalámbrico o un punto de acceso (AP) inalámbrico para que los usuarios puedan conectarse.

Existen varias consideraciones que se deben tener en cuenta al implementar una red inalámbrica, como los tipos de dispositivos inalámbricos que se debe utilizar y los requisitos de cobertura inalámbrica, así como las consideraciones de interferencia y de seguridad.

En el capítulo “LAN inalámbricas”, se detallan el funcionamiento y la implementación de la tecnología inalámbrica.

## LAN inalámbricas



### Capítulo 1: Introducción a escalamiento de redes 1.1.2.5 Ajuste de los protocolos de routing

#### Administración de la red enrutada

Los ISP y las redes empresariales generalmente utilizan protocolos más avanzados, como los protocolos de estado de enlace, debido a su diseño jerárquico y a la capacidad de escalamiento a redes más grandes.

Los protocolos de routing de estado de enlace, como el protocolo OSPF (Open Shortest Path First), que se muestra en la figura 1, funcionan bien en redes jerárquicas más grandes, donde es importante contar con una convergencia rápida. Los routers OSPF establecen y mantienen las adyacencias de vecinos con otros routers OSPF conectados. Cuando los routers inician una adyacencia con los vecinos, comienza un intercambio de actualizaciones de Link-State. Los routers alcanzan un estado de adyacencia PLENA al sincronizar las vistas de sus bases de datos de Link-State. Con OSPF se envían actualizaciones de Link-State cada vez que hay cambios en la red.

OSPF es un protocolo de routing de estado de enlace popular que se puede ajustar de muchas formas. En el capítulo “Ajuste y resolución de problemas de OSPF de área única”, se detallan algunas de las características más avanzadas de la configuración y la resolución de problemas de OSPF.

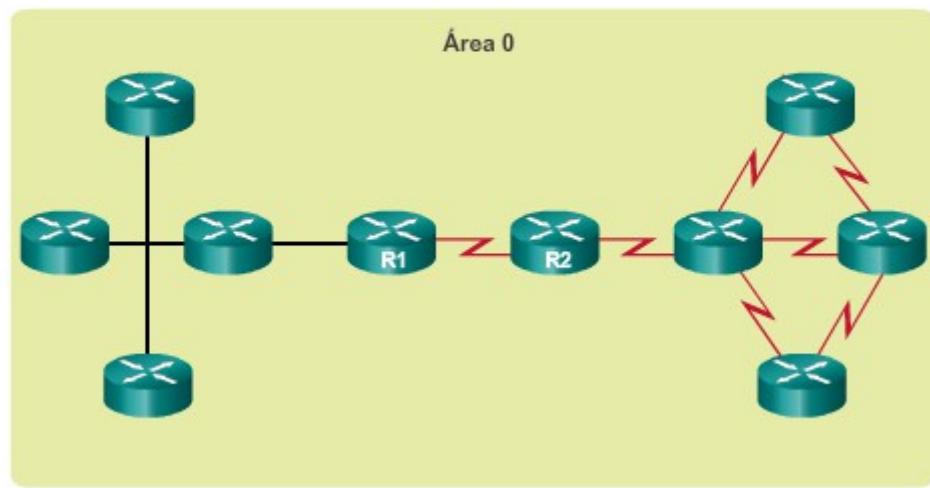
Además, OSPF admite un diseño jerárquico de dos capas, u OSPF multiárea, que se muestra en la figura 2. Todas las redes OSPF comienzan con un Área 0, llamada también área de red troncal. A medida que se expande la red, se pueden crear otras áreas que no son de red troncal. Todas las áreas que no son de red troncal se deben conectar directamente al

área 0. En el capítulo “OSPF multiárea”, se presentan los beneficios, el funcionamiento y la configuración de OSPF multiárea.

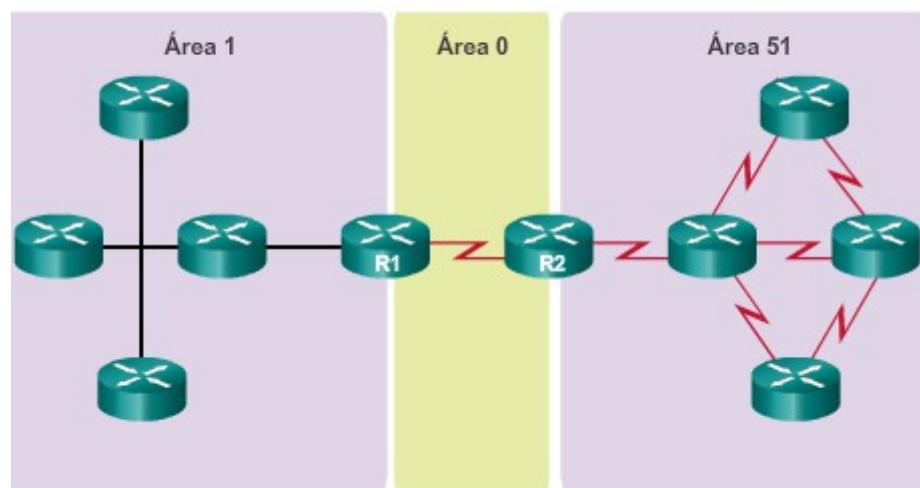
Otro protocolo de routing popular en redes más grandes es el protocolo de routing de gateway interior mejorado (EIGRP). Cisco desarrolló EIGRP como un protocolo de routing vector distancia exclusivo con capacidades mejoradas. Aunque la configuración de EIGRP es relativamente simple, este protocolo tiene amplias y sólidas características y opciones subyacentes. Por ejemplo, EIGRP utiliza varias tablas, que se muestran en la figura 3, para administrar el proceso de routing. EIGRP contiene muchas funciones que no posee ninguno de los otros protocolos de routing. Es una excelente opción para redes grandes de protocolos múltiples en las que se utilizan principalmente dispositivos de Cisco.

En el capítulo “EIGRP”, se presentan el funcionamiento y la configuración del protocolo de routing EIGRP, mientras que en el capítulo “Configuración avanzada y resolución de problemas de EIGRP” se abordan algunas de las opciones de configuración de EIGRP más avanzadas.

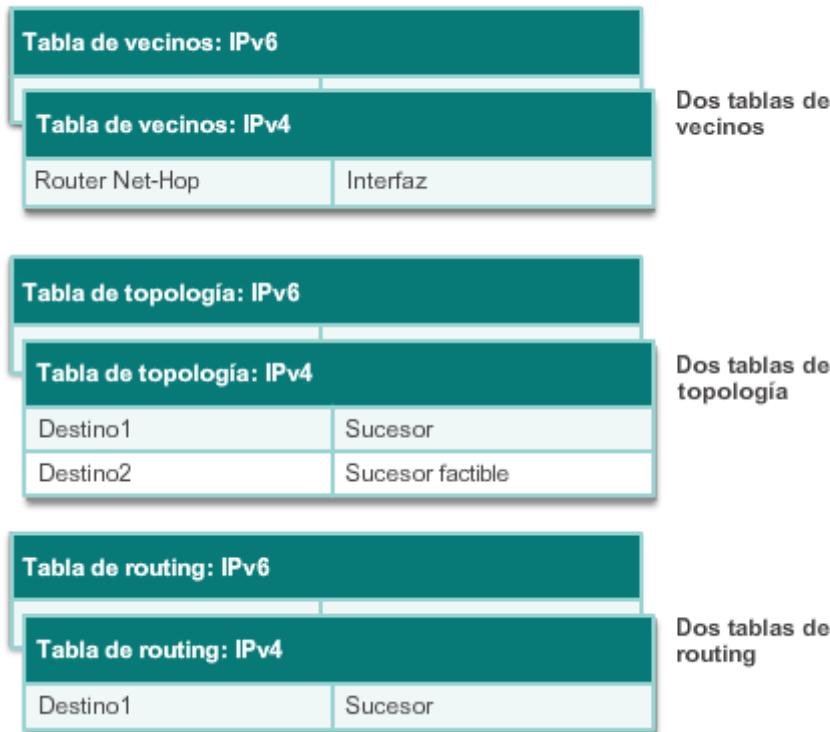
### OSPF de área única



### OSPF multiárea



## EIGRP con módulos dependientes de protocolo (PDM)



Capítulo 1: Introducción a escalamiento de redes 1.1.2.6 Actividad: Identificar la terminología de escalabilidad

### escalabilidad

Actividad: Identificar la terminología de escalabilidad  
Una cada término relacionado con el diseño de escalabilidad de red con su descripción.

que los ejecutivos comprendan	Descripciones
✓ EIGRP	Protocolo con comportamiento de vector distancia.
✓ Redundancia	Ruta de datos alternativa.
✓ Agregación de enlaces	Varios enlaces de interfaz Ethernet combinados en un único canal de ancho de banda.
✓ OSPF	Protocolo que utiliza un área de red troncal.

Capítulo 1: Introducción a escalamiento de redes 1.2.1.1 Plataformas de switch

Cuando se diseña una red, es importante seleccionar el hardware adecuado para cumplir con los requisitos actuales de la red, así como para permitir su crecimiento. Dentro de una red empresarial, tanto los switches como los routers desempeñan un papel muy importante en la comunicación de red.

Existen cinco categorías de switches para redes empresariales, que se muestran en la figura 1:

- **Switches LAN de campus:** para escalar el rendimiento de la red en una LAN empresarial, pueden utilizarse switches de núcleo, de distribución, de acceso y compactos. Estas plataformas de switch varían de switches sin ventilador con ocho puertos fijos a switches de 13 blades que admiten cientos de puertos. Las plataformas de switches LAN de campus incluyen los switches de Cisco de las series 2960, 3560, 3750, 3850, 4500, 6500 y 6800.
- **Switches administrados en la nube:** los switches de acceso administrados a través de la nube Cisco Meraki permiten el apilamiento virtual de switches. Estos controlan y configuran miles de puertos de switch en la Web, sin intervención del personal presencial de TI.
- **Switches de centros de datos:** los centros de datos se deben armar sobre la base de switches que promuevan la escalabilidad de la infraestructura, la continuidad de funcionamiento y la flexibilidad de transporte. Las plataformas de switches de centro de datos incluyen los switches de las series Cisco Nexus y Cisco Catalyst 6500.
- **Switches de proveedores de servicios:** estos switches se dividen en dos categorías, switches de agregación y switches de acceso Ethernet. Los switches de agregación son switches Ethernet de nivel de prestadora de servicios que agregan tráfico en el perímetro de la red. Los switches de acceso Ethernet de proveedores de servicios cuentan con inteligencia de aplicación, servicios unificados, virtualización, seguridad integrada y administración simplificada.
- **Redes virtuales:** las redes se vuelven cada vez más virtuales. Las plataformas de switches de redes virtuales Cisco Nexus proporcionan servicios multiinquilino seguros al incorporar tecnología de inteligencia de virtualización a la red del centro de datos.

Al seleccionar los switches, los administradores de red deben determinar los factores de forma de estos. Esto incluye las características de configuración fija (figura 2), configuración modular (figura 3), apilable (figura 4) y no apilable. El grosor del switch, que se expresa en el número de unidades de rack, también es importante en el caso de los switches que se montan en un rack. Por ejemplo, los switches de configuración fija que se muestran en la figura 2 son todas unidades de un rack (1U).

Además de estas consideraciones, en la figura 5 se destacan otras consideraciones empresariales comunes para tener en cuenta al seleccionar el equipo de switch.

**Consideraciones comerciales comunes que se deben tener en cuenta al seleccionar el equipo de switch:**

- **Costo:** el costo de un switch depende de la cantidad y la velocidad de las interfaces, de las funciones admitidas y de la capacidad de expansión.
- **Densidad de puertos:** los switches de red deben admitir una cantidad adecuada de dispositivos en la red.
- **Alimentación:** hoy en día, es común alimentar puntos de acceso, teléfonos IP e incluso switches compactos mediante la alimentación por Ethernet. Además de las consideraciones de alimentación por Ethernet, algunos switches basados en bastidor admiten fuentes de alimentación redundantes.
- **Confiabilidad:** el switch debe proporcionar acceso continuo a la red.
- **Velocidad del puerto:** la velocidad de la conexión de red es uno de los aspectos fundamentales para los usuarios finales.
- **Buffers para tramas:** la capacidad que tiene el switch de almacenar tramas es importante en las redes donde puede haber puertos congestionados conectados a servidores o a otras áreas de la red.
- **Escalabilidad:** en general, la cantidad de usuarios en una red aumenta con el tiempo; por lo tanto, el switch debe proporcionar la posibilidad de crecimiento.

Capítulo 1: Introducción a escalamiento de redes 1.2.1.2 Densidad de puertos

La densidad de puertos de un switch se refiere al número de puertos disponibles en un único switch. En la ilustración se muestra la densidad de puertos de tres switches diferentes.

Los switches de configuración fija generalmente admiten hasta 48 puertos en un único dispositivo. Presentan opciones para hasta cuatro puertos adicionales para dispositivos de factor de forma conectable (SFP) pequeños. Las altas densidades de puerto permiten un mejor uso del espacio y la energía limitados. Si hay dos switches de 24 puertos cada uno, podrían admitir hasta 46 dispositivos, dado que al menos uno de los puertos de cada switch se pierde en la conexión de cada switch al resto de la red. Además, se requieren dos tomas de alimentación eléctrica. Por otra parte, si hay un único switch de 48 puertos, se pueden admitir 47 dispositivos; en este caso, se utiliza un solo puerto para conectar el switch al resto de la red y un solo tomacorriente para admitir el switch.

Los switches modulares pueden admitir altas densidades de puertos mediante el agregado de varias tarjetas de línea de puertos de switch. Por ejemplo, algunos switches Catalyst 6500 pueden admitir más de 1000 puertos de switch.

Las grandes redes empresariales que admiten muchos miles de dispositivos de red requieren switches modulares de alta densidad para lograr el mejor uso del espacio y de la energía. Sin el uso de un switch modular de alta densidad, la red necesitaría muchos switches de configuración fija para incluir el número de dispositivos que necesitan acceso a la red. Este enfoque puede consumir muchas tomas de alimentación eléctrica y mucho espacio en el armario.

El diseñador de red también debe tener en cuenta el problema de los cuellos de botella de los uplinks: una serie de switches de configuración fija puede consumir muchos puertos adicionales para la agregación de ancho de banda entre switches, con el propósito de cumplir el objetivo de

rendimiento. Si se utiliza un único switch modular, la agregación de ancho de banda no se vuelve un problema, dado que el backplane del bastidor puede proporcionar el ancho de banda necesario para admitir los dispositivos conectados a las tarjetas de línea de puertos de switch.



#### Capítulo 1: Introducción a escalamiento de redes 1.2.1.3 Velocidades de reenvío

Las tasas de reenvío definen las capacidades de procesamiento de un switch mediante la estimación de la cantidad de datos que puede procesar por segundo el switch. Como se muestra en la ilustración, las líneas de productos de switch se clasifican según las velocidades de reenvío. Los switches básicos presentan velocidades de reenvío inferiores que los switches de nivel empresarial. Es importante considerar las velocidades de reenvío cuando se selecciona un switch. Si la velocidad es demasiado baja, no puede incluir una comunicación de velocidad de cable completa a través de todos sus puertos de switch. La velocidad de cable es la velocidad de datos que puede obtener cada puerto Ethernet en el switch. Las velocidades de datos pueden ser 100 Mb/s, 1 Gb/s, 10 Gb/s o 100 Gb/s.

Por ejemplo, un switch gigabit de 48 puertos típico que funciona a la máxima velocidad de cable genera 48 Gb/s de tráfico. Si el switch sólo admite una velocidad de reenvío de 32 Gb/s, no puede ejecutar la velocidad de cable completa a través de todos los puertos de forma simultánea. Por fortuna, por lo general los switches de capa de acceso no necesitan funcionar a la máxima velocidad de cable, debido a que están limitados físicamente por los uplinks a la capa de distribución. Esto significa que se pueden utilizar switches más económicos y de menor rendimiento en la capa de acceso, y switches de mayor rendimiento y más costosos en las capas de distribución y de núcleo, donde la velocidad de reenvío tiene un mayor impacto en el rendimiento de la red.

## Velocidad de envío

Switch Gigabit Ethernet de 24 puertos



Capaz de conmutar 24 Gbps de tráfico

Switch Gigabit Ethernet de 48 puertos



Capaz de conmutar 48 Gbps de tráfico

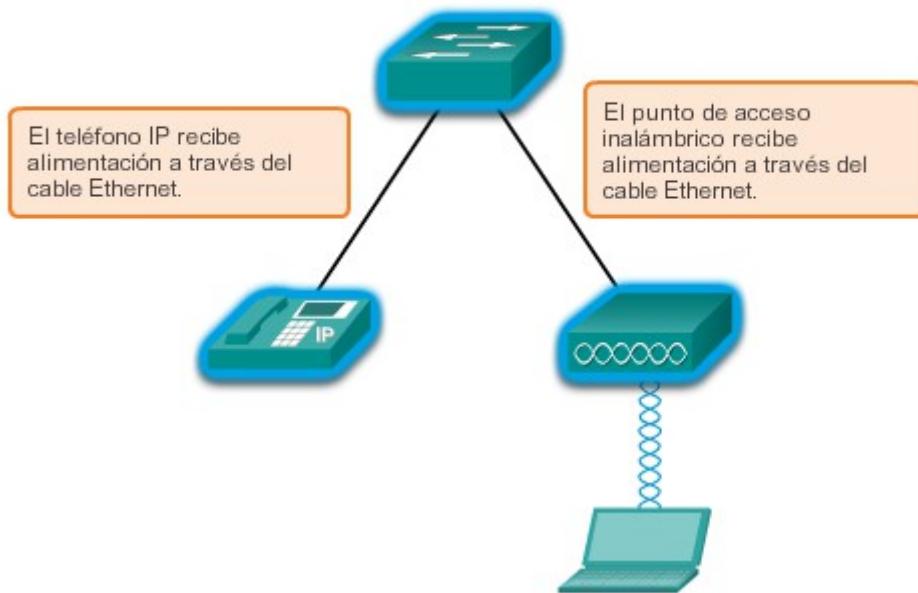
### Capítulo 1: Introducción a escalamiento de redes 1.2.1.4 Alimentación por Ethernet

La alimentación por Ethernet (PoE) permite que un switch suministre alimentación a un dispositivo a través del cableado Ethernet existente. Esta característica se puede utilizar en teléfonos IP y algunos puntos de acceso inalámbrico. Haga clic en los íconos resaltados en la figura 1 para ver los puertos PoE en cada dispositivo.

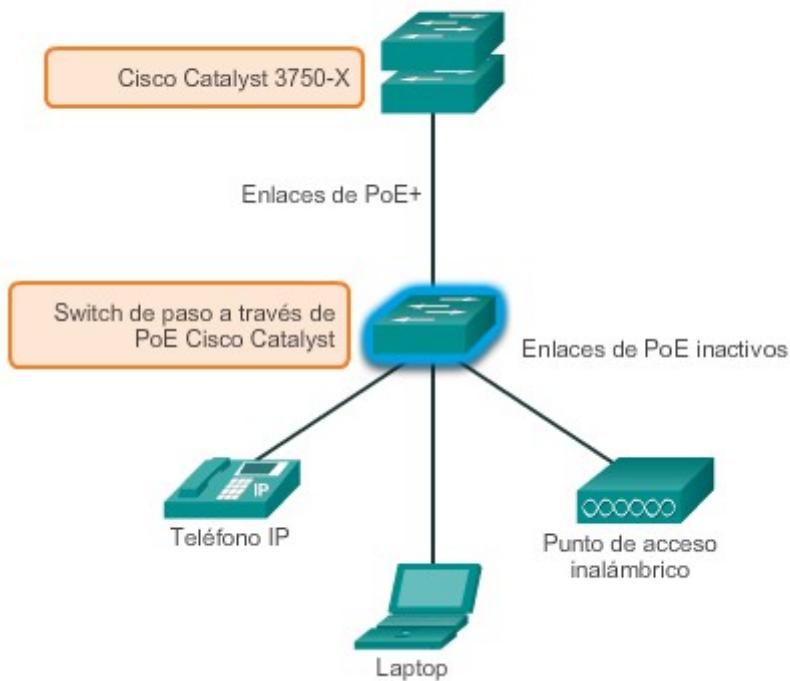
PoE brinda una mayor flexibilidad al instalar puntos de acceso inalámbrico y teléfonos IP, lo que permite que se puedan instalar en cualquier lugar que tenga un cable Ethernet. El administrador de red debe asegurarse de que se requieran las características de PoE, debido a que los switches que admiten PoE son costosos.

Los switches compactos relativamente nuevos de Cisco de las series Catalyst 2960-C y 3560-C admiten paso a través de PoE. El paso a través de PoE permite que el administrador de red alimente los dispositivos PoE conectados al switch, así como al switch mismo, por medio de energía obtenida de ciertos switches ascendentes. Haga clic en el ícono resaltado en la figura 2 para ver un switch Catalyst 2960-C de Cisco.

## Alimentación por Ethernet



## Paso a través de PoE

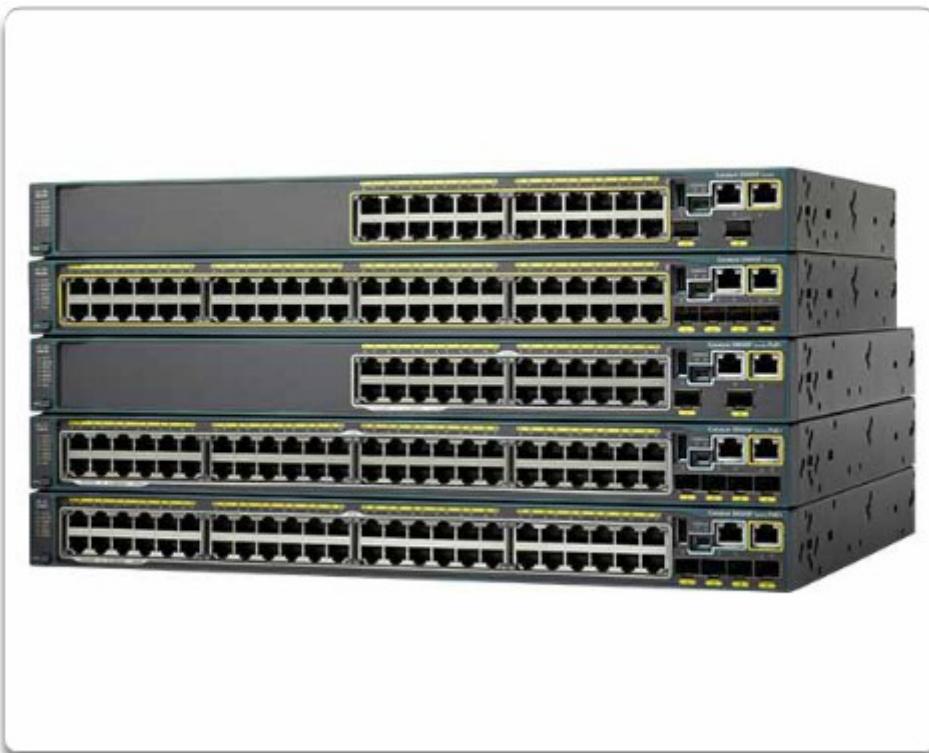


Generalmente, los switches multicapa se implementan en las capas de núcleo y de distribución de la red conmutada de una organización. Los switches multicapa se caracterizan por la capacidad de crear una tabla de routing, por admitir algunos protocolos de routing y por reenviar los paquetes IP a una velocidad similar a la de reenvío de capa 2. Los switches multicapa suelen admitir hardware especializado, como los circuitos integrados de aplicación específica (ASIC). Los ASIC, junto con estructuras de datos de software dedicadas, pueden simplificar el reenvío de paquetes IP en forma independiente de la CPU.

En el ámbito de la tecnología de redes, hay una tendencia hacia un entorno conmutado puramente de capa 3. Cuando se comenzaron a utilizar switches en las redes, ninguno de ellos admitía routing. Hoy en día, casi todos los switches lo hacen. Es probable que pronto todos los switches incorporen un procesador de ruta, dado que el costo de hacerlo es cada vez menor en relación con otras limitaciones. Finalmente, el término “switch multicapa” será redundante.

Los switches Catalyst 2960, que se muestran en la ilustración, representan la migración a un entorno puramente de capa 3. Con las versiones de IOS anteriores a 15.x, estos switches admitían solo una interfaz virtual conmutada (SVI) activa. Con la versión 15.x del IOS, estos switches ahora admiten varias SVI activas. Esto significa que se puede acceder al switch de forma remota mediante varias direcciones IP en diferentes redes.

#### Switches Cisco Catalyst de la serie 2960



Capítulo 1: Introducción a escalamiento de redes 1.2.1.6 Actividad: Seleccionar el hardware del switch

**Actividad: Seleccionar el hardware del switch**

Une cada característica con los criterios de selección de switch correspondientes.

Característica	Criterios de selección de switch
PoE	Provisión de energía eléctrica a las terminales mediante los cables de datos Ethernet.
Velocidades de reenvío	Velocidad con la que las interfaces procesan las tramas de Ethernet.
Configuración modular	Expansión de capacidad y velocidad mediante tarjetas de línea y de puerto que se pueden actualizar.
Configuración fija	Interfaces y puertos incorporados permanentes.
Apilable	Capacidad para interconectar varios switches para administrarlos de forma eficaz como si fuese un gran switch.
Densidad del puerto	Cantidad de puertos en un switch.

**Verificar**

**Restablecer**

[Capítulo 1: Introducción a escalamiento de redes 1.2.1.7 Packet Tracer: Comparación entre los switches 2960 y 3560](#)

**Información básica/situación**

En esta actividad, utilizará distintos comandos para examinar tres topologías de switching diferentes y comparar las similitudes y las diferencias entre los switches 2960 y 3560. También comparará la tabla de routing de un router 1941 con un switch 3560.

[Packet Tracer: Comparación entre los switches 2960 y 3560 \(instrucciones\)](#)

[Packet Tracer: Comparación entre los switches 2960 y 3560 \(PKA\)](#)

[Capítulo 1: Introducción a escalamiento de redes 1.2.1.8 Práctica de laboratorio: Selección del hardware de switching](#)

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: Explorar los productos de switches Cisco
- Parte 2: Seleccionar un switch de capa de acceso
- Parte 3: Seleccionar un switch de capa de distribución y de núcleo

[Práctica de laboratorio: Selección del hardware de switching](#)

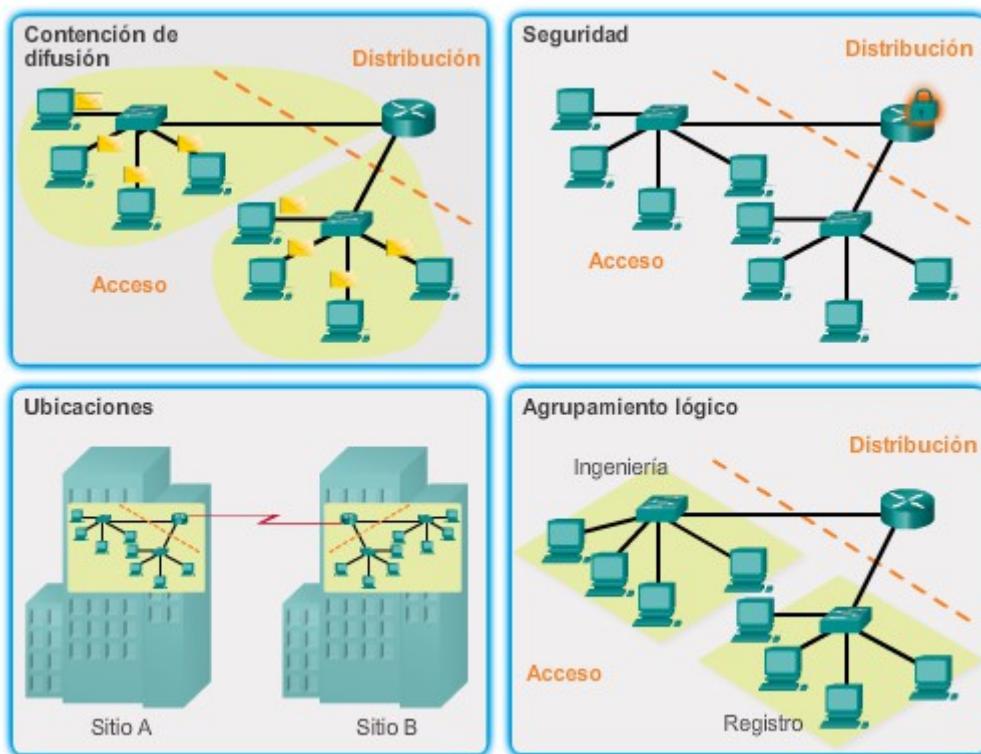
[Capítulo 1: Introducción a escalamiento de redes 1.2.2.1 Requisitos de los routers](#)

El routing es necesario en la capa de distribución de una red empresarial. Sin el proceso de routing, los paquetes no pueden salir de la red local.

Los routers cumplen un papel muy importante en la red, ya que interconectan múltiples sitios dentro de la red empresarial, lo que proporciona rutas redundantes y conecta los ISP en Internet. Los routers también pueden actuar como traductores entre los diferentes tipos de medios y protocolos. Por ejemplo, un router puede aceptar paquetes de una red Ethernet y volver a encapsularlos para transportarlos por una red serial.

Los routers usan la parte de la red de la dirección IP de destino para enrutar paquetes hacia el destino correcto. Seleccionan una ruta alternativa si el enlace deja de funcionar o si hay mucho tráfico. Todos los hosts de una red local especifican la dirección IP de la interfaz del router local en la configuración IP. Esta interfaz del router es el gateway predeterminado.

Los routers también cumplen otras funciones útiles:



#### Capítulo 1: Introducción a escalamiento de redes 1.2.2.2 Routers Cisco

A medida que crece la red, es importante seleccionar los routers adecuados para cumplir con los requisitos. Como se muestra en la ilustración, hay tres categorías de routers:

- **Routers de sucursal:** los routers de sucursal optimizan los servicios de sucursal en una única plataforma, al tiempo que proporcionan una experiencia de aplicación óptima en todas las infraestructuras de sucursal y de WAN. Maximizar la disponibilidad del servicio en la sucursal requiere que la red esté diseñada para estar activa todos los días, las 24 horas (los 365 días del año). Las redes de sucursal de alta disponibilidad deben asegurar una recuperación rápida de las fallas típicas y, al mismo tiempo, minimizar o

eliminar el impacto en el servicio y proporcionar una configuración y una administración de la red sencillas.

- **Routers de perímetro de la red:** los routers de perímetro de la red permiten que dicho perímetro preste servicios confiables de alto rendimiento y de alta seguridad que unen las redes de campus, de centro de datos y de sucursal. Los clientes esperan una experiencia de medios de alta calidad y más tipos de contenido que nunca. Los clientes buscan interactividad, personalización, movilidad y control para todo ese contenido. También quieren poder acceder al contenido en cualquier momento y lugar de su elección, y con cualquier dispositivo, ya sea desde su hogar, desde la oficina o cuando van de un lado a otro. Los routers de perímetro de la red deben proporcionar una calidad de servicio mejorada y capacidades de video y de tecnología móvil ininterrumpidas.
- **Routers de proveedores de servicios:** estos routers diferencian la cartera de servicios y aumentan las ganancias por medio de la provisión de soluciones de extremo a extremo escalables y servicios que reconocen a los suscriptores. Los operadores deben optimizar las operaciones, reducir los costos y mejorar la escalabilidad y la flexibilidad para poder proporcionar experiencias de Internet de última generación en todos los dispositivos y las ubicaciones. Estos sistemas están diseñados para simplificar y mejorar el funcionamiento y la implementación de las redes de prestación de servicios.

#### Plataformas de router



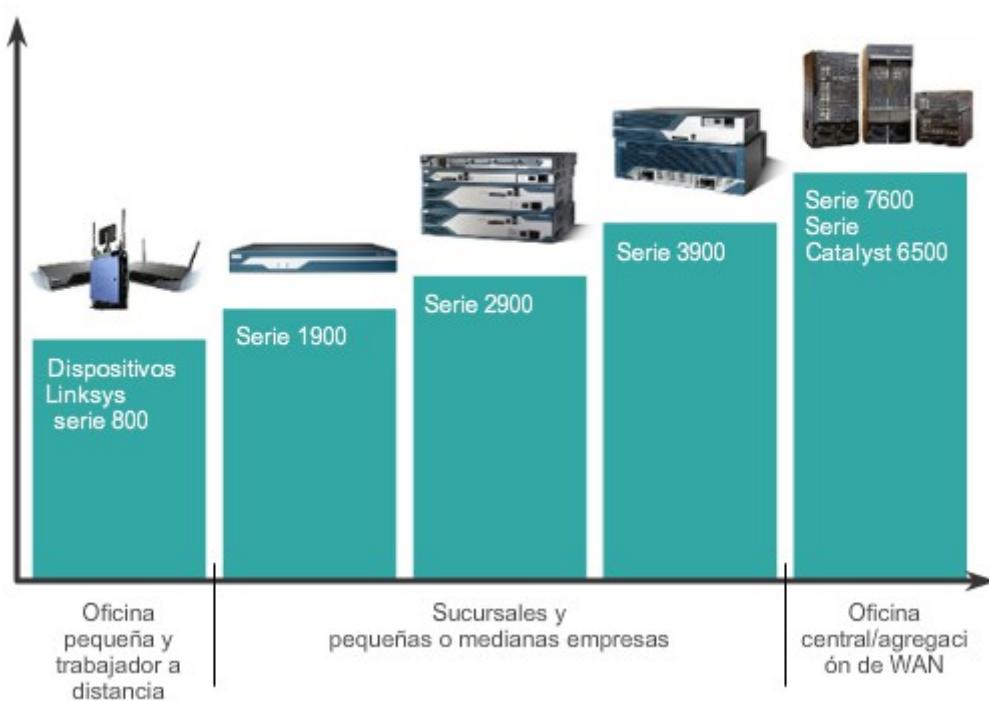
#### Capítulo 1: Introducción a escalamiento de redes 1.2.2.3 Hardware de routers

Además, los routers vienen en muchos factores de forma, como se muestra en la ilustración. Los administradores de red en un entorno empresarial deben poder brindar soporte a una

variedad de routers, desde un router de escritorio pequeño hasta uno montado en un rack o un modelo blade.

Los routers también pueden categorizarse como configuración fija o modular. Con la configuración fija, las interfaces de router deseadas están incorporadas. Los routers modulares cuentan con varias ranuras que permiten que el administrador de red modifique las interfaces en el router. Por ejemplo, el router Cisco 1841 cuenta con dos interfaces Fast Ethernet RJ-45 incorporadas y dos ranuras que pueden alojar diversos módulos de interfaz de red. Los routers tienen una variedad de interfaces distintas, tales como Fast y Gigabit Ethernet, Serial y de fibra óptica.

### Dispositivos de routing



Capítulo 1: Introducción a escalamiento de redes 1.2.2.4 Actividad: Identificar la categoría del

router

**Actividad: Identificar la categoría del router**

Una cada categoría de router con su descripción. Las categorías de router se pueden utilizar más de una vez.

Categoría de router	Descripciones de routers
Routers de perímetro de la red	Rápido rendimiento con alto nivel de seguridad para redes de centros de datos, campus y sucursales.
Routers de sucursal	Distribución completa de servicios de suscriptores.
Routers de perímetro de la red	Configuración y administración de red simples para LAN y WAN.
Routers de proveedores de servicios	Alta capacidad y escalabilidad con calidad de servicio jerárquica.
Routers de sucursal	Brinda experiencias de Internet de última generación en todos los dispositivos y ubicaciones.
Routers de proveedores de servicios	

**Verificar**

**Restablecer**

[Capítulo 1: Introducción a escalamiento de redes 1.2.3.1 Administración de licencias y archivos](#)

[del IOS](#)

Con una selección tan amplia de dispositivos de red para elegir en la línea de productos de Cisco, una organización puede seleccionar con detenimiento la combinación ideal para satisfacer las necesidades de los empleados y los clientes.

Al seleccionar o actualizar un dispositivo con IOS de Cisco, es importante elegir la imagen del IOS adecuada con el conjunto de características y la versión correctos. "IOS" se refiere al paquete de routing, switching, seguridad y otras tecnologías de internetworking integradas en un único sistema operativo multitarea. Cuando se envía un nuevo dispositivo, este tiene preinstalada la imagen del software y las licencias permanentes correspondientes para los paquetes y las características especificados por el cliente.

En cuanto a los routers, a partir de la versión 15.0 del software IOS de Cisco la compañía modificó el proceso para permitir nuevas tecnologías dentro de los conjuntos de características del IOS, como se muestra en la ilustración.

En el capítulo "Imágenes y licencias del IOS", se proporciona más información acerca de la administración y el mantenimiento de las licencias del IOS de Cisco.

## Familia de la versión 15 del software IOS de Cisco



Capítulo 1: Introducción a escalamiento de redes 1.2.3.2 Comparación entre administración en banda y fuera de banda

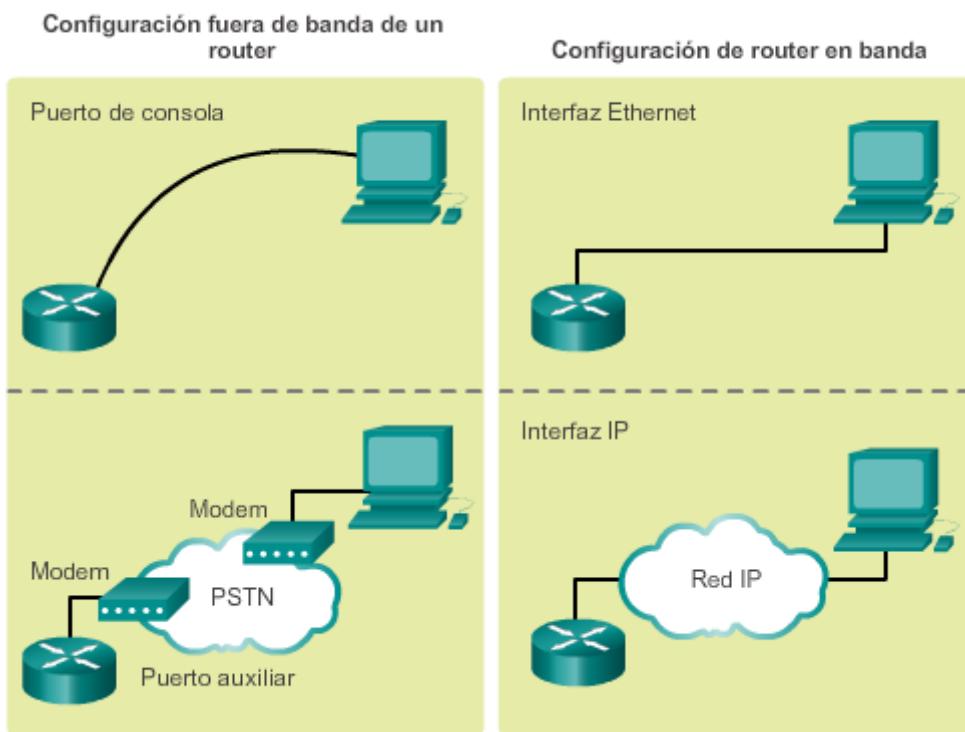
Más allá del dispositivo de red con IOS de Cisco que se implemente, existen dos métodos para conectar una computadora al dispositivo de red para realizar tareas de configuración y control. Estos métodos incluyen administración en banda y fuera de banda, como se muestra en la ilustración.

La administración fuera de banda se usa para la configuración inicial o cuando la conexión a la red no está disponible. La configuración que emplea administración fuera de banda requiere:

- Conexión directa al puerto de la consola o al puerto AUX
- Cliente de emulación de terminal

La administración en banda se utiliza para monitorear y hacer cambios de configuración en un dispositivo de red a través de una conexión de red. La configuración que emplea administración en banda requiere:

- Al menos, una interfaz de red en el dispositivo que se va a conectar y que va a funcionar
- Telnet, SSH o HTTP para acceder a un dispositivo Cisco



#### Capítulo 1: Introducción a escalamiento de redes 1.2.3.3 Comandos básicos de CLI del router

Una configuración básica de router incluye el nombre de host para la identificación, las contraseñas para la seguridad, la asignación de direcciones IP a las interfaces para la conectividad y, por último, routing básico. En la figura 1, se muestran los comandos que se introducen para habilitar un router con OSPF. Verifique y guarde los cambios en la configuración mediante el comando **copy running-config startup-config**. En la figura 2, se muestran los resultados de los comandos de configuración que se introdujeron en la figura 1. Para borrar la configuración del router, utilice el comando **erase startup-config** y, luego, el comando **reload**.

En la figura 3, utilice el verificador de sintaxis para verificar la configuración del router con estos comandos **show**.

## Habilitación de un router con OSPF

```
Router# configure terminal
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exec-timeout 0 0
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)# banner motd $ Authorized Access Only! $
R1(config)# interface GigabitEthernet0/0
R1(config-if)# description Link to LAN 1
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)# description Link to R2
R1(config-if)# ip address 172.16.3.1 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
R1(config-if)# ip address 192.168.10.5 255.255.255.252
R1(config-if)# no shut
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)# exit
R1(config)# end
```

### Capítulo 1: Introducción a escalamiento de redes 1.2.3.4 Comandos show básicos del router

A continuación, se muestran algunos de los comandos de IOS más utilizados para visualizar y verificar el estado operativo del router y la funcionalidad de la red relacionada con este estado. Estos comandos se clasifican en varias categorías.

En relación con el enrutamiento:

- **show ip protocols:** muestra información acerca de los protocolos de routing configurados. Si OSPF está configurado, en la información se incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110 (figura 1).
- **show ip route:** muestra la información de la tabla de routing, que incluye los códigos de routing, las redes conocidas, la distancia administrativa y las métricas, la forma en que

se descubrieron las rutas, el siguiente salto, las rutas estáticas y las rutas predeterminadas (figura 2).

- **show ip ospf neighbor:** muestra información acerca de los vecinos OSPF que se descubrieron, incluidos la ID del router del vecino, la prioridad, el estado (Full = se formó la adyacencia), la dirección IP y la interfaz local se que descubrió del vecino (figura 3).

En relación con la interfaz:

- **show interfaces:** muestra las interfaces con estado (del protocolo) de línea, ancho de banda, retraso, confiabilidad, encapsulación, dúplex y estadísticas de E/S. Se muestran todas las interfaces si están especificadas sin una designación de interfaz específica. Si se especifica una interfaz después del comando, solo se mostrará la información sobre esa interfaz. (figura 4).
- **show ip interfaces:** muestra información de la interfaz, incluidos el estado del protocolo, la dirección IP, si hay una dirección de ayuda configurada y si hay una ACL habilitada en la interfaz. Se muestran todas las interfaces si están especificadas sin una designación de interfaz específica. Si se especifica una interfaz después del comando, solo se mostrará la información sobre esa interfaz (figura 5).
- **show ip interface brief:** muestra todas las interfaces con información de direccionamiento IP y los estados de interfaz y de protocolo de línea (figura 6).
- **show protocols:** muestra información acerca del protocolo de routing que está habilitado y el estado del protocolo de las interfaces (figura 7).

Otros comandos relacionados con la conectividad incluyen el comando **show cdp neighbors** (figura 8). Este comando muestra información acerca de los dispositivos conectados directamente, incluidos la ID del dispositivo, la interfaz local a la que está conectado el dispositivo, la capacidad (R = router, S = switch), la plataforma y la ID del puerto del dispositivo remoto. La opción de detalles incluye información de direccionamiento IP y la versión del IOS.

Utilice el verificador de sintaxis en la figura 9 para verificar la configuración del router con estos comandos **show**.

### Comando show ip protocols

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          00:01:40
    2.2.2.2           110          00:17:53
  Distance: (default is 110)
```

### Comando show ip route

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

  172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C    172.16.1.0/24 is directly connected, GigabitEthernet0/0
L    172.16.1.1/32 is directly connected, GigabitEthernet0/0
C    172.16.3.0/30 is directly connected, Serial0/0/0
L    172.16.3.1/32 is directly connected, Serial0/0/0
O    192.168.2.0/24 [110/65] via 172.16.3.2, 00:18:52, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.10.6, 00:02:39, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.4/30 is directly connected, Serial0/0/1
L      192.168.10.5/32 is directly connected, Serial0/0/1
    192.168.23.0/30 is subnetted, 1 subnets
O      192.168.23.0 [110/128] via 192.168.10.6, 00:02:39, Serial0/0/1
                                  [110/128] via 172.16.3.2, 00:18:52, Serial0/0/0
```

### Comando show ip ospf neighbor

```
R1# show ip ospf neighbor

Neighbor ID      Pri      State      Dead Time      Address          Interface
3.3.3.3            0      FULL/ -      00:00:36    192.168.10.6    Serial0/0/1
2.2.2.2            0      FULL/ -      00:00:37    172.16.3.2      Serial0/0/0
```

### Comando show interfaces

```
R1# show interfaces gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c0
  (bia d48c.b5ce.a0c0)
  Description: Link to LAN 1
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is
  unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 01:16:14, output 00:00:15, 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
    3 packets input. 212 bytes. 0 no buffer
```

### Comando show ip interface

```
R1# show ip interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
```

**Comando show ip interface brief**

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status
Embedded-Service-Engine0/0 unassigned    YES unset administrati
GigabitEthernet0/0      172.16.1.1    YES manual up
GigabitEthernet0/1      unassigned    YES unset administrati
Serial0/0/0            172.16.3.1    YES manual up
Serial0/0/1            192.168.10.5  YES manual up
```

**Comando show protocols**

```
R1# show protocols
Global values:
  Internet Protocol routing is enabled
  Embedded-Service-Engine0/0 is administratively down, line prot
  GigabitEthernet0/0 is up, line protocol is up
    Internet address is 172.16.1.1/24
  GigabitEthernet0/1 is administratively down, line protocol is
  Serial0/0/0 is up, line protocol is up
    Internet address is 172.16.3.1/30
  Serial0/0/1 is up, line protocol is up
    Internet address is 192.168.10.5/30
```

**Comando show cdp neighbors**

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Rou
                  S - Switch, H - Host, I - IGMP, r - Repeater
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce     Holdtme     Capability  Platfor
R2              Ser 0/0/0        137          R S I      CISCO19
R3              Ser 0/0/1        178          R S I      CISCO19
```

En la configuración básica del switch, se incluyen el nombre de host para la identificación, las contraseñas para la seguridad y la asignación de direcciones IP para la conectividad. Para el acceso en banda, el switch debe tener una dirección IP. En la figura 1, se muestran los comandos que se introducen para habilitar un switch.

En la figura 2, se muestran los resultados de los comandos de configuración que se introdujeron en la figura 1. Verifique y guarde los cambios en la configuración del switch mediante el comando **copy running-config startup-config**. Para borrar la configuración del switch, utilice el comando **erase startup-config** y, luego, el comando **reload**. Es posible que también sea necesario borrar toda información de VLAN mediante el comando **delete flash:vlan.dat**. Cuando se haya establecido la configuración del switch, visualícela con el comando **show running-config**

### Habilitación del switch

```
Switch# enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# hostname S1
S1(config)# banner motd %Unauthorized access prohibited%
S1(config)# enable password cisco
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# interface vlan 1
S1(config-if)# ip address 192.168.1.5 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.1.1
S1(config)# interface fa0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
00:12:31: %SYS-5-CONFIG_I: Configured from console by console
S1#
S1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

## Configuración del switch

```
s1# show running-config
<resultado omitido>
Building configuration...
Current configuration : 1374 bytes
!
version 12.1
!
hostname s1
!
enable secret 5 $1$YpqJ$GKRD7WVFS.shosf2i5Pam/
enable password cisco
!
interface FastEthernet0/1
!
interface FastEthernet0/2
  switchport mode access
  switchport port-security
!
interface FastEthernet0/3
!
interface FastEthernet0/24
!
interface vlan1
  ip address 192.168.1.5 255.255.255.0
!
ip default-gateway 192.168.1.1
banner motd ^CUnauthorized access prohibited^C
!
line con 0
  password cisco
  login
line vty 0 4
  password cisco
  login
line vty 5 15
  login
end
```

### Capítulo 1: Introducción a escalamiento de redes 1.2.3.6 Comandos show básicos del switch

Los switches emplean comandos comunes de IOS para realizar la configuración, controlar la conectividad y visualizar el estado actual del switch. Haga clic en los botones 1 a 4 para ver resultados de ejemplo de los comandos y los datos importantes que puede reunir el administrador a partir de esa información.

En relación con el puerto / la interfaz:

- **show port-security:** muestra los puertos que tienen activada la seguridad. Para examinar una interfaz específica, incluya la ID de la interfaz. La información que se incluye en el resultado es la siguiente: la cantidad máxima de direcciones permitidas, el conteo actual, el conteo de infracciones de seguridad y la acción que se debe realizar (figura 1).
- **show port-security address:** muestra todas las direcciones MAC seguras configuradas en todas las interfaces del switch (figura 2).

- **show interfaces:** muestra una o todas las interfaces con estado (del protocolo) de línea, ancho de banda, retraso, confiabilidad, encapsulación, dúplex y estadísticas de E/S (figura 3).
- **show mac-address-table:** muestra todas las direcciones MAC que descubrió el switch, cómo se descubrieron esas direcciones (de forma dinámica o estática), el número de puerto y la VLAN asignada al puerto (figura 4).

Al igual que los routers, los switches también admiten el comando **show cdp neighbors**.

Las mismas técnicas de administración dentro y fuera de banda utilizadas para los routers también se utilizan para configurar el switch.

#### Comando show port-security

```
S1# show port-security interface fastethernet 0/19
Port Security           : Enabled
Port Status              : Secure-up
Violation Mode          : Shutdown
Aging Time               : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 50
Total MAC Addresses     : 1
Configured MAC Addresses: 0
Sticky MAC Addresses    : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count: 0
```

#### Comando show port-security address

```
S1# show port-security address
Secure Mac Address Table
-----
Vlan  Mac Address      Type        Ports  Remaining Age
                                         (mins)
-----
1    0025.83e6.4b01    SecureDynamic Fa0/18   -
1    0025.83e6.4b02    SecureSticky  Fa0/19   -
```

### Comando show interfaces

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01
  (bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is
  unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:06, 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
```

### Comando show mac-address-table

```
S1# show mac-address-table
      Mac Address Table
-----
Vlan      Mac Address          Type      Ports
----      -----
All       0014.6954.2480      STATIC    CPU
All       0100.0ccc.cccc      STATIC    CPU
All       0100.0ccc.cccc      STATIC    CPU
All       0100.0cdd.dddd      STATIC    CPU
1         000b.be02.a841      DYNAMIC   Fa0/1
1         000c.2999.758e      DYNAMIC   Fa0/2
1         000c.29c4.9e26      DYNAMIC   Fa0/3
1         000c.29ff.0744      DYNAMIC   Fa0/1
1         0014.6a46.e1c8      DYNAMIC   Fa0/2
1         0014.6a46.e1c9      DYNAMIC   Fa0/3
1         0016.763f.935d      DYNAMIC   Fa0/3
Total Mac Addresses for this criterion: 11
```

Capítulo 1: Introducción a escalamiento de redes 1.3.1.1 Actividad de clase: Simulación de diseño de red en capas

### **Simulación de diseño de red en capas**

Como administrador de una red muy pequeña, desea preparar una presentación de red simulada para explicarle al gerente de la sucursal cómo funciona actualmente la red.

La red pequeña incluye los siguientes equipos:

- Un router Cisco serie 2911
- Un switch serie 3560
- Un switch serie 2960
- Cuatro estaciones de trabajo de usuario (computadoras de escritorio o portátiles)
- Una impresora

[Actividad de clase: Simulación de diseño de red en capas](#)

Capítulo 1: Introducción a escalamiento de redes 1.3.1.2 Configuración básica del switch

**En esta actividad con verificador de sintaxis, se revisa la configuración básica del switch.**

**Configure el switch con el nombre de host "HQSw1".**

```
Switch# configure terminal
```

```
Switch(config)# hostname HQSw1
```

**Configure la contraseña cifrada "class" para el modo EXEC privilegiado.**

```
HQSw1(config)# enable secret class
```

**Establezca la contraseña "cisco" para todas las líneas, de modo que se requiera iniciar sesión, comenzando por la línea de consola. Establezca las líneas vty de 0 a 15.**

```
HQSw1(config)# line console 0
```

```
HQSw1(config-line)# password cisco
```

```
HQSw1(config-line)# login
```

```
HQSw1(config-line)# line vty 0 15
```

```
HQSw1(config-line)# password cisco
```

```
HQSw1(config-line)# login
```

**Vuelva al modo de configuración global. Introduzca el comando para encriptar la contraseña de texto no cifrado.**

```
HQSw1(config-line)# exit
```

```
HQSw1(config)# service password-encryption
```

**Configure la VLAN 1 con la dirección IP 192.168.10.2/24 y active la interfaz.**

```
HQSw1(config)# interface vlan 1:
```

```
HQSw1(config-if)# ip address 192.168.10.2 255.255.255.0:
```

```
HQSw1(config-if)# no shutdown:
```

```
%LINK-5-CHANGED: Interface Vlan1, changed state to up
```

**Vuelva directamente al modo EXEC privilegiado y muestre la configuración actual.**

```
HQSw1(config-if)# end
```

```
HQSw1# show running-config
```

```
Building configuration...
```

```
Current configuration : 1178 bytes
```

```
!
```

```
version 12.2
```

```
no service timestamps log datetime msec
```

```
no service timestamps debug datetime msec
```

```
service password-encryption
```

```
!
```

```
hostname HQSw1
```

```
!
```

```
enable secret 5 $1$MERrS9CTjUIEqNGurQiFU.Zecii
```

```
!
```

```
!
```

```
<resultado omitido>
```

```
!
```

```
!
```

```
interface Vlan1
```

```
  ip address 192.168.10.2 255.255.255.0:
```

```
!
```

```
!
```

```
line con 0
```

```
  password 7 0822455D0A16
```

```
  login
```

```
!
```

```
line vty 0 4
```

```
  password 7 0822455D0A16
```

```
  login
```

```
line vty 5 15
```

```
  password 7 0822455D0A16
```

```
  login
```

```
!
```

```
!
```

```
end
```

```
HQSw1#
```

**Completó correctamente la configuración básica del switch HQSw1.**

## Capítulo 1: Introducción a escalamiento de redes 1.3.1.3 Packet Tracer: desafío de integración

de habilidades

### **Información básica/situación**

Como técnico de LAN contratado recientemente, el administrador de red le solicitó que demuestre su habilidad para configurar una LAN pequeña. Sus tareas incluyen la configuración de parámetros iniciales en dos switches mediante IOS de Cisco y la configuración de parámetros de dirección IP en dispositivos host para proporcionar conectividad de extremo a extremo. Debe utilizar dos switches y dos hosts/PC en una red conectada por cable y con alimentación.

[Packet Tracer: desafío de habilidades de integración \(instrucciones\)](#)

[Packet Tracer: desafío de integración de habilidades \(PKA\)](#)

## Capítulo 1: Introducción a escalamiento de redes 1.3.1.4 Resumen

El modelo de diseño de red jerárquico divide la funcionalidad de la red en la capa de acceso, la de distribución y la de núcleo. La arquitectura empresarial de Cisco divide aún más la red en componentes funcionales.

Una red bien diseñada controla el tráfico y limita el tamaño de los dominios de fallas. Los routers y los switches multicapa se pueden implementar de a pares para que la falla de un único dispositivo no provoque interrupciones en el servicio.

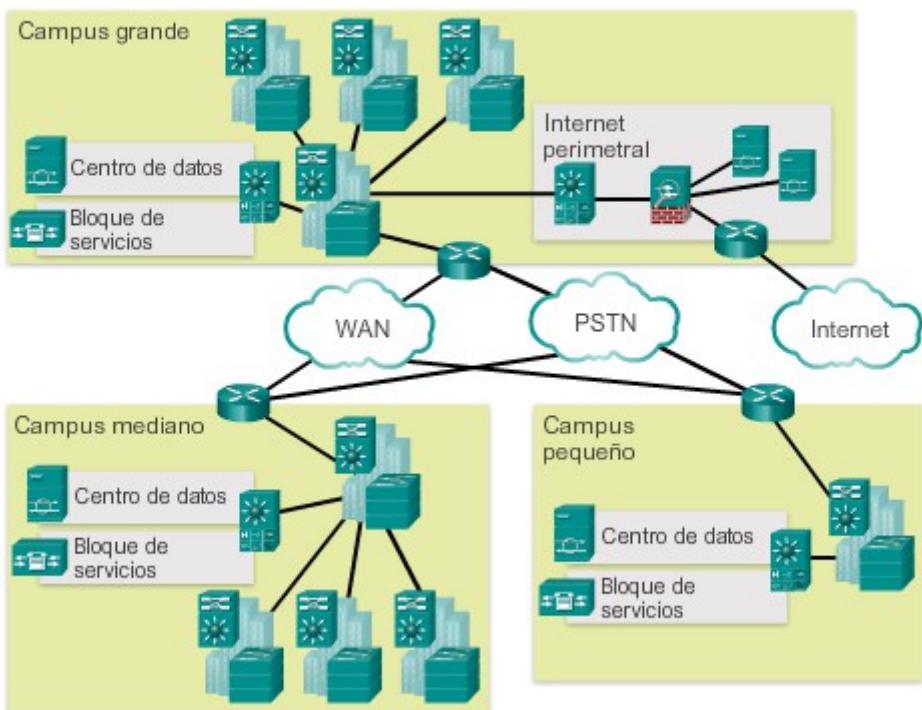
Un diseño de red debe incluir una estrategia de direccionamiento IP, protocolos de routing escalables y de convergencia rápida, protocolos de capa 2 adecuados y dispositivos modulares o agrupados en clústeres que puedan actualizarse fácilmente para incrementar la capacidad.

Un servidor crítico debe estar conectado a dos switches de capa de acceso diferentes. Debe contar con módulos redundantes, siempre que sea posible, y con una fuente de alimentación de respaldo. Incluso podría sería apropiado proporcionar varias conexiones a uno o varios ISP.

Los sistemas de control de seguridad y los sistemas de telefonía IP deben ser de alta disponibilidad y, por lo general, tienen consideraciones especiales de diseño.

El diseñador de red debe especificar un router de la categoría apropiada, ya sea un router de sucursal, un router de perímetro de la red o un router de proveedor de servicios. También es importante implementar el tipo de switch adecuado para un conjunto de requisitos, características y especificaciones de switch determinados y el flujo de tráfico esperado.

## Redes comutadas sin fronteras



### Capítulo 2: Redundancia de LAN 2.0.1.1 Introducción

La redundancia de red es clave para mantener la confiabilidad de la red. Varios enlaces físicos entre dispositivos proporcionan rutas redundantes. De esta forma, la red puede continuar funcionando si falló un único enlace o puerto. Los enlaces redundantes también pueden compartir la carga de tráfico y aumentar la capacidad.

Se deben administrar varias rutas para que no se produzcan bucles en la capa 2. Se eligen las mejores rutas, y se cuenta con una ruta alternativa de inmediato en caso de que falle una ruta principal. Los protocolos de árbol de expansión se utilizan para administrar la redundancia de capa 2.

Los dispositivos redundantes, como los routers o los switches multicapa, proporcionan la capacidad de que un cliente utilice un gateway predeterminado alternativo en caso de que falle el gateway predeterminado principal. Es posible que ahora un cliente posea varias rutas a más de un gateway predeterminado posible. Los protocolos de redundancia de primer salto se utilizan para administrar la forma en que se asigna un gateway predeterminado a un cliente y permitir el uso de un gateway predeterminado alternativo en caso de que falle el principal.

En este capítulo, se analizan los protocolos utilizados para administrar esas formas de redundancia. Además, se abordan algunos de los posibles problemas de redundancia y sus síntomas.

**Al completar este capítulo, usted podrá:**

- Describir los problemas de implementación de una red redundante.
- Describir el funcionamiento de STP IEEE 802.1D.
- Describir las diferentes variedades de árbol de expansión.
- Describir el funcionamiento de PVST+ en un entorno LAN conmutado.
- Describir el funcionamiento de PVST+ rápido en un entorno LAN conmutado.
- Configurar PVST+ en un entorno LAN conmutado.
- Configurar PVST+ rápido en un entorno LAN conmutado.
- Identificar los problemas de configuración de STP.
- Describir el propósito y el funcionamiento de los protocolos de redundancia de primer salto.
- Describir las diferentes variedades de protocolos de redundancia de primer salto.
- Utilizar los comandos del IOS de Cisco para verificar las implementaciones de HSRP y GLBP.

Capítulo

2: Redundancia de LAN 2.0.1.2 Actividad de clase: Tráfico intenso

**Tráfico intenso**

Es su primer día de trabajo como administrador de red de una pequeña a mediana empresa. El administrador de red anterior renunció repentinamente después de que se realizó una actualización de la red en la empresa.

Durante la actualización, se agregó un switch nuevo. Desde la actualización, muchos empleados se quejaron de que tienen problemas para acceder a Internet y a los servidores en la red. De hecho, la mayoría de ellos no puede acceder a la red en absoluto. Su administrador corporativo le solicita que investigue de inmediato las posibles causas de estos problemas y demoras en la conectividad.

Por eso, estudia el equipo que opera en la red en la instalación de distribución principal del edificio. Observa que, a la vista, la topología de la red parece ser correcta y que los cables se conectaron debidamente; los routers y switches están encendidos y en funcionamiento; y los switches están conectados entre sí para proporcionar respaldo o redundancia.

Sin embargo, una cosa que advierte es que todas las luces de actividad de los switches parpadean constantemente a una velocidad muy rápida, al punto de que casi parecen sólidos. Cree que encontró el problema de conectividad que los empleados están experimentando.

Utilice Internet para investigar STP. Mientras investiga, tome nota y describa lo siguiente:

- Tormenta de difusión
- Bucles de switching
- Propósito de STP
- Variaciones de STP

Complete las preguntas de reflexión que se proporcionan con el archivo PDF de esta actividad. Guarde su trabajo y esté preparado para compartir las respuestas con la clase.

### [Actividad de clase: Tráfico intenso](#)



*Protocolo de árbol de expansión: STP es un estándar IEEE que proporciona rutas despejadas de redes conmutadas.*

### Capítulo 2: Redundancia de LAN 2.1.1.1 Redundancia en las capas 1 y 2 del modelo OSI

El diseño de red jerárquico de tres niveles, que utiliza las capas de núcleo, de distribución y de acceso con redundancia, intenta eliminar un único punto de falla en la red. Varias rutas conectadas por cables entre switches proporcionan redundancia física en una red conmutada. Esto mejora la confiabilidad y la disponibilidad de la red. Tener rutas físicas alternativas para que los datos atraviesen la red permite que los usuarios accedan a los recursos de red, a pesar de las interrupciones de la ruta.

Haga clic en el botón Reproducir de la figura 1 para ver una animación acerca de la redundancia.

1. La PC1 se comunica con la PC4 a través de una topología de red redundante.
2. Cuando se interrumpe el enlace de red entre el S1 y el S2, la ruta entre la PC1 y la PC4 se ajusta automáticamente para compensar la interrupción.
3. Cuando se restaura la conexión de red entre el S1 y el S2, la ruta se vuelve a ajustar para enrutar el tráfico directamente del S2 al S1 para llegar a la PC4.

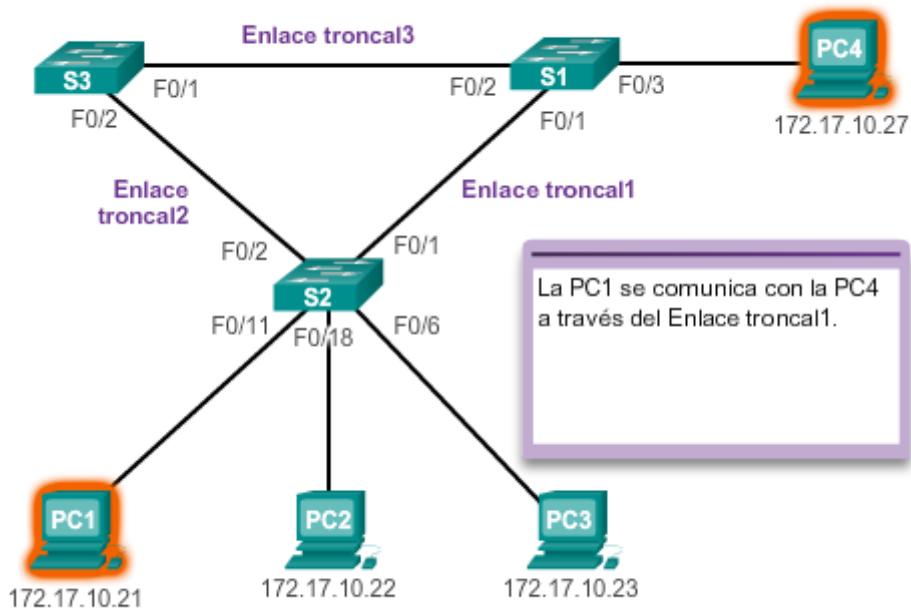
Para la mayoría de las organizaciones, la disponibilidad de la red es fundamental para cumplir con las necesidades empresariales; por lo tanto, el diseño de la infraestructura de red es un elemento crucial para empresas. La redundancia de rutas es una solución para proporcionar la disponibilidad necesaria de varios servicios de red mediante la eliminación de la posibilidad de un único punto de falla.

**Nota:** la redundancia en la capa 1 del modelo OSI se representa mediante el uso de varios enlaces y dispositivos, pero se necesita más que solo la planificación física para completar la configuración de la red. Para que la redundancia funcione de forma sistemática, también se deben utilizar protocolos de capa 2 del modelo OSI, como STP.

La redundancia es una parte importante del diseño jerárquico para evitar que se interrumpa la entrega de los servicios de red a los usuarios. Las redes redundantes requieren la adición de rutas físicas, pero la redundancia lógica también debe formar parte del diseño. Sin embargo, las rutas redundantes en una red Ethernet conmutada pueden causar bucles físicos y lógicos en la capa 2.

Los bucles físicos en la capa 2 pueden ocurrir como consecuencia del funcionamiento normal de los switches, en especial, del proceso de descubrimiento y reenvío. Cuando existen varias rutas entre dos dispositivos en una red y no se implementan protocolos de árbol de expansión en los switches, ocurre un bucle en la capa 2. Un bucle en la capa 2 puede provocar tres problemas principales, como se indica en la figura 2.

## Redundancia en una red jerárquica



### Consideraciones que se deben tener en cuenta al implementar la redundancia:

- Inestabilidad de la base de datos MAC:** la inestabilidad del contenido de la tabla de direcciones MAC se produce por recibir copias de la misma trama en diferentes puertos del switch. El reenvío de datos se puede ver afectado cuando el switch consume los recursos que lidian con la inestabilidad en la tabla de direcciones MAC.
- Tormentas de difusión:** los switches pueden saturar la red con difusiones incesantemente si no se implementa un proceso para evitar bucles. Esta situación se conoce comúnmente como "tormenta de difusión".
- Transmisión de varias tramas:** es posible que se entreguen varias copias de las tramas de unidifusión en las estaciones de destino. Muchos protocolos esperan recibir una única copia de cada transmisión. Varias copias de la misma trama pueden provocar errores de los que no se puede recuperar.

Capítulo 2: Redundancia de LAN 2.1.1.2 Problemas con la redundancia de capa 1: inestabilidad

de la base de datos MAC

**Inestabilidad de la base de datos MAC**

Las tramas de Ethernet no poseen un atributo de tiempo de vida (TTL) como los paquetes IP. Como resultado, si no hay un mecanismo habilitado para bloquear la propagación continua de estas tramas en una red conmutada, continúan propagándose entre los switches incesantemente, o hasta que un enlace se interrumpa y rompa el bucle. Esta propagación continua entre switches puede provocar la inestabilidad de la base de datos MAC. Esto puede ocurrir a causa del reenvío de tramas de difusión.

Las tramas de difusión se reenvían por todos los puertos de switch, excepto por el puerto de entrada original. Esto asegura que todos los dispositivos en un dominio de difusión reciban la trama. Si hay más de una ruta para reenviar la trama, se puede formar un bucle infinito. Cuando ocurre un bucle, la tabla de direcciones MAC en un switch puede cambiar constantemente con las actualizaciones de las tramas de difusión, lo que provoca la inestabilidad de la base de datos MAC.

Haga clic en el botón Reproducir en la ilustración para ver la animación. Cuando se detenga la animación, lea el texto a la izquierda de la topología. La animación continuará después de una pausa breve.

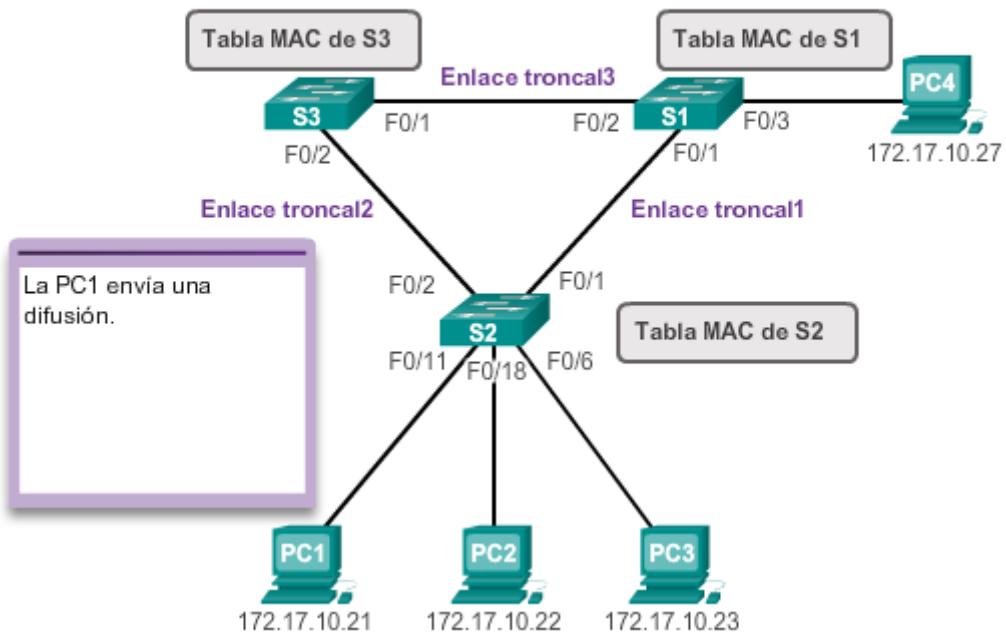
En la animación:

1. La PC1 envía una trama de difusión al S2. El S2 recibe la trama de difusión en F0/11. Cuando el S2 recibe la trama de difusión, actualiza su tabla de direcciones MAC para registrar que la PC1 está disponible en el puerto F0/11.
2. Debido a que es una trama de difusión, el S2 reenvía la trama por todos los puertos, incluidos el Enlace\_troncal1 y el Enlace\_troncal2. Cuando la trama de difusión llega al S3 y al S1, estos actualizan sus tablas de direcciones MAC para indicar que la PC1 está disponible en el puerto F0/1 del S1 y en el puerto F0/2 del S3.
3. Dado que es una trama de difusión, el S3 y el S1 reenvían la trama por todos los puertos, excepto el puerto de entrada. El S3 envía las tramas de difusión desde la PC1 hasta el S1. El S1 envía las tramas de difusión desde la PC1 hasta el S3. Cada switch actualiza su tabla de direcciones MAC con el puerto incorrecto para la PC1.
4. Cada switch vuelve a reenviar la trama de difusión por todos sus puertos, excepto el puerto de entrada, lo que provoca que los dos switches reenvíen la trama al S2.
5. Cuando el S2 recibe las tramas de difusión del S3 y el S1, la tabla de direcciones MAC se vuelve a actualizar, esta vez con la última entrada recibida de los otros dos switches.

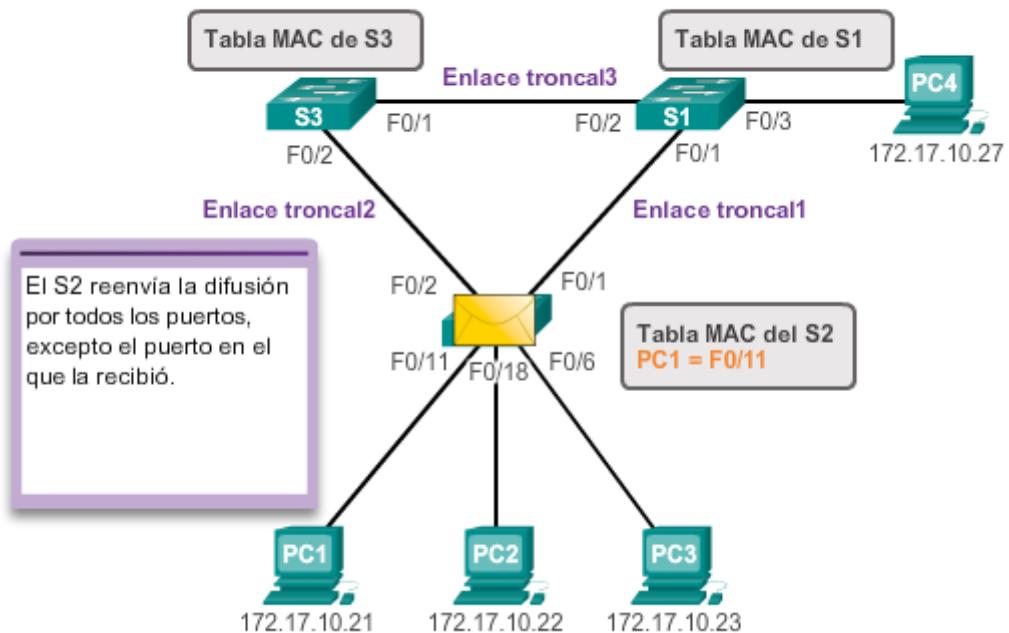
Este proceso se repite una y otra vez hasta que se rompe el bucle al desconectar físicamente las conexiones que lo causan o al apagar uno de los switches en el bucle. Esto crea una alta carga de CPU en todos los switches atrapados en el bucle. Debido a que se reenvían las mismas tramas constantemente entre todos los switches en el bucle, la CPU del switch debe procesar una gran cantidad de datos. Esto disminuye el rendimiento del switch cuando llega tráfico legítimo.

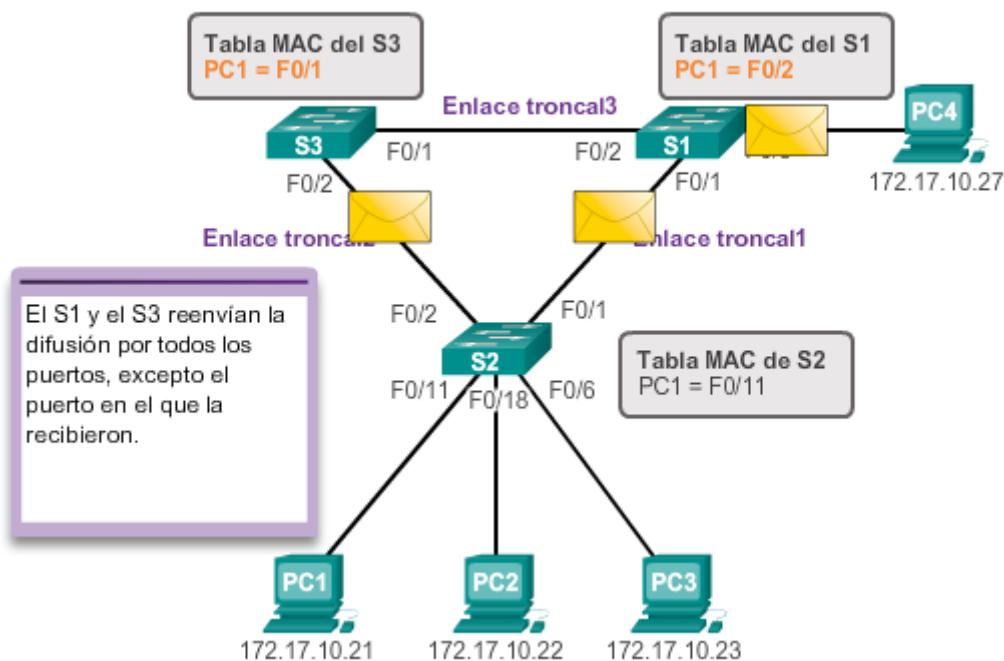
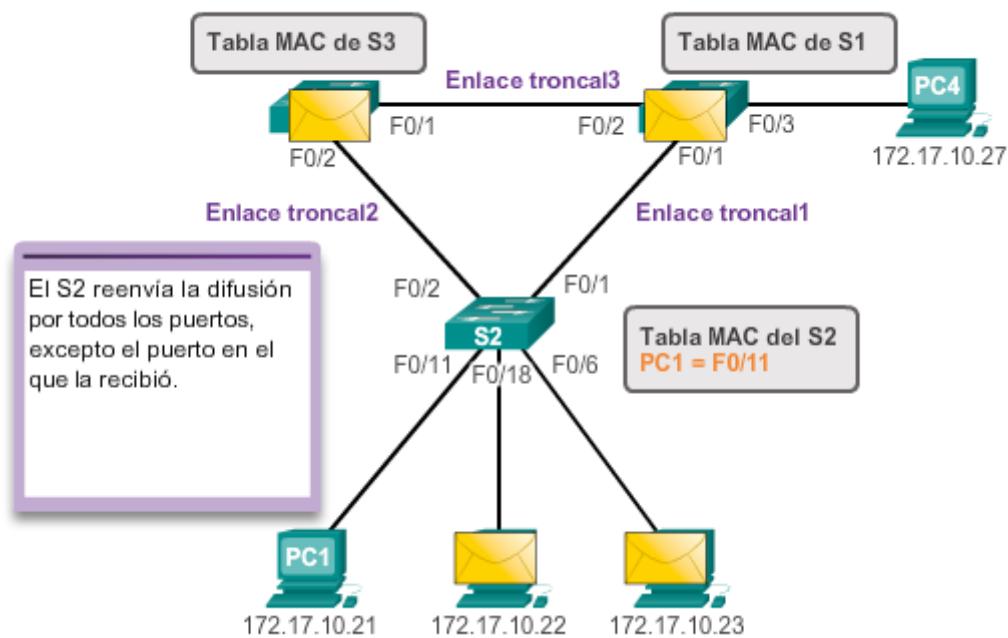
Un host atrapado en un bucle de red es inaccesible para otros hosts de la red. Además, debido a los constantes cambios en la tabla de direcciones MAC, el switch no sabe cuál es el puerto por el que debe reenviar las tramas de unidifusión. En el ejemplo anterior, los puertos que se indican para la PC1 en los switches son incorrectos. Cualquier trama de unidifusión destinada a la PC1 forma un bucle en la red, al igual que lo hacen las tramas de difusión. Al haber cada vez más tramas que forman bucles en la red, con el tiempo, se crea una tormenta de difusión.

### Bucles de la Capa 2

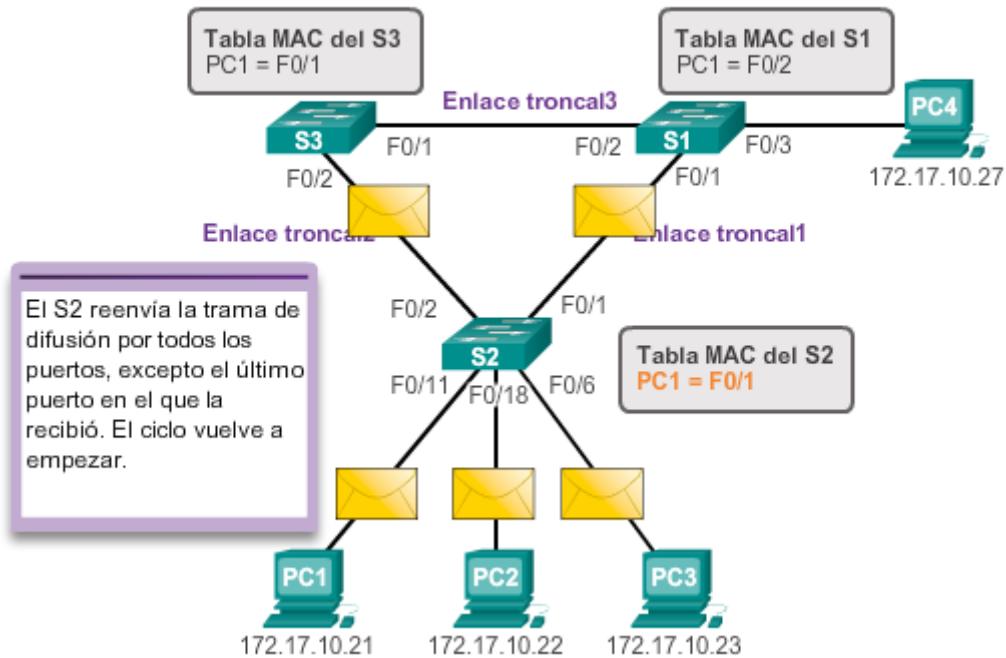


### Bucles de la Capa 2





## Bucles de la Capa 2



### Capítulo 2: Redundancia de LAN 2.1.1.3 Problemas con la redundancia de capa 1: tormentas de difusión

#### Tormenta de difusión

Una tormenta de difusión se produce cuando existen tantas tramas de difusión atrapadas en un bucle de Capa 2, que se consume todo el ancho de banda disponible. Como consecuencia, no hay ancho de banda disponible para el tráfico legítimo y la red deja de estar disponible para la comunicación de datos. Esto es una denegación de servicio eficaz.

La tormenta de difusión es inevitable en una red con bucles. A medida que más dispositivos envían difusiones a través de la red, más tráfico se concentra en el bucle, lo que consume recursos. Finalmente, se crea una tormenta de difusión que hace fallar la red.

Existen otras consecuencias de las tormentas de difusión. Debido a que el tráfico de difusión se envía a todos los puertos del switch, todos los dispositivos conectados deben procesar todo el tráfico de difusión que fluye indefinidamente en la red con bucles. Esto puede hacer que la terminal no funcione bien a causa de los altos requisitos de procesamiento para mantener una carga de tráfico tan elevada en la NIC.

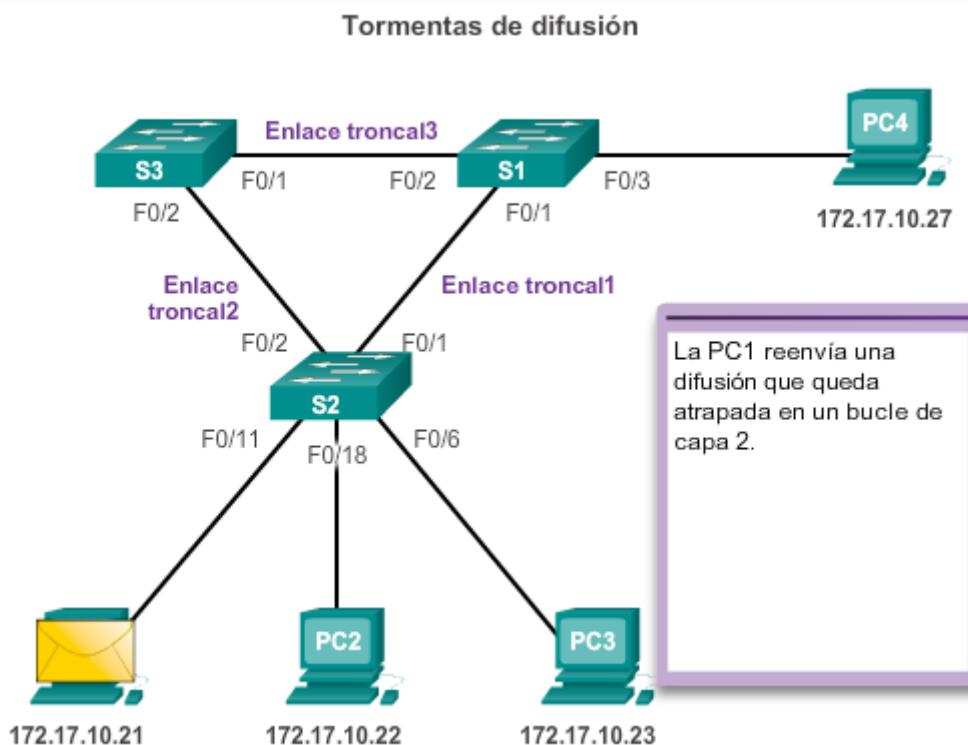
Haga clic en el botón Reproducir de la ilustración para ver una animación de una tormenta de difusión. Cuando se detenga la animación, lea el texto a la derecha de la topología. La animación continuará después de una pausa breve.

En la animación:

1. La PC1 envía una trama de difusión a la red con bucles.

2. La trama de difusión crea un bucle entre todos los switches interconectados en la red.
3. La PC4 también envía una trama de difusión a la red con bucles.
4. La trama de difusión de la PC4 también queda atrapada en el bucle entre todos los switches interconectados, al igual que la trama de difusión de la PC1.
5. A medida que más dispositivos envían difusiones a través de la red, más tráfico se concentra en el bucle, lo que consume recursos. Finalmente, se crea una tormenta de difusión que hace fallar la red.
6. Cuando la red se satura por completo con tráfico de difusión que genera un bucle entre los switches, el switch descarta el tráfico nuevo porque no lo puede procesar.

Dado que los dispositivos conectados a una red envían regularmente tramas de difusión, como las solicitudes de ARP, se puede formar una tormenta de difusión en segundos. Como resultado, cuando se crea un bucle, la red comunitada se desactiva con rapidez.



Capítulo 2: Redundancia de LAN 2.1.1.4 Problemas con la redundancia de capa 1: tramas de unidifusión duplicadas

### Transmisiones de múltiples tramas

Las tramas de difusión no son el único tipo de tramas que son afectadas por los bucles. Las tramas de unicast enviadas a una red con bucles pueden generar tramas duplicadas que llegan al dispositivo de destino.

Haga clic en el botón Reproducir de la ilustración para ver una animación de este problema. Cuando se detenga la animación, lea el texto a la derecha de la topología. La animación continuará después de una pausa breve.

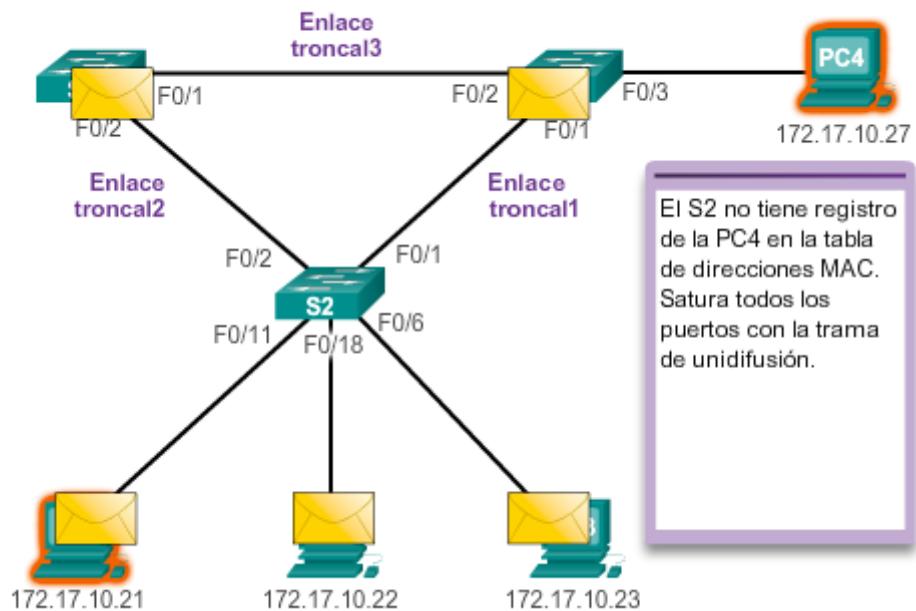
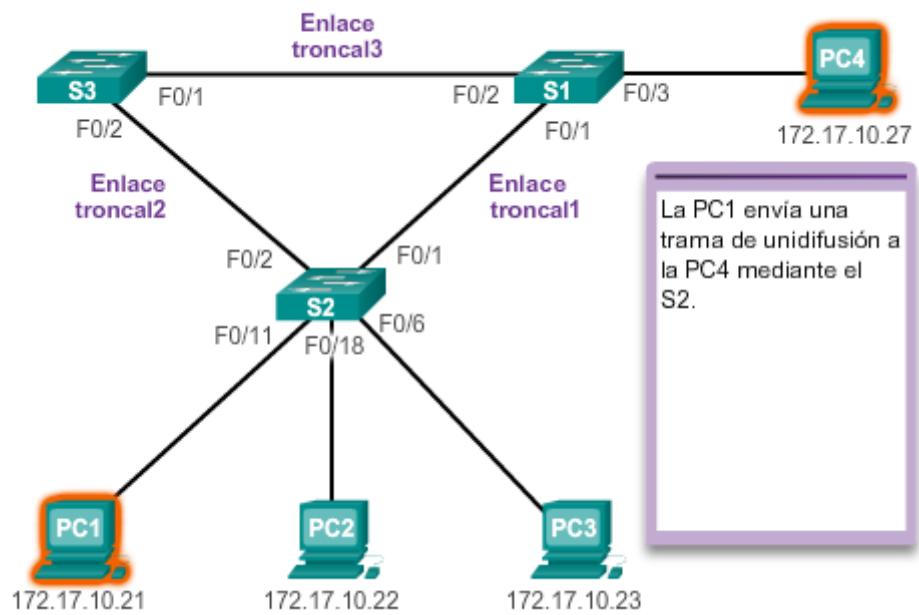
En la animación:

1. La PC1 envía una trama de unicast con destino a la PC4.
2. El S2 no tiene ninguna entrada para la PC4 en su tabla MAC, por lo que satura todos los puertos del switch con la trama de unidifusión para intentar encontrar a la PC4.
3. La trama llega a los switches S1 y S3.
4. S1 no posee una entrada de dirección MAC para la PC4, de forma que reenvía la trama a la PC4.
5. S3 también cuenta con una entrada en su tabla de direcciones MAC para la PC4, de manera que reenvía la trama de unicast a través del Enlace troncal3 a S1.
6. El S1 recibe la trama duplicada y la reenvía a la PC4.
7. La PC4 ha recibido ahora la misma trama dos veces.

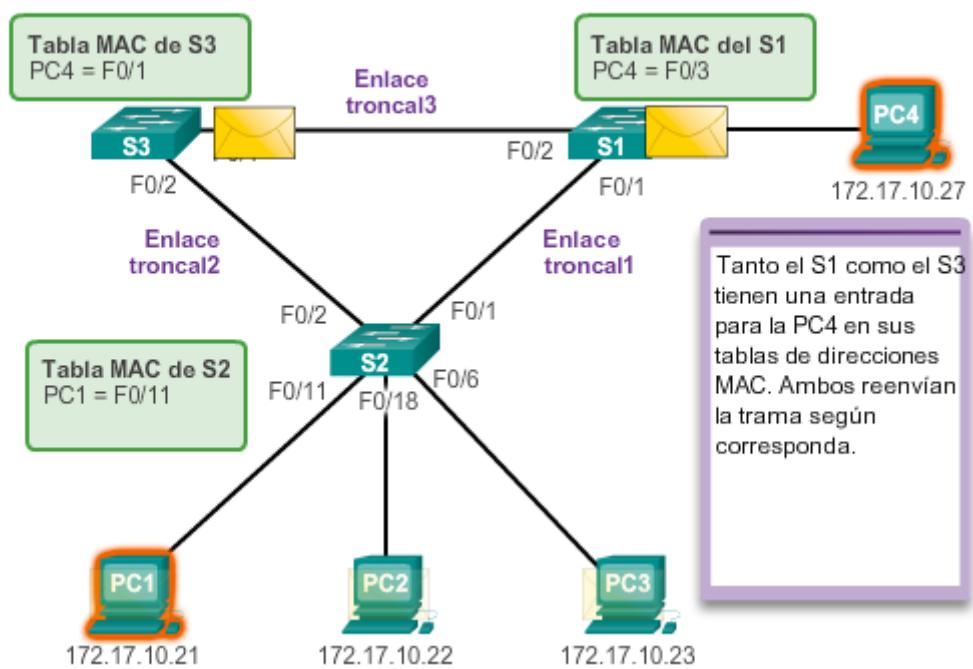
La mayoría de los protocolos de capa superior no están diseñados para reconocer las transmisiones duplicadas o lidiar con ellas. En general, los protocolos que utilizan un mecanismo de numeración en secuencia asumen que la transmisión ha fallado y que el número de secuencia se ha reciclado para otra sesión de comunicación. Otros protocolos intentan enviar la transmisión duplicada al protocolo de capa superior adecuado para que sea procesada y posiblemente descartada.

Los protocolos LAN de capa 2, como Ethernet, carecen de mecanismos para reconocer y eliminar las tramas que forman bucles incessantes. Algunos protocolos de capa 3 implementan un mecanismo de TTL que limita la cantidad de veces que un dispositivo de red de capa 3 puede volver a transmitir un paquete. Los dispositivos de capa 2, que carecen de este mecanismo, continúan retransmitiendo de forma indefinida el tráfico que genera bucles. STP, un mecanismo que sirve para evitar los bucles en la capa 2, se desarrolló para enfrentar estos problemas.

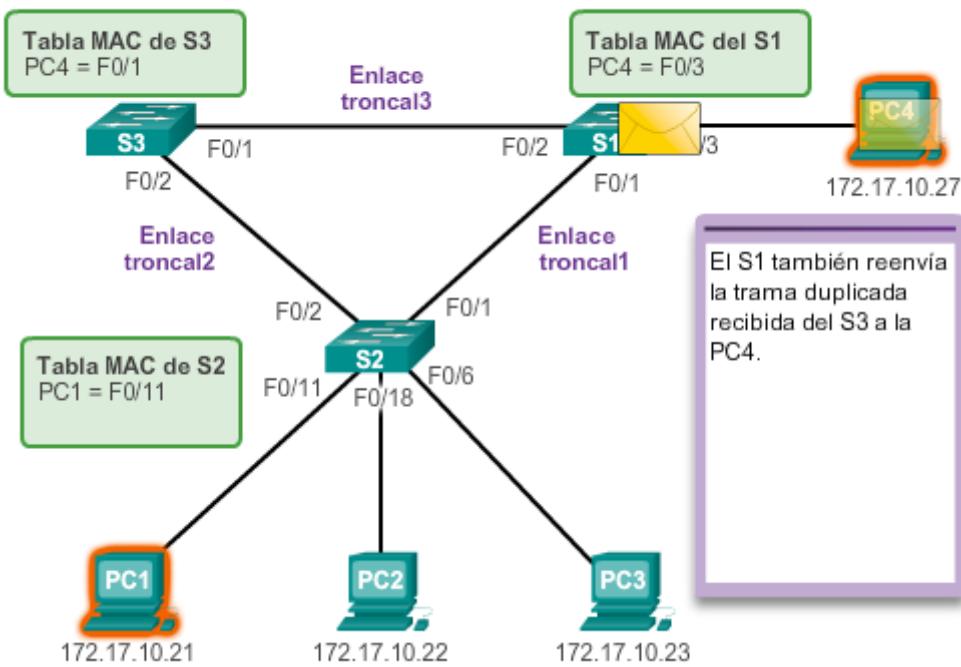
Para evitar que ocurran estos problemas en una red redundante, se debe habilitar algún tipo de árbol de expansión en los switches. De manera predeterminada, el árbol de expansión está habilitado en los switches Cisco para prevenir que ocurran bucles en la capa 2.



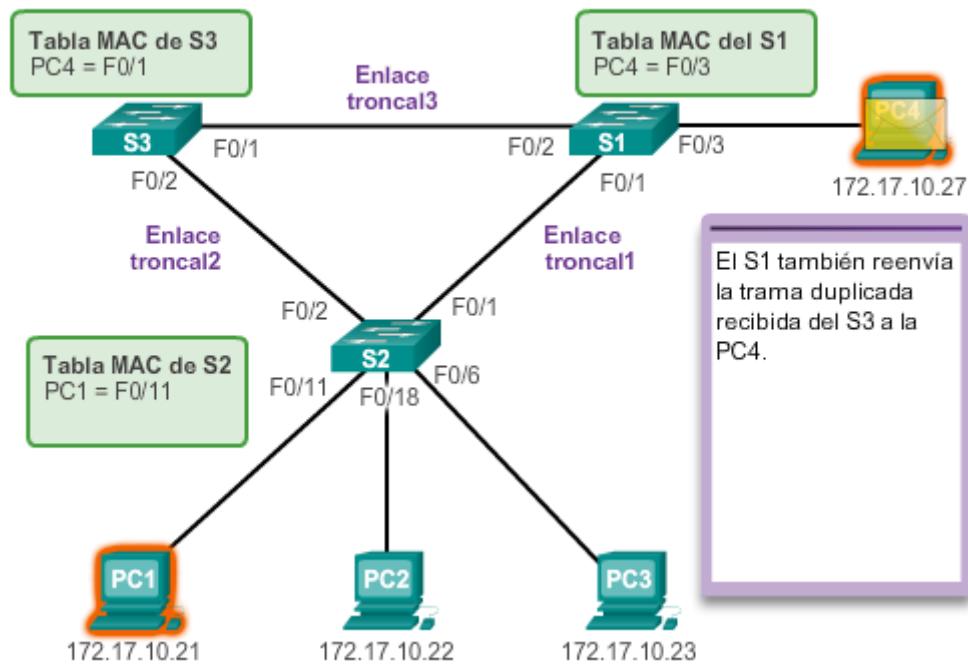
### Tramas de unidifusión duplicadas



### Tramas de unidifusión duplicadas



### Tramas de unidifusión duplicadas



Capítulo 2: Redundancia de LAN 2.1.1.5 Packet Tracer: Análisis de un diseño redundante

Información básica/situación

En esta actividad, observará cómo funciona STP, de manera predeterminada, y cómo reacciona ante fallas. Se agregaron switches que no requieren configuración a la red. Los switches de Cisco se pueden conectar a la red sin ninguna acción adicional requerida por parte del administrador de red. Se modificó la prioridad del puente a los fines de esta actividad.

[Packet Tracer: Análisis de un diseño redundante \(instrucciones\)](#)

[Packet Tracer: Análisis de un diseño redundante \(PKA\)](#)

#### Capítulo 2: Redundancia de LAN 2.1.2.1 Algoritmo de árbol de expansión: introducción

La redundancia aumenta la disponibilidad de la topología de red al proteger la red de un único punto de falla, como un cable de red o switch que fallan. Cuando se introduce la redundancia física en un diseño, se producen bucles y se duplican las tramas. Esto trae consecuencias graves para las redes conmutadas. El protocolo de árbol de expansión (STP) fue desarrollado para enfrentar estos inconvenientes.

STP asegura que exista sólo una ruta lógica entre todos los destinos de la red, al realizar un bloqueo de forma intencional a aquellas rutas redundantes que puedan ocasionar un bucle. Se considera que un puerto está bloqueado cuando no se permite que entren o salgan datos de usuario por ese puerto. Esto no incluye las tramas de unidad de datos de protocolo puente (BPDU) utilizadas por STP para evitar bucles. El bloqueo de las rutas redundantes es fundamental para evitar bucles en la red. Las rutas físicas aún existen para proporcionar la redundancia, pero las mismas se deshabilitan para evitar que se generen bucles. Si alguna vez la ruta es necesaria para compensar la falla de un cable de red o de un switch, STP vuelve a calcular las rutas y desbloquea los puertos necesarios para permitir que la ruta redundante se active.

Haga clic en el botón Reproducir de la figura 1 para ver el protocolo STP en acción.

En el ejemplo, STP está habilitado en todos los switches.

1. La PC1 envía un difusión a la red.
2. El S2 está configurado con STP y estableció el puerto para Enlace\_troncal2 en estado de bloqueo. El estado de bloqueo evita que se utilicen los puertos para reenviar datos de usuario, de modo de evitar que ocurra un bucle. El S2 reenvía una trama de difusión por todos los puertos del switch, excepto el puerto de origen de la PC1 y el puerto para Enlace\_troncal2.
3. El S1 recibe la trama de difusión y la reenvía por todos sus puertos de switch, por donde llega a la PC4 y al S3. El S3 reenvía la trama por el puerto para Enlace\_troncal2, y el S2 descarta la trama. Se evita el bucle de Capa 2.

Haga clic en el botón Reproducir de la figura 2 para ver el nuevo cálculo de STP cuando ocurre una falla.

En este ejemplo:

1. La PC1 envía un difusión a la red.

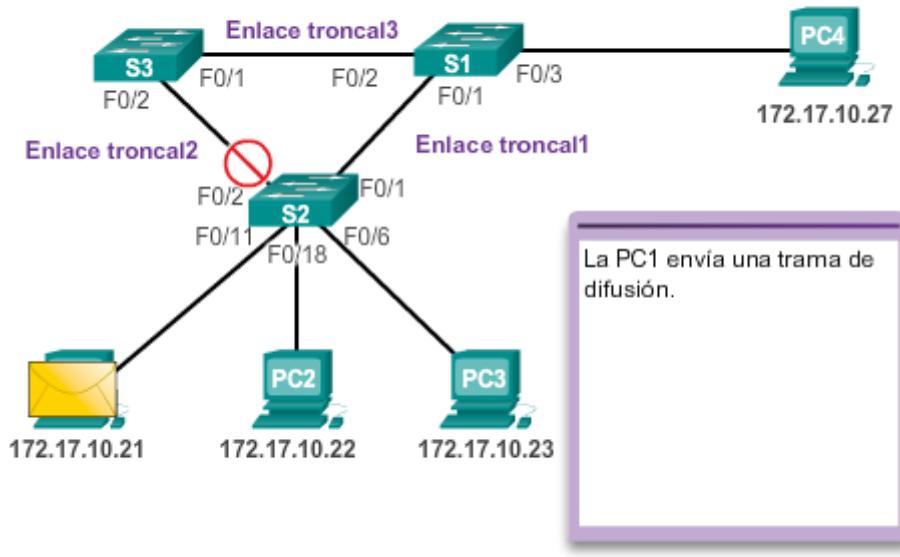
2. Luego la difusión se envía a través de la red, de la misma forma que en la animación anterior.
3. El enlace troncal entre el S2 y el S1 falla, lo que provoca una interrupción en la ruta anterior.
4. El S2 desbloquea el puerto que se había bloqueado anteriormente para Enlace\_troncal2 y permite que el tráfico de difusión atraviese la ruta alternativa alrededor de la red, lo que permite que continúe la comunicación. Si este enlace vuelve a activarse, STP vuelve a converger y el puerto en el S2 se vuelve a bloquear.

STP evita que ocurran bucles mediante la configuración de una ruta sin bucles a través de la red, con puertos “en estado de bloqueo” ubicados estratégicamente. Los switches que ejecutan STP pueden compensar las fallas mediante el desbloqueo dinámico de los puertos bloqueados anteriormente y el permiso para que el tráfico se transmita por las rutas alternativas.

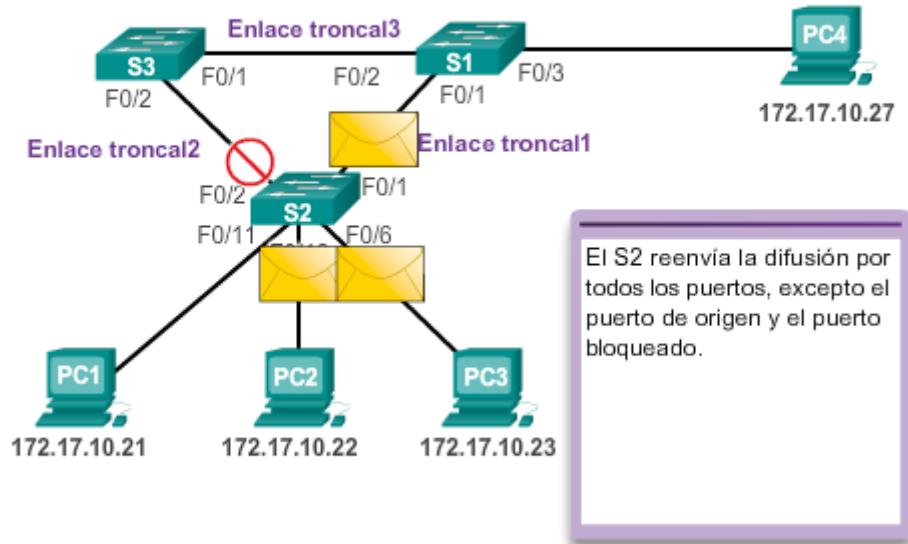
Hasta ahora, utilizamos el término “protocolo de árbol de expansión” y el acrónimo STP. El uso del término “protocolo de árbol de expansión” y del acrónimo STP puede ser engañoso. La mayoría de los profesionales suele utilizar estas denominaciones para referirse a las diversas implementaciones del árbol de expansión, como el protocolo de árbol de expansión rápido (RSTP) y el protocolo de árbol de expansión múltiple (MSTP). Para poder explicar los conceptos de árbol de expansión correctamente, es importante consultar la implementación o el estándar específico en contexto. El documento más reciente del IEEE acerca del árbol de expansión, IEEE-802-1D-2004, establece que “STP se reemplazó con el protocolo de árbol de expansión rápido (RSTP)”. Como se ve, el IEEE utiliza “STP” para referirse a la implementación original del árbol de expansión y “RSTP” para describir la versión del árbol de expansión especificada en IEEE-802.1D-2004. En este currículo, cuando se analiza el protocolo de árbol de expansión original, se utiliza la frase “árbol de expansión 802.1D original” para evitar confusiones.

**Nota:** STP se basa en un algoritmo que Radia Perlman creó mientras trabajaba para Digital Equipment Corporation, y que se publicó en el ensayo realizado en 1985 denominado “An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN”.

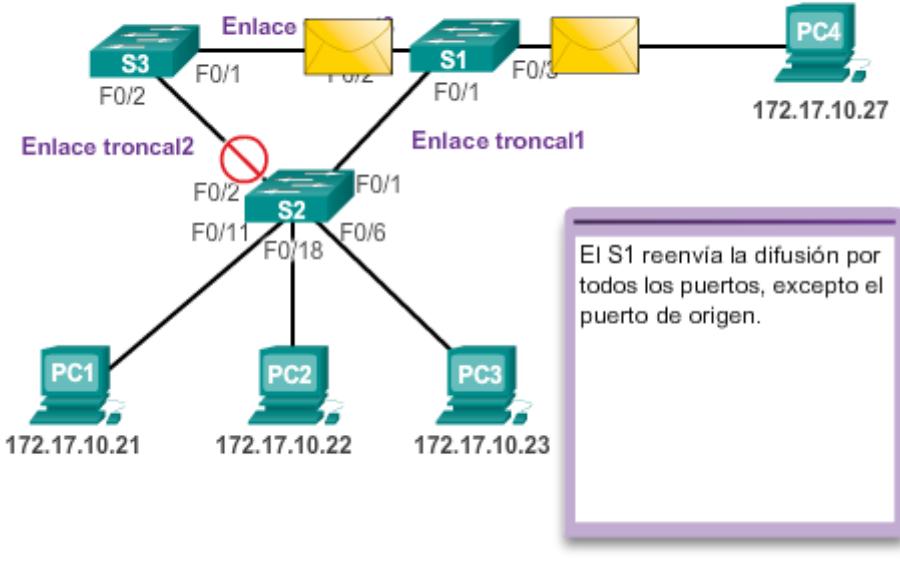
### Funcionamiento normal de STP



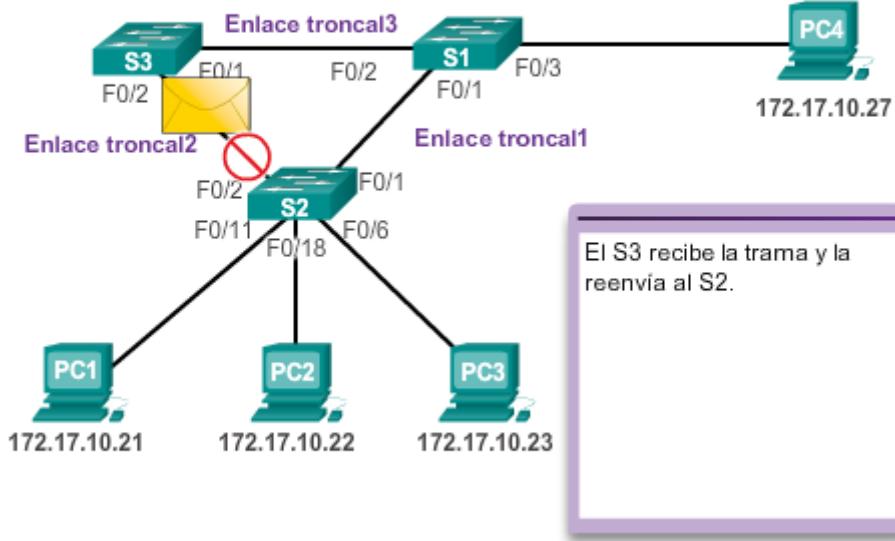
### Funcionamiento normal de STP



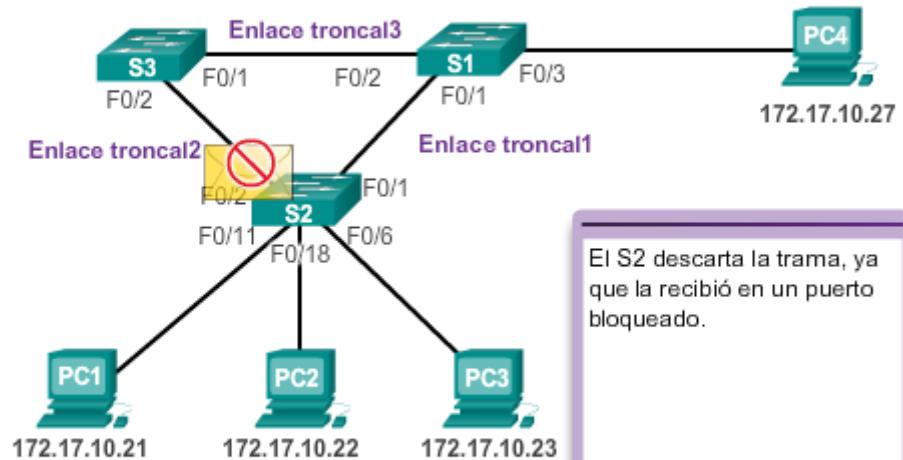
### Funcionamiento normal de STP



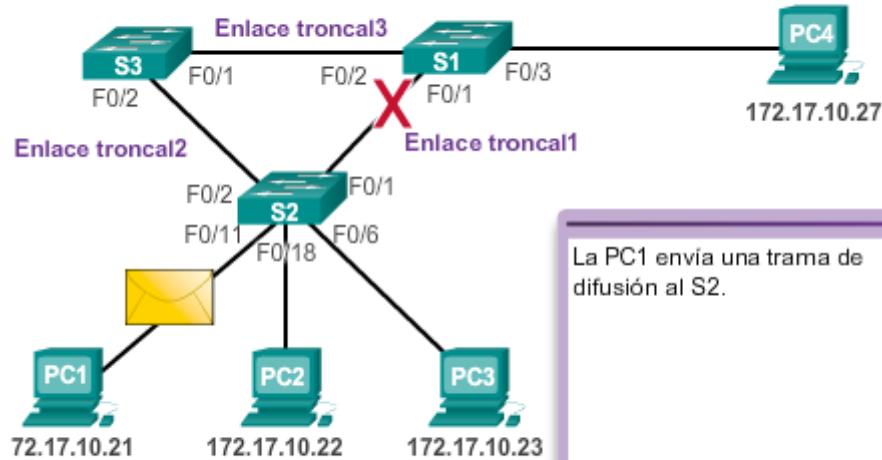
### Funcionamiento normal de STP



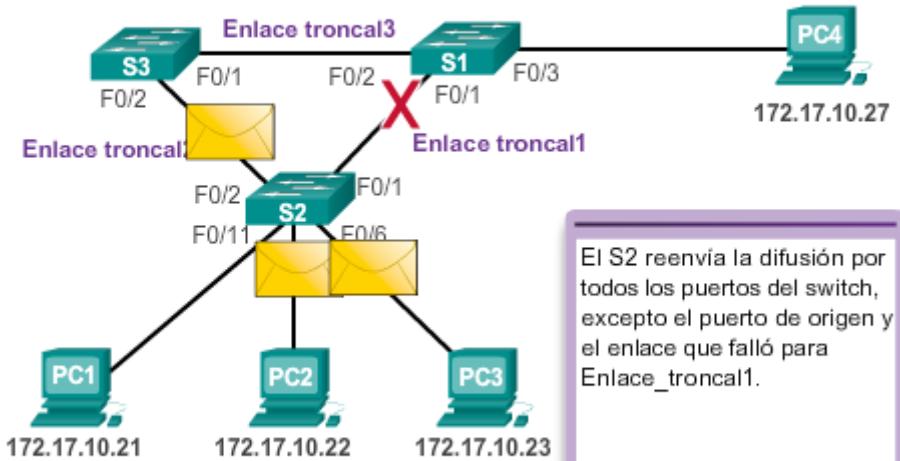
### Funcionamiento normal de STP



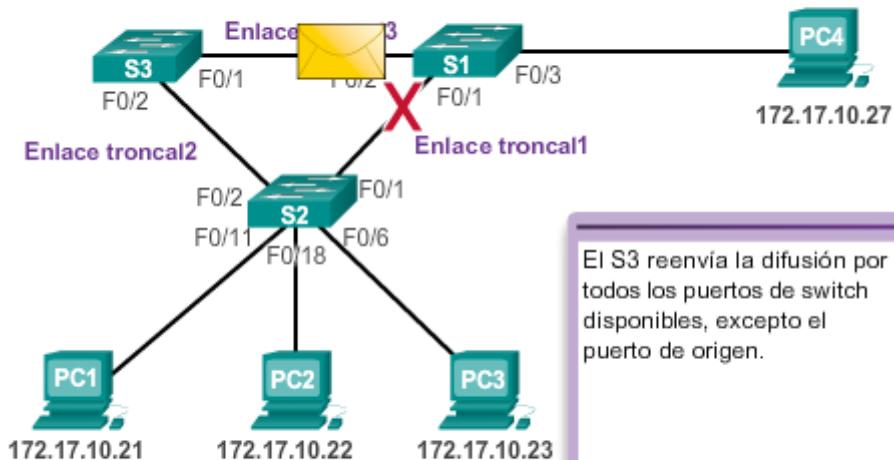
### STP compensa una falla de red



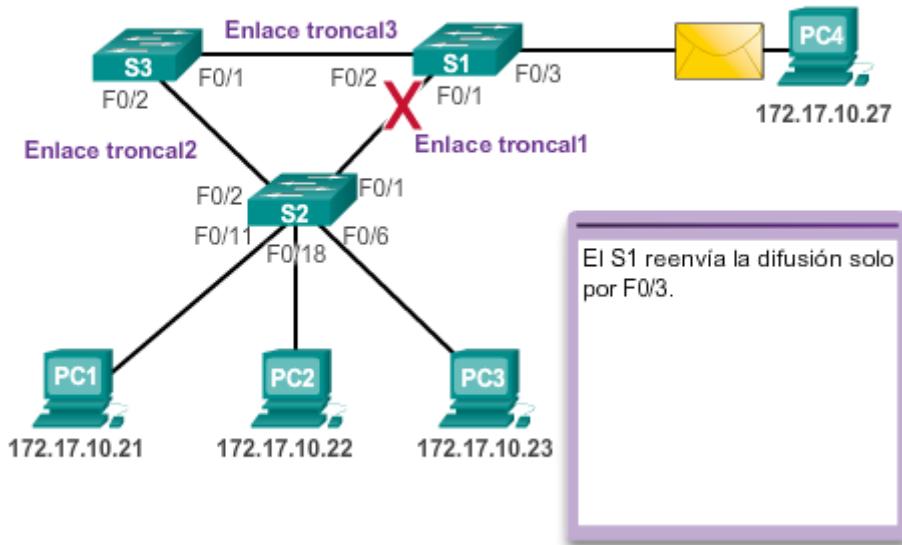
### STP compensa una falla de red



### STP compensa una falla de red



### STP compensa una falla de red



#### Capítulo 2: Redundancia de LAN 2.1.2.2 Algoritmo de árbol de expansión: funciones de puerto

La versión IEEE 802.1D de STP utiliza el algoritmo de árbol de expansión (STA) para determinar qué puertos de switch de una red se deben colocar en estado de bloqueo y evitar que ocurran bucles. El STA designa un único switch como puente raíz y lo utiliza como punto de referencia para todos los cálculos de rutas. En la ilustración, el puente raíz (el switch S1) se elige mediante un proceso de elección. Todos los switches que comparten STP intercambian tramas de BPDU para determinar el switch que posee el menor ID de puente (BID) en la red. El switch con el menor BID se transforma en el puente raíz en forma automática según los cálculos del STA.

**Nota:** para simplificar, suponga que todos los puertos en todos los switches están asignados a la VLAN 1, hasta que se indique lo contrario. Cada switch posee una dirección MAC única asociada a la VLAN 1.

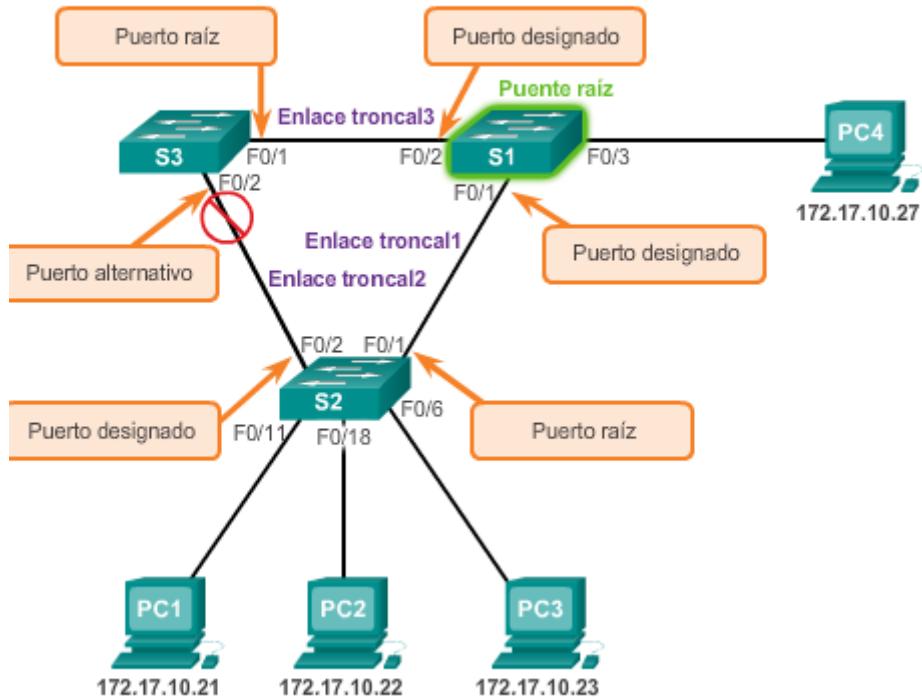
Una BPDU es una trama de mensaje que intercambian los switches para STP. Cada BPDU contiene un BID que identifica al switch que envió la BPDU. El BID contiene un valor de prioridad, la dirección MAC del switch emisor y una ID de sistema extendido optativa. El valor de BID más bajo lo determina la combinación de estos tres campos.

Después de determinar el puente raíz, el STA calcula la ruta más corta hacia dicho puente. Todos los switches utilizan el STA para determinar los puertos que deben bloquearse. Mientras el STA determina las mejores rutas al puente raíz para todos los puertos de switch en el dominio de difusión, se evita que el tráfico se reenvíe a través de la red. El STA tiene en cuenta tanto los costos de ruta como de puerto cuando determina qué puertos bloquear. El costo de la ruta se calcula mediante los valores de costo de puerto asociados con las velocidades de los puertos para cada puerto de switch que atraviesa una ruta determinada. La suma de los valores de costo de puerto determina el costo de ruta total para el puente raíz. Si existe más de una ruta a escoger, el STA elige la de menor costo de ruta.

Una vez que el STA determinó las rutas más deseables en relación con cada switch, asigna funciones de puerto a los puertos de switch que participan. Las funciones de puerto describen la relación que estos tienen en la red con el puente raíz y si se les permite reenviar tráfico:

- **Puertos raíz:** los puertos de switch más cercanos al puente raíz. En la ilustración, el puerto raíz en el S2 es F0/1, configurado para el enlace troncal entre el S2 y el S1. El puerto raíz en el S3 es F0/1, configurado para el enlace troncal entre el S3 y el S1. Los puertos raíz se seleccionan por switch.
- **Puertos designados:** todos los puertos que no son raíz y que aún pueden enviar tráfico a la red. En la ilustración, los puertos de switch (F0/1 y F0/2) en el S1 son puertos designados. El puerto F0/2 del S2 también está configurado como puerto designado. Los puertos designados se seleccionan por enlace troncal. Si un extremo de un enlace troncal es un puerto raíz, el otro extremo es un puerto designado. Todos los puertos en el puente raíz son puertos designados.
- **Puertos alternativos y de respaldo:**los puertos alternativos y de respaldo están configurados en estado de bloqueo para evitar bucles. En la ilustración, el STA configuró el puerto F0/2 en el S3 en la función alternativa. El puerto F0/2 en el S3 está en estado de bloqueo. Los puertos alternativos se seleccionan solo en los enlaces troncales en los que ninguno de los extremos es un puerto raíz. Observe en la ilustración que solo un extremo del enlace troncal está bloqueado. Esto permite una transición más rápida al estado de reenvío, cuando es necesario. (Los puertos en estado de bloqueo solo entran en acción cuando hay dos puertos en el mismo switch conectados entre sí mediante un hub o un único cable).
- **Puertos deshabilitados:** un puerto deshabilitado es un puerto de switch que está desactivado.

## Algoritmo STP



### Capítulo 2: Redundancia de LAN 2.1.2.3 Algoritmo de árbol de expansión: puente raíz

Como se muestra en la figura 1, todas las instancias de árbol de expansión (LAN comutada o dominio de difusión) tienen un switch designado como puente raíz. El puente raíz sirve como punto de referencia para todos los cálculos de árbol de expansión para determinar las rutas redundantes que deben bloquearse.

Un proceso de elección determina el switch que se transforma en el puente raíz.

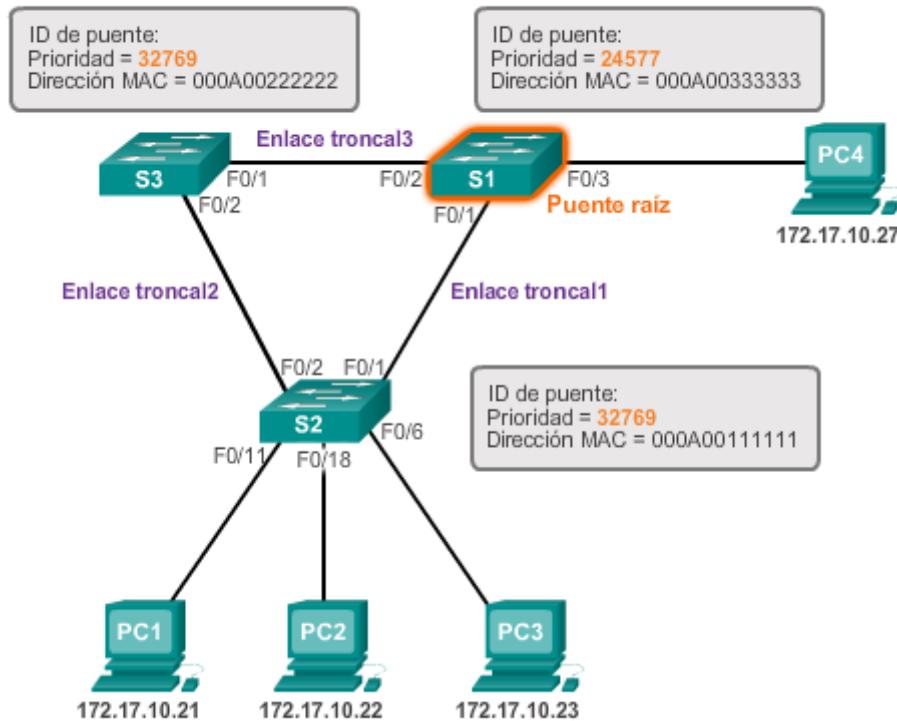
En la figura 2, se muestran los campos de BID. El BID está compuesto por un valor de prioridad, una ID de sistema extendido y la dirección MAC del switch.

Todos los switches del dominio de difusión participan del proceso de elección. Una vez que el switch arranca, comienza a enviar tramas BPDU cada dos segundos. Estas BPDU contienen el BID del switch y la ID de raíz.

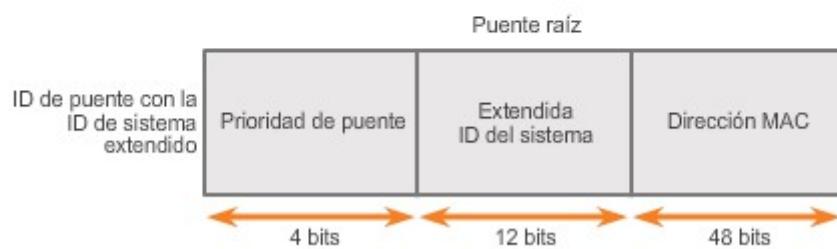
A medida que los switches reenvían sus tramas BPDU, los switches adyacentes en el dominio de difusión leen la información de la ID de raíz de las tramas BPDU. Si la ID de raíz que se recibe de una BPDU es inferior a la ID de raíz del switch receptor, este switch actualiza su ID de raíz e identifica al switch adyacente como puente raíz. En realidad, es posible que no sea un switch adyacente, ya que puede ser cualquier otro switch en el dominio de difusión. Luego el switch envía nuevas tramas de BPDU con el menor ID de raíz a los otros switches adyacentes. Finalmente, el switch con el menor BID es el que se identifica como puente raíz para la instancia de árbol de expansión.

Se elige un puente raíz para cada instancia de árbol de expansión. Es posible tener varios puentes raíz diferentes. Si todos los puertos de todos los switches pertenecen a la VLAN 1, solo se da una instancia de árbol de expansión. La ID de sistema extendido cumple una función en la determinación de las instancias de árbol de expansión.

### Puente raíz



### Campos BID



### Capítulo 2: Redundancia de LAN 2.1.2.4 Algoritmo de árbol de expansión: costo de la ruta

Una vez que se eligió el puente raíz para la instancia de árbol de expansión, el STA comienza el proceso para determinar las mejores rutas hacia el puente raíz desde todos los destinos en el dominio de difusión. La información de ruta se determina mediante la suma de los costos

individuales de los puertos que atraviesa la ruta desde el destino al puente raíz. Cada “destino” es, en realidad, un puerto de switch.

Los costos de los puertos predeterminados se definen por la velocidad a la que funcionan los mismos. Como se muestra en la figura 1, el costo de puerto de los puertos Ethernet de 10 Gb/s es 2, el de los puertos Ethernet de 1 Gb/s es 4, el de los puertos Ethernet de 100 Mb/s es 19 y el de los puertos Ethernet de 10 Mb/s es 100.

**Nota:** a medida que se introducen tecnologías Ethernet más modernas y veloces en el mercado, es posible que se modifiquen los valores de costo de ruta para admitir las distintas velocidades disponibles. Los números no lineales de la tabla incluyen algunas mejoras del antiguo estándar Ethernet. Los valores ya se modificaron para admitir el estándar Ethernet de 10 Gb/s. Para ilustrar el cambio continuo relacionado con la tecnología de redes de alta velocidad, los switches Catalyst 4500 y 6500 admiten un método de costo de ruta mayor; por ejemplo, el costo de la ruta de 10 Gb/s es 2000, el de 100 Gb/s es 200 y el de 1 Tb/s es 20.

Pese a que los puertos de switch cuentan con un costo de puerto predeterminado asociado a los mismos, tal costo puede configurarse. La capacidad de configurar costos de puerto individuales le da al administrador la flexibilidad para controlar de forma manual las rutas de árbol de expansión hacia el puente raíz.

Para configurar el costo de puerto de una interfaz (figura 2), introduzca el comando **spanning-tree cost valor** en el modo de configuración de interfaz. El valor puede variar entre 1 y 200 000 000.

En el ejemplo, el puerto de switch F0/1 se configuró con el costo de puerto 25 mediante el comando **spanning-tree cost 25** del modo de configuración de interfaz en la interfaz F0/1.

Para restaurar el costo de puerto al valor predeterminado 19, introduzca el comando **no spanning-tree cost** del modo de configuración de interfaz.

El costo de la ruta es igual a la suma de todos los costos de puerto a lo largo de la ruta hacia el puente raíz (figura 3). Las rutas con el costo más bajo se convierten en las preferidas, y el resto de las rutas redundantes se bloquean. En el ejemplo, el costo de la ruta del S2 al puente raíz S1 a través de la ruta 1 es 19 (según el costo de puerto individual especificado por el IEEE), mientras que el costo de la ruta a través de la ruta 2 es 38. Dado que la ruta 1 tiene un menor costo de ruta general hacia el puente raíz, es la ruta preferida. Luego, STP configura la ruta redundante que debe bloquearse y evita así la generación de bucles.

Para verificar los costos de puerto y de ruta hacia el puente raíz, introduzca el comando **show spanning-tree** (figura 4). El campo Cost cerca de la parte superior del resultado es el costo de la ruta total hacia el puente raíz. Este valor varía según la cantidad de puertos de switch que se deban atravesar para llegar al puente raíz. En el resultado, cada interfaz también se identifica con un costo de puerto individual de 19.

## Las mejores rutas al puente raíz

Velocidad de enlace	Costo (especificación IEEE revisada)	Costo (especificación IEEE anterior)
10 Gb/s	2	1
1 Gb/s	4	1
100 Mb/s	19	10
10 Mb/s	100	100

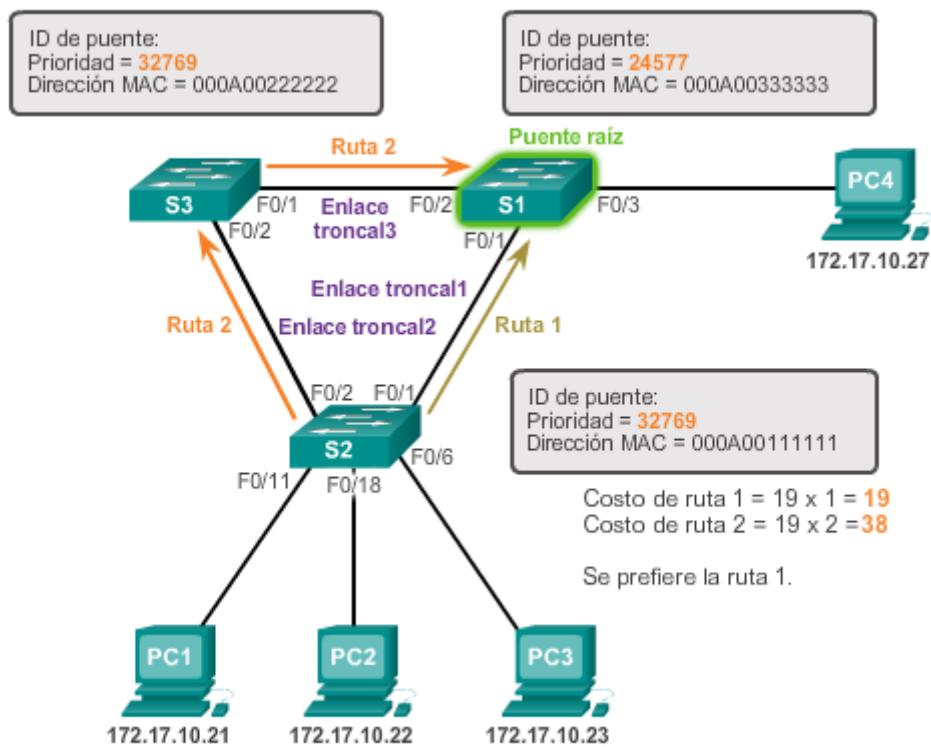
## Las mejores rutas al puente raíz

### Configurar costo del puerto

```
S2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# spanning-tree cost 25
S2(config-if)# end
S2#
```

### Restablecer costo del puerto

```
S2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)# interface f0/1
S2(config-if)# no spanning-tree cost
S2(config-if)# end
S2#
```



### Las mejores rutas al puente raíz

```

S2# show spanning-tree

VLAN001
    Spanning tree enabled protocol ieee
    Root ID      Priority  24577
                  Address   000A.0033.3333
                  Cost      19
                  Port      1
                  Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

    Bridge ID  Priority      32769  (priority 32768 sys-id-ext 1)
                  Address   000A.0011.1111
                  Hello time 2 sec Max Age 20 sec Forward Delay 15 sec
                  Aging Time 300

    Interface    Role      Sts  Cost      Prio.Nbr  Type
    -----  -----
    F0/1        Root     FWD    19      128.1    Edge P2p
    F0/2        Desg    FWD    19      128.2    Edge P2p
  
```

Capítulo

### o 2: Redundancia de LAN 2.1.2.5 Formato de trama BPDU 802.1D

El algoritmo de árbol de expansión depende del intercambio de BPDU para determinar un puente raíz. Una trama BPDU contiene 12 campos distintos que transmiten información de ruta y de prioridad que se utiliza para determinar el puente raíz y las rutas a este.

Haga clic en los campos de BPDU en la figura 1 para obtener más detalles.

- Los primeros cuatro campos identifican el protocolo, la versión, el tipo de mensaje y los señaladores de estado.
- Los cuatro campos siguientes se utilizan para identificar el puente raíz y el costo de la ruta hacia éste.
- Los últimos cuatro campos son todos campos de temporizador que determinan la frecuencia con la que se envían los mensajes de BPDU y el tiempo que se retiene la información que se recibe mediante el proceso de BPDU (próximo tema).

En la figura 2, se muestra una trama BPDU que se capturó mediante Wireshark. En el ejemplo, la trama de BPDU contiene más campos de los que se describieron anteriormente. El mensaje de BPDU se encapsula en una trama de Ethernet cuando se transmite a través de la red. El encabezado 802.3 indica las direcciones de origen y destino de la trama de BPDU. Esta trama tiene la dirección MAC de destino 01:80:C2:00:00:00, que es una dirección de multidifusión para el grupo de árbol de expansión. Cuando se asigna esta dirección MAC a una trama, cada switch configurado para árbol de expansión acepta y lee la información de la trama. El resto de los dispositivos en la red ignoran la trama.

En este ejemplo, el ID de raíz y el BID son iguales en la trama de BPDU capturada. Esto indica que la trama se capturó de un puente raíz. Todos los temporizadores se establecen en sus valores predeterminados.

## Campos BPDU

Número de campo	Bytes	Campo
1-4	2	ID de protocolo
	1	Versión
	1	Tipo de mensaje
	1	Indicadores
5 a 8	8	ID de raíz
	4	Costo de la ruta
	8	ID de puente
	2	ID de puerto
9 a 12	2	Antigüedad del mensaje
	2	Antigüedad máxima
	2	Tiempo de saludo
	2	Retraso de envío

### ID de protocolo

El campo ID de protocolo indica el tipo de protocolo que se utiliza. Este campo contiene el valor cero.

## BPDU de ejemplo

```
Frame 1 (60 bytes on wire, 60 bytes captured)
  IEEE 802.3 Ethernet
    Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
    Source: Cisco_9e:93:03 (00:19:aa:9e:93:03)
    Length: 38
    Trailer: 0000000000000000
  Logical-Link control
  Spanning Tree Protocol
    Protocol Identifier: Spanning Tree Protocol (0x0000)
    Protocol Version Identifier: spanning tree (0)
    BPDU Type: Configuration (0x00)
    BPDU flags: 0x01 (Topology Change)
    Root Identifier: 24577 / 00:19:aa:9e:93:00
    Root Path Cost: 0
    Bridge Identifier: 24577 / 00:19:aa:9e:93:00
    Port identifier: 0x8003
    Message Age: 0
    Max Age: 20
    Hello Time: 2
    Forward Delay: 15
```

En principio, cada switch en el dominio de difusión supone que es el puente raíz para una instancia de árbol de expansión, por lo que las tramas BPDU que se envían contienen el BID del switch local como ID de raíz. De manera predeterminada, las tramas BPDU se envían cada dos segundos después de que arranca el switch; es decir, el valor predeterminado del temporizador de saludo especificado en la trama BPDU es dos segundos. Cada switch mantiene información local acerca de su propio BID, el ID de raíz y el costo de la ruta hacia la raíz.

Cuando los switches adyacentes reciben una trama BPDU, comparan la ID de raíz de la trama BPDU con la ID de raíz local. Si la ID de raíz en la BPDU es inferior a la local, el switch actualiza la ID de raíz local y la ID en sus mensajes de BPDU. Estos mensajes indican el nuevo puente raíz en la red. La distancia al puente raíz también la indica la actualización del costo de la ruta. Por ejemplo, si se recibió la BPDU en un puerto de switch Fast Ethernet, el costo de la ruta aumentaría 19 números. Si la ID de raíz local es inferior a la ID de raíz que se recibe en la trama BPDU, se descarta la trama.

Después de que se ha actualizado un ID de ruta para identificar un nuevo puente raíz, todas las tramas de BPDU subsiguientes enviadas por ese switch contienen el ID de raíz nuevo y el costo de la ruta actualizado. De esta manera, todos los otros switches adyacentes pueden ver el menor ID de raíz identificado en todo momento. A medida que las tramas de BPDU se transmiten entre otros switches adyacentes, el costo de la ruta se actualiza en forma constante para indicar el costo de ruta total hacia el puente raíz. Todos los switches del árbol de expansión utilizan sus costos de ruta para identificar la mejor ruta posible al puente raíz.

A continuación se resume el proceso BPDU:

**Nota:** la prioridad es el factor decisivo inicial cuando se elige un puente raíz. Si las prioridades de todos los switches son las mismas, el dispositivo con la dirección MAC más baja se convierte en el puente raíz.

1. En principio, todos los switches se identifican como puente raíz. El S2 reenvía tramas BPDU por todos los puertos de switch. (figura 1).
2. Cuando el S3 recibe una BPDU del switch S2, el S3 compara su ID de raíz con la trama BPDU que recibió. Las prioridades son iguales, de manera que el switch debe examinar la parte de dirección MAC para determinar cuál es la de menor valor. Debido a que el S2 posee un valor de dirección MAC inferior, el S3 actualiza su ID de raíz con la ID de raíz del S2. En ese momento, el S3 considera que el S2 es el puente raíz. (figura 2).
3. Cuando el S1 compara su ID de raíz con la que recibió en la trama BPDU, identifica la ID de raíz local como el valor más bajo y descarta la BPDU del S2. (figura 3).
4. Cuando el S3 envía sus tramas BPDU, la ID de raíz incluida en la trama BPDU es la del S2. (figura 4).
5. Cuando S2 recibe la trama de BPDU, la descarta después de verificar que el ID de raíz de la BPDU coincide con su ID de raíz local. (figura 5)
6. Debido a que S1 posee un valor de prioridad menor en su ID de raíz, descarta la trama de BPDU recibida de S3. (figura 6)
7. S1 envía sus tramas de BPDU. (figura 7)

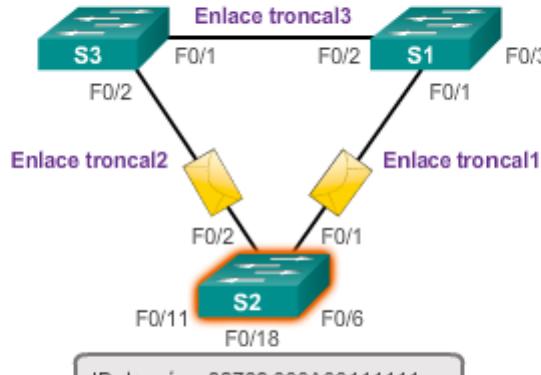
8. El S3 identifica la ID de raíz en la trama BPDU como una de menor valor y, por lo tanto, actualiza sus valores de ID de raíz para indicar que el S1 ahora es el puente raíz (figura 8).

9. El S2 identifica la ID de raíz en la trama BPDU como una de menor valor y, por lo tanto, actualiza sus valores de ID de raíz para indicar que el S1 ahora es el puente raíz (figura 9).

### El proceso BPDU

ID de raíz = 32769.000A00222222  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente = 24577.000A00333333  
Costo de ruta = 19

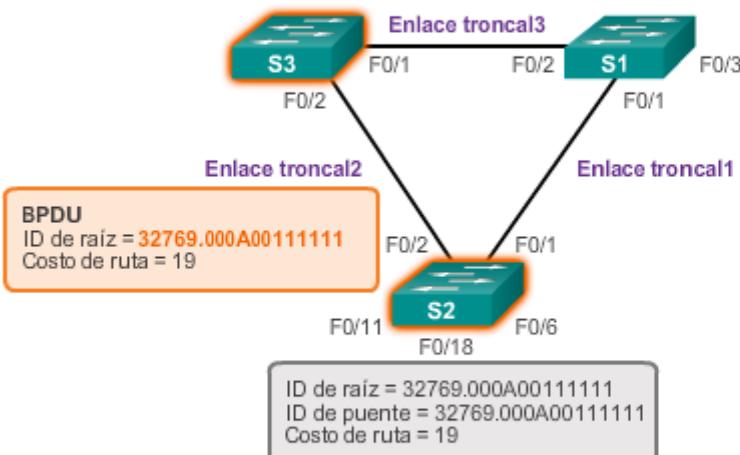


En principio, todos los switches creen que son el puente raíz. El S2 reenvía tramas BPDU por todos los puertos de switch. La trama BPDU contiene la ID de puente y la ID de raíz del S2, lo que indica que es el puente raíz.

### El proceso BPDU

ID de raíz = **32769.000A00111111**  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente = 24577.000A00333333  
Costo de ruta = 19

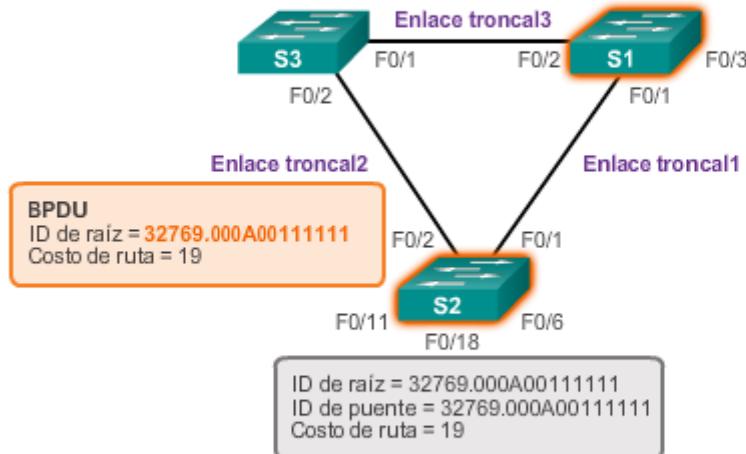


El S3 compara la ID de raíz recibida con la propia e identifica al S2 como la menor ID de raíz.  
El S3 actualiza su ID de raíz con la del S2.

### El proceso BPDU

ID de raíz = 32769.000A00111111  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente = 24577.000A00333333  
Costo de ruta = 19

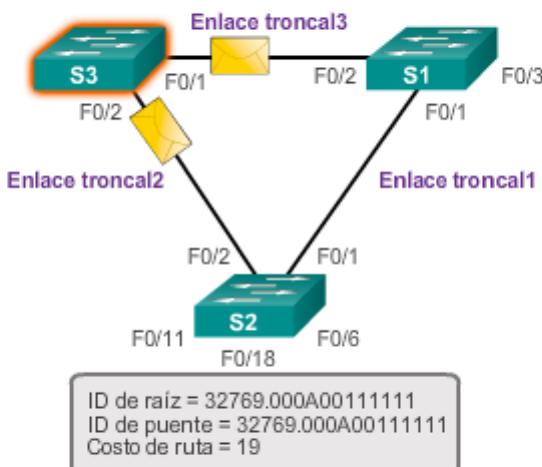


Cuando S1 compara su ID de raíz con la que recibió en la trama BPDU de S2, identifica al ID de raíz local como el valor inferior y descarta la BPDU de S2. El S1 todavía se considera el puente raíz.

### El proceso BPDU

ID de raíz = 32769.000A00111111  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente = 24577.000A00333333  
Costo de ruta = 19

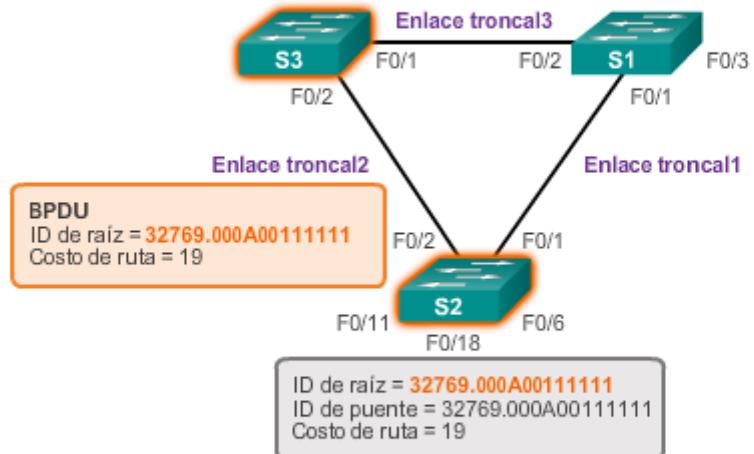


El S3 reenvía tramas BPDU por todos los puertos de switch. La trama BPDU contiene la ID de raíz del S2, lo que indica que es el puente raíz.

### El proceso BPDU

ID de raíz = 32769.000A00111111  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente = 24577.000A00333333  
Costo de ruta = 19

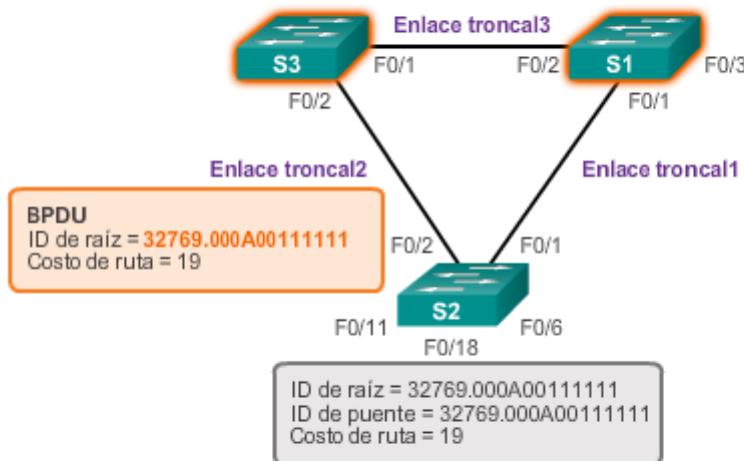


El S2 compara la ID de raíz de la BPDU recibida con la propia e identifica que estas coinciden. El S2 continúa creyendo que es el puente raíz en la red. El S2 no actualiza el costo de la ruta.

### El proceso BPDU

ID de raíz = 32769.000A00111111  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente = 24577.000A00333333  
Costo de ruta = 19

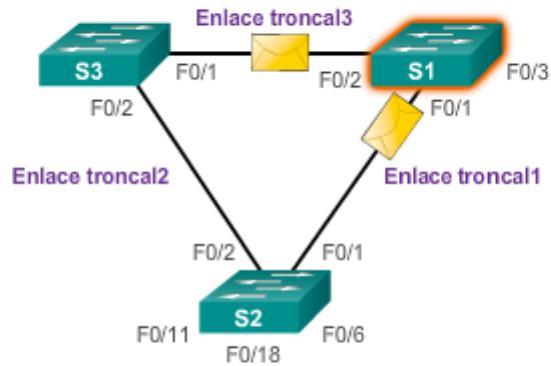


El S1 compara la ID de raíz de la BPDU recibida con la propia e identifica que la suya es menor. El S1 continúa creyendo que es el puente raíz en la red. El S1 no actualiza el costo de la ruta.

### El proceso BPDU

ID de raíz = 32769.000A00111111  
ID de puente = 32769.000A00222222  
Costo de ruta = 19

ID de raíz = 24577.000A00333333  
ID de puente= 24577.000A00333333  
Costo de ruta = 19



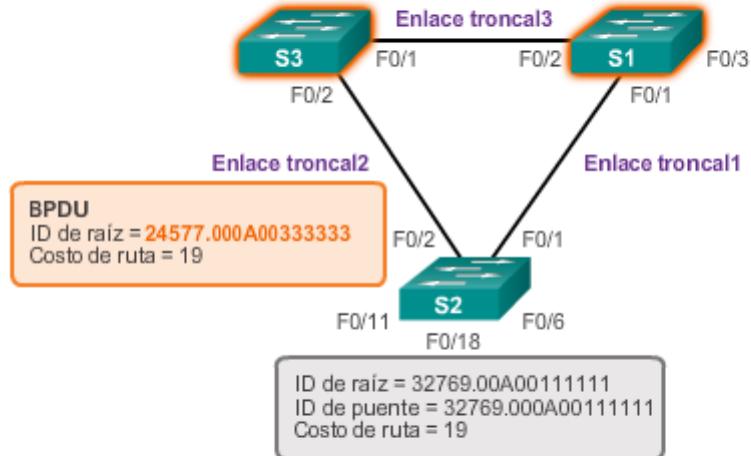
ID de raíz = 32769.000A00111111  
ID de puente = 32769.000A00111111  
Costo de ruta = 19

El S1 reenvía tramas BPDU por todos los puertos de switch. La trama BPDU contiene la ID de puente y la ID de raíz del S1, lo que indica que es el puente raíz.

### El proceso BPDU

ID de raíz = **24577.000A00333333**  
 ID puente = 32769.000A00222222  
 Costo de ruta = 19

ID de raíz = 24577.000A00333333  
 ID de puente = 24577.000A00333333  
 Costo de ruta = 19

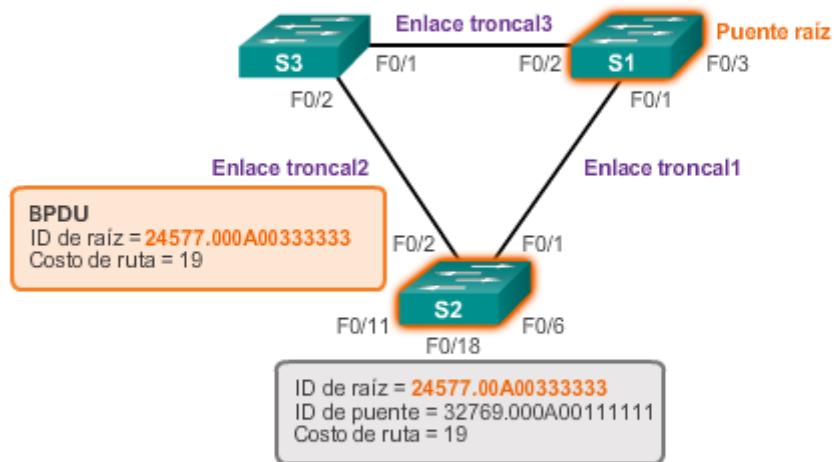


El S3 compara la ID de raíz recibida con la propia e identifica al S1 como la menor ID de raíz. El S3 actualiza su ID de raíz con la del S1. Ahora, el S3 considera que el S1 es el puente raíz. El S3 actualiza el costo de la ruta a 19,

### El proceso BPDU

ID de raíz = 24577.000A00333333  
 ID puente = 32769.000A00222222  
 Costo de ruta = 19

ID de raíz = 24577.000A00333333  
 ID de puente = 24577.000A00333333  
 Costo de ruta = 19



El S2 compara la ID de raíz recibida con la propia e identifica al S1 como la menor ID de raíz. El S2 actualiza su ID de raíz con la del S1. Ahora, el S2 considera que el S1 es el puente raíz. El S2 actualiza el costo de la ruta a 19,

El ID de puente (BID) se utiliza para determinar el puente raíz de una red. El campo BID de una trama de BPDU contiene tres campos separados:

- Prioridad del puente
- ID de sistema extendido
- Dirección MAC

Cada campo se utiliza durante la elección del puente raíz.

### Prioridad de puente

La prioridad del puente es un valor personalizable que se puede utilizar para influir en la elección del switch como puente raíz. El switch con la menor prioridad, que implica el BID más bajo, se convierte en el puente raíz, dado que prevalece un valor de prioridad menor. Por ejemplo, para asegurar que un switch específico sea siempre el puente raíz, establezca la prioridad en un valor inferior al del resto de los switches de la red. El valor de prioridad predeterminado para todos los switches Cisco es 32768. El rango va de 0 a 61440 y aumenta de a 4096. Los valores de prioridad válidos son 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 y 61440. El resto de los valores se rechazan. La prioridad de puente 0 prevalece sobre el resto de las prioridades de puente.

### ID de sistema extendido

Las primeras implementaciones de IEEE 802.1D estaban diseñadas para redes que no utilizaban VLAN. Existía un único árbol de expansión común para todos los switches. Por este motivo, en los switches Cisco más antiguos, se puede omitir la ID de sistema extendido en las tramas BPDU. A medida que las VLAN se volvieron más comunes en la segmentación de la infraestructura de red, se fue mejorando 802.1D para incluir a las VLAN, con el requisito de que se incluyera la ID de VLAN en la trama BPDU. La información de VLAN se incluye en la trama BPDU mediante el uso de la ID de sistema extendido. Todos los switches más modernos incluyen el uso de la ID de sistema extendido de manera predeterminada.

Como se muestra en la figura 1, el campo de prioridad del puente tiene una longitud de 2 bytes o 16 bits; 4 bits se utilizan para la prioridad del puente y 12 bits para la ID de sistema extendido, que identifica la VLAN que participa en este proceso STP en particular. Si se utilizan estos 12 bits para la ID de sistema extendido, se reduce la prioridad del puente a 4 bits. Este proceso reserva los 12 bits del extremo derecho para la ID de VLAN y los 4 bits del extremo izquierdo para la prioridad del puente. Esto explica por qué el valor de prioridad del puente solo se puede configurar en múltiplos de 4096, o  $2^{12}$ . Si los bits del extremo izquierdo son 0001, la prioridad del puente es 4096; si los bits del extremo derecho son 1111, la prioridad del puente es 61440 ( $= 15 \times 4096$ ). Los switches de las series Catalyst 2960 y 3560 no permiten configurar la prioridad del puente en 65536 ( $= 16 \times 4096$ ), dado que supone el uso de un quinto bit que no está disponible debido al uso de la ID de sistema extendido.

El valor de ID de sistema extendido se agrega al valor de prioridad de puente en el BID para identificar la prioridad y la VLAN de la trama de BPDU.

Cuando dos switches se configuran con la misma prioridad y tienen la misma ID de sistema extendido, el switch que posee la dirección MAC con el menor valor hexadecimal es el que tiene el menor BID. Inicialmente, todos los switches se configuran con el mismo valor de prioridad predeterminado. Luego, la dirección MAC es el factor de decisión sobre el cual el

switch se convertirá en puente raíz. Para asegurar que el puente raíz elegido cumpla con los requisitos de la red, se recomienda que el administrador configure el switch de puente raíz deseado con una prioridad menor. Esto también permite asegurar que, si se agregan nuevos switches a la red, no se produzca una nueva elección de árbol de expansión, lo que puede interrumpir la comunicación de red mientras se selecciona un nuevo puente raíz.

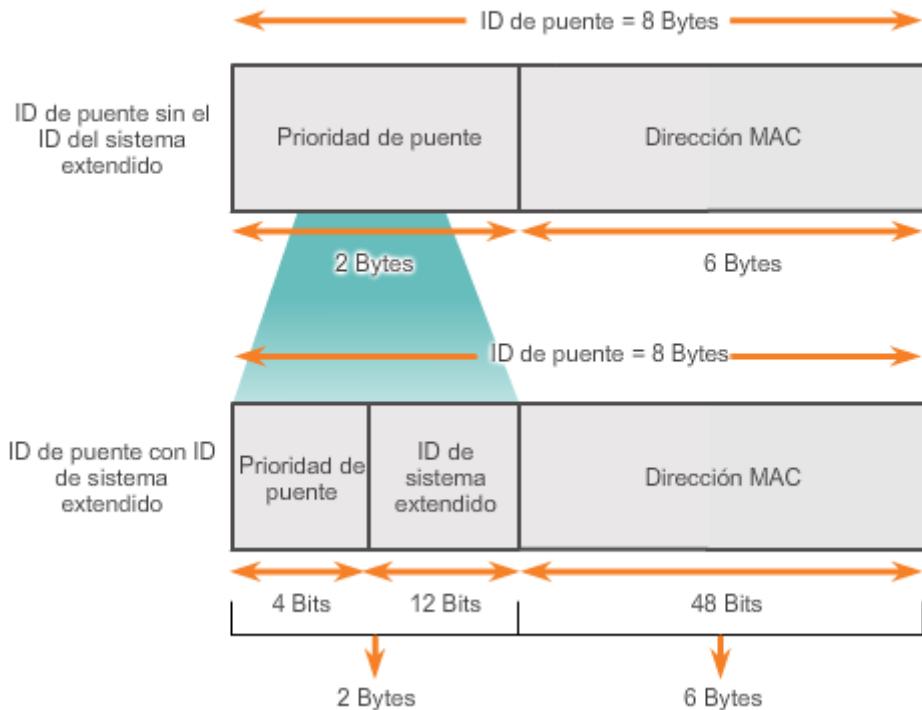
En la figura 2, el S1 tiene una prioridad inferior a la del resto de los switches; por lo tanto, se lo prefiere como puente raíz para esa instancia de árbol de expansión.

Cuando todos los switches están configurados con la misma prioridad, como es el caso de los switches que mantienen la configuración predeterminada con la prioridad 32768, la dirección MAC se vuelve el factor decisivo en la elección del switch que se convertirá en el puente raíz (figura 3).

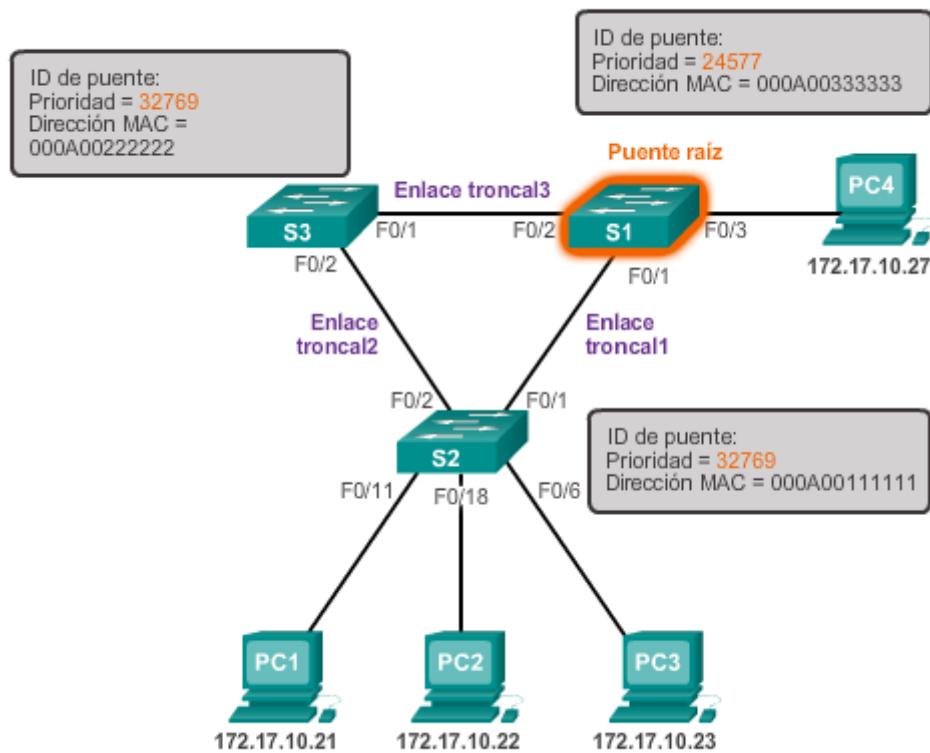
**Nota:** en el ejemplo, la prioridad de todos los switches es 32769. El valor se basa en la prioridad predeterminada 32768 y la asignación de la VLAN 1 relacionada con cada switch (32768 + 1).

La dirección MAC con el menor valor hexadecimal se considera como preferida para puente raíz. En el ejemplo, el S2 tiene la dirección MAC con el valor más bajo y, por lo tanto, se lo designa como puente raíz para esa instancia de árbol de expansión.

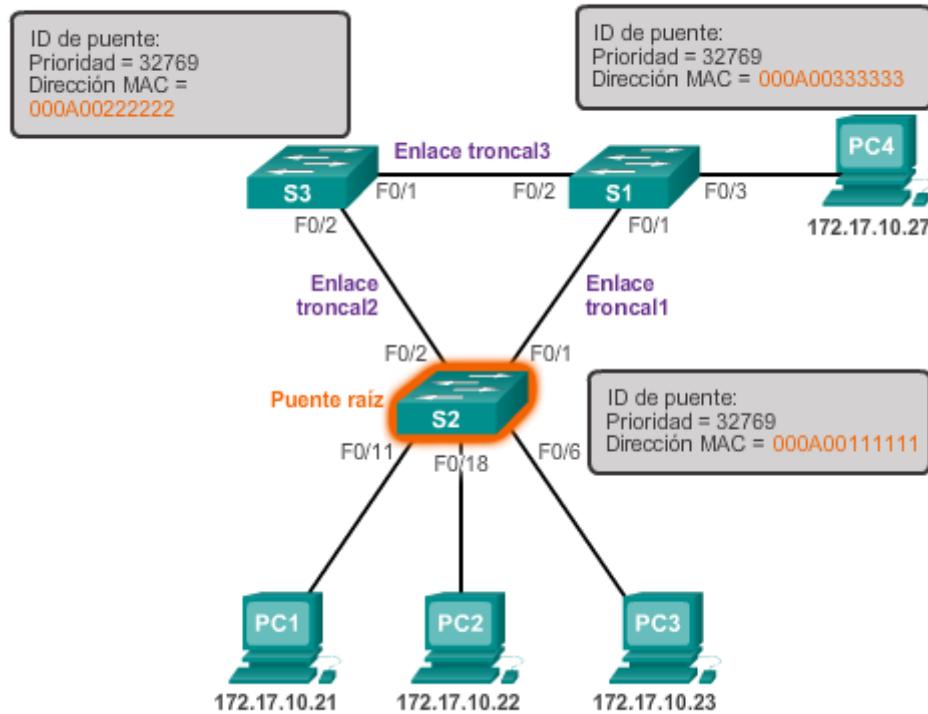
### Campos BID



### Decisión basada en la prioridad



## Decisión basada en la dirección MAC



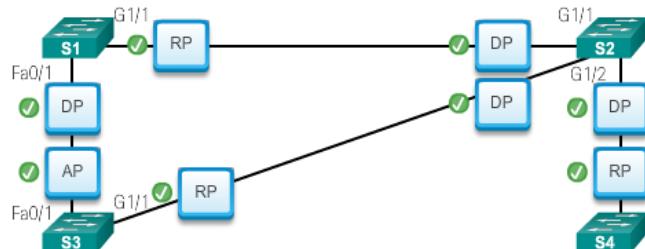
### Capítulo 2: Redundancia de LAN 2.1.2.8 Actividad: Identificar las funciones de puerto 802.1D

**Actividad: Funciones de puerto RSTP 802.1D**  
 Arrastra los nombres de las funciones de puerto RSTP hasta los puertos de switch correspondientes en la topología. Los nombres de función de los puertos se pueden utilizar más de una vez.

- Puerto raíz
- Puerto designado
- Puerto alternativo

**Correcto**

Identificó correctamente los nombres de las funciones de puerto RSTP para cada puerto de switch.



	Prioridad	Dirección MAC
S1	32769	000A00111111
S2	24577	000A00222222
S3	32769	000A00333333
S4	32769	000A00444444

### Capítulo 2: Redundancia de LAN 2.1.2.10 Práctica de laboratorio: Armado de una red

comutada con enlaces redundantes

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos

- Parte 2: Determinar el puente raíz
- Parte 3: Observar la selección del puerto STP sobre la base del costo de puerto
- Parte 4: Observar la selección del puerto STP sobre la base de la prioridad de puerto

[Práctica de laboratorio: Armado de una red comutada con enlaces redundantes](#)

Capítulo 2: Redundancia de LAN 2.2.1.1 Lista de protocolos de árbol de expansión

Desde el lanzamiento del estándar IEEE 802.1D original, surgió una gran variedad de protocolos de árbol de expansión.

Las variedades de protocolos de árbol de expansión incluyen lo siguiente:

- **STP:** es la versión original de IEEE 802.1D (802.1D-1998 y anterior), que proporciona una topología sin bucles en una red con enlaces redundantes. El árbol de expansión común (CTS) asume una instancia de árbol de expansión para toda la red enlazada, independientemente de la cantidad de VLAN.
- **PVST+:** esta es una mejora de Cisco de STP que proporciona una instancia de árbol de expansión 802.1D para cada VLAN configurada en la red. La instancia aparte admite PortFast, UplinkFast, BackboneFast, la protección BPDU, el filtro BPDU, la protección de raíz y la protección de bucle.
- **802.1D-2004:** esta es una versión actualizada del estándar STP que incorpora IEEE 802.1w.
- **Protocolo de árbol de expansión rápido (RSTP) o IEEE 802.1w:** esta es una evolución de STP que proporciona una convergencia más veloz que STP.
- **PVST+ rápido:** esta es una mejora de Cisco de RSTP que utiliza PVST+. PVST+ rápido proporciona una instancia de 802.1w distinta por VLAN. La instancia aparte admite PortFast, la protección BPDU, el filtro BPDU, la protección de raíz y la protección de bucle.
- **Protocolo de árbol de expansión múltiple (MSTP):** es un estándar IEEE inspirado en la anterior implementación de STP de varias instancias (MISTP), exclusivo de Cisco. MSTP asigna varias VLAN en la misma instancia de árbol de expansión. MST es la implementación de Cisco de MSTP, que proporciona hasta 16 instancias de RSTP y combina varias VLAN con la misma topología física y lógica en una instancia de RSTP común. Cada instancia admite PortFast, protección BPDU, filtro BPDU, protección de raíz y protección de bucle.

Es posible que un profesional de red, cuyas tareas incluyen la administración de los switches, deba decidir cuál es el tipo de protocolo de árbol de expansión que se debe implementar.

**Nota:** las características antiguas UplinkFast y BackboneFast exclusivas de Cisco no se describen en este curso. Estas características fueron reemplazadas por la implementación de PVST+ rápido, que las incorpora como parte de la implementación del estándar RSTP.

#### Tipos de protocolos de árbol de expansión

- **802.1D-1998:** es el estándar antiguo de puentes y STP.
  - **CST:** asume una instancia de árbol de expansión para toda la red enlazada, independientemente de la cantidad de VLAN.
- **PVST+:** es una mejora de Cisco de STP que proporciona una instancia de árbol de expansión 802.1D distinta para cada VLAN configurada en la red.
- **802.1D-2004:** es un estándar de puentes y STP actualizado.
- **802.1w (RSTP):** mejora la convergencia de STP 1998 al agregar funciones a los puertos y mejorar los intercambios de BPDU.
- **PVST+ rápido:** es una mejora de Cisco de RSTP que utiliza PVST+.
- **802.1s (MSTP):** asigna varias VLAN a la misma instancia de árbol de expansión.

#### Capítulo 2: Redundancia de LAN 2.2.1.2 Características de los protocolos de árbol de

#### expansión

A continuación, se detallan características de los diversos protocolos de árbol de expansión. Las palabras en cursiva indican si ese protocolo de árbol de expansión en particular es exclusivo de Cisco o una implementación del estándar IEEE.

- **STP:** asume una instancia de árbol de expansión *IEEE 802.1D* para toda la red enlazada, independientemente de la cantidad de VLAN. Debido a que solo hay una instancia, los requisitos de CPU y de memoria para esta versión son menos que para el resto de los protocolos. Sin embargo, dado que solo hay una instancia, también hay solo un puente raíz y un árbol. El tráfico para todas las VLAN fluye por la misma ruta, lo que puede provocar flujos de tráfico poco óptimos. Debido a las limitaciones de 802.1D, la convergencia de esta versión es lenta.
- **PVST+:** es una mejora de Cisco de STP que proporciona una instancia diferente de la implementación de Cisco de 802.1D para cada VLAN que se configura en la red. La instancia aparte admite PortFast, UplinkFast, BackboneFast, la protección BPDU, el filtro BPDU, la protección de raíz y la protección de bucle. La creación de una instancia para cada VLAN aumenta los requisitos de CPU y de memoria, pero admite los puentes raíz por VLAN. Este diseño permite la optimización del árbol de expansión para el tráfico de cada VLAN. La convergencia de esta versión es similar a la convergencia de 802.1D. Sin embargo, la convergencia es por VLAN.
- **RSTP (o IEEE 802.1w):** es una evolución del árbol de expansión que proporciona una convergencia más rápida que la implementación original de 802.1D. Esta versión resuelve varios problemas de convergencia, pero dado que aún proporciona una única instancia de STP, no resuelve los problemas de flujo de tráfico poco óptimo. Para admitir una convergencia más rápida, los requisitos de uso de CPU y de memoria de esta versión son apenas más exigentes que los de CTS, pero menos que los de RSTP+.
- **PVST+ rápido:** es una mejora de Cisco de RSTP que utiliza PVST+. Proporciona una instancia de 802.1w distinta por VLAN. La instancia aparte admite PortFast, la protección BPDU, el filtro BPDU, la protección de raíz y la protección de bucle. Esta versión resuelve tanto los problemas de convergencia como los de flujo de tráfico poco óptimo. Sin embargo, esta versión tiene los requisitos de CPU y de memoria más exigentes.

- **MSTP:** es el estándar *IEEE 802.1s*, inspirado en la anterior implementación de MISTP, exclusivo de Cisco. Para reducir el número de instancias de STP requeridas, MSTP asigna varias VLAN con los mismos requisitos de flujo de tráfico en la misma instancia de árbol de expansión.
- **MST:** es la implementación de Cisco de MSTP, que proporciona hasta 16 instancias de RSTP (802.1w) y combina muchas VLAN con la misma topología física y lógica en una instancia de RSTP común. Cada instancia admite PortFast, protección BPDU, filtro BPDU, protección de raíz y protección de bucle. Los requisitos de CPU y de memoria de esta versión son menos que los de PVST+ rápido pero más que los de RSTP.

El modo de árbol de expansión predeterminado para los switches Cisco Catalyst es PVST+, que está habilitado en todos los puertos. PVST+ tiene una convergencia mucho más lenta que PVST+ rápido después de un cambio en la topología.

**Nota:** es importante distinguir entre el estándar IEEE 802.1D-1998 antiguo (y anteriores) y el estándar IEEE 802.1D-2004. IEEE 802.1D-2004 incorpora la funcionalidad de RSTP, mientras que IEEE 802.1D-1998 se refiere a la implementación original del algoritmo de árbol de expansión. Los switches Cisco más modernos que ejecutan versiones más actuales del IOS, como los switches Catalyst 2960 que poseen el IOS 15.0, ejecutan PVST+ de manera predeterminada pero incorporan muchas especificaciones de IEEE 802.1D-1998 en este modo (como los puertos alternativos en lugar de los puertos no designados de antes). Sin embargo, para ejecutar el árbol de expansión rápido en ese tipo de switch, todavía se lo debe configurar explícitamente para el modo de árbol de expansión rápido.

### Características del protocolo de árbol de expansión

Protocolo	Estándar	Recursos necesarios	Convergencia	Cálculo de árbol
STP	802.1D	Baja	Lento	Todo VLAN
PVST+	Cisco	Alto	Lento	Por VLAN
RSTP	802.1w	Medio	Rápido	Todo VLAN
PVST+ rápido	Cisco	Muy alto	Rápido	Por VLAN
MSTP	802.1s, Cisco	Medio o alto	Rápido	Por instancia

Capítulo 2: Redundancia de LAN 2.2.1.3 Actividad: Identificar los tipos de protocolos de árbol de expansión

**Actividad: Tipos de protocolos de árbol de expansión**

Arrastra el tipo de protocolo de árbol de expansión hasta la descripción correspondiente.

<input checked="" type="checkbox"/> PVST+	Es una mejora de Cisco de STP. Proporciona una instancia de árbol de expansión 802.1D distinta para cada VLAN.
<input checked="" type="checkbox"/> PVST+ rápido	Es una mejora de Cisco de RSTP.
<input checked="" type="checkbox"/> STP	Utiliza una instancia de árbol de expansión IEEE 802.1D para toda la red enlazada, independientemente de la cantidad de VLAN.
<input checked="" type="checkbox"/> RSTP	Es una evolución de STP que proporciona una convergencia más rápida de STP.
<input checked="" type="checkbox"/> MSTP	Asigna varias VLAN que tienen los mismos requisitos de flujo de tráfico a la misma instancia de árbol de expansión.

**Correcto**

Unió correctamente los tipos de STP con las descripciones.

## Capítulo 2: Redundancia de LAN 2.2.2.1 Descripción general de PVST+

El estándar IEEE 802.1D original define un árbol de expansión común (CST) que asume solo una instancia de árbol de expansión para toda la red comutada, independientemente de la cantidad de VLAN. Las redes que ejecutan CST presentan las siguientes características:

- No es posible compartir la carga. Un uplink debe bloquear todas las VLAN.
- Se preserva la CPU. Solo se debe calcular una instancia de árbol de expansión.

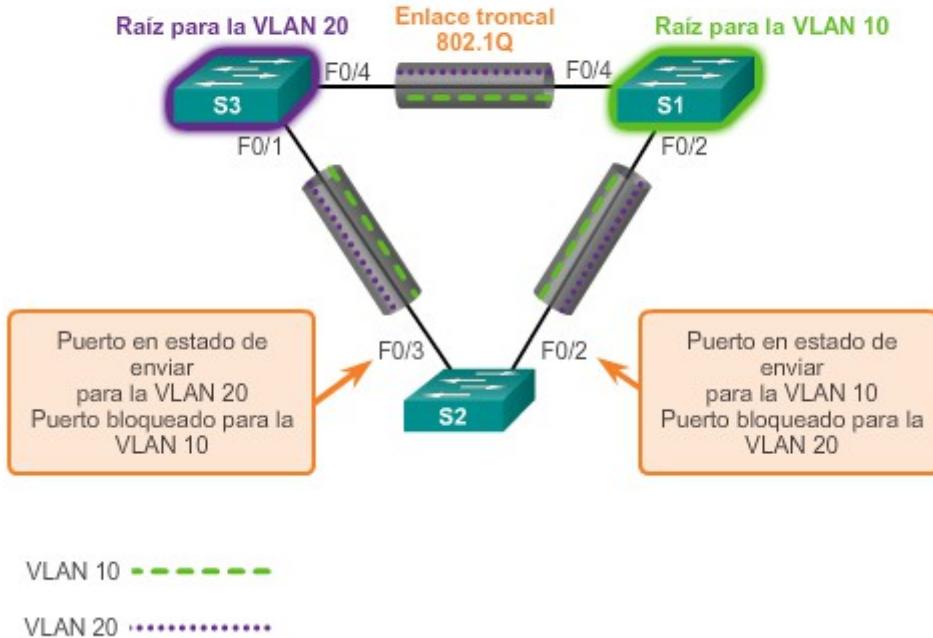
Cisco desarrolló PVST+ para que una red pueda ejecutar una instancia independiente de la implementación de Cisco de IEEE 802.1D para cada VLAN en la red. Con PVST+, un puerto de enlace troncal en un switch puede bloquear una VLAN sin bloquear otras. PVST+ se puede utilizar para implementar el balanceo de carga de capa 2. Debido a que cada VLAN ejecuta una instancia de STP distinta, los switches en un entorno PVST+ requieren un mayor procesamiento de CPU y un mayor consumo de ancho de banda de BPDU que la implementación de CST tradicional de STP.

En un entorno PVST+, los parámetros de árbol de expansión se pueden ajustar para que la mitad de las VLAN reenvíen en cada enlace troncal de uplink. En la ilustración, el puerto F0/3 en el S2 es el puerto de reenvío para la VLAN 20, y el F0/2 en el S2 es el puerto de reenvío para la VLAN 10. Esto se logra mediante la configuración de un switch como puente raíz para la mitad de las VLAN en la red y de un segundo switch como puente raíz para la otra mitad de las VLAN. En la ilustración, el S3 es el puente raíz para la VLAN 20, y el S1 es el puente raíz para la VLAN 10. Si hay varios puentes raíz STP por VLAN, se aumenta la redundancia en la red.

Las redes que ejecutan PVST+ presentan las siguientes características:

- El balanceo de carga puede funcionar de forma óptima.
- Una instancia de árbol de expansión para cada VLAN que se mantiene puede significar un gran desperdicio de ciclos de CPU para todos los switches en la red (además del ancho de banda que se utiliza en cada instancia para enviar su propia BPDU). Esto solo representaría un problema si se configurara una gran cantidad de redes VLAN.

## PVST+



### Capítulo 2: Redundancia de LAN 2.2.2.2 Estados de los puertos y funcionamiento de PVST+

STP facilita la ruta lógica sin bucles en todo el dominio de difusión. El árbol de expansión se determina a través de la información obtenida en el intercambio de tramas de BPDU entre los switches interconectados. Para facilitar el aprendizaje del árbol de expansión lógico, cada puerto de switch sufre una transición a través de cinco estados posibles y tres temporizadores de BPDU.

El árbol de expansión queda determinado inmediatamente después de que el switch finaliza el proceso de arranque. Si un puerto de switch pasa directamente del estado de bloqueo al de reenvío sin información acerca de la topología completa durante la transición, el puerto puede crear un bucle de datos temporal. Por este motivo, STP introduce los cinco estados de puerto. En la ilustración, se describen los siguientes estados de puerto que aseguran que no se produzcan bucles durante la creación del árbol de expansión lógico:

- **Bloqueo:** el puerto es un puerto alternativo y no participa en el reenvío de tramas. El puerto recibe tramas de BPDU para determinar la ubicación y el ID de raíz del switch del puente raíz y las funciones de puertos que cada uno de éstos debe asumir en la topología final de STP activa.
- **Escucha:** escucha la ruta hacia la raíz. STP determinó que el puerto puede participar en el reenvío de tramas según las tramas BPDU que recibió el switch hasta ahora. A esta altura, el puerto de switch no solo recibe tramas BPDU, sino que además transmite sus propias tramas BPDU e informa a los switches adyacentes que el puerto de switch se prepara para participar en la topología activa.

- **Aprendizaje:** aprende las direcciones MAC. El puerto se prepara para participar en el reenvío de tramas y comienza a completar la tabla de direcciones MAC.
- **Reenvío:** el puerto se considera parte de la topología activa. Reenvía tramas de datos, además de enviar y recibir tramas BPDU.
- **Deshabilitado:** el puerto de capa 2 no participa en el árbol de expansión y no reenvía tramas. El estado deshabilitado se establece cuando el puerto de switch se encuentra administrativamente deshabilitado.

Observe que la cantidad de puertos en cada uno de los diversos estados (bloqueo, escucha, aprendizaje o reenvío) se puede mostrar con el comando **show spanning-tree summary**.

Para cada VLAN en una red conmutada, PVST+ sigue cuatro pasos para proporcionar una topología de red lógica sin bucles:

- 1. Elegir un puente raíz:** solo un switch puede funcionar como puente raíz (para una determinada VLAN). El puente raíz es el switch con la menor ID de puente. En el puente raíz, todos los puertos son puertos designados (en particular, los que no son puertos raíz).
- 2. Seleccionar el puerto raíz en cada puerto que no es raíz:** STP establece un puerto raíz en cada puente que no es raíz. El puerto raíz es la ruta de menor costo desde el puente que no es raíz hasta el puente raíz, que indica la dirección de la mejor ruta hacia el puente raíz. Generalmente, los puertos raíz están en estado de reenvío.
- 3. Seleccionar el puerto designado en cada segmento:** STP establece un puerto designado en cada enlace. El puerto designado se selecciona en el switch que posee la ruta de menor costo hacia el puente raíz. Por lo general, los puertos designados están en estado de reenvío y reenvían el tráfico para el segmento.
- 4. El resto de los puertos en la red conmutada son puertos alternativos:** en general, los puertos alternativos se mantienen en estado de bloqueo para romper la topología de bucle de forma lógica. Cuando un puerto está en estado de bloqueo, no reenvía tráfico pero puede procesar los mensajes BPDU recibidos.

#### Estados de los puertos

Operación permitida	Estado del puerto				
	Bloquear	Escuchar	Aprendizaje	Reenvío	Deshabilitado
Puede recibir y procesar BPDU.	SÍ	SÍ	SÍ	SÍ	NO
Puede reenviar tramas de datos recibidas en la interfaz.	NO	NO	NO	SÍ	NO
Puede reenviar tramas de datos conmutadas desde otra interfaz.	NO	NO	NO	SÍ	NO
Puede descubrir las direcciones MAC.	NO	NO	SÍ	SÍ	NO

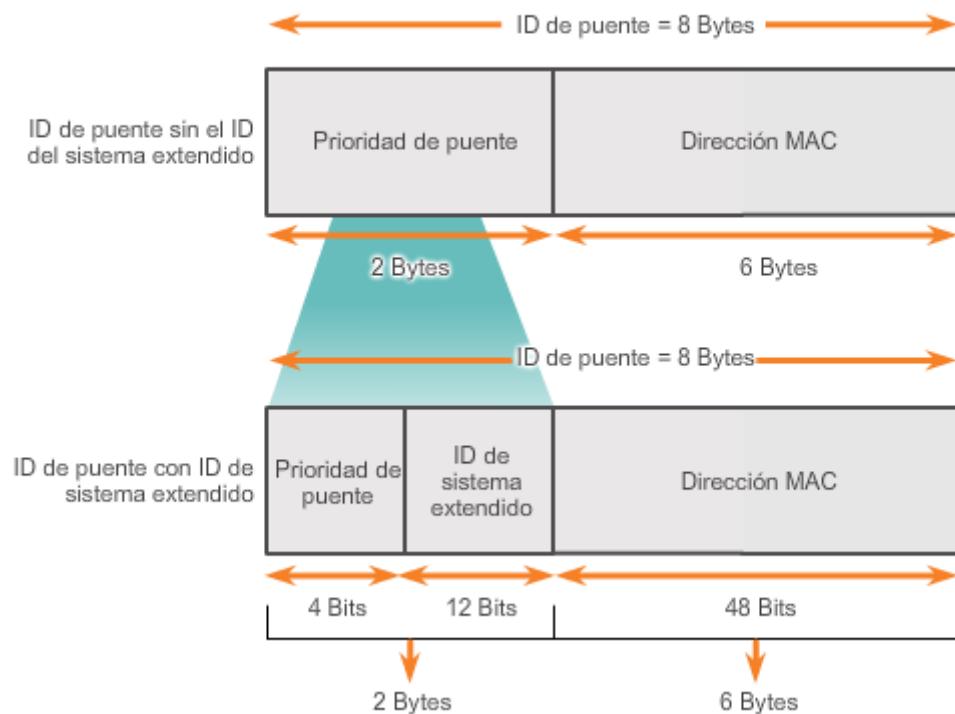
## Capítulo 2: Redundancia de LAN 2.2.2.3 ID de sistema extendido y funcionamiento de PVST+

En un entorno PVST+, la ID de switch extendido asegura que el switch tenga un BID exclusivo para cada VLAN.

Por ejemplo, el BID predeterminado de la VLAN 2 sería 32770 (32768 de prioridad, más 2 de ID de sistema extendido). Si no se configuró ninguna prioridad, todos los switches tienen la misma prioridad predeterminada, y la elección de la raíz para cada VLAN se basa en la dirección MAC. Este método es un medio aleatorio para seleccionar el puente raíz.

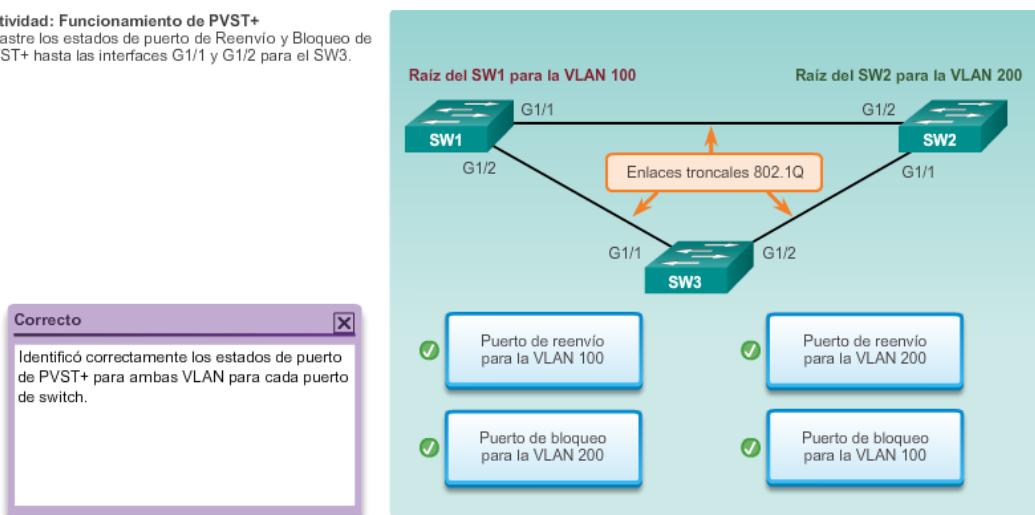
Hay situaciones en las que es posible que el administrador desee seleccionar un switch específico como puente raíz. Esto se puede deber a varios motivos, incluso que el switch esté ubicado en un lugar más central en el diseño de la LAN, que tenga una mayor capacidad de procesamiento o que simplemente sea más fácil acceder a este y administrarlo de forma remota. Para manipular la elección del puente raíz, asigne una prioridad más baja al switch que se debe seleccionar como puente raíz.

### PVST+ e ID de sistema extendido



## Capítulo 2: Redundancia de LAN 2.2.2.4 Actividad: Identificar el funcionamiento de PVST+

**Actividad: Funcionamiento de PVST+**  
Arrastre los estados de puerto de Reenvío y Bloqueo de PVST+ hasta las interfaces G1/1 y G1/2 para el SW3.



## Capítulo 2: Redundancia de LAN 2.2.3.1 Descripción general de PVST+ rápido

RSTP (IEEE 802.1w) es una evolución del estándar 802.1D original y se incorpora al estándar IEEE 802.1D-2004. La terminología de STP 802.1w sigue siendo fundamentalmente la misma que la de STP IEEE 802.1D original. La mayoría de los parámetros no se modificaron, de modo que los usuarios familiarizados con STP pueden configurar el nuevo protocolo con facilidad. PVST+ rápido es, simplemente, la implementación de Cisco de RSTP por VLAN. Con PVST+ rápido, se ejecuta una instancia de RSTP independiente para cada VLAN.

En la ilustración, se muestra una red que ejecuta RSTP. El S1 es el puente raíz con dos puertos designados en estado de reenvío. RSTP admite un nuevo tipo de puerto: el puerto F0/3 en el S2 es un puerto alternativo en estado de descarte. Observe que no existen puertos bloqueados. RSTP no posee el estado de puerto de bloqueo. RSTP define los estados de puertos como de descarte, aprender o enviar.

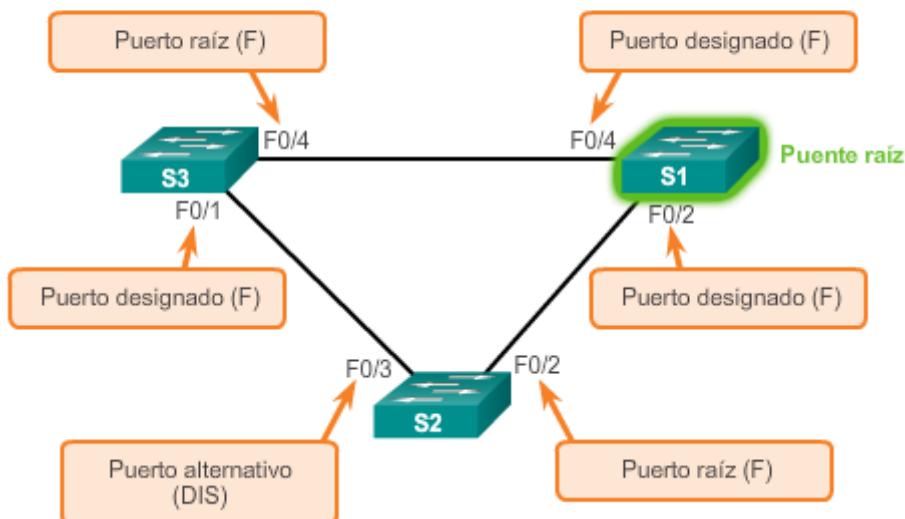
RSTP aumenta la velocidad de recálculo del árbol de expansión cuando cambia la topología de la red de la Capa 2. RSTP puede lograr una convergencia mucho más rápida en una red configurada en forma adecuada, a veces sólo en unos pocos cientos de milisegundos. RSTP redefine los tipos de puertos y sus estados. Si un puerto está configurado como puerto alternativo o de respaldo, puede cambiar automáticamente al estado de reenvío sin esperar a que converja la red. A continuación se describen brevemente las características de RSTP:

- RSTP es el protocolo preferido para evitar los bucles de Capa 2 en un entorno de red commutada. La mayoría de las diferencias se establecieron con las mejoras del estándar 802.1D original exclusivas de Cisco. Estas mejoras, como las BPDU que transportan y envían información acerca de las funciones de los puertos sólo a los switches vecinos, no requieren configuración adicional y por lo general poseen un mejor rendimiento que las versiones anteriores propiedad de Cisco. Ahora son transparentes y se integran al funcionamiento del protocolo.
- Las mejoras al estándar 802.1D original exclusivas de Cisco, como UplinkFast y BackboneFast, no son compatibles con RSTP.
- RSTP (802.1w) reemplaza al estándar 802.1D original y, al mismo tiempo, mantiene la compatibilidad con versiones anteriores. Se mantiene la mayor parte de la terminología

del estándar 802.1D original, y la mayoría de los parámetros no se modificaron. Además, 802.1w se puede revertir al estándar 802.1D antiguo para interoperar con switches antiguos por puerto. Por ejemplo, el algoritmo de árbol de expansión de RSTP elige un puente raíz de la misma forma que lo hace el estándar 802.1D original.

- RSTP mantiene el mismo formato de BPDU que el estándar IEEE 802.1D original, excepto que el campo Versión está establecido en 2 para indicar el protocolo RSTP y el campo Indicadores utiliza los 8 bits.
- RSTP puede confirmar de manera activa que un puerto puede sufrir una transición segura al estado de enviar sin depender de ninguna configuración de temporizadores.

### ¿Qué es RSTP?



### Capítulo 2: Redundancia de LAN 2.2.3.2 BPDU en RSTP

RSTP utiliza BPDU tipo 2, versión 2. El protocolo STP 802.1D original utiliza BPDU tipo 0, versión 0. Sin embargo, los switches que ejecutan RSTP se pueden comunicar directamente con los switches que ejecutan el protocolo STP 802.1D original. RSTP envía BPDU y completa el byte del indicador de una forma ligeramente diferente a la del estándar 802.1D original:

- La información de protocolo se puede vencer de inmediato en un puerto si no se reciben los paquetes de saludo durante tres tiempos de saludo consecutivos (seis segundos de manera predeterminada) o si caduca el temporizador de antigüedad máxima.
- Debido a que las BPDU se utilizan como un mecanismo de actividad, tres BPDU perdidas en forma consecutiva indican la pérdida de la conectividad entre un puente y su raíz vecina o puente designado. La rápida expiración de la información permite que las fallas se detecten muy rápidamente.

**Nota:** al igual que STP, los switches RSTP envían una BPDU con su información actual cada tiempo de saludo (dos segundos, de manera predeterminada), incluso si el puente RSTP no recibe ninguna BPDU del puente raíz.

Como se muestra en la ilustración, RSTP utiliza el byte del indicador de la BPDU versión 2:

- Los bits 0 y 7 se utilizan para el cambio de topologías y el acuse de recibo, al igual que en el estándar 802.1D original.
- Los bits 1 y 6 se utilizan para el proceso de Acuerdo de propuesta (para la convergencia rápida).
- Los bits del 2 al 5 codifican la función y el estado del puerto.
- Los bits 4 y 5 se utilizan para codificar la función del puerto mediante un código de 2 bits.

### BPDU en RSTP

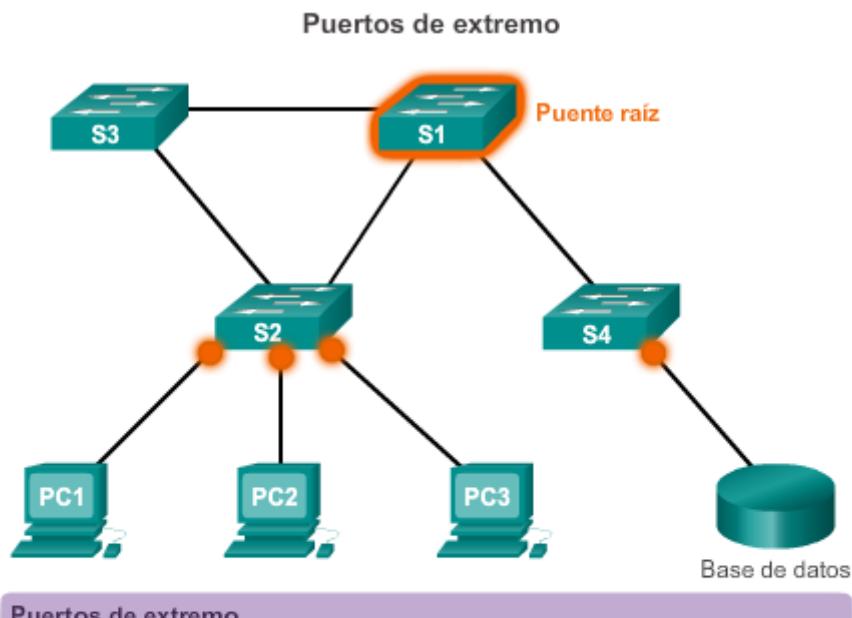
BPDU en RSTP Versión 2		Campo señalador	
Campo	Longitud de byte	Bit del campo	Bit
ID de protocolo = 0x0000	2	Cambio en la topología	0
ID de versión del protocolo = 0x02	1	Propuesta	1
Tipo de BPDU = 0X02	1	Función de puerto Puerto desconocido Puerto alternativo o de respaldo Puerto raíz Puerto designado	2-3 00 01 10 11
Indicadores	1	Aprendizaje	4
ID de raíz	8	Reenvío	5
Costo de la ruta raíz	4	Acuerdo	6
ID de puente	8	Acuse de recibo de cambio de topología	7
ID de puerto	2		
Antigüedad del mensaje	2		
Antigüedad máxima	2		
Tiempo de saludo	2		
Retraso de envío	2		

### Capítulo 2: Redundancia de LAN 2.2.3.3 Puertos de extremo

La implementación de Cisco de RSTP, PVST+ rápido, conserva la palabra clave PortFast mediante el comando **spanning-tree portfast** para la configuración de puertos de perímetro. Esto hace que la transición de STP a RSTP se dé sin inconvenientes.

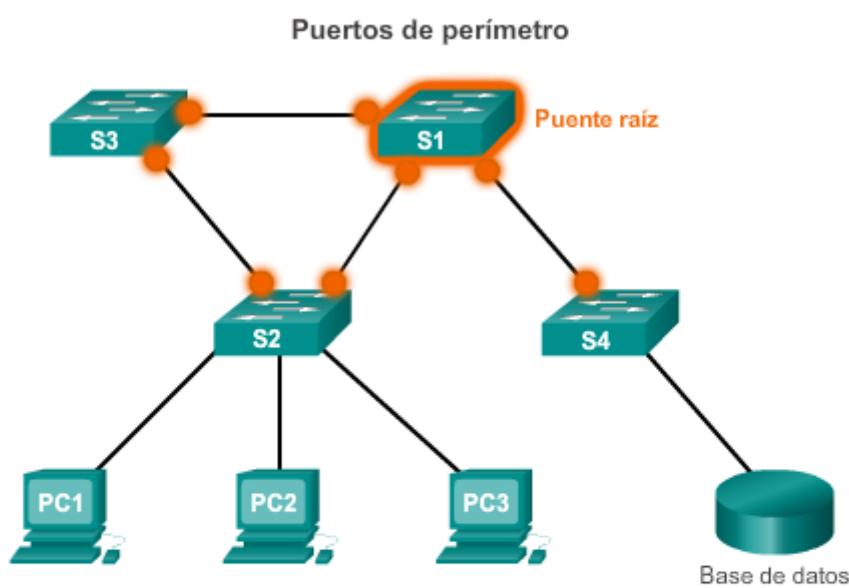
En la figura 1, se muestran ejemplos de puertos que se pueden configurar como puertos de perímetro. En la figura 2, se muestran ejemplos de puertos que no son de perímetro.

**Nota:** no se recomienda configurar un puerto de perímetro para conectarlo a otro switch. Esto puede tener consecuencias negativas para RSTP, ya que puede ocurrir un bucle temporal, lo que posiblemente retrase la convergencia de RSTP.



**Puertos de extremo**

- Nunca se conectan a un switch.
- Pasan de inmediato al estado de reenvío.
- Funcionan de forma similar a un puerto configurado con Cisco PortFast.
- En los switches Cisco, se configuran mediante el comando **spanning-tree portfast**.



**Puertos de perímetro**

Son puertos que pueden estar conectados a otros dispositivos de switch y no se deben configurar como puertos perimetrales.

## Capítulo 2: Redundancia de LAN 2.2.3.4 Tipos de enlace

Mediante el uso del modo dúplex en el puerto, el tipo de enlace proporciona una categorización para cada puerto que participa en RSTP. Según lo que se conecta a cada puerto, se pueden identificar dos tipos diferentes de enlace:

- **Punto a punto:** un puerto que funciona en modo full-duplex generalmente conecta un switch a otro y es candidato para la transición rápida al estado de reenvío.
- **Compartido:** un puerto que funciona en modo half-duplex conecta un switch a un hub que conecta varios dispositivos.

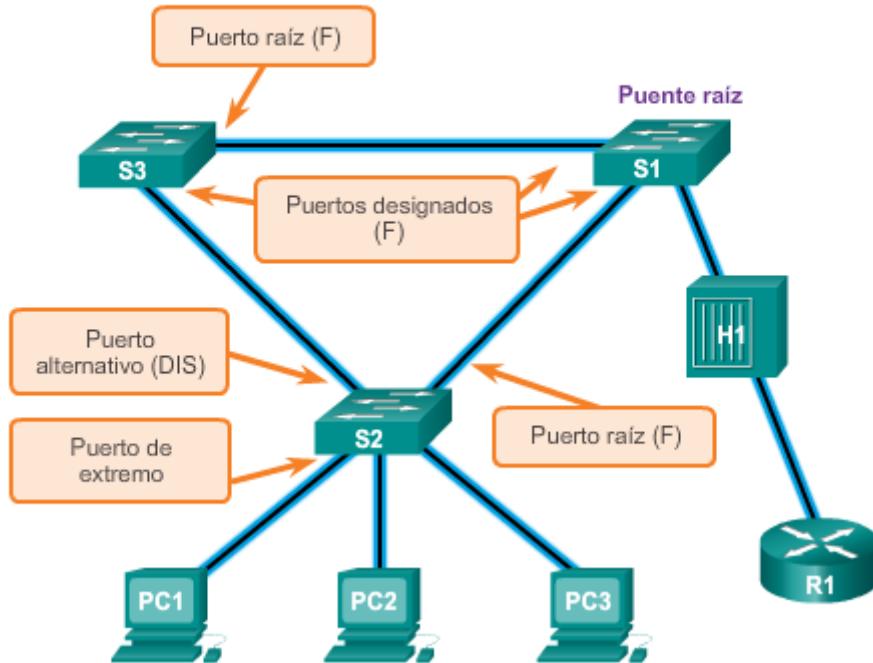
En la ilustración, haga clic en cada enlace para obtener información acerca de los tipos de enlace.

El tipo de enlace puede determinar si el puerto puede pasar de inmediato al estado de reenvío, suponiendo que se cumplan ciertas condiciones. Estas condiciones son distintas para los puertos de extremo y para los puertos que no son de extremo. Los puertos que no son de extremo se categorizan en dos tipos de enlaces, punto a punto y compartido. El tipo de enlace se determina automáticamente, pero se puede anular con una configuración de puerto explícita mediante el comando **spanning-tree link-type parameter**.

Las conexiones de puerto de perímetro y punto a punto son candidatas para la transición rápida al estado de reenvío. Sin embargo, antes de que se considere el parámetro de tipo de enlace, RSTP debe determinar la función de puerto. Las características de las funciones de puerto en relación con los tipos de enlace incluyen lo siguiente:

- Los puertos raíz no utilizan el parámetro de tipo de enlace. Los puertos raíz son capaces de realizar una transición rápida al estado de enviar siempre que el puerto se encuentre sincronizado.
- En la mayoría de los casos, los puertos alternativos y de respaldo no utilizan el parámetro de tipo de enlace.
- Los puertos designados son los que más utilizan el parámetro de tipo de enlace. La transición rápida al estado de reenvío para el puerto designado ocurre solo si el parámetro de tipo de enlace se establece en *point-to-point*.

## Tipos de enlace

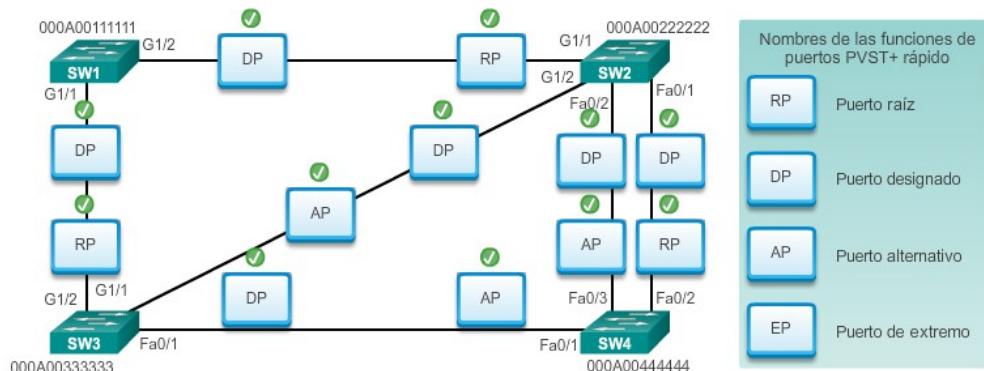


Capítulo 2: Redundancia de LAN 2.2.3.5 Actividad: Identificar las funciones de puerto en

### PVST+ rápido

#### Actividad: PVST+ rápido

Arrastre los nombres de las funciones de puerto PVST+ rápido hasta las ubicaciones de los puertos de switch correspondientes proporcionadas en la topología. Los nombres de función de los puertos se pueden utilizar más de una vez.



Capítulo 2: Redundancia de LAN 2.2.3.6 Actividad: Comparar PVST+ y PVST+ rápido

**Actividad: Comparar PVST+ y PVST+ rápido**

Haga clic en el campo correspondiente junto a cada característica para indicar si esa característica se relaciona con PVST+, PVST+ rápido o ambos.

	PVST+	PVST+ rápido	Ambos
1. Utiliza 802.1D para ejecutar una instancia distinta para cada VLAN.	✓		
2. Es posible compartir la carga con algunas VLAN de reenvío en cada enlace troncal.		✓	
3. El procesamiento de la CPU y el uso de ancho de banda del enlace troncal son superiores a los de STP.		✓	
4. La suma más baja de ID de VLAN, MAC y BID determina el puente raíz.		✓	
5. Protocolo exclusivo de Cisco.		✓	
6. Los puertos pueden pasar al estado de reenvío sin necesidad de un temporizador.	✓		
7. Funciones de puerto: raíz, designado, alternativo, perimetral, de respaldo.	✓		
8. Envía un mensaje de saludo BPDU cada dos segundos.		✓	

Capítulo 2: Redundancia de LAN 2.3.1.1 Configuración predeterminada de un switch Catalyst

2960

En la tabla, se muestra la configuración predeterminada de árbol de expansión para un switch Cisco de la serie Catalyst 2960. Observe que el modo de árbol de expansión predeterminado es

PVST+.

**Configuración de un switch de manera predeterminada**

Característica	Configuración predeterminada
Estado habilitado	Habilitado en la VLAN 1
Modo de árbol de expansión	PVST+ (PVST+ rápido y MSTP están deshabilitados)
Prioridad de switch	32768
Prioridad de puerto de árbol de expansión (configurable por interfaz)	128
Costo de puerto de árbol de expansión (configurable por interfaz)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Prioridad de puerto de VLAN de árbol de expansión (configurable por VLAN)	128
Costo de puerto de VLAN de árbol de expansión (configurable por VLAN)	1000 Mb/s: 4 100 Mb/s: 19 10 Mb/s: 100
Temporizadores de árbol de expansión	Tiempo de saludo: 2segundos Tiempo de retraso de reenvío: 15 segundos Tiempo máximo de vencimiento: 20 segundos Conteo de espera de transmisión: 6BPDU

Capítulo 2: Redundancia de LAN 2.3.1.2 Configuración y verificación de la ID de puente

Cuando un administrador desea seleccionar un switch específico como puente raíz, se debe ajustar el valor de prioridad del puente para asegurarse de que sea inferior a los valores de prioridad del puente del resto de los switches en la red. Existen dos métodos diferentes para configurar el valor de prioridad del puente en un switch Cisco Catalyst.

### Método 1

Para asegurar que un switch tenga el valor de puente más bajo, utilice el comando **spanning-tree vlan id-vlan root primary** en el modo de configuración global. La prioridad para el switch está establecida en el valor predefinido 24576 o en el múltiplo más alto de 4096, menos que la prioridad del puente más baja detectada en la red.

Si se desea otro puente raíz, utilice el comando **spanning-tree vlan id-vlan root secondary** del modo de configuración global. Este comando establece la prioridad para el switch en el valor predeterminado 28672. Esto asegura que el switch alternativo se convierta en el puente raíz si falla el puente raíz principal. Se supone que el resto de los switches en la red tienen definido el valor de prioridad predeterminado 32768.

En la figura 1, el S1 se asignó como puente raíz principal mediante el comando **spanning-tree vlan 1 root primary**, y el S2 se configuró como puente raíz secundario mediante el comando **spanning-tree vlan 1 root secondary**.

### Método 2

Otro método para configurar el valor de prioridad del puente es utilizar el comando **spanning-tree vlan id-vlan priority valor** del modo de configuración global. Este comando da un control más detallado del valor de prioridad del puente. El valor de prioridad se configura en incrementos de 4096 entre 0 y 61440.

En el ejemplo, se asignó el valor de prioridad de puente 24576 al S3 mediante el comando **spanning-tree vlan 1 priority 24576**.

Para verificar la prioridad del puente de un switch, utilice el comando **show spanning-tree**. En la figura 2, la prioridad del switch se estableció en 24576. Además, observe que el switch está designado como puente raíz para la instancia de árbol de expansión.

Utilice el verificador de sintaxis de la figura 3 para configurar los switches S1, S2 y S3. Mediante el método 2 descrito anteriormente, configure el S3 de forma manual y establezca el valor de prioridad en 24576 para la VLAN 1. Mediante el método 1, configure el S2 como raíz secundaria para la VLAN 1 y el S1 como raíz principal para la VLAN 1. Verifique la configuración con el comando **show spanning-tree** en el S1.

## Configurar y verificar el BID

### Método 1

```
s1(config)# spanning-tree VLAN 1 root primary
s1(config)# end
```

### Método 2

```
s3(config)# spanning-tree VLAN 1 priority 24576
s3(config)# end
```

### Método 1

```
s2(config)# spanning-tree VLAN 1 root secondary
s2(config)# end
```

## Configurar y verificar el BID

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    24577
              Address     00A.0033.3333
              This bridge is the root
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID  Priority    24577 (priority 24576 sys-id-ext 1)
              Address     000A.0033.3333
              Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time   300

  Interface   Role      Sts       Cost      Prio.Nbr      Type
  -----       ----      --       ----      -----        -----
  Fa0/1       Desg     FWD       4          128.1        p2p
  Fa0/2       Desg     FWD       4          128.2        p2p
S3#
```

## Capítulo 2: Redundancia de LAN 2.3.1.3 PortFast y protección BPDU

PortFast es una característica de Cisco para los entornos PVST+. Cuando un puerto de switch se configura con PortFast, ese puerto pasa del estado de bloqueo al de reenvío de inmediato, omitiendo los estados de transición de STP 802.1D usuales (los estados de escucha y aprendizaje). Puede utilizar PortFast en los puertos de acceso para permitir que estos dispositivos se conecten a la red inmediatamente, en lugar de esperar a que STP IEEE 802.1D

converja en cada VLAN. Los puertos de acceso son puertos conectados a una única estación de trabajo o a un servidor.

En una configuración de PortFast válida, nunca se deben recibir BPDU, ya que esto indicaría que hay otro puente o switch conectado al puerto, lo que podría causar un bucle de árbol de expansión. Los switches Cisco admiten una característica denominada “protección BPDU”. Cuando se habilita, la protección BPDU coloca al puerto en estado *deshabilitado por error* al recibir una BPDU. Esto desactiva el puerto completamente. La característica de protección BPDU proporciona una respuesta segura a la configuración no válida, ya que se debe volver a activar la interfaz de forma manual.

La tecnología Cisco PortFast es útil para DHCP. Sin PortFast, un equipo puede enviar una solicitud de DHCP antes de que el puerto se encuentre en estado de enviar e impedirle al host la posibilidad de obtener una dirección IP utilizable y cualquier otra información. Debido a que PortFast cambia el estado a enviar de manera inmediata, el equipo siempre obtiene una dirección IP utilizable.

**Nota:** debido a que el propósito de PortFast es minimizar el tiempo que los puertos de acceso deben esperar a que converja el árbol de expansión, solo se debe utilizar en puertos de acceso. Si habilita PortFast en un puerto que se conecta a otro switch, corre el riesgo de crear un bucle de árbol de expansión.

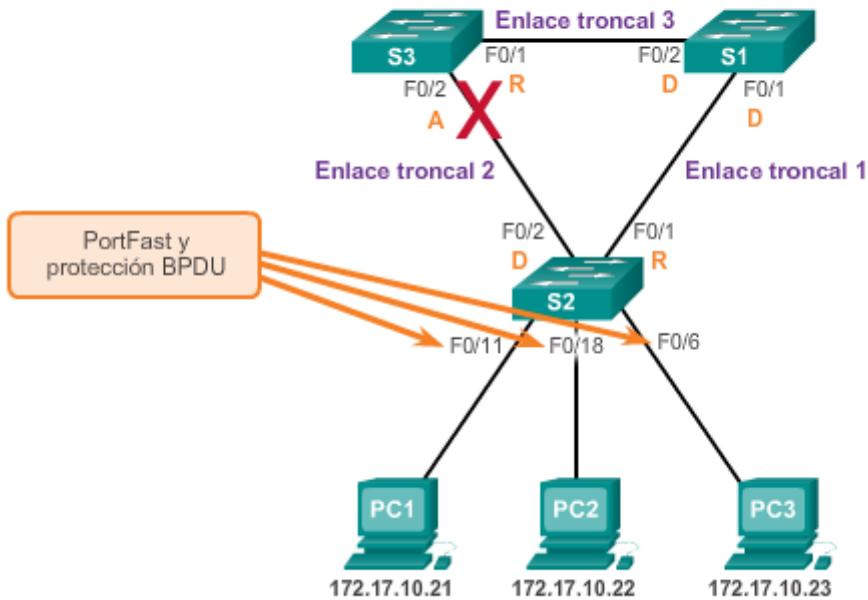
Para configurar PortFast en un puerto de switch, introduzca el comando **spanning-tree portfast** del modo de configuración de interfaz en cada interfaz en la que se deba habilitar PortFast, como se muestra en la figura 2. El comando **spanning-tree portfast default** del modo de configuración global habilita PortFast en todas las interfaces no troncales.

Para configurar la protección BPDU en un puerto de acceso de capa 2, utilice el comando **spanning-tree bpduguard enable** del modo de configuración de interfaz. El comando **spanning-tree portfast bpduguard default** del modo de configuración global habilita la protección BPDU en todos los puertos con PortFast habilitado.

Para verificar que se hayan habilitado PortFast y la protección BPDU para un puerto de switch, utilice el comando **show running-config**, como se muestra en la figura 3. La característica PortFast y la protección BPDU están deshabilitadas en todas las interfaces de manera predeterminada.

Utilice el verificador de sintaxis de la figura 4 para configurar y verificar los switches S1 y S2 con PortFast y la protección BPDU.

## PortFast y protección BPDU



### Configuración de PortFast y protección BPDU

```
S2(config)# interface FastEthernet 0/11
S2(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to
a single host. Connecting hubs, concentrators, switches,
bridges, etc... to this interface when portfast is enabled,
can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/11 but will only
have effect when the interface is in a non-trunking mode.
S2(config-if)# spanning-tree bpduguard enable
S2(config-if)# end
```

### PortFast y protección BPDU

```
S2# show running-config interface f0/11
Building configuration...

Current configuration : 90 bytes
!
interface FastEthernet0/11
  spanning-tree portfast
  spanning-tree bpduguard enable
end

S2#
```

## Capítulo 2: Redundancia de LAN 2.3.1.4 Balanceo de carga de PVST+

En la topología de la figura 1, se muestran tres switches conectados mediante enlaces troncales 802.1Q. Hay dos VLAN, 10 y 20, que se enlazan de forma troncal a través de estos enlaces. El objetivo es configurar el S3 como puente raíz para la VLAN 20 y el S1 como puente raíz para la VLAN 10. El puerto F0/3 en el S2 es el puerto de reenvío para la VLAN 20 y el puerto de bloqueo para la VLAN 10. El puerto F0/2 en el S2 es el puerto de reenvío para la VLAN 10 y el puerto de bloqueo para la VLAN 20.

Además de establecer un puente raíz, también es posible establecer uno secundario. Un puente raíz secundario es un switch que se puede convertir en puente raíz para una VLAN si falla el puente raíz principal. Si se tiene en cuenta que los otros puentes de la VLAN retienen su prioridad de STP predeterminada, este switch se convierte en el puente raíz en el caso de producirse una falla en el puente raíz principal.

Los pasos para configurar PVST+ en esta topología de ejemplo son los siguientes:

**Paso 1.** Seleccionar los switches que desea como puentes raíz principal y secundario para cada VLAN. Por ejemplo, en la figura 1, el S3 es el puente principal y el S1 es el puente secundario para la VLAN 20.

**Paso 2.** Configure el switch como puente principal para la VLAN mediante el comando **spanning-tree vlannumber root primary**, como se muestra en la figura 2.

**Paso 3.** Configure el switch como puente secundario para la VLAN mediante el comando **spanning-tree vlannumber root secondary**.

Otra forma de especificar el puente raíz es establecer la prioridad de árbol de expansión de cada switch en el menor valor, de modo que se seleccione el switch como puente principal para la VLAN asociada.

Observe que, en la figura 2, el S3 está configurado como puente raíz principal para la VLAN 20 y el S1 está configurado como puente raíz principal para la VLAN 10. El S2 mantuvo la prioridad de STP predeterminada.

En la ilustración, también se observa que el S3 está configurado como puente raíz secundario para la VLAN 10 y el S1 está configurado como puente raíz secundario para la VLAN 20. Esta configuración habilita el balanceo de carga de árbol de expansión, en el que el tráfico de la VLAN 10 pasa por el S1 y el de la VLAN 20 pasa por el S3.

Como se muestra en la figura 3, otra forma de especificar el puente raíz es establecer la prioridad de árbol de expansión de cada switch en el menor valor, de modo que se seleccione el switch como puente principal para la VLAN asociada. Se puede establecer la prioridad de switch para cualquier instancia de árbol de expansión. Esta configuración afecta la posibilidad de que un switch se elija como puente raíz. Un valor menor provoca el aumento de la probabilidad de que el switch sea seleccionado. El rango varía entre 0 y 61440 en incrementos de 4096; el resto de los valores se descarta. Por ejemplo, un valor de prioridad válido sería  $4096 \times 2 = 8192$ .

Como se muestra en la figura 4, el comando **show spanning-tree active** solo muestra los detalles de configuración de árbol de expansión para las interfaces activas. El resultado que se

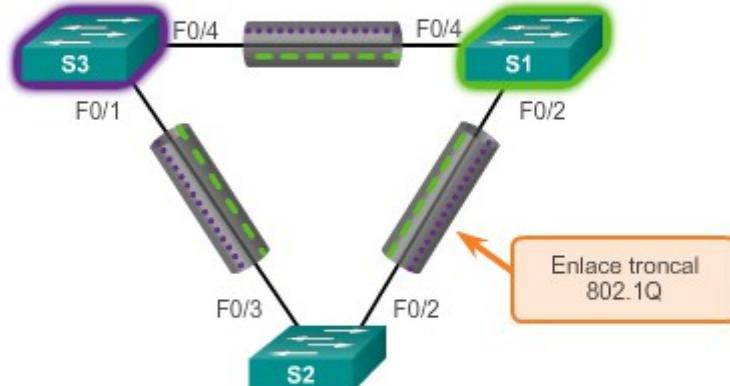
muestra pertenece al S1 configurado con PVST+. Existen varios parámetros de comandos del IOS de Cisco relacionados con el comando **show spanning-tree**.

En la figura 5, el resultado muestra que la prioridad de la VLAN 10 es 4096, la más baja de las tres prioridades de VLAN respectivas.

Utilice el verificador de sintaxis de la figura 6 para configurar y verificar el árbol de expansión para el S1 y el S3.

## Configurar PVST+

Puente raíz principal para la VLAN 20      Puente raíz principal para VLAN 10  
Puente raíz secundario para la VLAN 10      Puente raíz secundario para VLAN 20



VLAN 10 -----

VLAN 20 .....

## Configurar PVST+

```
S3(config)# spanning-tree vlan 20 root primary
```

Este comando hace que el S3 sea la raíz principal para la VLAN 20.

```
S3(config)# spanning-tree vlan 10 root secondary
```

Este comando hace que el S3 sea la raíz secundaria para la VLAN 10.

```
S1(config)# spanning-tree vlan 10 root primary
```

Este comando hace que el S1 sea la raíz principal para la VLAN 10.

```
S1(config)# spanning-tree vlan 20 root secondary
```

Este comando hace que el S1 sea la raíz secundaria para la VLAN 20.

## Configurar PVST+

```
S3(config)# spanning-tree vlan 20 priority 4096
```

Este comando establece la prioridad del S3 para que sea la más baja posible, lo que brinda más posibilidades de que el S3 sea la raíz principal para la VLAN 20.

```
S1(config)# spanning-tree vlan 10 priority 4096
```

Este comando establece la prioridad del S1 para que sea la más baja posible, lo que brinda más posibilidades de que el S1 sea la raíz principal para la VLAN 10.

## Configurar PVST+

```
S1# show spanning-tree active
<resultado omitido>
VLAN0010
  Spanning tree enabled protocol ieee
    Root ID    Priority 4106
      Address 0019.aa9e.b000
      This bridge is the root
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
    Bridge ID  Priority 4106 (priority 4096 sys-id-ext 10)
      Address 0019.aa9e.b000
      Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
      Aging Time 300

    Interface   Role     Sts      Cost      Prio.Nbr      Type
    -----      ---      ---      ---      -----
    Fa0/2       Desg    FWD      19        128.2        p2p
    Fa0/4       Desg    FWD      19        128.4        p2p

<resultado omitido>
```

## Configurar PVST+

```
S1# show running-config
Building configuration...

Current configuration : 1595 bytes
!
version 12.2
<resultado omitido>
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
```

Capítulo 2: Redundancia de LAN 2.3.1.5 Packet Tracer: Configuración de PVST+

### Información básica/situación

En esta actividad, configurará redes VLAN y enlaces troncales, y examinará y configurará los puentes raíz principales y secundarios del protocolo de árbol de expansión. También optimizará la topología conmutada mediante PVST+, PortFast y la protección BPDU.

[Packet Tracer: Configuración de PVST+ \(instrucciones\)](#)

[Packet Tracer: configuración de PVST+ \(PKA\)](#)

## Capítulo 2: Redundancia de LAN 2.3.2.1 Modo de árbol de expansión

PVST+ rápido es la implementación de Cisco de RSTP. Este admite RSTP por VLAN. La topología en la figura 1 posee dos VLAN: 10 y 20.

**Nota:** la configuración predeterminada de árbol de expansión en un switch Cisco de la serie Catalyst 2960 es PVST+. Los switches Cisco de la serie Catalyst 2960 admiten PVST+, PVST+ rápido y MST, pero solo puede haber una versión activa para todas las VLAN al mismo tiempo.

Los comandos de PVST+ rápido controlan la configuración de las instancias de árbol de expansión de las VLAN. La instancia de árbol de expansión se crea cuando se asigna una interfaz a una VLAN y se elimina cuando la última interfaz se traslada a otra VLAN. Además, puede configurar los parámetros de puertos y switches STP antes de que se cree una instancia de árbol de expansión. Estos parámetros se aplican cuando se crea una instancia de árbol de expansión.

En la figura 2, se muestra la sintaxis de comandos Cisco IOS que se necesita para configurar PVST+ rápido en un switch Cisco. El comando necesario para configurar PVST+ rápido es el comando **spanning-tree mode rapid-pvst** del modo de configuración global. Cuando se especifica la interfaz que se debe configurar, las interfaces válidas incluyen puertos físicos, redes VLAN y canales de puertos. El rango de ID de la VLAN es de 1 a 4094 cuando está instalada la imagen mejorada del software (EI) y de 1 a 1005 cuando está instalada la imagen estándar del software (SI). El intervalo de canales de puerto es de 1 a 6.

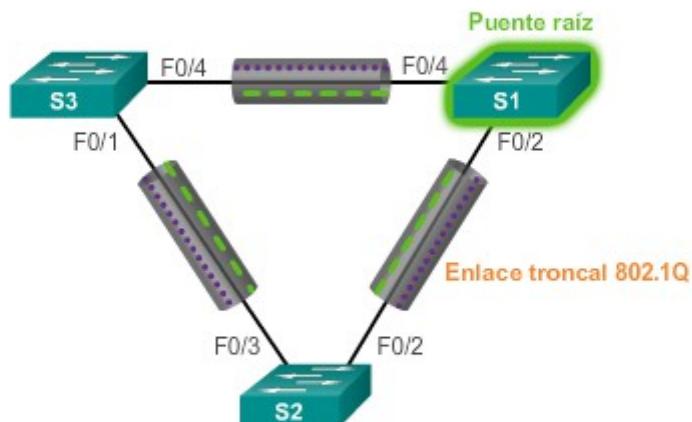
En la figura 3, se muestran los comandos de PVST+ rápido configurados en el S1.

En la figura 4, el comando **show spanning-tree vlan 10** muestra la configuración de árbol de expansión para la VLAN 10 en el switch S1. Observe que la prioridad de BID está establecida en 4096. En el resultado, la instrucción “Spanning tree enabled protocol rstp” indica que el S1 ejecuta PVST+ rápido. Dado que el S1 es el puente raíz para la VLAN 10, todas sus interfaces son puertos designados.

En la figura 5, el comando **show running-config** se utiliza para verificar la configuración de PVST+ rápido en el S1.

**Nota:** por lo general, no es necesario configurar el parámetro *tipo-enlace* punto a punto para PVST+ rápido, ya que no es común que se dé un *tipo-enlace* compartido. En la mayoría de los casos, la única diferencia entre la configuración de PVST+ y PVST+ rápido es el comando **spanning-tree mode rapid-pvst**.

## Configurar PVST+ rápido



VLAN 10 - - - - -

VLAN 20 ..... - - - - -

## Configurar PVST+ rápido

### Sintaxis de comandos Cisco IOS

Ingrese al modo de configuración global.	<code>configure terminal</code>
Configura el modo de árbol de expansión PVST+ rápido.	<code>spanning-tree mode rapid-pvst</code>
Ingres al modo de configuración de interfaz y especifica una interfaz para configurar. Las interfaces válidas incluyen puertos físicos, VLAN y canales de puerto.	<code>interface interface-id</code>
Especificar que el tipo de enlace para este puerto es punto a punto.	<code>spanning-tree link-type point-to-point</code>
Volver al modo EXEC privilegiado.	<code>end</code>
Borrar todos los STP detectados.	<code>clear spanning-tree detected-protocols</code>

## Configurar PVST+ rápido

```
S1# configure terminal
S1(config)# spanning-tree mode rapid-pvst
S1(config)# interface f0/2
S1(config-if)# spanning-tree link-type point-to-point
S1(config-if)# end
S1# clear spanning-tree detected-protocols
```

## Configurar PVST+ rápido

```
S1# show spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol rstp
    Root ID    Priority    4106
                Address     0019.aa9e.b000
                This bridge is the root
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
    Bridge ID   Priority    4106  (priority 4096 sys-id-ext 10)
                Address     0019.aa9e.b000
                Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                Aging Time 300
  Interface      Role Sts Cost      Prio.Nbr Type
  -----
  Fa0/2          Desg LRN 19      128.2    P2p
  Fa0/4          Desg LRN 19      128.4    P2p
<resultado omitido>
S1#
```

## Configurar PVST+ rápido

```
S1# show run
<resultado omitido>
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 4096
spanning-tree vlan 20 priority 28672
!
<resultado omitido>
S1#
```

Capítulo 2: Redundancia de LAN 2.3.2.2 Packet Tracer: Configuración de PVST+ rápido

Información básica/situación

En esta actividad, configurará redes VLAN y enlaces troncales, y examinará y configurará los puentes raíz principales y secundarios del árbol de expansión. Además, lo optimizará mediante el uso de PVST+ rápido, PortFast y la protección BPDU.

[Packet Tracer: Configuración de PVST+ rápido \(instrucciones\)](#)

[Packet Tracer: Configuración de PVST+ rápido \(PKA\)](#)

Capítulo 2: Redundancia de LAN 2.3.2.3 Práctica de laboratorio: Configuración de PVST+ rápido, PortFast y protección BPDU

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar redes VLAN, VLAN nativa y enlaces troncales
- Parte 3: Configurar el puente raíz y examinar la convergencia de PVST+
- Parte 4: Configurar el PVST+ rápido, PortFast, la protección BPDU, y examinar la convergencia

[Práctica de laboratorio: Configuración de PVST+ rápido, PortFast y protección BPDU](#)

Capítulo 2: Redundancia de LAN 2.3.3.1 Análisis de la topología STP

Para analizar la topología STP, siga estos pasos:

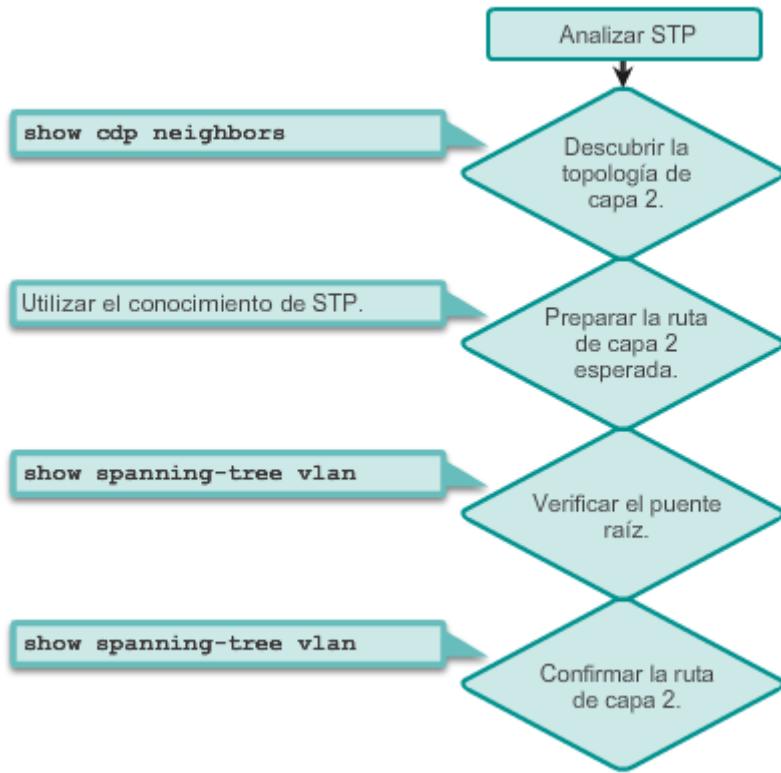
**Paso 1.** Descubra la topología de capa 2. Utilice la documentación de red, si existe, o utilice el comando **show cdp neighbors** para descubrir la topología de capa 2.

**Paso 2.** Después de descubrir la topología de capa 2, aplique sus conocimientos de STP para determinar la ruta de capa 2 esperada. Es necesario saber qué switch es el puente raíz.

**Paso 3.** Utilice el comando **show spanning-tree vlan** para determinar qué switch es el puente raíz.

**Paso 4.** Utilice el comando **show spanning-tree vlan** en todos los switches para descubrir cuáles son los puertos que están en estado de bloqueo o de reenvío, y para confirmar la ruta de capa 2 esperada.

## Análisis de la topología STP

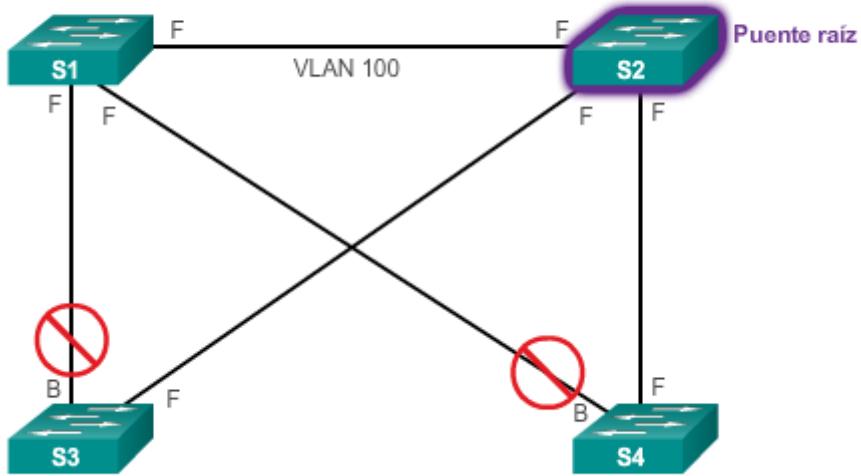


### Capítulo 2: Redundancia de LAN 2.3.3.2 Comparación entre la topología esperada y la topología real

En muchas redes, la topología STP óptima se determina como parte del diseño de red y se implementa mediante la manipulación de los valores de prioridad y costo de STP. Se pueden producir situaciones en las que STP no se haya tenido en cuenta en el diseño y la implementación de la red, o en las que se haya tenido en cuenta y se lo haya implementado antes de que la red se expandiera y sufriera modificaciones a gran escala. En dichas situaciones, es importante saber analizar la topología STP real en la red en funcionamiento.

Una gran parte de la resolución de problemas implica comparar el estado real de la red con el estado que se espera de esta y detectar las diferencias para reunir pistas acerca del problema que se debe resolver. Un profesional de red debe poder examinar los switches y determinar la topología real, además de poder entender cuál debería ser la topología de árbol de expansión subyacente.

## Verificación de la coincidencia entre la topología real y la topología esperada



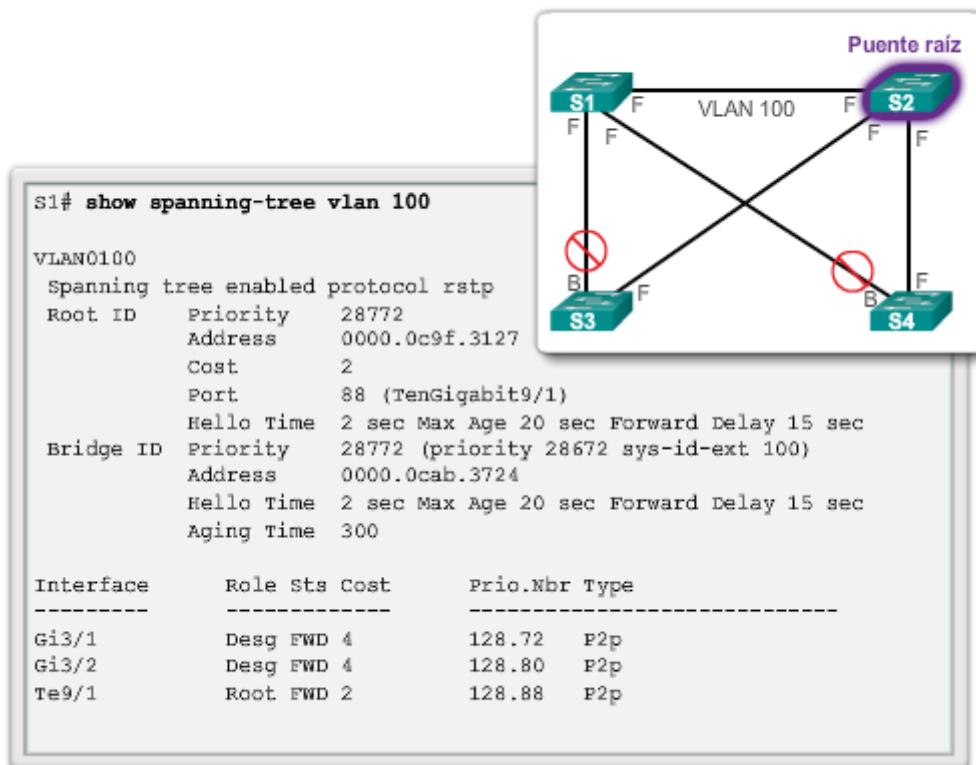
### Capítulo 2: Redundancia de LAN 2.3.3.3 Descripción general del estado del árbol de expansión

Si se utiliza el comando **show spanning-tree** sin especificar ninguna opción adicional, se obtiene una breve descripción general del estado de STP para todas las VLAN definidas en el switch. Si solo le interesa una VLAN en particular, limite el alcance de este comando especificando esa VLAN como opción.

Utilice el comando **show spanning-tree vlan id\_vlan** para obtener información acerca de STP de una VLAN específica. Utilice este comando para obtener información acerca de la función y el estado de cada puerto del switch. En el resultado de ejemplo en el switch S1, se muestran los tres puertos en estado de reenvío (FWD) y la función de estos como puertos designados o raíz. Para los puertos que están bloqueados, el resultado muestra el estado "BLK".

El resultado también muestra información acerca del BID del switch local y la ID de raíz, que es el BID del puente raíz.

## Descripción general del estado de STP



### Capítulo 2: Redundancia de LAN 2.3.3.4 Consecuencias de las fallas del árbol de expansión

En la mayoría de los protocolos, una falla significa que se pierde la funcionalidad que proporcionaba el protocolo. Por ejemplo, si OSPF funciona mal en un router, es posible que se pierda la conectividad a las redes a las que se puede llegar mediante ese router. En general, esto no afectaría el resto de la red OSPF. Si todavía está disponible la conectividad al router, es posible diagnosticar y resolver el problema.

Existen dos tipos de falla en STP. La primera es similar al problema de OSPF. Es posible que STP bloquee por error los puertos que se deberían haber colocado en estado de reenvío. Se puede perder la conectividad para el tráfico que normalmente pasaría por este switch, pero el resto de la red no se ve afectada. El segundo tipo de falla es mucho más perjudicial, como se muestra en la figura 1. Esta falla se produce cuando STP pasa uno o más puertos al estado de reenvío por error.

Recuerde que el encabezado de las tramas de Ethernet no incluye un campo TTL, lo que significa que los switches continúan reenviando indefinidamente cualquier trama que entre en un bucle de puente. Las únicas excepciones son las tramas que tienen la dirección de destino registrada en la tabla de direcciones MAC de los switches. Estas tramas simplemente se reenvían al puerto asociado a la dirección MAC y no ingresan a ningún bucle. Sin embargo, cualquier trama que un switch use para saturar los puertos ingresa al bucle (figura 2). Esto puede incluir difusiones, multidifusiones y unidifusiones con una dirección MAC de destino desconocida globalmente.

¿Cuáles son las consecuencias y los síntomas correspondientes de la falla de STP (figura 3)?

La carga de todos los enlaces en la LAN conmutada comienza a aumentar rápidamente a medida que ingresan cada vez más tramas al bucle. Este problema no se limita a los enlaces que forman el bucle, sino que además afecta al resto de los enlaces en el dominio conmutado, dado que las tramas saturan todos los enlaces. Cuando la falla del árbol de expansión se limita a una única VLAN, solo los enlaces de esa VLAN se ven afectados. Los switches y los enlaces troncales que no transportan esa VLAN funcionan con normalidad.

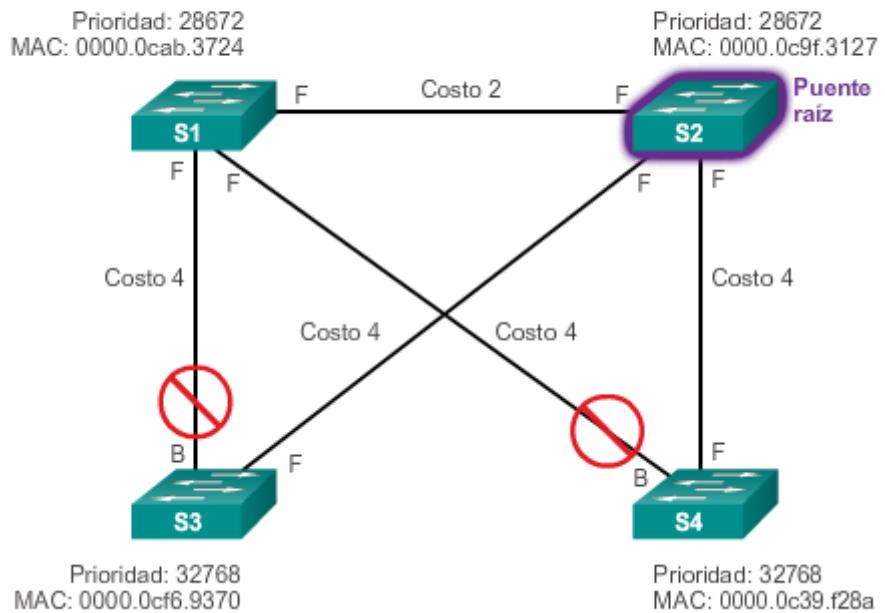
Si la falla del árbol de expansión creó un bucle de puente, el tráfico aumenta exponencialmente. Los switches saturan varios puertos con las difusiones. Esto crea copias de las tramas cada vez que los switches las reenvían.

Cuando el tráfico del plano de control comienza a ingresar al bucle (por ejemplo, los saludos OSPF o EIGRP), los dispositivos que ejecutan esos protocolos comienzan a sobrecargarse rápidamente. Las CPU se acercan al 100% de utilización mientras intentan procesar una carga de tráfico del plano de control en constante aumento. En muchos casos, el primer indicio de esta tormenta de difusión en proceso es que los routers o los switches de capa 3 informan fallas en el plano de control y que están funcionando con una elevada carga de CPU.

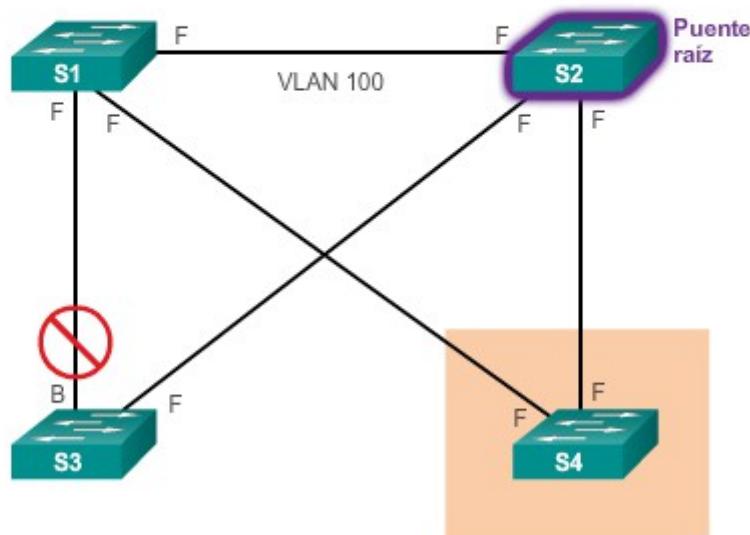
Los switches experimentan modificaciones frecuentes en la tabla de direcciones MAC. Si existe un bucle, es posible que un switch vea que una trama con determinada dirección MAC de origen ingresa por un puerto y que después vea que otra trama con la misma dirección MAC de origen ingresa por otro puerto una fracción de segundo más tarde. Esto provoca que el switch actualice la tabla de direcciones MAC dos veces para la misma dirección MAC.

Debido a la combinación de una carga muy alta en todos los enlaces con el funcionamiento de las CPU del switch a la carga máxima, por lo general, no se puede llegar a estos dispositivos. Esto hace que sea muy difícil diagnosticar el problema mientras ocurre.

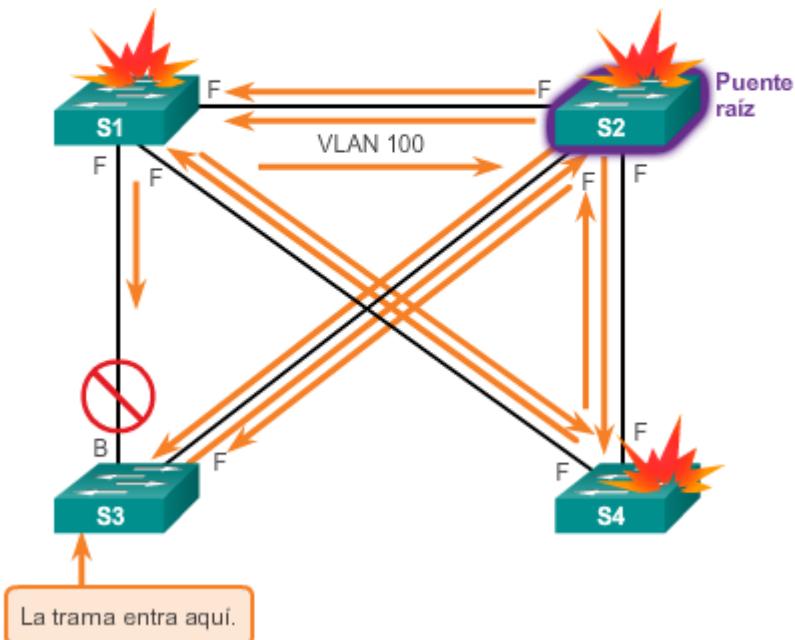
### La falla de STP puede ser catastrófica



### Transición errónea al estado de reenvío



## Las consecuencias de la falla de STP son graves



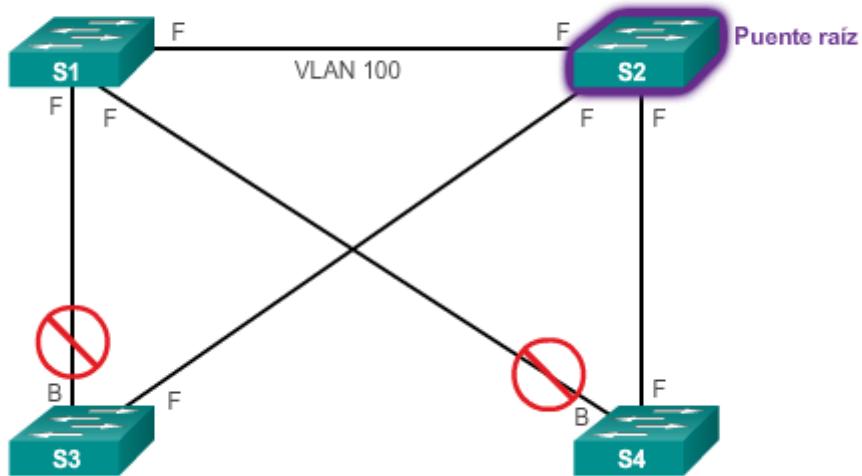
### Capítulo 2: Redundancia de LAN 2.3.3.5 Reparación de un problema del árbol de expansión

Una forma de corregir la falla del árbol de expansión es eliminar de manera manual los enlaces redundantes en la red comutada, ya sea físicamente o mediante la configuración, hasta eliminar todos los bucles de la topología. Cuando se rompen los bucles, las cargas de tráfico y de CPU deberían disminuir a niveles normales, y la conectividad a los dispositivos debería restaurarse.

Si bien esta intervención restaura la conectividad a la red, el proceso de resolución de problemas no finaliza aquí. Se eliminó toda la redundancia de la red comutada, y ahora se deben restaurar los enlaces redundantes.

Si no se resolvió la causa subyacente de la falla del árbol de expansión, es probable que al restaurar los enlaces redundantes se desate una nueva tormenta de difusión. Antes de restaurar los enlaces redundantes, determine y corrija la causa de la falla del árbol de expansión. Controle atentamente la red para asegurarse de que se haya resuelto el problema.

## Reparación de un problema del árbol de expansión



Capítulo 2: Redundancia de LAN 2.3.3.6 Actividad: Resolver problemas de configuración de STP

### Actividad: Resolver los problemas de configuración de STP, situación 2

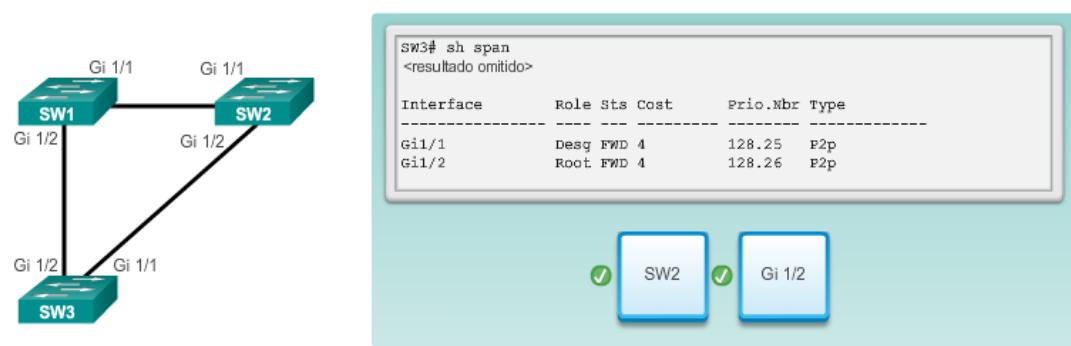
Arrastra hasta los espacios proporcionados el nombre de switch y el número de puerto para el switch con un puerto en modo de bloqueo de STP según la topología proporcionada y el resultado del comando `show`.

Interface	Role	Sts	Cost	Prio.xbr	Type
Gi1/1	Desg	FWD	4	128.25	P2p
Gi1/2	Root	FWD	4	128.26	P2p

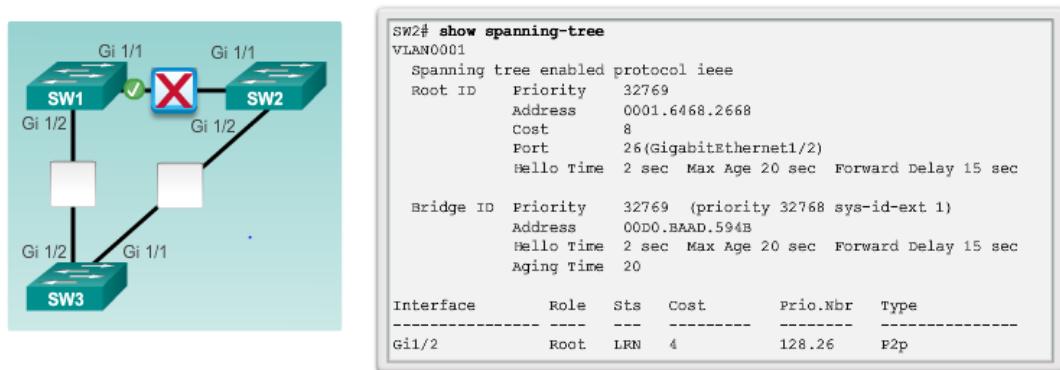
✓ SW2 ✓ Gi 1/2

**Actividad: Resolver los problemas de configuración de STP, situación 2**

Arrastra hasta los espacios proporcionados el nombre de switch y el número de puerto para el switch con un puerto en modo de bloqueo de STP según la topología proporcionada y el resultado del comando `show`.

**Actividad: Resolver los problemas de configuración de STP, situación 3**

Hay un enlace que no participa en STP entre dos de los switches. Arrastra la "x" de color rojo hasta el enlace que está inactivo según el resultado del comando `show`.



## Capítulo 2: Redundancia de LAN 2.4.1.1 Limitaciones del gateway predeterminado

Los protocolos de árbol de expansión permiten la redundancia física en una red comutada. Sin embargo, los hosts en la capa de acceso de una red jerárquica también se benefician de los gateways predeterminados alternativos. Si falla un router o una interfaz del router (que funciona como gateway predeterminado), los hosts configurados con ese gateway predeterminado quedan aislados de las redes externas. Se necesita un mecanismo para proporcionar gateways predeterminados alternativos en las redes comutadas donde hay dos o más routers conectados a las mismas VLAN.

**Nota:** a los efectos del análisis de la redundancia de los routers, no existe ninguna diferencia funcional entre un switch multicapa y un router en la capa de distribución. En la práctica, es común que un switch multicapa funcione como gateway predeterminado para cada VLAN en una red comutada. Este análisis se centra en la funcionalidad del *routing*, independientemente del dispositivo físico que se utilice.

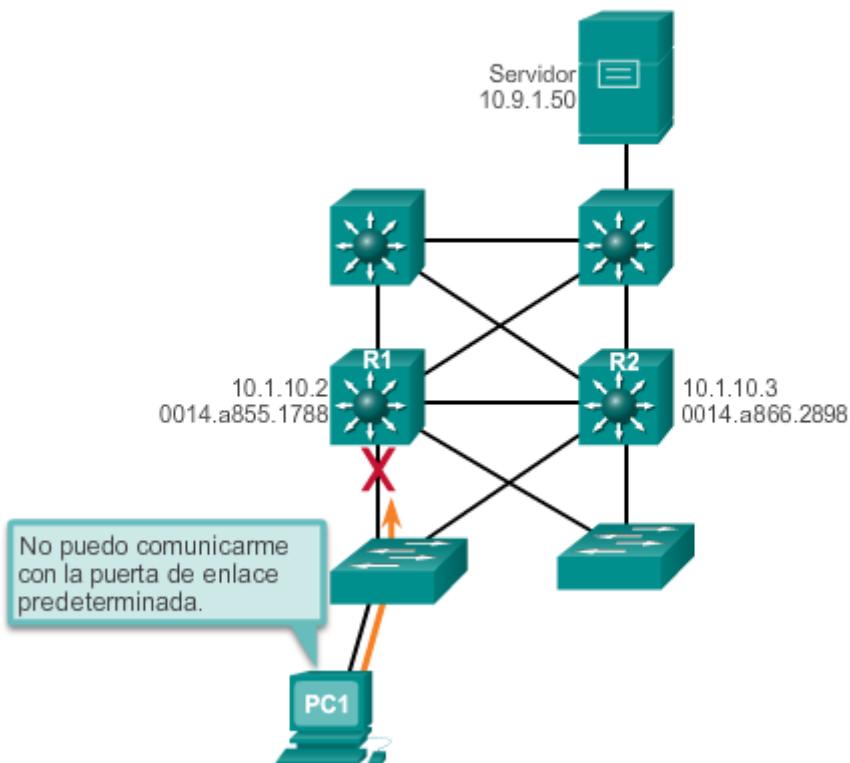
En una red comutada, cada cliente recibe solo un gateway predeterminado. No hay forma de configurar un gateway secundario, incluso si existe una segunda ruta que transporte paquetes fuera del segmento local.

En la ilustración, el R1 es el responsable de enrutar los paquetes de la PC1. Si el R1 deja de estar disponible, los protocolos de routing pueden converger de forma dinámica. Ahora, el R2 enruta paquetes de redes externas que habrían pasado por el R1. Sin embargo, el tráfico de la red interna asociado al R1, incluido el tráfico de las estaciones de trabajo, de los servidores y

de las impresoras que se configuraron con el R1 como gateway predeterminado, aún se envía al R1 y se descarta.

Por lo general, las terminales se configuran con una única dirección IP para el gateway predeterminado. Esta dirección no se modifica cuando cambia la topología de la red. Si no se puede llegar a esa dirección IP de gateway predeterminado, el dispositivo local no puede enviar paquetes fuera del segmento de red local, lo que lo desconecta completamente del resto de la red. Aunque exista un router redundante que sirva como puerta de enlace predeterminada para ese segmento, no hay un método dinámico para que estos dispositivos puedan determinar la dirección de una nueva puerta de enlace predeterminada.

### Limitaciones del gateway predeterminado



### Capítulo 2: Redundancia de LAN 2.4.1.2 Redundancia del router

Una forma de evitar un único punto de falla en el gateway predeterminado es implementar un router virtual. Como se muestra en la ilustración, para implementar este tipo de redundancia de router, se configuran varios routers para que funcionen juntos y así dar la sensación de que hay un único router a los hosts en la LAN. Al compartir una dirección IP y una dirección MAC, dos o más routers pueden funcionar como un único router virtual.

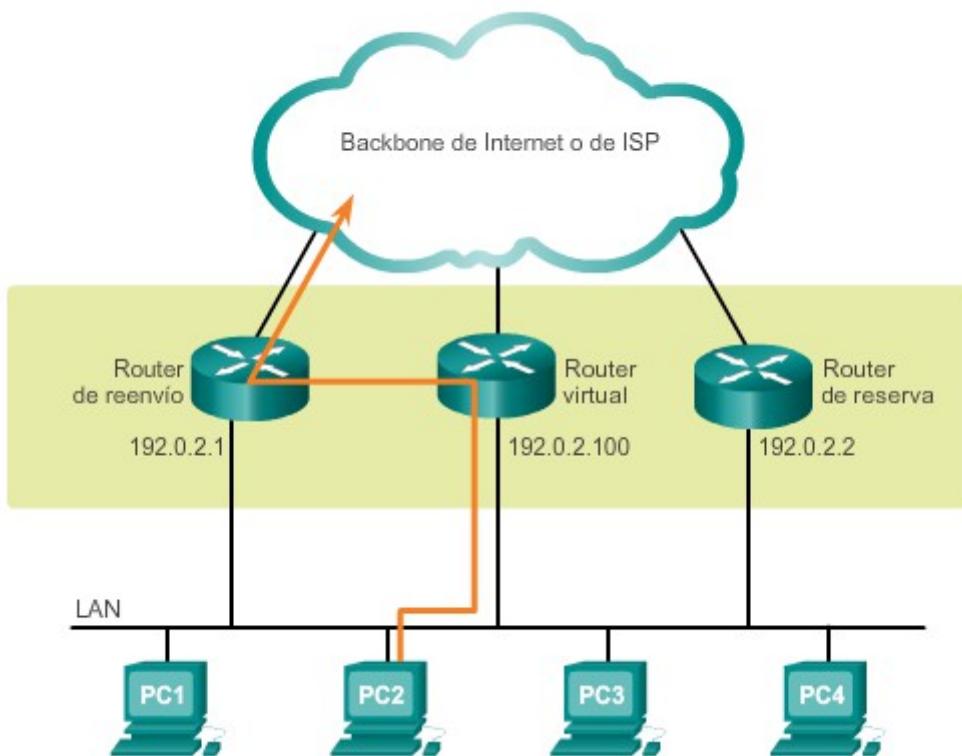
La dirección IP del router virtual se configura como la puerta de enlace predeterminada para las estaciones de trabajo de un segmento específico de IP. Cuando se envían tramas desde los dispositivos host hacia el gateway predeterminado, los hosts utilizan ARP para resolver la dirección MAC asociada a la dirección IP del gateway predeterminado. La resolución de ARP devuelve la dirección MAC del router virtual. El router actualmente activo dentro del grupo de routers virtuales puede procesar físicamente las tramas que se envían a la dirección MAC del router virtual. Los protocolos se utilizan para identificar dos o más routers como los dispositivos

responsables de procesar tramas que se envían a la dirección MAC o IP de un único router virtual. Los dispositivos host envían el tráfico a la dirección del router virtual. El router físico que reenvía este tráfico es transparente para los dispositivos host.

Un protocolo de redundancia proporciona el mecanismo para determinar qué router debe cumplir la función activa en el reenvío de tráfico. Además, determina cuándo un router de reserva debe asumir la función de reenvío. La transición entre los routers de reenvío es transparente para los dispositivos finales.

La capacidad que tiene una red para recuperarse dinámicamente de la falla de un dispositivo que funciona como gateway predeterminado se conoce como “redundancia de primer salto”.

### Redundancia del router

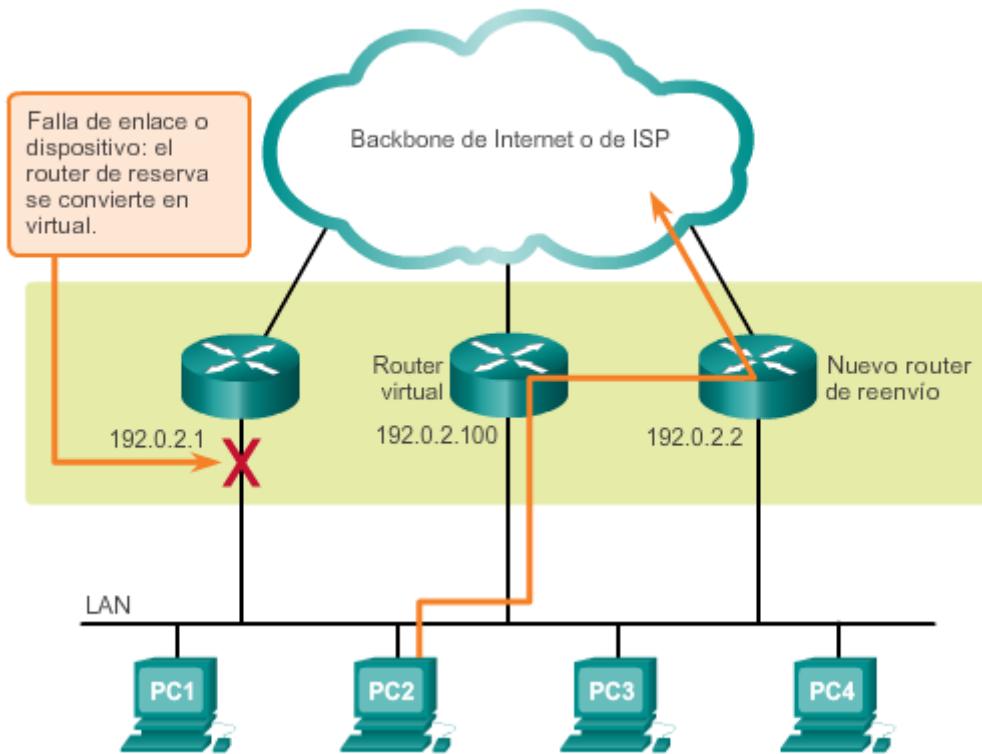


#### Capítulo 2: Redundancia de LAN 2.4.1.3 Pasos para la commutación por falla del router

Cuando falla el router activo, el protocolo de redundancia hace que el router de reserva asuma el nuevo rol de router activo. Estos son los pasos que se llevan a cabo cuando falla el router activo:

1. El router de reserva deja de recibir los mensajes de saludo del router de reenvío.
2. El router de reserva asume la función del router de reenvío.
3. Debido a que el nuevo router de reenvío asume tanto la dirección IP como la dirección MAC del router virtual, los dispositivos host no perciben ninguna interrupción en el servicio.

## Pasos para la conmutación por falla del router



### Capítulo 2: Redundancia de LAN 2.4.1.4 Actividad: Identificar la terminología de FHRP

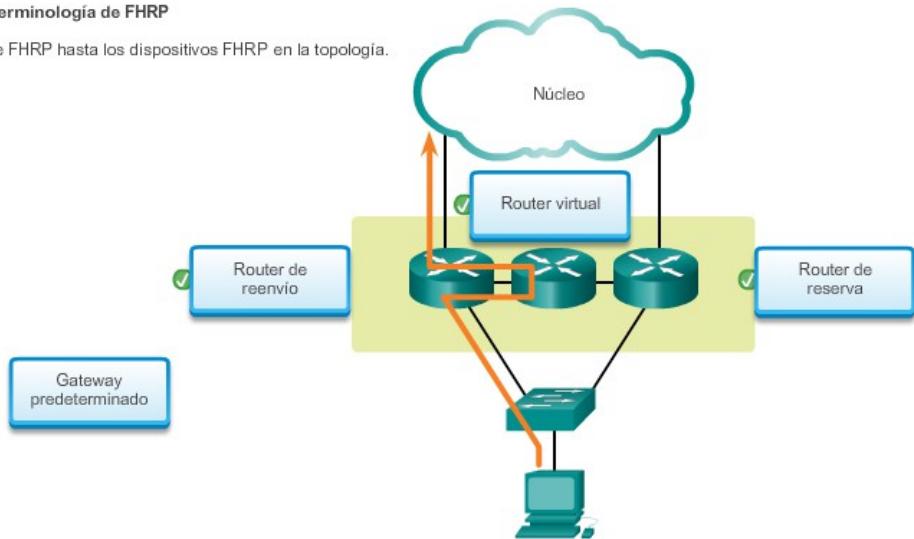
#### Actividad: Identificar la terminología de FHRP

Arrastre la terminología de FHRP hasta la definición correspondiente. Haga clic en el botón 2 para continuar la actividad.

<input checked="" type="checkbox"/> Gateway predeterminado	Es un dispositivo que dirige el tráfico destinado a los segmentos de red más allá del segmento de red de origen y para el cual el nodo emisor puede no tener información de routing.
<input checked="" type="checkbox"/> Router virtual	Es un conjunto de routers que trabajan juntos para dar la sensación de un único router a los hosts en un segmento de LAN.
<input checked="" type="checkbox"/> Dirección IP virtual	Es una dirección de capa 3 asignada a un protocolo que comparte la única dirección entre varios dispositivos.
<input checked="" type="checkbox"/> Router de reserva	Es un dispositivo que forma parte de un grupo de routers virtuales al que se asigna la función de gateway predeterminado alternativo.
<input checked="" type="checkbox"/> Dirección MAC virtual	Es la dirección de capa 2 que devuelve ARP para un gateway FHRP.
<input checked="" type="checkbox"/> Router de reenvío	Es un dispositivo que forma parte de un grupo de routers virtuales al que se asigna la función de gateway predeterminado.

Actividad: Identificar la terminología de FHRP

Arrastra la terminología de FHRP hasta los dispositivos FHRP en la topología.



Capítulo 2: Redundancia de LAN 2.4.2.1 Protocolos de redundancia de primer salto

En la siguiente lista, se definen las opciones disponibles para los protocolos de redundancia de primer salto (FHRP), como se muestra en la ilustración.

- **Protocolo de routing de reserva activa (HSRP):** es un protocolo exclusivo de Cisco diseñado para permitir la conmutación por falla transparente de un dispositivo IPv4 de primer salto. HSRP proporciona una alta disponibilidad de red, ya que proporciona redundancia de routing de primer salto para los hosts IPv4 en las redes configuradas con una dirección IPv4 de gateway predeterminado. HSRP se utiliza en un grupo de routers para seleccionar un dispositivo activo y un dispositivo de reserva. En un grupo de interfaces de dispositivo, el dispositivo activo es aquel que se utiliza para enrutar paquetes, y el dispositivo de reserva es el que toma el control cuando falla el dispositivo activo o cuando se cumplen condiciones previamente establecidas. La función del router de reserva HSRP es controlar el estado operativo del grupo HSRP y asumir rápidamente la responsabilidad de reenvío de paquetes si falla el router activo.
- **HSRP para IPv6:** FHRP exclusivo de Cisco que proporciona la misma funcionalidad de HSRP pero en un entorno IPv6. Un grupo IPv6 HSRP tiene una dirección MAC virtual derivada del número del grupo HSRP y una dirección IPv6 link-local virtual derivada de la dirección MAC virtual HSRP. Cuando el grupo HSRP está activo, se envían anuncios de router (RA) periódicos para la dirección IPv6 link-local virtual HSRP. Cuando el grupo deja de estar activo, estos RA finalizan después de que se envía un último RA.
- **Protocolo de redundancia de router virtual versión 2 (VRRPv2):** es un protocolo de elección no exclusivo que asigna de forma dinámica la responsabilidad de uno o más routers virtuales a los routers VRRP en una LAN IPv4. Esto permite que varios routers en un enlace de accesos múltiples utilicen la misma dirección IPv4 virtual. Los routers VRRP se configuran para ejecutar el protocolo VRRP en conjunto con uno o más routers conectados a una LAN. En una configuración VRRP, se elige un router como router virtual maestro, mientras que el resto funciona como respaldo en caso de que falle el router virtual maestro.
- **VRRPv3:** proporciona la capacidad de admitir direcciones IPv4 e IPv6. VRRPv3 funciona en entornos de varios proveedores y es más escalable que VRRPv2.

- **Protocolo de balanceo de carga de gateway (GLBP):** FHRP exclusivo de Cisco que protege el tráfico de datos contra una falla de router o de circuito, como HSRP y VRRP, a la vez que permite el balanceo de carga (también denominado “uso compartido de carga”) entre un grupo de routers redundantes.
- **GLBP para IPv6:** FHRP exclusivo de Cisco que proporciona la misma funcionalidad de GLBP pero en un entorno IPv6. GLBP para IPv6 proporciona un respaldo de router automático para los hosts IPv6 configurados con un único gateway predeterminado en una LAN. Se combinan varios routers de primer salto en la LAN para ofrecer un único router IPv6 virtual de primer salto y, al mismo tiempo, compartir la carga de reenvío de paquetes IPv6.
- **Protocolo de descubrimiento de router ICMP (IRDP):** se especifica en RFC 1256; es una solución FHRP antigua. IRDP permite que los hosts IPv4 ubiquen routers que proporcionan conectividad IPv4 a otras redes IP (no locales).

#### Opciones de redundancia de router de primer salto



- HSRP define un grupo de routers: uno activo y uno de reserva.
- Las direcciones IP y MAC virtuales se comparten entre los dos routers.
- Para verificar el estado de HSRP, utilice el comando `show standby`.
- HSRP es exclusivo de Cisco.
- VRRP es un protocolo estándar.

Capítulo 2: Redundancia de LAN 2.4.2.2 Actividad: Identificar el tipo de FHRP

**Actividad: Identificar el tipo de FHRP**

Arrastre el tipo de FHRP hasta la definición correspondiente. Cada tipo de FHRP se puede utilizar más de una vez en varias definiciones.

<input checked="" type="checkbox"/> GLBP	Es el protocolo FHRP exclusivo de Cisco que protege el tráfico de datos de un router o un circuito defectuoso y, al mismo tiempo, permite <b>compartir la carga</b> entre un grupo de routers redundantes.
<input checked="" type="checkbox"/> HSRP	Se utiliza en un grupo de routers para seleccionar un dispositivo <b>activo</b> y un dispositivo <b>de reserva</b> .
<input checked="" type="checkbox"/> HSRP	Es el protocolo FHRP exclusivo de Cisco diseñado para permitir la comutación por falla transparente de los dispositivos IPv4 de primer salto.
<input checked="" type="checkbox"/> VRRP	Se elige un router como router virtual <b>maestro</b> , mientras que el resto funciona como <b>respaldo</b> en caso de que falle el router virtual maestro.
<input checked="" type="checkbox"/> VRRP	Es un protocolo de elección no exclusivo que permite que varios routers en un enlace de acceso múltiple utilicen la misma dirección IPv4 virtual.

[Capítulo 2: Redundancia de LAN 2.4.3.1 Verificación de HSRP](#)

Un router HSRP activo presenta las siguientes características:

- Responde a las solicitudes de ARP del gateway predeterminado con la MAC del router virtual.
- Asume el reenvío activo de paquetes para el router virtual.
- Envía mensajes de saludo.
- Conoce la dirección IP del router virtual.

Un router HSRP de reserva presenta las siguientes características:

- Escucha los mensajes de saludo periódicos.
- Asume el reenvío activo de paquetes si no percibe actividad del router activo.

Utilice el comando **show standby** para verificar el estado de HSRP. En la ilustración, el resultado muestra que el router está en estado activo.

```

Router# show standby
Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Gratuitous ARP 14 sent, next in 7.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
  Tracking 2 objects, 0 up
    Down Interface Ethernet0/2, pri 15
    Down Interface Ethernet0/3
Group name is "HSRP1" (cfgd)
Follow by groups:
Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.666)
Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec

```

#### Capítulo 2: Redundancia de LAN 2.4.3.2 Verificación de GLBP

Aunque el HSRP y el VRRP proporcionan recuperabilidad a la puerta de enlace, para miembros de reserva del grupo de redundancia, el ancho de banda corriente arriba no se utiliza mientras el dispositivo se encuentra en modo de reserva.

Solo el router activo de los grupos HSRP y VRRP envía tráfico hacia la dirección MAC virtual. Los recursos que no se asocian con el router de reserva no se utilizan al máximo. Es posible lograr un equilibrio de carga con estos protocolos mediante la creación de varios grupos y la asignación de varias puertas de enlace predeterminadas, pero esta configuración genera una carga administrativa.

GLBP es una solución propia de Cisco que permite la selección automática y la utilización simultánea de varias puertas de enlace disponibles, además de la comutación por falla automática entre esas puertas de enlace. Como se muestra en la figura 1, varios routers comparten la carga de las tramas que, desde la perspectiva del cliente, se envían a una única dirección de gateway predeterminado.

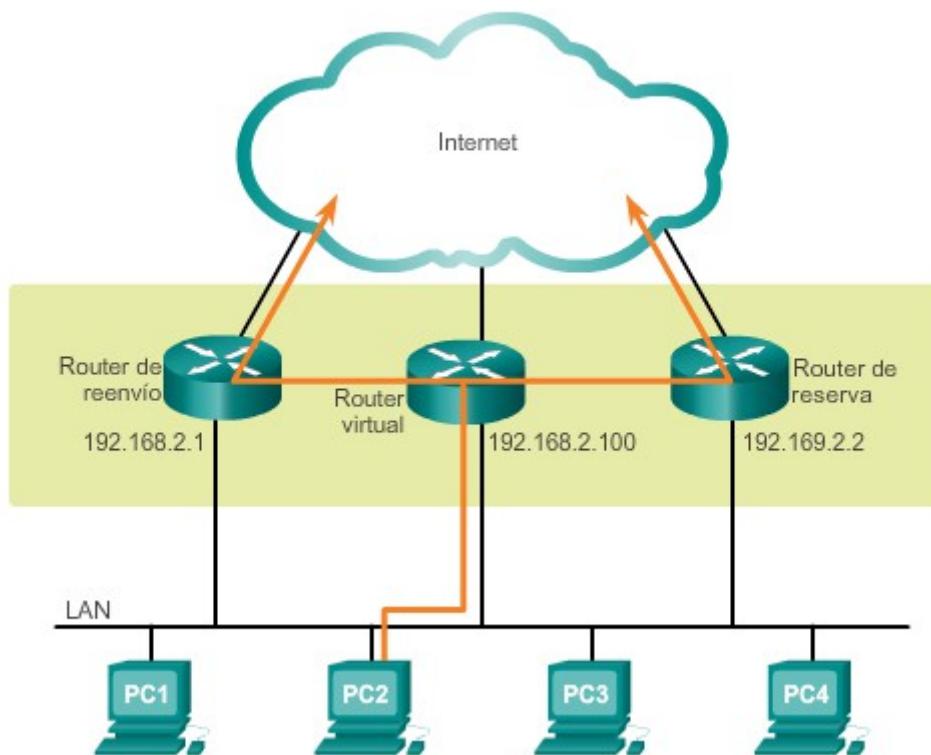
Con GLBP, podrán utilizar al máximo los recursos sin la carga administrativa de configurar varios grupos y administrar varias configuraciones de puerta de enlace predeterminadas. GLBP tiene las siguientes características:

- Permite el pleno uso de los recursos en todos los dispositivos, sin la carga administrativa de crear varios grupos.
- Proporciona una única dirección IP virtual y varias direcciones MAC virtuales.

- Enruta el tráfico al único gateway distribuido a través de los routers.
- Permite volver a enrutar de forma automática en caso de falla.

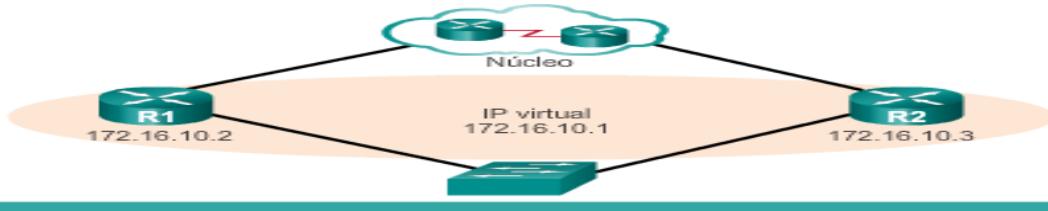
Utilice el comando **show glbp** para verificar el estado de GLBP. En la figura 2, se muestra que el grupo GLBP 1 está en estado activo con la dirección IP virtual 192.168.2.100.

#### Protocolo de equilibrio de carga de la puerta de enlace



```
Router# show glbp
FastEthernet0/1 - Group 1
  State is Active
    1 state change, last state change 00:02:34
  virtual IP address is 192.168.2.100
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.288 secs
  Redirect time 600 sec, forwarder timeout 14400 sec
  Preemption disabled
  Active is local
  Standby is 192.168.2.2, priority 100 (expires in 8.640 sec)
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    001e.7aa3.5e71 (192.168.2.1) local
    001e.7aa3.5f31 (192.168.2.2)
  There are 2 forwarders (1 active)
  Forwarder 1
    State is Active
      1 state change, last state change 00:02:23
      MAC address is 0007.b400.0101 (default)
      Owner ID is 001e.7aa3.5e71
      Redirection enabled
  Preemption enabled, min delay 30 sec
  Active is local, weighting 100
```

#### Capítulo 2: Redundancia de LAN 2.4.3.3 Verificador de sintaxis: HSRP y GLBP



El R2 se configuró para el grupo 10 de HSRP, con una prioridad de 110, la dirección IP 172.16.10.3 y la dirección IP virtual 172.16.10.1. Emita el comando "show running-config interface GigabitEthernet0/1" para ver la configuración de reserva en el R2.

```
R2# show running-config interface GigabitEthernet0/1
<resultado omitido>
interface GigabitEthernet0/1
 ip address 172.16.10.3 255.255.255.0
 standby 10 ip 172.16.10.1
 standby 10 priority 110
<resultado omitido>
```

Utilice el resultado del R2 como ejemplo para configurar el R1 como router HSRP activo con una prioridad de 150 y la dirección IP virtual 172.16.10.1.

Configurado actualmente en el R1:

```
R1(config)#interface GigabitEthernet0/1
R1(config)#ip address 172.16.10.2 255.255.255.0
R1(config)#no shutdown
R1(config-if)# standby 10 ip 172.16.10.1
R1(config-if)# standby 10 priority 150
%HSRP-6-STATECHANGE: GigabitEthernet0/0 Grp 10 state Speak -> Standby
```

Vuelva al modo EXEC privilegiado y muestre el estado de reserva resumido.

```
R1(config-if)# end
R1# show standby brief
          P indicates configured to preempt. !
Interface Grp Pri P State Active Standby Virtual IP
Gi0/1 10 150 Active local 172.16.10.3 172.16.10.1
```

La empresa decidió implementar GLBP en lugar de HSRP. Se eliminó toda la configuración HSRP.

El R2 se configuró para el grupo 10 de GLBP, con una prioridad de 110, la dirección IP 172.16.10.3 y la dirección IP virtual 172.16.10.1. Emita el comando "show running-config interface GigabitEthernet0/1" para ver la configuración GLBP en el R2.

```
R2# show running-config interface GigabitEthernet0/1
<resultado omitido>
interface GigabitEthernet0/1
 ip address 172.16.10.3 255.255.255.0
 glbp 10 ip 172.16.10.1
 glbp 10 priority 110
<resultado omitido>
```

Utilice el resultado del R2 como ejemplo para configurar GLBP en el R1 con una prioridad de 150 y la dirección IP virtual 172.16.10.1.

Configurado actualmente en el R1:

```
R1(config)#interface GigabitEthernet0/1
R1(config)#ip address 172.16.10.2 255.255.255.0
R1(config)#no shutdown
R1(config-if)# glbp 10 ip 172.16.10.1
R1(config-if)# glbp 10 priority 150
*Jun 16 19:26:45.871: %GLBP-6-FWDSTATECHANGE: GigabitEthernet0/0
Grp 10 Fwd 1 state Listen -> Active
```

Vuelva al modo EXEC privilegiado y muestre el estado de GLBP sin ningún parámetro.

```
R1(config-if)# end
R1# show glbp
GigabitEthernet0/0 - Group 10
  State is Active
    1 state change, last state change 00:03:05
    virtual IP address is 172.16.10.1
    Hello time 3 sec, hold time 10 sec
      Next hello sent in 1.792 secs
    Redirect time 600 sec, forwarder timeout 14400 sec
    Preemption disabled
    Active is local
    Standby is 172.16.10.3, priority 100 (expires in 9.024 sec)
    Priority 150 (configured)
    Weighting 100 (default 100), thresholds: lower 1, upper 100
    Load balancing: round-robin
    Group members:
      0006.f671.db58 (172.16.10.2) local
      0006.f671.eb38 (172.16.10.3)
    There are 2 forwarders (1 active)
    Forwarder 1
      State is Active
        1 state change, last state change 00:02:53
        MAC address is 0007.b400.0a01 (default)
        Owner ID is 0006.f671.db58
        Redirection enabled
        Preemption enabled, min delay 30 sec
        Active is local, weighting 100
    Forwarder 2
      State is Listen
        MAC address is 0007.b400.0a02 (learnt)
        Owner ID is 0006.f671.eb38
        Redirection enabled, 599.040 sec remaining (maximum 600 sec)
        Time to live: 14399.040 sec (maximum 14400 sec)
        Preemption enabled, min delay 30 sec
        Active is 172.16.10.3 (primary), weighting 100 (expires in 9.312 sec)
```

Configuró correctamente HSRP y GLBP.

## Capítulo 2: Redundancia de LAN 2.4.3.4 Práctica de laboratorio: Configuración de HSRP y

### GLBP

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y verificar la conectividad
- Parte 2: Configurar la redundancia de primer salto mediante HSRP
- Parte 3: Configurar la redundancia de primer salto mediante GLBP

## [Práctica de laboratorio: Configuración de HSRP y GLBP](#)

## Capítulo 2: Redundancia de LAN 2.5.1.1 Actividad de clase: Árbol de documentación

### **Árbol de documentación**

Los empleados de su edificio tienen problemas para acceder a un servidor web en la red. Usted busca la documentación de red que utilizó el ingeniero de red anterior antes de cambiar de trabajo. Sin embargo, no encuentra ningún tipo de documentación de red.

Por lo tanto, decide crear su propio sistema de registro de red. Decide comenzar por la capa de acceso de la jerarquía de la red. Aquí es donde se ubican los switches redundantes, así como los servidores, las impresoras y los hosts locales de la empresa.

Crea una matriz para registrar la documentación e incluye switches de capa de acceso en la lista. Además, decide registrar los nombres de los switches, los puertos en uso, las conexiones de cableado, los puertos raíz, los puertos designados y los puertos alternativos.

## [Actividad de clase: Árbol de documentación](#)

## Capítulo 2: Redundancia de LAN 2.5.1.2 Resumen

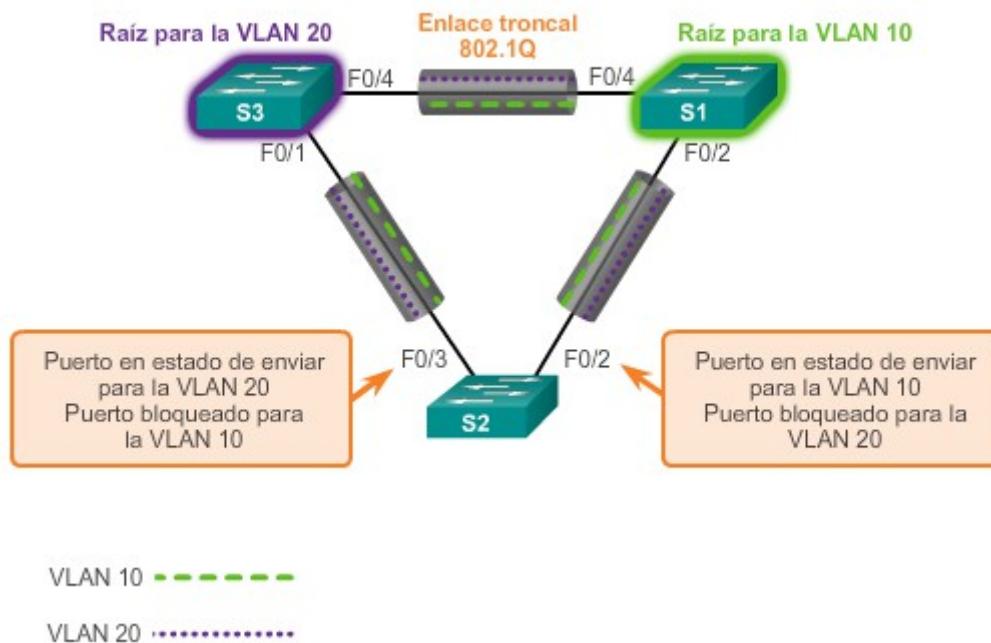
Los problemas que pueden surgir de una red de capa 2 redundante incluyen las tormentas de difusión, la inestabilidad de la base de datos MAC y la duplicación de tramas unidifusión. STP es un protocolo de capa 2 que asegura que exista solo una ruta lógica entre todos los destinos en la red mediante el bloqueo intencional de las rutas redundantes que pueden provocar un bucle.

STP envía tramas BPDU para la comunicación entre los switches. Se elige un switch como puente raíz para cada instancia de árbol de expansión. Los administradores pueden controlar esta elección cambiando la prioridad del puente. Los puentes raíz se pueden configurar para habilitar el balanceo de carga del árbol de expansión por VLAN o por grupo de VLAN, según el protocolo de árbol de expansión que se utilice. Después, STP asigna una función de puerto a cada puerto participante mediante un costo de ruta. El costo de la ruta es igual a la suma de todos los costos de puerto a lo largo de la ruta hacia el puente raíz. Se asigna un costo de puerto automáticamente a cada puerto. Sin embargo, también se puede configurar de forma

manual. Las rutas con el costo más bajo se convierten en las preferidas, y el resto de las rutas redundantes se bloquean.

PVST+ es la configuración predeterminada de IEEE 802.1D en los switches Cisco. Ejecuta una instancia de STP para cada VLAN. RSTP, un protocolo de árbol de expansión más moderno y de convergencia más rápida, se puede implementar en los switches Cisco por VLAN en forma de PVST+ rápido. El árbol de expansión múltiple (MST) es la implementación de Cisco del protocolo de árbol de expansión múltiple (MSTP), en la que se ejecuta una instancia de árbol de expansión para un grupo definido de VLAN. Las características como PortFast y la protección BPDU aseguran que los hosts del entorno comutado obtengan acceso inmediato a la red sin interferir en el funcionamiento del árbol de expansión.

Los protocolos de redundancia de primer salto, como HSRP, VRRP y GLBP, proporcionan gateways predeterminados alternativos a los hosts en un entorno de router redundante o comutado multicapa. Varios routers comparten una dirección IP y una dirección MAC virtuales que se utilizan como gateway predeterminado en un cliente. Esto asegura que los hosts mantengan la conectividad en caso de falla de un dispositivo que funciona como gateway predeterminado para una VLAN o un grupo de VLAN. Cuando se utiliza HSRP o VRRP, un router está en estado activo o de reenvío para un grupo en particular, mientras que los demás están en modo de reserva. GLBP permite el uso simultáneo de varios gateways, además de proporcionar la comutación por falla automática.



### Capítulo 3: Agregación de enlaces 3.0.1.1 Introducción

La agregación de enlaces es la capacidad de crear un único enlace lógico mediante varios enlaces físicos entre dos dispositivos. Esto permite compartir la carga entre los enlaces físicos, en lugar de hacer que STP bloquee uno o más enlaces. EtherChannel es una forma de agregación de enlaces que se usa en las redes comutadas.

En este capítulo, se describen EtherChannel y los métodos que se usan para crear un EtherChannel. Un EtherChannel se puede configurar de forma manual o se puede negociar mediante el protocolo de agregación de puertos (PAgP), exclusivo de Cisco, o el protocolo de control de agregación de enlaces (LACP), definido en IEEE 802.3ad. Se analizan la configuración, la verificación y la resolución de problemas de EtherChannel.

**Al completar este capítulo, usted podrá:**

- Describir la agregación de enlaces.
- Describir la tecnología EtherChannel.
- Configurar la agregación de enlaces con EtherChannel.
- Resolver los problemas de la agregación de enlaces con EtherChannel.

[Capítulo 3: Agregación de enlaces 3.0.1.2 Actividad de clase: Imagine esto](#)

**Imagine esto**

El día laborable terminó. En su pequeña a mediana empresa, intenta explicar a los ingenieros de red acerca de EtherChannel y cómo se ve cuando está configurado físicamente. Los ingenieros de red tienen dificultades para imaginar cómo se pueden conectar dos switches mediante varios enlaces que actúen colectivamente como un único canal o una única conexión. Definitivamente está en los planes de la empresa implementar una red EtherChannel.

Por lo tanto, concluye la reunión con una tarea para los ingenieros. A fin de prepararse para la reunión del día siguiente, los ingenieros deben investigar y traer a la reunión una representación gráfica de una conexión de red EtherChannel. Se les asigna la tarea de explicar a los otros ingenieros cómo funciona una red EtherChannel.

Cuando se investiga EtherChannel, una buena pregunta para buscar es “¿Qué aspecto tiene EtherChannel?”. Prepare algunas diapositivas que demuestren su investigación para presentar al grupo de ingenieros de red. En estas diapositivas, se debe proporcionar una comprensión sólida de cómo se crea físicamente EtherChannel dentro de la topología de una red. Su objetivo es asegurarse de que todos los que salgan de la próxima reunión comprendan bien por qué es recomendable cambiar la topología de la red por la opción de EtherChannel.

[Actividad de clase: Imagine esto](#)

[Capítulo 3: Agregación de enlaces 3.1.1.1 Introducción a la agregación de enlaces](#)

En la ilustración, el tráfico proveniente de varios enlaces (normalmente, 100 Mb/s o 1000 Mb/s) se agrega en el switch de acceso y se debe enviar a los switches de distribución. Debido a la agregación de tráfico, debe haber enlaces con un ancho de banda superior entre los switches de acceso y de distribución.

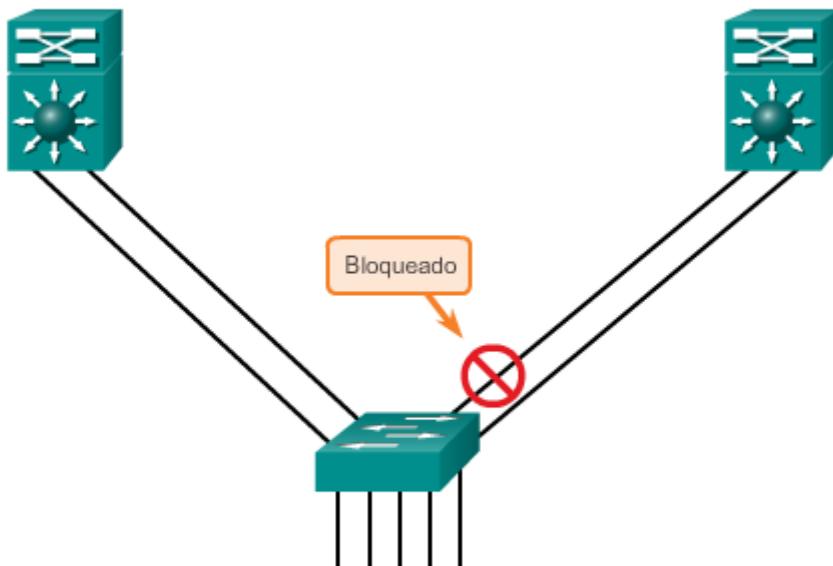
Tal vez sea posible usar enlaces más rápidos (por ejemplo, de 10 Gb/s) en el enlace agregado entre los switches de capa de acceso y de distribución. Sin embargo, agregar enlaces más

rápidos es costoso. Además, como la velocidad aumenta en los enlaces de acceso, ni siquiera el puerto más rápido posible en el enlace agregado es lo suficientemente rápido para agregar el tráfico proveniente de todos los enlaces de acceso.

También es posible multiplicar la cantidad de enlaces físicos entre los switches para aumentar la velocidad general de la comunicación switch a switch. Sin embargo, STP está habilitado de manera predeterminada en los dispositivos de switch. STP bloquea los enlaces redundantes para evitar los bucles de routing.

Por estos motivos, la mejor solución es implementar una configuración de EtherChannel.

### Enlaces redundantes con STP



De manera predeterminada, STP bloquea los enlaces redundantes.

### Capítulo 3: Agregación de enlaces 3.1.1.2 Ventajas de EtherChannel

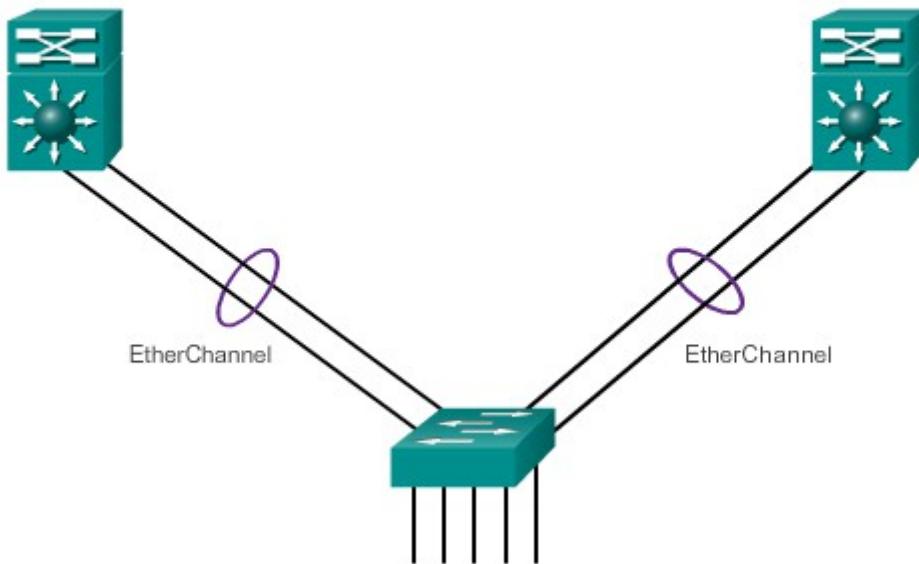
En los inicios, Cisco desarrolló la tecnología EtherChannel como una técnica switch a switch LAN para agrupar varios puertos Fast Ethernet o Gigabit Ethernet en un único canal lógico. Cuando se configura un EtherChannel, la interfaz virtual resultante se denomina “canal de puertos”. Las interfaces físicas se agrupan en una interfaz de canal de puertos.

La tecnología EtherChannel tiene muchas ventajas:

- La mayoría de las tareas de configuración se pueden realizar en la interfaz EtherChannel en lugar de en cada puerto individual, lo que asegura la coherencia de configuración en todos los enlaces.

- El EtherChannel depende de los puertos de switch existentes. No es necesario actualizar el enlace a una conexión más rápida y más costosa para tener más ancho de banda.
- El balanceo de carga ocurre entre los enlaces que forman parte del mismo EtherChannel. Según la plataforma de hardware, se pueden implementar uno o más métodos de balanceo de carga. Estos métodos incluyen balanceo de carga de la MAC de origen a la MAC de destino o balanceo de carga de la IP de origen a la IP de destino, a través de enlaces físicos.
- EtherChannel crea una agregación que se ve como un único enlace lógico. Cuando existen varios grupos EtherChannel entre dos switches, STP puede bloquear uno de los grupos para evitar los bucles de switching. Cuando STP bloquea uno de los enlaces redundantes, bloquea el EtherChannel completo. Esto bloquea todos los puertos que pertenecen a ese enlace EtherChannel. Donde solo existe un único enlace EtherChannel, todos los enlaces físicos en el EtherChannel están activos, ya que STP solo ve un único enlace (lógico).
- EtherChannel proporciona redundancia, ya que el enlace general se ve como una única conexión lógica. Además, la pérdida de un enlace físico dentro del canal no crea ningún cambio en la topología, por lo que no es necesario volver a calcular el árbol de expansión. Suponiendo que haya por lo menos un enlace físico presente, el EtherChannel permanece en funcionamiento, incluso si su rendimiento general disminuye debido a la pérdida de un enlace dentro del EtherChannel.

#### Ventajas de EtherChannel



EtherChannel se puede implementar al agrupar varios puertos físicos en uno o más enlaces EtherChannel lógicos.

**Nota:** no se pueden mezclar los tipos de interfaz; por ejemplo, no se pueden mezclar Fast Ethernet y Gigabit Ethernet dentro de un único EtherChannel.

El EtherChannel proporciona un ancho de banda full-duplex de hasta 800 Mb/s (Fast EtherChannel) u 8 Gb/s (Gigabit EtherChannel) entre un switch y otro switch o host. En la actualidad, cada EtherChannel puede constar de hasta ocho puertos Ethernet configurados de manera compatible. El switch con IOS de Cisco actualmente puede admitir seis EtherChannels. Sin embargo, a medida que se desarrollan nuevos IOS y cambian las plataformas, algunas tarjetas y plataformas pueden admitir una mayor cantidad de puertos dentro de un enlace EtherChannel, así como una mayor cantidad de Gigabit EtherChannels. El concepto es el mismo, independientemente de las velocidades o la cantidad de enlaces que estén involucrados. Cuando se configure EtherChannel en los switches, tenga en cuenta los límites y las especificaciones de la plataforma de hardware.

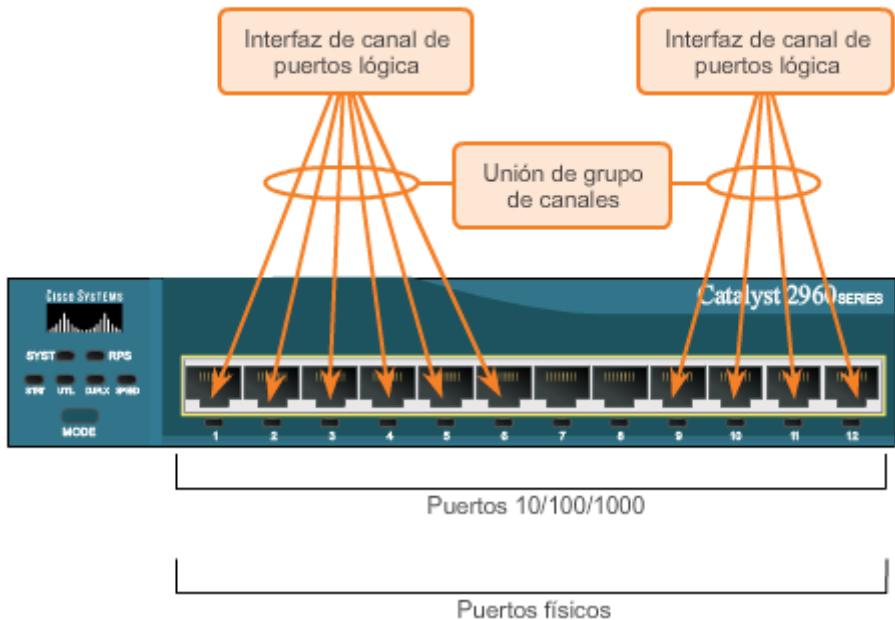
El propósito original de EtherChannel es aumentar la capacidad de velocidad en los enlaces agregados entre los switches. Sin embargo, el concepto se extendió a medida que la tecnología EtherChannel adquirió más popularidad, y ahora muchos servidores también admiten la agregación de enlaces con EtherChannel. EtherChannel crea una relación de uno a uno, es decir, un enlace EtherChannel conecta solo dos dispositivos. Se puede crear un enlace EtherChannel entre dos switches o entre un servidor con EtherChannel habilitado y un switch. Sin embargo, no se puede enviar el tráfico a dos switches diferentes a través del mismo enlace EtherChannel.

La configuración de los puertos individuales que forman parte del grupo EtherChannel debe ser coherente en ambos dispositivos. Si los puertos físicos de un lado se configuran como enlaces troncales, los puertos físicos del otro lado también se deben configurar como enlaces troncales dentro de la misma VLAN nativa. Además, todos los puertos en cada enlace EtherChannel se deben configurar como puertos de capa 2.

**Nota:** los EtherChannels de capa 3 se pueden configurar en los switches multicapa Cisco Catalyst, como el Catalyst 3560, pero estos no se exploran en este curso. Un EtherChannel de capa 3 tiene una única dirección IP asociada a la agregación lógica de los puertos de switch en el EtherChannel.

Cada EtherChannel tiene una interfaz de canal de puertos lógica, como se muestra en la ilustración. La configuración aplicada a la interfaz de canal de puertos afecta a todas las interfaces físicas que se asignan a esa interfaz.

## Restricciones de implementación



### Capítulo 3: Agregación de enlaces 3.1.2.2 Protocolo de agregación de puertos

Los EtherChannels se pueden formar por medio de una negociación con uno de dos protocolos: PAgP o LACP. Estos protocolos permiten que los puertos con características similares formen un canal mediante una negociación dinámica con los switches adyacentes.

**Nota:** también es posible configurar un EtherChannel estático o incondicional sin PAgP o LACP.

#### PAgP

PAgP es un protocolo exclusivo de Cisco que ayuda en la creación automática de enlaces EtherChannel. Cuando se configura un enlace EtherChannel mediante PAgP, se envían paquetes PAgP entre los puertos aptos para EtherChannel para negociar la formación de un canal. Cuando PAgP identifica enlaces Ethernet compatibles, agrupa los enlaces en un EtherChannel. El EtherChannel después se agrega al árbol de expansión como un único puerto.

Cuando se habilita, PAgP también administra el EtherChannel. Los paquetes PAgP se envían cada 30 segundos. PAgP revisa la coherencia de la configuración y administra los enlaces que se agregan, así como las fallas entre dos switches. Cuando se crea un EtherChannel, asegura que todos los puertos tengan el mismo tipo de configuración.

**Nota:** en EtherChannel, es obligatorio que todos los puertos tengan la misma velocidad, la misma configuración de dúplex y la misma información de VLAN. Cualquier modificación de los puertos después de la creación del canal también modifica a los demás puertos del canal.

PAgP ayuda a crear el enlace EtherChannel al detectar la configuración de cada lado y asegurarse de que los enlaces sean compatibles, de modo que se pueda habilitar el enlace EtherChannel cuando sea necesario. En la ilustración, se muestran los modos para PAgP.

- **Encendido:** este modo obliga a la interfaz a proporcionar un canal sin PAgP. Las interfaces configuradas en el modo encendido no intercambian paquetes PAgP.
- **PAgP deseado:** este modo PAgP coloca una interfaz en un estado de negociación activa en el que la interfaz inicia negociaciones con otras interfaces al enviar paquetes PAgP.
- **PAgP automático:** este modo PAgP coloca una interfaz en un estado de negociación pasiva en el que la interfaz responde a los paquetes PAgP que recibe, pero no inicia la negociación PAgP.

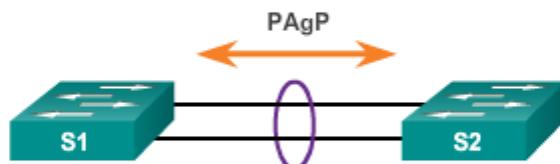
Los modos deben ser compatibles en cada lado. Si se configura un lado en modo automático, se lo coloca en estado pasivo, a la espera de que el otro lado inicie la negociación del EtherChannel. Si el otro lado se establece en modo automático, la negociación nunca se inicia y no se forma el canal EtherChannel. Si se deshabilitan todos los modos mediante el comando **no** o si no se configura ningún modo, entonces se deshabilita el EtherChannel.

El modo encendido coloca manualmente la interfaz en un EtherChannel, sin ninguna negociación. Funciona solo si el otro lado también se establece en modo encendido. Si el otro lado se establece para negociar los parámetros a través de PAgP, no se forma ningún EtherChannel, ya que el lado que se establece en modo encendido no negocia.

### Protocolo de agregación de puertos

#### Modos PAgP:

- **On (Encendido):** miembro del canal sin negociación (sin protocolo).
- **Deseado:** pregunta activamente si el otro lado puede participar va a hacerlo.
- **Automático:** espera pasivamente al otro lado.



S1	S2	Establecimiento de canales
On	On	Sí
Automático/deseado	Deseable	Sí
Encendido/automático/deseado	Sin configurar	No
On	Deseable	No
Automático/encendido	Automático	No

### Capítulo 3: Agregación de enlaces 3.1.2.3 Protocolo de control de agregación de enlaces

#### **Protocolo de control de agregación de enlaces (LACP)**

LACP forma parte de una especificación IEEE (802.3ad) que permite agrupar varios puertos físicos para formar un único canal lógico. LACP permite que un switch negocie un grupo automático mediante el envío de paquetes LACP al peer. Realiza una función similar a PAgP con EtherChannel de Cisco. Debido a que LACP es un estándar IEEE, se puede usar para facilitar los EtherChannels en entornos de varios proveedores. En los dispositivos de Cisco, se admiten ambos protocolos.

**Nota:** en los inicios, LACP se definió como IEEE 802.3ad. Sin embargo, LACP ahora se define en el estándar más moderno IEEE 802.1AX para la redes de área local y metropolitana.

LACP proporciona los mismos beneficios de negociación que PAgP. LACP ayuda a crear el enlace EtherChannel al detectar la configuración de cada lado y al asegurarse de que sean compatibles, de modo que se pueda habilitar el enlace EtherChannel cuando sea necesario. En la ilustración, se muestran los modos para LACP.

- **Encendido:** este modo obliga a la interfaz a proporcionar un canal sin LACP. Las interfaces configuradas en el modo encendido no intercambian paquetes LACP.
- **LACP activo:** este modo LACP coloca un puerto en estado de negociación activa. En este estado, el puerto inicia negociaciones con otros puertos mediante el envío de paquetes LACP.
- **LACP pasivo:** este modo LACP coloca un puerto en estado de negociación pasiva. En este estado, el puerto responde a los paquetes LACP que recibe, pero no inicia la negociación de paquetes LACP.

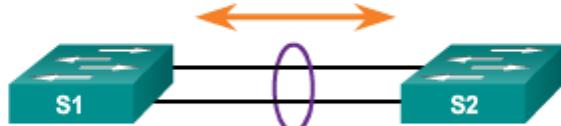
Al igual que con PAgP, los modos deben ser compatibles en ambos lados para que se forme el enlace EtherChannel. Se repite el modo encendido, ya que crea la configuración de EtherChannel incondicionalmente, sin la negociación dinámica de PAgP o LACP.

## Protocolo de control de agregación de enlaces

### Modos LACP:

- **On (Encendido):** miembro del canal sin negociación (sin protocolo).
- **Activo:** pregunta activamente si el otro lado puede participar o va a hacerlo.
- **Pasivo:** espera pasivamente al otro lado.

Protocolo de control de agregación de enlaces (LACP)



S1	S2	Establecimiento de canales
On	On	Sí
Activo/pasivo	Activo	Sí
Encendido/activo/pasivo	Sin configurar	No
On	Activo	No
Pasivo/encendido	Pasiva	No

### Capítulo 3: Agregación de enlaces 3.1.2.4 Actividad: Identificar los modos PAgP y LACP

Actividad (parte 1): Unir los términos relacionados con la negociación PAgP y LACP con la descripción

Arrastre los términos relacionados con la negociación de interfaces PAgP y LACP hasta las descripciones correspondientes en la tabla. Haga clic en el botón 2 para continuar la actividad.

Término	Descripción de los términos relacionados con la negociación PAgP y LACP
Automático	Coloca la interfaz en un estado de respuesta pasivo. No inicia negociaciones PAgP.
Activo	Inicia las negociaciones LACP con otras interfaces.
Deseable	Inicia activamente las negociaciones PAgP con otras interfaces.
On	Fuerza un estado EtherChannel sin iniciar negociaciones PAgP o LACP.
Pasiva	Coloca la interfaz en un estado de respuesta pasivo. No inicia negociaciones LACP.

#### Actividad (parte 2): Identificar los modos PAgP

Revise la topología y después compare los modos de negociación PAgP del Switch 1 y el Switch 2 en la tabla. Determine si se establecería un EtherChannel. Arrastre las etiquetas "Sí" o "No" hasta los campos proporcionados. Haga clic en el botón 3 para continuar la actividad.

Modo de switch 1	Modo de switch 2	¿Se estableció un EtherChannel?
Deseable	Deseable	Sí ✓
Automático	Automático	No ✓
On	Sin configurar	No ✓
Automático	Deseable	Sí ✓
On	Deseable	No ✓

#### Actividad (parte 3): Identificar los modos LACP

Revise la topología y después compare los modos de negociación LACP del Switch 1 y el Switch 2 en la tabla. Determine si se establecería un EtherChannel. Arrastre las etiquetas "Sí" o "No" hasta los campos proporcionados.

Modo de switch 1	Modo de switch 2	¿Se estableció un EtherChannel?
Pasiva	On	No ✓
On	Activo	No ✓
On	On	Sí ✓
Pasiva	Activo	Sí ✓
Pasiva	Pasiva	No ✓

### Capítulo 3: Agregación de enlaces 3.2.1.1 Pautas para la configuración

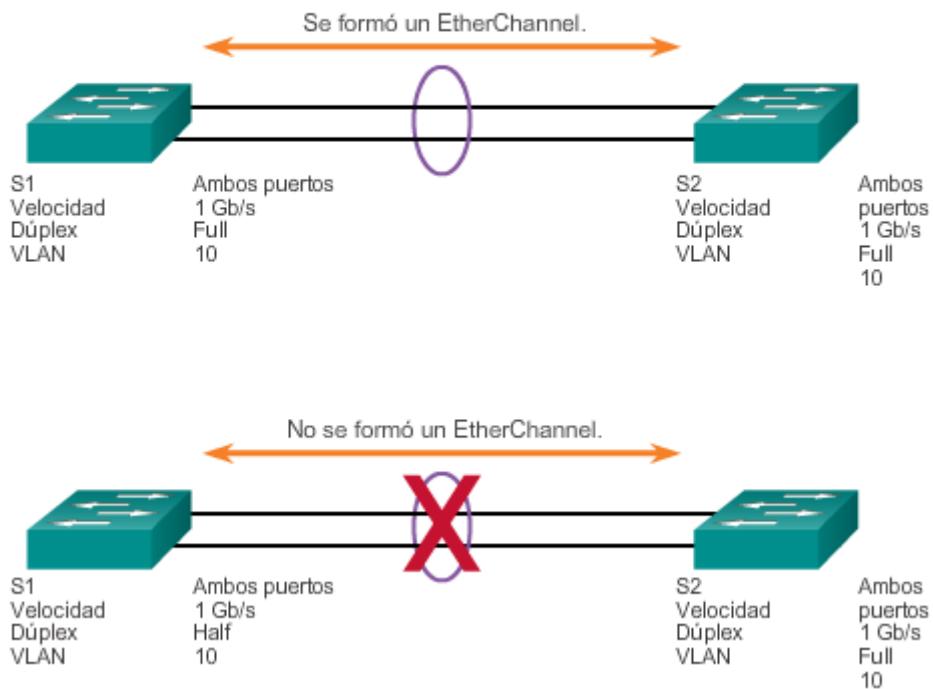
Las siguientes pautas y restricciones son útiles para configurar EtherChannel:

- **Soporte de EtherChannel:** todas las interfaces Ethernet en todos los módulos deben admitir EtherChannel, sin necesidad de que las interfaces sean físicamente contiguas o estén en el mismo módulo.
- **Velocidad y dúplex:** configure todas las interfaces en un EtherChannel para que funcionen a la misma velocidad y en el mismo modo dúplex, como se muestra en la ilustración.
- **Coincidencia de VLAN:** todas las interfaces en el grupo EtherChannel se deben asignar a la misma VLAN o se deben configurar como enlace troncal, lo que también se muestra en la ilustración.
- **Rango de VLAN:** un EtherChannel admite el mismo rango permitido de VLAN en todas las interfaces de un EtherChannel de enlace troncal. Si el rango permitido de VLAN no es

el mismo, las interfaces no forman un EtherChannel, incluso si se establecen en modo **automático** o deseado.

Si se deben modificar estos parámetros, configúrelos en el modo de configuración de interfaz de canal de puertos. Después de configurar la interfaz de canal de puertos, cualquier configuración que se aplique a esta interfaz también afecta a las interfaces individuales. Sin embargo, las configuraciones que se aplican a las interfaces individuales no afectan a la interfaz de canal de puertos. Por ello, realizar cambios de configuración a una interfaz que forma parte de un enlace EtherChannel puede causar problemas de compatibilidad de interfaces.

### Pautas de configuración de EtherChannel



### Capítulo 3: Agregación de enlaces 3.2.1.2 Configuración de interfaces

La configuración de EtherChannel con LACP se realiza en dos pasos:

**Paso 1.** Especifique las interfaces que componen el grupo EtherChannel mediante el comando **interface range interface** del modo de configuración global. La palabra clave **range** le permite seleccionar varias interfaces y configurarlas a la vez. Se recomienda comenzar desactivando esas interfaces, de modo que ninguna configuración incompleta cree actividad en el enlace.

**Paso 2.** Cree la interfaz de canal de puertos con el comando **channel-group identifier mode active** en el modo de configuración de rango de interfaces. El identificador especifica el número del grupo del canal. Las palabras clave **mode active** identifican a esta configuración como EtherChannel LACP.

**Nota:** EtherChannel está deshabilitado de manera predeterminada.

En la figura 1, FastEthernet0/1 y FastEthernet0/2 se agrupan en el canal de puertos de interfaz EtherChannel 1.

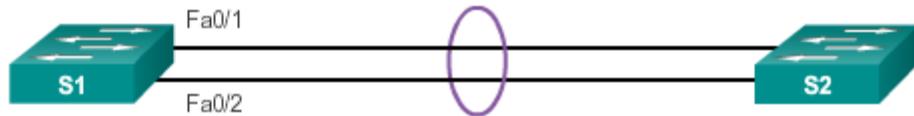
Para cambiar la configuración de capa 2 en la interfaz de canal de puertos, ingrese al modo de configuración de interfaz de canal de puertos mediante el comando `interface port-channel`, seguido del identificador de la interfaz. En el ejemplo, el EtherChannel está configurado como interfaz de enlace troncal con VLAN permitidas específicas. En la figura 1, también se muestra que el canal de puertos de interfaz 1 está configurado como enlace troncal con las VLAN permitidas 1, 2 y 20.

Utilice el verificador de sintaxis de la figura 2 para configurar EtherChannel en el switch S1.

#### Configuración de EtherChannel con LACP

```
S1(config)# interface range FastEthernet0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

Crea el EtherChannel y configura el enlace troncal.



## Configuración de EtherChannel

**Ingrese al modo interface range para FastEthernet0/1 y FastEthernet0/2. Muestre las opciones del grupo de canales mediante la ayuda contextual (?).**

```
S1(config)# interface range FastEthernet0/1 - 2  
S1(config-if-range)# channel-group ?  
<1-6> Channel group number
```

**Seleccione channel-group 1 y muestre la siguiente opción.**

```
S1(config-if-range)# channel-group 1 ?  
mode Etherchannel Mode of the interface
```

**Introduzca la palabra clave mode y muestre la siguiente opción.**

```
S1(config-if-range)# channel-group 1 mode ?  
active Enable LACP unconditionally  
auto Enable PAgP only if a PAgP device is detected  
desirable Enable PAgP unconditionally  
on Enable Etherchannel only  
passive Enable LACP only if a LACP device is detected
```

**Configure el grupo de canales para que use LACP incondicionalmente.**

```
S1(config-if-range)# channel-group 1 mode active  
S1(config-if-range)#
*Mar 21 00:02:28.184: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state
to down
*Mar 21 00:02:28.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/2, changed state
to down
*Mar 21 00:02:36.179: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state
to up
*Mar 21 00:02:36.674: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/2, changed state
to up
S1(config-if-range)#
*Mar 21 00:04:31.170: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state
to down
*Mar 21 00:04:31.186: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/2, changed state
to down
*Mar 21 00:04:33.116: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/1, changed state
to up
*Mar 21 00:04:34.114: %LINK-3-UPDOWN: Interface Port-channel1,
changed state to up
*Mar 21 00:04:35.037: %LINEPROTO-5-UPDOWN: Line protocol on
Interface FastEthernet0/2, changed state
to up
*Mar 21 00:04:35.121: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Port-channel1, changed state to
up
```

**Configure los parámetros de switchport para el canal de puertos que se creó. Configure port-channel 1 como enlace troncal y permita que las VLAN 1, 2 y 20 crucen el enlace troncal.**

```
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
Configuró correctamente EtherChannel.
```

### Capítulo 3: Agregación de enlaces 3.2.1.3 Packet Tracer: configuración de EtherChannel

#### **Información básica/situación**

Se acaban de instalar tres switches. Entre los switches, hay uplinks redundantes. Por lo general, se puede utilizar solo uno de estos enlaces; de lo contrario, se podría originar un bucle de puente. Sin embargo, si se usa un solo enlace, se utiliza solo la mitad del ancho de banda disponible. EtherChannel permite agrupar hasta ocho enlaces redundantes en un único enlace lógico. En esta práctica de laboratorio, configurará el protocolo de agregación de puertos (PAgP), que es un protocolo de EtherChannel de Cisco, y el protocolo de control de agregación de enlaces (LACP), una versión de estándar abierto IEEE 802.3ad de EtherChannel.

[Packet Tracer: Configuración de EtherChannel \(instrucciones\)](#)

[Packet Tracer: Configuración de EtherChannel \(PKA\)](#)

### Capítulo 3: Agregación de enlaces 3.2.1.4 Práctica de laboratorio: configuración de EtherChannel

#### EtherChannel

#### **En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: Configurar los parámetros básicos del switch
- Parte 2: configurar PAgP
- Parte 3: configurar LACP

[Práctica de laboratorio: configuración de EtherChannel](#)

### Capítulo 3: Agregación de enlaces 3.2.2.1 Verificación de EtherChannel

Existe una variedad de comandos para verificar una configuración EtherChannel. Primero, el comando **show interface port-channel** muestra el estado general de la interfaz de canal de puertos. En la figura 1, la interfaz de canal de puertos 1 está activa.

Cuando se configuren varias interfaces de canal de puertos en el mismo dispositivo, use el comando **show etherchannel summary** para mostrar una única línea de información por canal de puertos. En la figura 2, el switch tiene configurado un EtherChannel; el grupo 1 usa LACP.

El grupo de interfaces consta de las interfaces FastEthernet0/1 y FastEthernet0/2. El grupo es un EtherChannel de capa 2 y está en uso, según lo indican las letras SU junto al número de canal de puertos.

Use el comando **show etherchannel port-channel** para mostrar la información sobre una interfaz de canal de puertos específica, como se muestra en la figura 3. En el ejemplo, la interfaz de canal de puertos 1 consta de dos interfaces físicas, FastEthernet0/1 y FastEthernet0/2. Esta usa LACP en modo activo. Está correctamente conectada a otro switch

con una configuración compatible, razón por la cual se dice que el canal de puertos está en uso.

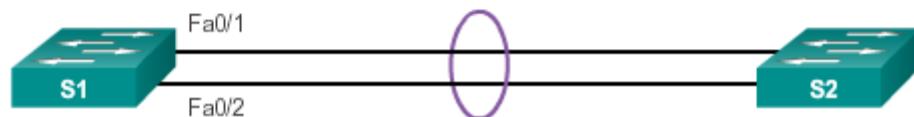
En cualquier miembro de una interfaz física de un grupo EtherChannel, el comando **show interfaces etherchannel** puede proporcionar información sobre la función de la interfaz en el EtherChannel, como se muestra en la figura 4. La interfaz FastEthernet0/1 forma parte del grupo EtherChannel 1. El protocolo para este EtherChannel es LACP.

Utilice el verificador de sintaxis de la figura 5 para verificar EtherChannel en el switch S1.

#### Verificación de EtherChannel

```
S1# show interface port-channel1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0cd9.96e8.8a02 (bia
  0cd9.96e8.8a02)
    MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
<resultado omitido>
```

Verifica el estado de la interfaz.



## Verificación de EtherChannel

```
Si# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use       f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1 (SU)     LACP        Fa0/1(P)   Fa0/2(P)
```

Muestra un resumen de una línea por cada grupo de canales.

## Verificación de EtherChannel

```
Si# show etherchannel port-channel
Channel-group listing:
-----
Group: 1
-----
Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 0d:06h:23m:49s
Logical slot/port = 2/1          Number of ports = 2
HotStandBy port = null
Port state           = Port-channel Ag-Inuse
Protocol            = LACP
Port security        = Disabled
-----
Ports in the Port-channel:
Index  Load  Port    EC state      No of bits
```

Muestra la información del canal de puertos.

## Verificación de EtherChannel

```
S1# show interfaces f0/1 etherchannel
Port state = Up Mstr Assoc In-Bndl
Channel group = 1 Mode = Active Gcchange = -
Port-channel = Po1 GC = - Pseudo port-
Port index = 0 Load = 0x00 Protocol =
Flags: S - Device is sending Slow LACPDU F - Device is sending
       A - Device is in active mode. P - Device is in pass
Local information:
          LACP port Admin Oper Port
Port   Flags State Priority Key Key Num
Fa0/1 SA     bndl    32768  0x1   0x1   0x1
Partner's information:
          LACP port Admin Oper
Port   Flags Priority Dev ID Age key Key
Fa0/1 SA     32768   0cd9.96d2.4000 13s 0x0   0x1
Age of the port in the current state: 0d:06h:06m:51s
```

Muestra la función de una interfaz específica en un EtherChannel.

**Muestre el estado de la interfaz port-channel1.**

```
S1# show interface Port-channel1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0cd9.96e8.8a01 (bia
  0cd9.96e8.8a01)
    MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full-duplex, 100Mb/s, link type is auto, media type is unknown
    input flow-control is off, output flow-control is unsupported
    Members in this channel: Fa0/1 Fa0/2
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 00:00:00, output 00:04:21, 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 2000 bits/sec, 2 packets/sec
    5 minute output rate 1000 bits/sec, 1 packets/sec
      799 packets input, 89672 bytes, 0 no buffer
      Received 689 broadcasts (585 multicasts)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 585 multicast, 0 pause input
      0 input packets with dribble condition detected
      352 packets output, 46085 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      0 unknown protocol drops
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier, 0 pause output
      0 output buffer failures, 0 output buffers swapped out
```

**Muestre el resumen de los EtherChannels configurados.**

```
S1# show etherchannel summary
Flags: D - down P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      U - in use   f - failed to allocate aggregator
      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
```

Number of channel-groups in use: 1  
 Number of aggregators: 1

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	LACP	Fa0/1 (P) Fa0/2 (P)

**Muestre la información del canal de puertos para el EtherChannel.**

```
S1# show etherchannel Port-channel
  channel-group listing:
  -----
  Group: 1
  -----
    Port-channels in the group:
    -----
    Port-channel: Po1      (Primary Aggregator)
    -----
      Age of the Port-channel = 0d:00h:25m:17s
      Logical slot/port = 2/1          Number of ports = 2
      HotStandBy port = null
      Port state        = Port-channel Ag-Inuse
      Protocol          = LACP
      Port security     = disabled
    Ports in the Port-channel:
    -----
      Index Load Port      EC state      No of bits
      -----+-----+-----+-----+
      0     00  Fa0/1     Active       0
      0     00  Fa0/2     Active       0
    Time since last port bundled: 0d:00h:05m:41s  Fa0/2
    Time since last port Un-bundled: 0d:00h:05m:48s  Fa0/2
```

**Muestre la información de EtherChannel para F0/1 con el comando show interfaces.**

```
S1# show interfaces f0/1 etherchannel
Port state = up Mstr Assoc In-Bndl
Channel group = 1 Mode = Active
Port-channel = Po1 GC = -
Port index = 0 load = 0x00
Flags: S - Device is sending Slow LACPDUs  F - Device is sending fast LACPDUs.
      A - Device is in active mode.          P - Device is in passive mode.

Local information:
  Port      Flags  State      Priority      LACP port      Admin      Oper      Port      Port
  Port      flags  State      priority     LACP port      key       key      number     state
  Fa0/1     SA     Bndl      32768       Fa0/1        0x1       0x1      0x102     0x3D

Partner's information:
  Port      Flags  Priority      Dev ID      LACP port      Admin      Oper      Port      Port
  Port      flags  priority     dev id      LACP port      key       key      number     state
  Fa0/1     SA     32768       0cd9.96d2.4000  Fa0/1        0x0       0x1      0x102     0x3D

Age of the port in the current state: 0d:00h:24m:59s
```

**Verificó correctamente EtherChannel.**

### Capítulo 3: Agregación de enlaces 3.2.2.2 Solución de problemas de EtherChannel

Todas las interfaces dentro de un EtherChannel deben tener la misma configuración de velocidad y modo dúplex, de VLAN nativas y permitidas en los enlaces troncales, y de la VLAN de acceso en los puertos de acceso.

- Asigne todos los puertos en el EtherChannel a la misma VLAN o configúrelos como enlace troncal. Los puertos con VLAN nativas diferentes no pueden formar un EtherChannel.
- Cuando se configure un EtherChannel desde puertos de enlace troncal, verifique que el modo de enlace troncal sea el mismo en todos los enlaces troncales. Los modos de enlace troncal incoherentes en los puertos EtherChannel pueden hacer que EtherChannel no funcione y que se desactiven los puertos (estado errdisabled).
- Un EtherChannel admite el mismo rango permitido de VLAN en todos los puertos. Si el rango permitido de VLAN no es el mismo, los puertos no forman un EtherChannel, incluso cuando PAgP se establece en modo **auto odesirable**.
- Las opciones de negociación dinámica para PAgP y LACP se deben configurar de manera compatible en ambos extremos del EtherChannel.

**Nota:** es fácil confundir PAgP o LACP con DTP, ya que ambos son protocolos que se usan para automatizar el comportamiento en los enlaces troncales. PAgP y LACP se usan para la agregación de enlaces (EtherChannel). DTP se usa para automatizar la creación de enlaces troncales. Cuando se configura un enlace troncal de EtherChannel, normalmente se configura primero EtherChannel (PAgP o LACP) y después DTP.

En la figura 1, las interfaces F0/1 y F0/2 en los switches S1 y S2 se conectan con un EtherChannel. El resultado indica que el EtherChannel está inactivo.

En la figura 2, un resultado más detallado indica que existen modos PAgP incompatibles configurados en los switches S1 y S2.

En la figura 3, se cambia el modo PAgP en el EtherChannel a deseado, y el EtherChannel se activa.

**Nota:** EtherChannel y el árbol de expansión deben interoperar. Por este motivo, el orden en el que se introducen los comandos relacionados con EtherChannel es importante, y por ello (en la figura 3) se puede ver que se quitó el canal de puertos de interfaz 1 y después se volvió a agregar con el comando **channel-group**, y que no se cambió directamente. Si se intenta cambiar la configuración directamente, los errores del árbol de expansión hacen que los puertos asociados entren en estado de bloqueo o errdisabled.

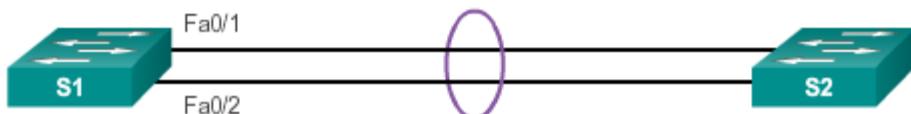
## Solución de problemas de EtherChannel

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone  S - suspended
      H - Hot-standby (LACP only)
      R - Layer3        L - Layer2
      U - in use        F - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
-----+-----+-----+
1    Po1 (SD)      -      Fa0/1(D)  Fa0/2(D)
```



## Solución de problemas de EtherChannel

```
S1# show run | begin interface port-channel
interface Port-channel1
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
  channel-group 1 mode on
!
interface FastEthernet0/2
  switchport mode trunk
  channel-group 1 mode on
!
<resultado omitido>

S2# show run | begin interface port-channel
interface Port-channel1
  switchport mode trunk
!
interface FastEthernet0/1
  switchport mode trunk
  channel-group 1 mode desirable
!
interface FastEthernet0/2
  switchport mode trunk
  channel-group 1 mode desirable
```

## Solución de problemas de EtherChannel

```
S1(config)# no interface port-channel 1
S1(config)# interface range f0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1

S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3       S - Layer2
      U - in use       f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+
1      Po1 (SU)      PAgP        Fa0/1(P)   Fa0/2(P)
```

[Capítulo 3: Agregación de enlaces 3.2.2.3 Packet Tracer: Resolución de problemas de EtherChannel](#)

### Información básica/situación

Recientemente, un técnico principiante configuró cuatro switches. Los usuarios se quejan de que la red funciona con lentitud y desean que usted investigue el problema.

[Packet Tracer: Resolución de problemas de EtherChannel \(instrucciones\)](#)

[Packet Tracer: Resolución de problemas de EtherChannel \(PKA\)](#)

[Capítulo 3: Agregación de enlaces 3.2.2.4 Práctica de laboratorio: resolución de problemas de EtherChannel](#)

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y cargar las configuraciones de los dispositivos

- Parte 2: Resolver problemas de EtherChannel

### [Práctica de laboratorio: resolución de problemas de EtherChannel](#)

#### Capítulo 3: Agregación de enlaces 3.3.1.1 Actividad de clase: Creando enlaces

##### **Creando enlaces**

En la red de su pequeña a mediana empresa, se producen muchos cuellos de botella aunque haya configurado redes VLAN, STP y otras opciones de tráfico de red en los switches de la empresa.

En lugar de mantener la configuración actual de los switches, le gustaría probar EtherChannel como opción para al menos una parte de la red, a fin de ver si disminuye la congestión de tráfico entre los switches de capa de acceso y de distribución.

La empresa usa switches Catalyst 3560 en la capa de distribución y switches Catalyst 2960 y 2950 en la capa de acceso de la red. Para verificar si estos switches pueden realizar funciones de EtherChannel, consulte el sitio [System Requirements to Implement EtherChannel on Catalyst Switches](#). En este sitio, puede obtener más información para determinar si EtherChannel es una buena opción para los equipos y la red instalados actualmente.

Después de investigar los modelos, decide utilizar un programa de software de simulación para practicar la configuración de EtherChannel antes de implementarla concretamente en la red. Como parte de este procedimiento, se asegura de que el equipo simulado en Packet Tracer admite esta configuración de práctica.

##### [Actividad de clase: Creando enlaces](#)

#### Capítulo 3: Agregación de enlaces 3.3.1.2 Packet Tracer: desafío de integración de habilidades

##### **Información básica/situación**

En esta actividad, hay dos routers configurados para comunicarse entre sí. Usted es responsable de configurar las subinterfaces para que se comuniquen con los switches. Configurará redes VLAN, enlaces troncales y EtherChannel con PVST. Todos los dispositivos de Internet se configuraron previamente.

##### [Packet Tracer: desafío de habilidades de integración \(instrucciones\)](#)

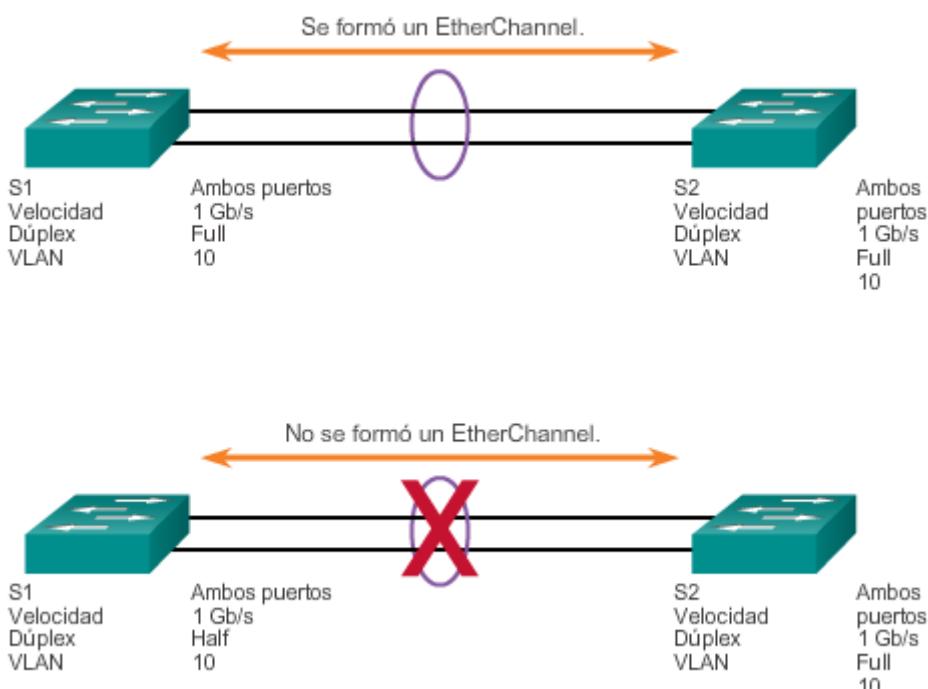
##### [Packet Tracer: desafío de integración de habilidades \(PKA\)](#)

#### Capítulo 3: Agregación de enlaces 3.3.1.3 Resumen

EtherChannel agrega varios enlaces conmutados para equilibrar la carga a través de rutas redundantes entre dos dispositivos. Todos los puertos en un EtherChannel deben tener la misma velocidad, la misma configuración de dúplex y la misma información de VLAN en todas las interfaces en los dispositivos de ambos extremos. Los parámetros configurados en el modo

de configuración de interfaz de canal de puertos también se aplican a las interfaces individuales en ese EtherChannel. Los parámetros configurados en las interfaces individuales no se aplican al EtherChannel o a las demás interfaces en el EtherChannel.

PAgP es un protocolo exclusivo de Cisco que ayuda en la creación automática de enlaces EtherChannel. Los modos PAgP son encendido, PAgP deseable y PAgP automático. LACP forma parte de una especificación IEEE que también permite agrupar varios puertos físicos en un único canal lógico. Los modos LACP son encendido, LACP activo y LACP pasivo. PAgP y LACP no interoperan. El modo encendido se repite en PAgP y LACP debido a que crea un EtherChannel incondicionalmente, sin el uso de PAgP o LACP. La forma predeterminada para EtherChannel consiste en que no haya ningún modo configurado.



#### Capítulo 4: LAN inalámbricas 4.0.1.1 Introducción

Las redes inalámbricas pueden proporcionar movilidad para los clientes, la capacidad de conectarse en cualquier momento y lugar, así como la capacidad de moverse y seguir conectado. Una LAN inalámbrica (WLAN) es una clasificación de red inalámbrica que se usa comúnmente en entornos domésticos, de oficina y de campus. Si bien usa radiofrecuencias en lugar de cables, en general se implementa en un entorno de red conmutada, y su formato de trama es similar a Ethernet.

En este capítulo, se aborda la tecnología, los componentes, la seguridad, la planificación, la implementación y la resolución de problemas de WLAN. Se analizan los tipos de ataques a los que las redes inalámbricas son particularmente vulnerables.

**Al completar este capítulo, usted podrá:**

- Describir la tecnología LAN inalámbrica y sus estándares.
- Describir los componentes de una infraestructura LAN inalámbrica.
- Describir las topologías inalámbricas.
- Describir la estructura de trama 802.11.
- Describir el método de acceso a los medios que usa la tecnología inalámbrica.
- Describir la administración de canales en una WLAN.
- Describir las amenazas para las LAN inalámbricas.
- Describir los mecanismos de seguridad de una LAN inalámbrica.
- Configurar un router inalámbrico para dar soporte a un sitio remoto.
- Configurar clientes inalámbricos para conectarse a un router inalámbrico.
- Resolver problemas comunes de la configuración inalámbrica.

Capítulo 4: LAN inalámbricas 4.0.1.2 Actividad de clase: Que la mía sea inalámbrica

**Que la mía sea inalámbrica**

Como administrador de red de su pequeña a mediana empresa, se da cuenta de que se debe actualizar la red inalámbrica, tanto dentro como fuera del edificio. Por lo tanto, decide investigar cómo otras empresas y otros grupos educativos y comunitarios configuran las WLAN para acceder mejor a sus empleados y clientes.

Para investigar este tema, visite el sitio web “[Customer Case Studies and Research](#)” para ver cómo otras empresas usan la tecnología inalámbrica. Después de ver algunos videos y de leer PDF de casos prácticos, decide seleccionar dos para mostrarle al director de la empresa a fin de fundamentar la actualización a una solución inalámbrica más sólida para su empresa.

Para completar esta actividad de clase de creación de modelos, abra el PDF correspondiente a esta actividad para obtener más instrucciones sobre cómo continuar.

[Actividad de clase: Que la mía sea inalámbrica](#)

Capítulo 4: LAN inalámbricas 4.1.1.1 Compatibilidad con la movilidad

Las redes empresariales actuales evolucionan para dar soporte a la gente que está en continuo movimiento. Las personas se conectan mediante varios dispositivos, como computadoras de escritorio y portátiles, tablet PC y smartphones. Esta es la visión de movilidad en la cual las personas pueden viajar y llevar con ellas su conexión a la red.

Existen muchas infraestructuras diferentes (LAN conectada por cable, redes de proveedores de servicios) que hacen posible este tipo de movilidad; sin embargo, en un entorno empresarial, la más importante es la LAN inalámbrica (WLAN).

La productividad ya no está restringida a una ubicación de trabajo fija o a un período de tiempo definido. Hoy en día, las personas esperan estar conectadas en cualquier momento y lugar, desde la oficina hasta el aeropuerto o el hogar. Los empleados que viajan solían estar restringidos a utilizar teléfonos públicos para verificar sus mensajes y para devolver algunas llamadas telefónicas entre vuelos. Ahora, los empleados pueden revisar su correo electrónico, su correo de voz y el estado de los proyectos en los smartphones.

En la actualidad, los usuarios esperan poder moverse y seguir conectados de forma inalámbrica. La capacidad móvil permite que un dispositivo inalámbrico mantenga el acceso a Internet sin perder la conexión.

Reproduzca el video de la ilustración para ver un ejemplo de cómo las redes inalámbricas permiten la movilidad.

#### Capítulo 4: LAN inalámbricas 4.1.1.2 Beneficios de la tecnología inalámbrica

Existen muchos beneficios de admitir redes inalámbricas en el entorno empresarial y doméstico. Algunos de los beneficios incluyen el aumento de la flexibilidad y la productividad, la reducción de costos y la capacidad de crecer y adaptarse a requisitos cambiantes.

En la figura 1, se proporcionan ejemplos de flexibilidad inalámbrica para el empleado móvil.

Para las operaciones diarias dentro de la oficina, la mayoría de las empresas dependen de LAN basadas en switches. Sin embargo, los empleados se mueven cada vez más y desean mantener el acceso a los recursos de la LAN de la empresa desde otras ubicaciones además de su escritorio. Los trabajadores quieren llevar sus dispositivos inalámbricos a las reuniones, las oficinas de sus compañeros de trabajo, las salas de conferencias e incluso a los sitios de los clientes y, al mismo tiempo, mantener el acceso a los recursos de la oficina. Las redes inalámbricas proporcionan este tipo de flexibilidad. En lugar de pasar una cantidad de tiempo considerable transportando el material necesario de la empresa o buscando conexiones por cable para acceder a los recursos de la red, los recursos LAN pueden estar disponibles fácilmente para una variedad de dispositivos inalámbricos mediante el uso de la red inalámbrica.

Si bien es difícil de medir, el acceso inalámbrico puede generar un aumento de la productividad y hacer que los empleados estén más relajados. Con las redes inalámbricas, los empleados tienen flexibilidad para trabajar cuando quieran, donde quieran. Pueden responder a las preguntas de un cliente en la oficina o en un restaurante durante la cena. Pueden acceder al correo electrónico y a otros recursos relacionados con el trabajo de forma rápida y fácil, lo que proporciona una mejor administración, mejores resultados y más rápidos para los clientes, y mayores ganancias.

Las redes inalámbricas también permiten reducir los costos. En las empresas que ya cuentan con una infraestructura inalámbrica, los ahorros se materializan cada vez que se cambian los equipos o se realizan mudanzas, como cuando se reubica a un empleado dentro de un edificio, se reorganizan equipos o un laboratorio, o se trasladan a ubicaciones o a sitios de proyecto temporarios.

Otro beneficio importante de las redes inalámbricas es la capacidad para adaptarse a las necesidades y las tecnologías cambiantes. Agregar nuevos equipos a la red es muy sencillo con las redes inalámbricas. Considere la conectividad inalámbrica en el hogar. Los usuarios pueden navegar la Web desde la mesa de la cocina, la sala o incluso en exteriores. Los usuarios domésticos conectan nuevos dispositivos, como smartphones, smartpads, computadoras portátiles y televisores inteligentes.

Como se muestra en la figura 2, un router doméstico inalámbrico permite que el usuario se conecte a estos dispositivos sin el costo adicional ni los inconvenientes relacionados con instalar cables en diferentes sitios del hogar.

## Reducción de costos



### Capítulo 4: LAN inalámbricas 4.1.1.3 Tecnologías inalámbricas

Las comunicaciones inalámbricas se usan en una variedad de profesiones.

Si bien la combinación de tecnologías inalámbricas se expande continuamente, este análisis se centra en las redes inalámbricas que permiten que los usuarios se muevan. En términos generales, las redes inalámbricas se clasifican en los siguientes tipos:

- **Redes de área personal inalámbrica (WPAN):** tienen un alcance de unos pocos metros. En las WPAN, se utilizan dispositivos con Bluetooth o Wi-Fi Direct habilitado.
- **LAN inalámbricas (WLAN):** tienen un alcance de unos 30 m, como en una sala, un hogar, una oficina e incluso un campus.
- **Redes de área extensa inalámbrica (WWAN):** tienen un alcance de kilómetros, como un área metropolitana, una jerarquía de datos móviles o incluso los enlaces entre ciudades mediante retransmisiones de microondas.

Haga clic en cada componente de la ilustración para mostrar más información acerca de las diversas tecnologías inalámbricas disponibles para conectar los dispositivos a estas redes inalámbricas.

- **Bluetooth:** originalmente era un estándar de WPAN IEEE 802.15 que usa un proceso de emparejamiento de dispositivos para comunicarse a través de distancias de hasta 0,05 mi (100 m). El Bluetooth Special Interest Group (<https://www.bluetooth.org/>) estandariza las versiones más recientes de Bluetooth.

- **Fidelidad inalámbrica (Wi-Fi):** es un estándar de WLAN IEEE 802.11 que se implementa generalmente para proporcionar acceso a la red a los usuarios domésticos y empresariales, que permite incluir tráfico de datos, voz y video a distancias de hasta 300 m (0,18 mi)
- **Interoperabilidad mundial para el acceso por microondas (WiMAX):** es un estándar de WWAN IEEE 802.16 que proporciona acceso a servicios de banda ancha inalámbrica hasta 30 mi (50 km) WiMAX es una alternativa a las conexiones de banda ancha por cable y DSL. Se agregó la movilidad a WiMAX en 2005, y los proveedores de servicios ahora la pueden usar para proporcionar banda ancha de datos móviles.
- **Banda ancha celular:** consta de varias organizaciones empresariales, nacionales e internacionales que usan el acceso de datos móviles de un proveedor de servicios para proporcionar conectividad de red de banda ancha celular. Disponible por primera vez en 1991 con los teléfonos celulares de segunda generación (2G), con mayores velocidades disponibles en 2001 y 2006 como parte de la tercera (3G) y la cuarta (4G) generación de la tecnología de comunicaciones móviles.
- **Banda ancha satelital:** proporciona acceso de red a sitios remotos mediante el uso de una antena parabólica direccional que se alinea con un satélite específico en la órbita geoestacionaria (GEO) de la Tierra. Normalmente es más costosa y requiere una línea de vista despejada.

Existen muchos tipos de tecnologías inalámbricas disponibles. Sin embargo, este capítulo se centra en las WLAN 802.11.

#### Tecnologías inalámbricas comunes



Bluetooth



Banda ancha celular



Satelital



Wi-Fi



WiMAX

#### Capítulo 4: LAN inalámbricas 4.1.1.4 Radiofrecuencias

Todos los dispositivos inalámbricos funcionan en la banda de las ondas de radio del espectro electromagnético. Es responsabilidad del Sector de Radiocomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-R) regular la asignación del espectro de radiofrecuencia (RF). Los rangos de frecuencia, denominados “bandas”, se asignan con distintos propósitos. Algunas bandas en el espectro electromagnético están reguladas en gran medida y se usan para aplicaciones como las redes de control del tráfico aéreo y de comunicaciones de respuesta de emergencias. Otras bandas no tienen licencia, como la banda industrial, científica y médica (ISM) y la banda de infraestructura de la información nacional (UNII).

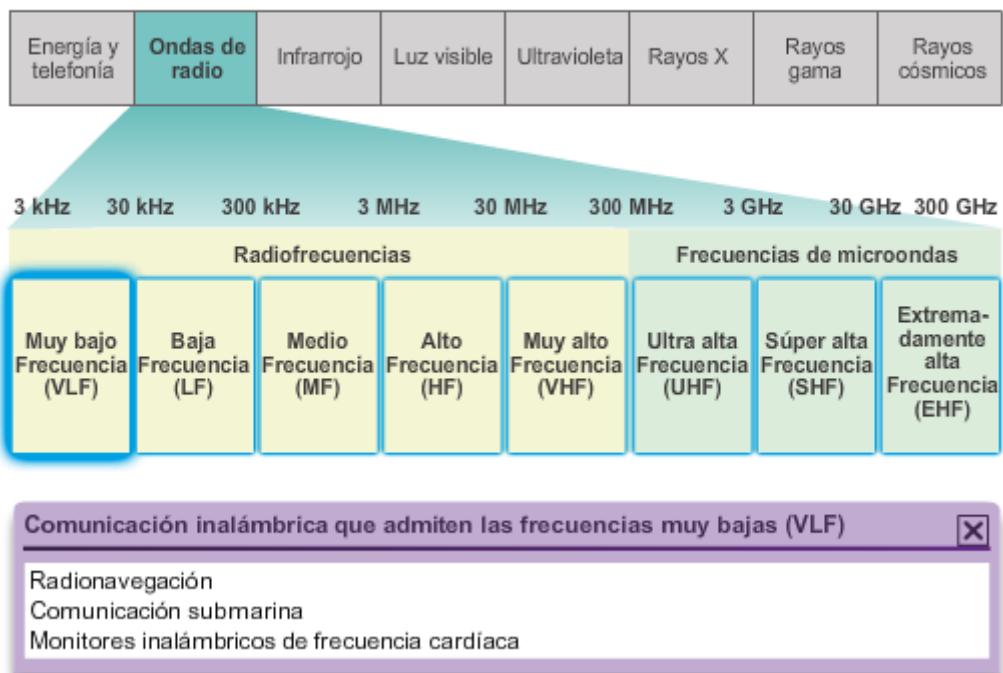
**Nota:** las redes WLAN funcionan en la banda de frecuencia ISM de 2,4 GHz y en la banda UNII de 5 GHz.

La comunicación inalámbrica ocurre en la banda de las ondas de radio (es decir, de 3 Hz a 300 GHz) del espectro electromagnético, como se muestra en la ilustración. La banda de las ondas de radio se subdivide en una sección de radiofrecuencias y una sección de frecuencias de microondas. Observe que las comunicaciones de WLAN, Bluetooth, datos móviles y satelitales operan en las bandas de microondas UHF, SHF y EHF.

Los dispositivos LAN inalámbricos tienen transmisores y receptores sintonizados en frecuencias específicas de la banda de ondas de radio. Específicamente, se asignan las siguientes bandas de frecuencia a las LAN inalámbricas 802.11:

- **2,4 GHz (UHF):** 802.11b/g/n/ad
- **5 GHz (SHF):** 802.11a/n/ac/ad
- **Banda de 60 GHz (EHF):** 802.11ad

## Ondas de radio del espectro electromagnético



### Capítulo 4: LAN inalámbricas 4.1.1.5 Estándares 802.11

El estándar de WLAN IEEE 802.11 define cómo se usa la RF en las bandas de frecuencia ISM sin licencia para la capa física y la subcapa MAC de los enlaces inalámbricos.

Con el correr de los años, se desarrollaron varias implementaciones del estándar IEEE 802.11. A continuación, se presentan estos estándares:

- **802.11:** lanzado en 1997 y ahora obsoleto, es la especificación de WLAN original que funcionaba en la banda de 2,4 GHz y ofrecía velocidades de hasta 2 Mb/s. Cuando se lanzó, las LAN conectadas por cable funcionaban a 10 Mb/s, por lo que la nueva tecnología inalámbrica no se adoptó con entusiasmo. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas.
- **IEEE 802.11a:** lanzado en 1999, funciona en la banda de frecuencia de 5 GHz, menos poblada, y ofrece velocidades de hasta 54 Mb/s. Posee un área de cobertura menor y es menos efectivo al penetrar estructuras edilicias ya que opera en frecuencias superiores. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas. Los dispositivos que funcionan conforme a este estándar no son interoperables con los estándares 802.11b y 802.11g.
- **IEEE 802.11b:** lanzado en 1999, funciona en la banda de frecuencia de 2,4 GHz y ofrece velocidades de hasta 11 Mb/s. Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejor las estructuras edilicias que los dispositivos basados en 802.11a. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas.

- **IEEE 802.11g:** lanzado en 2003, funciona en la banda de frecuencia de 2,4 GHz y ofrece velocidades de hasta 54 Mb/s. Por lo tanto, los dispositivos que implementan este estándar funcionan en la misma radiofrecuencia y en el mismo rango que 802.11b, pero con el ancho de banda de 802.11a. Los dispositivos inalámbricos tienen una antena para transmitir y recibir señales inalámbricas. Es compatible con el estándar anterior 802.11b. Sin embargo, cuando admite un cliente 802.11b, se reduce el ancho de banda general.
- **IEEE 802.11n:** lanzado en 2009, funciona en las bandas de frecuencia de 2,4 GHz y 5 GHz, y se conoce como “dispositivo de doble banda”. Las velocidades de datos típicas van desde 150 Mb/s hasta 600 Mb/s, con un alcance de hasta 70 m (0,5 mi). Sin embargo, para lograr mayores velocidades, los AP y los clientes inalámbricos requieren varias antenas con tecnología de múltiple entrada múltiple salida (MIMO). MIMO usa varias antenas como transmisor y receptor para mejorar el rendimiento de la comunicación. Se pueden admitir hasta cuatro antenas. El estándar 802.11n es compatible con dispositivos 802.11a/b/g anteriores. Sin embargo, si se admite un entorno mixto, se limitan las velocidades de datos previstas.
- **IEEE 802.11ac:** lanzado en 2013, funciona en la banda de frecuencia de 5 GHz y proporciona velocidades de datos que van desde 450 Mb/s hasta 1,3 Gb/s (1300 Mb/s). Usa la tecnología MIMO para mejorar el rendimiento de la comunicación. Se pueden admitir hasta ocho antenas. El estándar 802.11ac es compatible con dispositivos 802.11a/n anteriores; sin embargo, admitir un entorno mixto limita las velocidades de datos esperadas.
- **IEEE 802.11ad:** programado para su lanzamiento en 2014 y también conocido como “WiGig”, utiliza una solución de Wi-Fi de triple banda con 2,4 GHz, 5 GHz y 60 GHz, y ofrece velocidades teóricas de hasta 7 Gb/s. Sin embargo, la banda de 60 GHz es una tecnología de línea de vista y, por lo tanto, no puede penetrar las paredes. Cuando un usuario se mueve, el dispositivo cambia a las bandas más bajas de 2,4 GHz y 5 GHz. Es compatible con dispositivos Wi-Fi anteriores existentes. Sin embargo, si se admite un entorno mixto, se limitan las velocidades de datos previstas.

En la ilustración, se resume cada estándar 802.11.

#### Comparación de los estándares 802.11

Estándar IEEE	Velocidad máxima	Frecuencia	Compatibilidad con versiones anteriores
802.11	2 Mb/s	2,4 GHz	—
802.11a	54 Mb/s	5 GHz	—
802.11b	11 Mb/s	2,4 GHz	—
802.11g	54 Mb/s	2,4 GHz	802.11b
802.11n	600 Mb/s	2,4GHz y 5GHz	802.11a/b/g
802.11ac	1,3 Gb/s (1300 Mb/s)	5 GHz	802.11a/n
802.11ad	7Gb/s (7000Mb/s)	2,4GHz, 5GHz y 60 GHz	802.11a/b/g/n/ac

Los estándares aseguran interoperabilidad entre dispositivos hechos por diferentes fabricantes. Las tres organizaciones que influyen en los estándares de WLAN en todo el mundo son las siguientes:

- **ITU-R:** regula la asignación del espectro de RF y las órbitas satelitales.
- **IEEE:** especifica cómo se modula la RF para transportar la información. Mantiene los estándares para las redes de área local y metropolitana (MAN) con la familia de estándares de LAN y MAN IEEE 802. Los estándares dominantes en la familia IEEE 802 son Ethernet 802.3 y WLAN 802.11. Si bien el IEEE especificó los estándares para los dispositivos de modulación de RF, no especificó los estándares de fabricación; por lo tanto, las interpretaciones de los estándares 802.11 por parte de los diferentes proveedores pueden causar problemas de interoperabilidad entre los dispositivos.
- **Wi-Fi Alliance:** Wi-Fi Alliance® (<http://www.wi-fi.org>) es una asociación comercial global del sector sin fines de lucro dedicada a promover el crecimiento y la aceptación de las redes WLAN. Es una asociación de proveedores cuyo objetivo es mejorar la interoperabilidad de los productos basados en el estándar 802.11 mediante la certificación de los proveedores por el cumplimiento de las normas del sector y la observancia de los estándares.

Wi-Fi Alliance certifica la compatibilidad de Wi-Fi con los siguientes productos:

- Compatibilidad con IEEE 802.11a/b/g/n/ac/ad
- IEEE 802.11i seguro con WPA2™ y el protocolo de autenticación extensible (EAP)
- Configuración protegida de Wi-Fi (WPS) para simplificar la conexión de los dispositivos
- Wi-Fi Direct para compartir medios entre dispositivos
- Wi-Fi Passpoint para simplificar de forma segura la conexión a las redes de zona de cobertura Wi-Fi
- Wi-Fi Miracast para mostrar video sin inconvenientes entre dispositivos

**Nota:** existen otros productos de certificación Wi-Fi, como WMM® (Wi-Fi Multimedia™), Tunneled Direct Link Setup (TDLS) y Ahorro de energía WMM.

En la figura 1, se muestran los logos de Wi-Fi Alliance que identifican la compatibilidad con una característica específica. Los dispositivos que muestran logos específicos admiten la característica identificada. Los dispositivos pueden mostrar una combinación de estos logos.

Haga clic en el botón Reproducir de las figuras 2 a 4 para ver videos entretenidos sobre las características de Wi-Fi Direct, Wi-Fi Passpoint y Wi-Fi Miracast.

### Logos Wi-Fi Certified comunes

	Logo genérico de Wi-Fi Alliance que señala que el producto se probó y cumple con la característica Wi-Fi especificada.
	Logo Wi-Fi que certifica que el producto interopera con dispositivos 802.11a/b/g/n.
	Logo Wi-Fi que certifica que el dispositivo tiene configuración protegida de Wi-Fi y está certificado para simplificar la conectividad inicial del dispositivo.
	Logo Wi-Fi que certifica que el dispositivo tiene capacidad para Wi-Fi Direct, lo que simplifica el uso compartido de medios entre dispositivos.

#### Capítulo 4: LAN inalámbricas 4.1.1.7 Comparación entre las redes WLAN y una LAN

Las WLAN comparten un origen similar con las LAN Ethernet. El IEEE adoptó la cartera 802 LAN/MAN de estándares de arquitectura de red de computadoras. Los dos grupos de trabajo 802 dominantes son Ethernet 802.3 y WLAN 802.11. Sin embargo, hay diferencias importantes entre ellos.

Las WLAN usan RF en lugar de cables en la capa física y la subcapa MAC de la capa de enlace de datos. Comparada con el cable, la RF tiene las siguientes características:

- La RF no tiene límites, como los límites de un cable envuelto. Esto permite que las tramas de datos que se transmiten a través de los medios de RF estén disponibles para cualquier persona que pueda recibir la señal de RF.
- La señal RF no está protegida de señales exteriores, como sí lo está el cable en su envoltura aislante. Las radios que funcionan de manera independiente en la misma área geográfica, pero con una RF igual o similar, pueden interferir entre sí.
- La transmisión RF está sujeta a los mismos desafíos inherentes a cualquier tecnología basada en ondas, como la radio comercial. Por ejemplo, a medida que la radio se aleja del origen, es posible que las emisoras de radio comiencen a reproducirse una por encima de la otra y que aumente el ruido estático. Finalmente, la señal se pierde por completo. Las LAN conectadas tienen cables que son del largo apropiado para mantener la fuerza de la señal.

- Las bandas RF se regulan en forma diferente en cada país. La utilización de las WLAN está sujeta a regulaciones adicionales y a conjuntos de estándares que no se aplican a las LAN conectadas por cable.

Las WLAN también difieren de las LAN conectadas por cable de la siguiente manera:

- Las WLAN conectan clientes a la red mediante puntos de acceso (AP) inalámbrico o un router inalámbrico, en lugar de hacerlo mediante un switch Ethernet.
- Las WLAN conectan los dispositivos móviles que, en general, están alimentados por batería, en lugar de los dispositivos conectados de la LAN. Las NIC inalámbricas tienden a reducir la duración de la batería de los dispositivos móviles.
- Las WLAN admiten hosts que se disputan el acceso a los medios RF (bandas de frecuencia). Para evitar proactivamente las colisiones dentro de los medios, el estándar 802.11 recomienda la prevención de colisiones (CSMA/CA) en lugar de la detección de colisiones (CSMA/CD) para el acceso a los medios.
- Las WLAN utilizan un formato de trama diferente al de las LAN Ethernet conectadas por cable. Las WLAN requieren información adicional en el encabezado de la Capa 2 de la trama.
- Las WLAN tienen mayores inconvenientes de privacidad debido a que las frecuencias de radio pueden salir fuera de las instalaciones.

#### **Comparación entre WLAN y LAN**

<b>Característica</b>	<b>LAN inalámbrica 802.11</b>	<b>Redes LAN Ethernet 802.3</b>
Capa física	Radiofrecuencia (RF)	Cable
Acceso a medios	Prevención de colisiones	Detección de colisiones
Disponibilidad	Cualquiera con una radio NIC en el rango de un punto de acceso	Se requiere conexión por cable
Interferencia en la señal	Sí	Irrelevante
Regulación	Normas adicionales emitidas por las autoridades de cada país	El estándar IEEE dictamina

Capítulo 4: LAN inalámbricas 4.1.1.8 Actividad: Identificar la tecnología inalámbrica

	Bluetooth Banda ancha	Wi-Fi	WiMAX	Datos móviles Banda ancha	Satelital Banda ancha
Transmisiones a distancias de hasta 100 m.	✓				
Proporciona acceso por banda ancha a sitios remotos mediante una antena parabólica direccional.					✓
IEEE 802.11		✓			
Proporciona acceso por banda ancha móvil mediante redes de datos móviles.				✓	
IEEE 802.16			✓		
Se requiere una línea de vista despejada.					✓
Transmisiones a distancias de hasta 300 m.	✓				
Usa las variantes 2G, 3G y 4G.				✓	
Admite velocidades de hasta 1 Gb/s.		✓			
Admite velocidades de hasta 24 Mb/s.	✓				
IEEE 802.15	✓				
Distancias de transmisión de hasta 30 mi (50 km).			✓		

#### Capítulo 4: LAN inalámbricas 4.1.1.9 Actividad: Comparar los estándares inalámbricos

##### Actividad (parte 1): Comparar los estándares inalámbricos

Arrastre las opciones de velocidades, frecuencias y compatibilidad con versiones anteriores de la tecnología inalámbrica hasta los estándares IEEE 802.11 correspondientes. Algunas opciones se pueden usar más de una vez. Haga clic en el botón 2 para continuar la actividad.

—	2 Mb/s	7 Gb/s
802.11b	11 Mb/s	2,4 GHz y 5 GHz
802.11a/n	54 Mb/s	2,4 GHz, 5 GHz y 60 GHz
802.11a/b/g	600 Mb/s	2,4 GHz
802.11 a/b/g/n/ac	1,3 Gb/s	5 GHz

Estándar IEEE	Velocidad máxima	Frecuencia	Compatibilidad con versiones anteriores
802.11	✓ 2 Mb/s	✓ 2,4 GHz	✓ —
802.11a	✓ 54 Mb/s	✓ 5 GHz	✓ —
802.11b	✓ 11 Mb/s	✓ 2,4 GHz	✓ —
802.11g	✓ 54 Mb/s	✓ 2,4 GHz	✓ 802.11b
802.11n	✓ 600 Mb/s	✓ 2,4 GHz y 5 GHz	✓ 802.11a/b/g
802.11ac	✓ 1,3 Gb/s	✓ 5 GHz	✓ 802.11a/n
802.11ad		✓ 2,4 GHz, 5 GHz y 60 GHz	✓ 802.11 a/b/g/n/ac

**Actividad (parte 2): Identificar las radiofrecuencias de microondas para cada estándar**

Una las estándares de WLAN con las radiofrecuencias de microondas. Para indicar sus respuestas, arrastre la marca de verificación hasta los campos correspondientes en cada columna. Se puede indicar más de una respuesta por columna. Haga clic en el botón 3 para continuar la actividad.



Estándares de WLAN y radiofrecuencias de microondas			
2.4 GHz (UHF)	5 GHz (SHF)	60 GHz (EHF)	
802.11a		802.11a	802.11a
802.11b	✓	✓	802.11b
802.11g	✓	✓	802.11g
802.11n	✓	✓	802.11n
802.11ac		✓	802.11ac
802.11ad	✓	✓	802.11ad

**Actividad (parte 3): Identificar la radiofrecuencia para cada estándar inalámbrico**

Una las aplicaciones de radiofrecuencia de microondas con el estándar inalámbrico. Las respuestas se pueden usar más de una vez.

Radioastronomía	Aplicaciones de radiofrecuencia de microondas
Comunicaciones satelitales	2.4 GHz (UHF) ✓ Bluetooth ✓ Banda ancha de datos móviles ✓ Sistemas GPS
Bluetooth	5 GHz (SHF) ✓ Radioastronomía ✓ Comunicaciones satelitales ✓ Comunicaciones mediante microondas
Sistemas de aterrizaje por radar	60 GHz (EHF) ✓ Radioastronomía ✓ Sistemas de aterrizaje por radar
Banda ancha de datos móviles	
Comunicaciones mediante microondas	
Sistemas GPS	

**Capítulo 4: LAN inalámbricas 4.1.1.10 Actividad: Comparar las WLAN y las LAN**

**Actividad: Comparar las tecnologías WLAN y LAN**

Arrastre la tecnología WLAN o LAN hasta los enunciados que describen esa tecnología.

✓ WLAN 802.11	Se usa la radiofrecuencia (RF) para interconectar dispositivos.
✓ WLAN 802.11	Prevención de colisiones (CSMA/CA).
✓ LAN 802.3	Se usan cables para interconectar dispositivos.
✓ LAN 802.3	Proporciona mayor seguridad.
✓ WLAN 802.11	Se pueden aplicar leyes y normas adicionales en las áreas locales.
✓ LAN 802.3	La interferencia de señales no suele ser un problema.
✓ LAN 802.3	Detección de colisiones (CSMA/CD).
✓ WLAN 802.11	Permite la movilidad de los dispositivos.

#### Capítulo 4: LAN inalámbricas 4.1.2.1 NIC inalámbricas

La red inalámbrica más simple requiere, como mínimo, dos dispositivos. Cada dispositivo debe tener un transmisor de radio y un receptor de radio sintonizados en las mismas frecuencias.

Sin embargo, la mayoría de las implementaciones inalámbricas requieren lo siguiente:

- Terminales con NIC inalámbricas
- Dispositivo de infraestructura, como un router o un AP inalámbricos

Para comunicarse de forma inalámbrica, los terminales requieren una NIC inalámbrica que incorpore un transmisor o un receptor de radio y el controlador de software necesario para que funcione. Las computadoras portátiles, las tablet PC y los smartphones ahora incluyen NIC inalámbricas integradas. Sin embargo, si un dispositivo no tiene una NIC inalámbrica integrada, se puede usar un adaptador inalámbrico USB.

En la ilustración, se muestran dos adaptadores inalámbricos USB.

#### Capítulo 4: LAN inalámbricas 4.1.2.2 Router doméstico inalámbrico

El tipo de dispositivo de infraestructura al que se asocia una terminal y con el que se autentica varía según el tamaño y los requisitos de la WLAN.

Por ejemplo, un usuario doméstico normalmente interconecta dispositivos inalámbricos mediante un pequeño router inalámbrico integrado. Estos routers integrados más pequeños funcionan como lo siguiente:

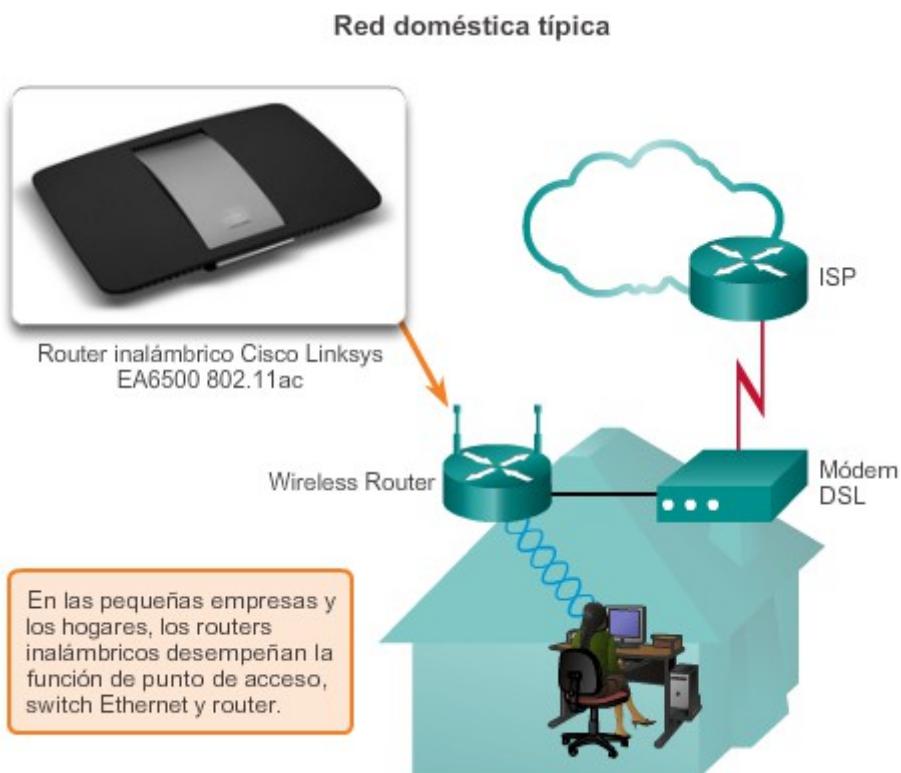
- **Punto de acceso:** proporciona acceso inalámbrico 802.11a/b/g/n/ac.
- **Switch:** proporciona un switch Ethernet 10/100/1000, full-duplex, de cuatro puertos para conectar dispositivos por cable.
- **Router:** proporciona un gateway predeterminado para la conexión a otras infraestructuras de la red.

Por ejemplo, el router Cisco Linksys EA6500, que se muestra en la figura 1, se suele implementar como dispositivo de acceso inalámbrico residencial o de una pequeña empresa. El router inalámbrico se conecta al módem DLS del ISP y anuncia sus servicios mediante el envío de señales que contienen su identificador de conjunto de servicios compartidos (SSID). Los dispositivos internos detectan de manera inalámbrica el SSID del router e intentan asociarse y autenticarse con él para acceder a Internet.

La carga esperada en el router Linksys EA6500, en este entorno, es lo suficientemente baja como para que el router pueda administrar la disposición de WLAN y Ethernet 802.3, y para conectarse a un ISP. También proporciona características avanzadas, como el acceso de alta velocidad, un diseño óptimo para la transmisión de video, compatibilidad con IPv6, QoS, fácil configuración mediante Wi-Fi WPS y puertos USB para conectar impresoras o unidades portátiles.

Además, para los usuarios domésticos que desean ampliar los servicios de su red, tanto inalámbricos como conectados por cable, se pueden implementar adaptadores de línea eléctrica inalámbricos. Con estos dispositivos, se puede conectar un dispositivo directamente a la red por medio de tomacorrientes eléctricos, lo que es ideal para la transmisión de video en HD y los juegos en línea. Son fáciles de instalar: simplemente enchúfelo en un tomacorriente de pared o una toma múltiple y conecte el dispositivo con solo presionar un botón.

Haga clic en el botón Reproducir de la figura 2 para ver una descripción general de los adaptadores de línea eléctrica Linksys.



#### Capítulo 4: LAN inalámbricas 4.1.2.3 Soluciones inalámbricas para empresas

Las organizaciones que proporcionan conectividad inalámbrica a sus usuarios requieren una infraestructura WLAN para proporcionar opciones adicionales de conectividad.

**Nota:** IEEE 802.11 denomina “estación” (STA) a un cliente inalámbrico. En este capítulo, el término “cliente inalámbrico” se utiliza para describir cualquier dispositivo con capacidad inalámbrica.

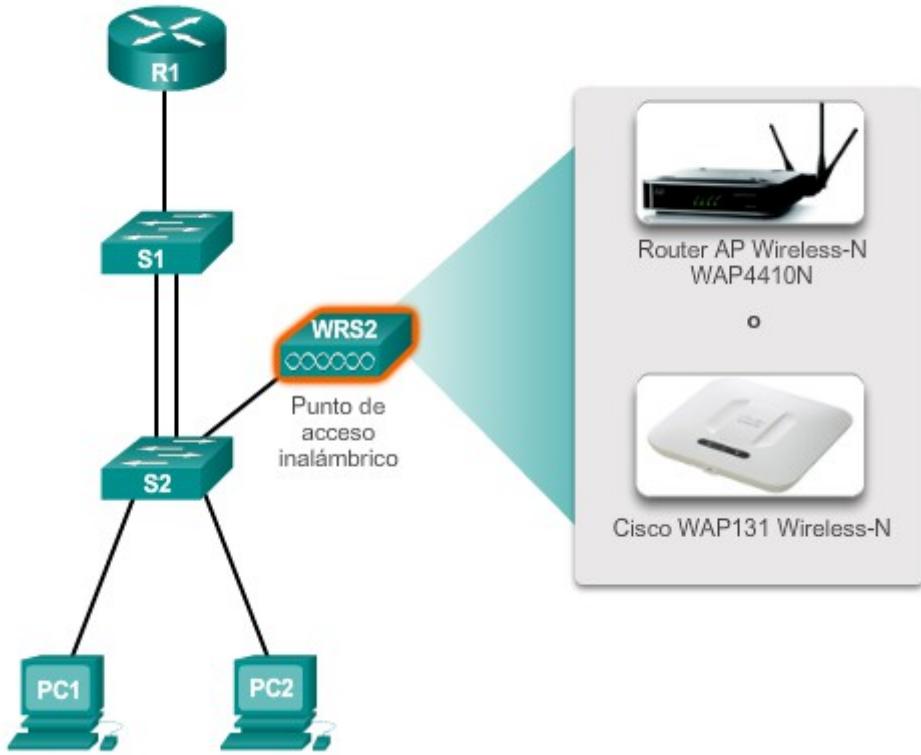
La red de una pequeña empresa que se muestra en la figura 1 es una LAN Ethernet 802.3. Cada cliente (es decir, la PC1 y la PC2) se conecta a un switch mediante un cable de red. El switch es el punto donde los clientes acceden a la red. Observe que el AP inalámbrico también se conecta al switch. En este ejemplo, se puede usar tanto el AP Cisco WAP4410N como el AP WAP131 para proporcionar conectividad de red inalámbrica.

Los clientes inalámbricos usan la NIC inalámbrica para detectar los AP cercanos que anuncian su SSID. Los clientes después intentan asociarse y autenticarse con un AP, como se muestra

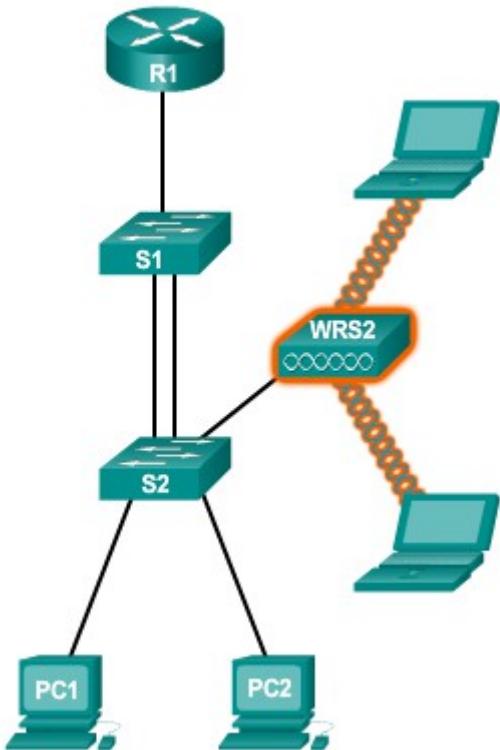
en la figura 2. Después de la autenticación, los usuarios inalámbricos tienen acceso a los recursos de la red.

**Nota:** las necesidades inalámbricas de una pequeña organización difieren de las de una organización grande. Las implementaciones inalámbricas a gran escala requieren hardware inalámbrico adicional para simplificar la instalación y la administración de la red inalámbrica.

El punto de acceso se conecta a la infraestructura conectada por cable



Los clientes se conectan al AP



#### Capítulo 4: LAN inalámbricas 4.1.2.4 Puntos de acceso inalámbrico

Los AP se pueden categorizar como AP autónomos o AP basados en controladores.

##### **AP autónomos**

Los AP autónomos, a veces denominados “AP pesados”, son dispositivos autónomos que se configuran mediante la CLI de Cisco o una GUI. Los AP autónomos son útiles en situaciones en las que solo se requiere un par de AP en la red. De manera optativa, se pueden controlar varios AP mediante los servicios de dominio inalámbrico (WDS) y se pueden administrar mediante el motor de soluciones de LAN inalámbricas (WLSE) CiscoWorks.

**Nota:** un router doméstico es un ejemplo de un AP autónomo, ya que toda la configuración del AP reside en el dispositivo.

En la figura 1, se muestra un AP autónomo en una red pequeña. Si aumentaran las demandas inalámbricas, se requerirían más AP. Cada AP funcionaría de manera independiente de los otros AP y requeriría una configuración y una administración manuales.

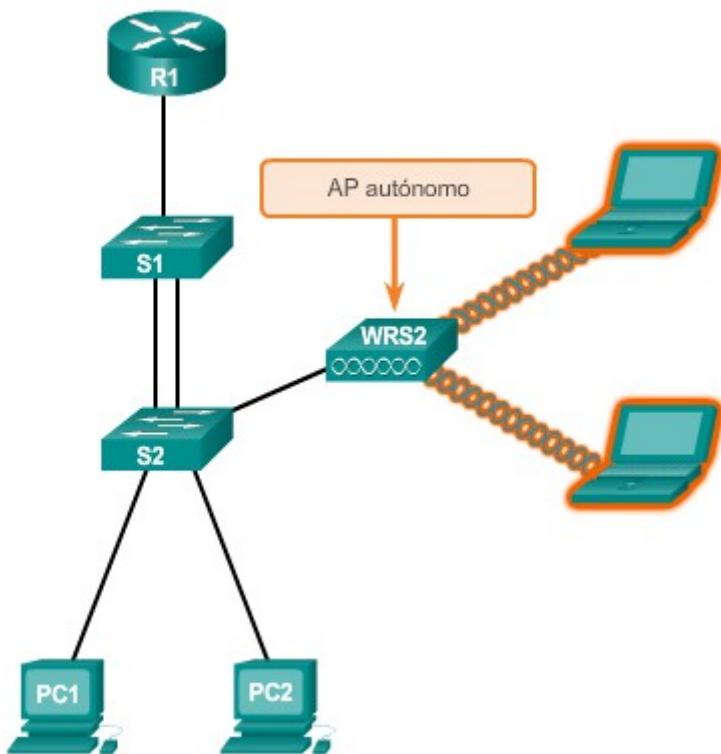
##### **AP basados en controladores**

Los AP basados en controladores son dispositivos que dependen del servidor y no requieren una configuración inicial. Cisco ofrece dos soluciones basadas en controladores. Los AP basados en controladores son útiles en situaciones en las que se requieren muchos AP en la red. A medida que se agregan más AP, un controlador de WLAN configura y administra cada AP automáticamente.

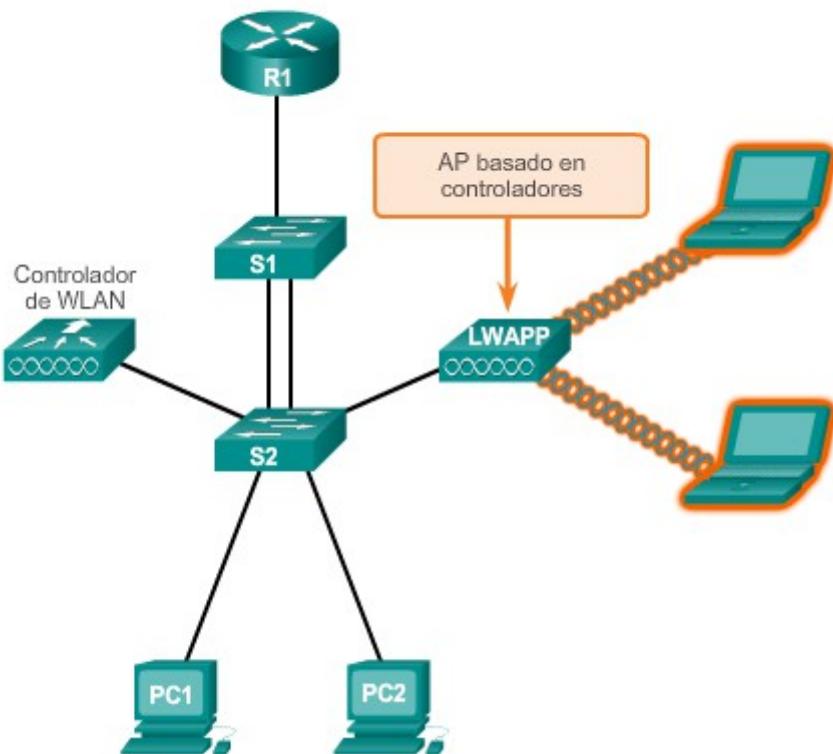
En la figura 2, se muestra un AP basado en controladores en una red pequeña. Observe cómo ahora se requiere un controlador de WLAN para administrar los AP. El beneficio del controlador es que se puede usar para administrar muchos AP.

**Nota:** algunos modelos de AP pueden funcionar en modo autónomo o en modo basado en controladores.

**AP autónomo**



**AP basado en controladores**



#### Capítulo 4: LAN inalámbricas 4.1.2.5 Soluciones de implementación de tecnología inalámbrica

##### a pequeña escala

Para los requisitos de implementación de tecnología inalámbrica a pequeña escala, Cisco ofrece las siguientes soluciones de AP autónomos inalámbricos:

- **AP Cisco WAP4410N:** este AP es ideal para una organización pequeña que requiere dos AP y admite un grupo pequeño de usuarios.
- **AP Cisco WAP121 y WAP321:** estos AP son ideales para las organizaciones pequeñas que desean simplificar su implementación de tecnología inalámbrica mediante varios AP.
- **AP Cisco AP541N:** este AP es ideal para las organizaciones pequeñas y medianas que desean un grupo de AP sólido y fácil de administrar.

**Nota:** la mayoría de los AP de nivel empresarial admiten alimentación por Ethernet.

En la figura 1, se muestran y se resumen los AP Cisco para pequeñas empresas.

En la figura 2, se muestra una topología de ejemplo para la red de una pequeña empresa con AP WAP4410N. Cada AP se configura y se administra individualmente. Esto puede ser un problema cuando se requieren varios AP.

Por este motivo, los AP WAP121, WAP321 y AP541N admiten la agrupación de AP en clústeres sin el uso de un controlador. El clúster proporciona un único punto de administración y permite que el administrador vea la implementación de los AP como una única red inalámbrica, en lugar de una serie de dispositivos inalámbricos separados. La capacidad de agrupación facilita la configuración y la administración de una red inalámbrica en expansión. Se pueden implementar varios AP a fin de insertar una única configuración para todos los dispositivos dentro del clúster y administrar la red inalámbrica como un único sistema, sin preocuparse por la interferencia entre los AP y sin configurar cada AP como un dispositivo separado.

Especificamente, el WAP121 y el WAP321 admiten la configuración de punto único (SPS), que hace que la implementación del AP sea más fácil y rápida, como se muestra en la figura 3. SPS permite que la LAN inalámbrica escale hasta cuatro dispositivos WAP121 y ocho dispositivos WAP321 para proporcionar una cobertura más amplia y admitir usuarios adicionales a medida que cambian y crecen las necesidades comerciales. El AP Cisco AP541N puede agrupar hasta 10 AP y puede admitir varios clústeres.

Se puede formar un clúster entre dos AP si se cumplen las siguientes condiciones:

- El modo de agrupación en clústeres está habilitado en los AP.
- Los AP que se unen al clúster tienen el mismo nombre de clúster.
- Los AP se conectan al mismo segmento de red.
- Los AP usan el mismo modo de radio (es decir, ambas radios usan 802.11n).

Acceda a un [emulador](#) de AP541N en línea.

### AP autónomos Cisco para pequeñas empresas



#### Cisco WAP4410N

- AP básico para pequeñas empresas.
- Configurado mediante una GUI
- Alimentación por Ethernet o CA



#### Cisco WAP121 y WAP321

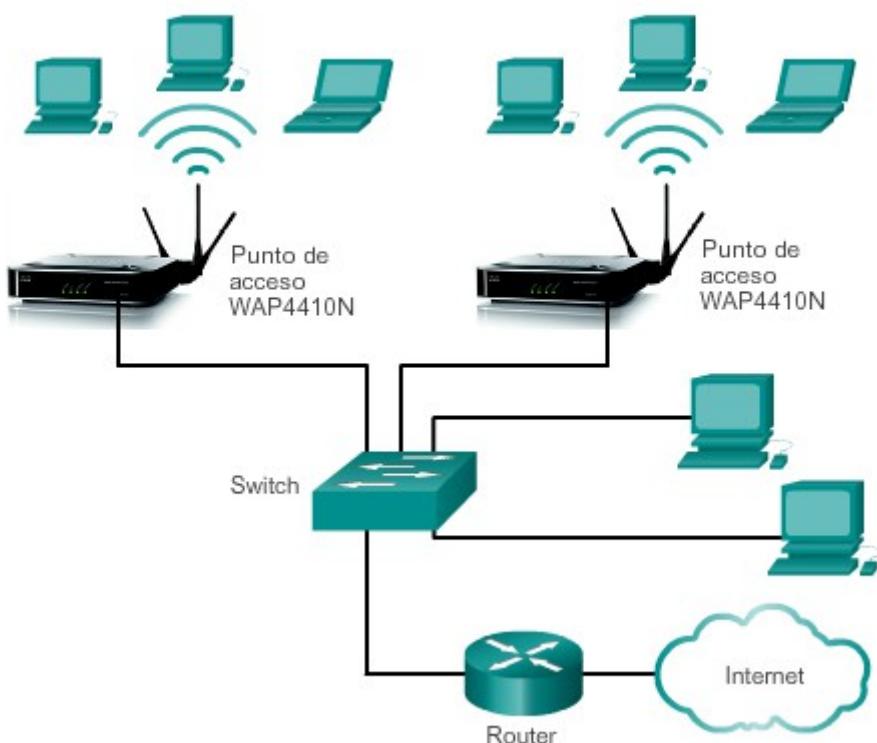
- AP de pequeña empresa de nivel medio
- Se configura y se administra mediante una GUI o una CLI.
- Admite la agrupación en clústeres con configuración de punto único.
- Alimentación por Ethernet o CA



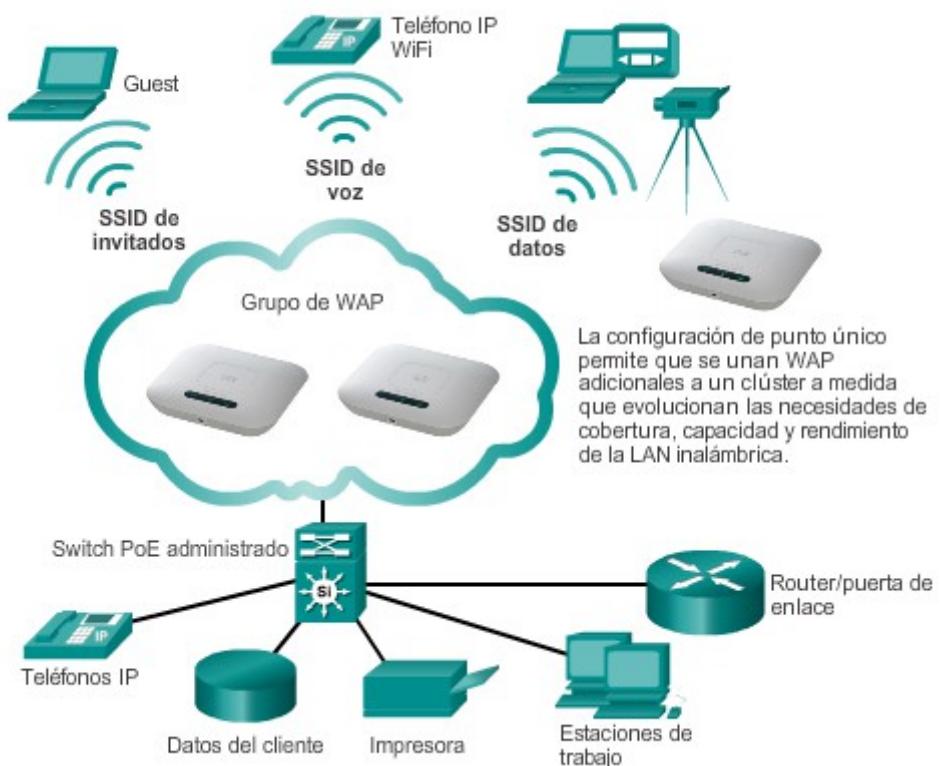
#### Cisco AP541N

- AP de pequeña empresa de nivel medio
- Configurado mediante una GUI
- Admite la tecnología de agrupación en clústeres sin controladores.
- Alimentación por Ethernet o CA

### WLAN simple con AP WAP4410N



### WLAN simple con clúster de AP WAP321



## Capítulo 4: LAN inalámbricas 4.1.2.6 Soluciones de implementación de tecnología inalámbrica

### a gran escala

Las organizaciones que requieren la agrupación en clústeres de varios AP necesitan una solución más sólida y escalable. Para las organizaciones más grandes con muchos AP, Cisco proporciona soluciones basadas en controladores, que incluyen la arquitectura administrada a través de la nube Cisco Meraki y la arquitectura de red inalámbrica Cisco Unified.

**Nota:** existen otras soluciones basadas en controladores, como los controladores que usan el modo Flex. Visite<http://www.cisco.com> para obtener más información.

### **Arquitectura administrada a través de la nube Cisco Meraki**

La arquitectura de la nube Cisco Meraki es una solución de administración utilizada para simplificar la implementación de la tecnología inalámbrica. Con esta arquitectura, los AP se administran de forma centralizada desde un controlador en la nube, como se muestra en la figura 1. Las redes y la administración a través de la nube proporcionan una administración, una visibilidad y un control centralizados, sin el costo y la complejidad de aparatos controladores o de un software de administración de superposición.

Este proceso reduce los costos y la complejidad. El controlador inserta la configuración de administración, como las actualizaciones de firmware, la configuración de seguridad, la red inalámbrica y la configuración de SSID en los AP Meraki.

**Nota:** solo los datos de administración fluyen a través de la infraestructura de la nube Meraki. El tráfico de usuarios no pasa a través de los centros de datos de Meraki. Por lo tanto, si Cisco Meraki no puede acceder a la nube, la red continúa funcionando con normalidad. Esto significa que los usuarios todavía pueden autenticar, que las reglas de firewall siguen vigentes y que el tráfico fluye a la máxima velocidad de línea. Solo se interrumpen las funciones de administración, como los informes y las herramientas de configuración.

La arquitectura administrada a través de la nube Cisco Meraki requiere lo siguiente:

- **AP inalámbricos administrados a través de la nube Cisco MR:** existen varios modelos para abordar las variadas opciones de implementación de la tecnología inalámbrica.
- **Controlador en la nube Meraki (MCC):** el MCC proporciona una administración, una optimización y un monitoreo centralizados del sistema WLAN Meraki. El MCC no es un aparato que se deba adquirir e instalar para administrar los AP inalámbricos. En cambio, el MCC es un servicio basado en la nube que constantemente monitorea, optimiza e informa el comportamiento de la red.
- **Tablero basado en Web:** el tablero de Meraki basado en Web realiza la configuración y el diagnóstico de manera remota.

Haga clic en cada componente de la figura 2 para leer más información sobre la arquitectura Cisco Meraki.

#### **AP inalámbrico administrado mediante la nube**



#### Puntos de acceso inalámbrico administrados mediante la nube MR



## AP inalámbricos MR12, MR16 y MR24 administrados mediante la nube



## Controlador en la nube Meraki (MCC)



## AP inalámbricos MR62 y MR66 administrados mediante la nube

## Capítulo 4: LAN inalámbricas 4.1.2.7 Soluciones de implementación de tecnología inalámbrica a gran escala (cont.)

## Arquitectura de Cisco Unified Wireless Network

La solución de la arquitectura de red inalámbrica Cisco Unified, que utiliza un diseño MAC dividido, controla los AP mediante un controlador de WLAN (WLC) y se puede administrar de manera optativa mediante los sistemas de control inalámbrico (WCS) de Cisco. Los AP ligeros se comunican con el controlador de WLAN mediante el protocolo de punto de acceso ligero (LWAPP). El controlador tiene toda la inteligencia para la comunicación, y el AP es una "terminal no inteligente" que simplemente procesa paquetes.

La arquitectura de red inalámbrica Cisco Unified requiere los siguientes dispositivos:

- **AP ligeros:** los modelos de AP inalámbricos Cisco Aironet 1600, 2600 o 3600 proporcionan acceso de red inalámbrica confiable y sólido para los hosts.
- **Controladores para las pequeñas y medianas empresas:** los controladores inalámbricos de la serie 2500, el controlador inalámbrico virtual o el módulo de controladores inalámbricos Cisco para ISR G2 de Cisco proporcionan implementaciones de WLAN con conexión inalámbrica básica para datos a una sucursal pequeña de una empresa o a una empresa con un único sitio.

También existen controladores WLAN de mayor capacidad. Por ejemplo, el controlador inalámbrico Cisco 5760 y el controlador Cisco de la serie 8500 se diseñaron para administrar, proteger y optimizar de forma rentable el rendimiento de las redes inalámbricas grandes, como las implementaciones de un proveedor de servicios o un campus grande.

En la figura 1, se resumen los AP ligeros.

Haga clic en cada componente de la figura 2 para mostrar más información sobre los controladores para pequeñas y medianas empresas.

## AP inalámbricos basados en controladores



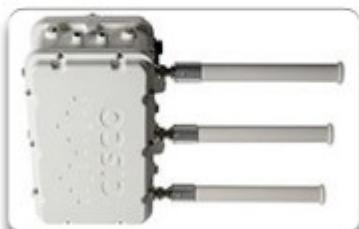
### Series Cisco Aironet 1600, 2600 y 3600

AP robustos basados en controladores



### Serie Cisco Aironet 600 OfficeExtend

Utilizados para extender la cobertura inalámbrica 802.11n al entorno de trabajo desde el hogar



### AP robustos para exteriores serie Cisco 1552

AP robusto para exteriores basado en controladores

## Controladores para pequeñas y medianas empresas



Cisco Virtual Controller



Controlador inalámbrico de Cisco en Cisco Services Ready Engine (SRE)



Routers Cisco de la serie 2500

La mayoría de los AP de clase empresarial requieren el uso de antenas externas para convertirlas en unidades de funcionamiento pleno. Cisco desarrolló antenas diseñadas específicamente para usar con AP 802.11 y que admiten condiciones de implementación específicas, incluidas la disposición física, la distancia y la estética.

Los AP Cisco Aironet pueden usar lo siguiente:

- **Antenas Wi-Fi omnidireccionales:** con frecuencia, el engranaje Wi-Fi de fábrica usa antenas dipolos básicas, conocidas como “antenas de goma”, similares a aquellas usadas en las radios walkie-talkie. Las antenas omnidireccionales proporcionan cobertura de 360° y son ideales para áreas de oficinas abiertas, pasillos, salas de conferencias y exteriores.
- **Antenas Wi-Fi direccionales:** las antenas direccionales concentran la señal de radio en un sentido determinado. Esto mejora la señal desde y hasta el AP en el sentido que apunta la antena, lo que proporciona una mayor potencia de señal en un sentido, así como una menor potencia de señal en todos los demás sentidos.
- **Antenas Yagi:** son un tipo de antena de radio direccional que se puede usar para las redes Wi-Fi de larga distancia. Normalmente, estas antenas se usan para extender el alcance de las zonas de cobertura exteriores en un sentido específico o para llegar a un edificio externo.

En la ilustración, se muestran diversas antenas Cisco de interiores y exteriores.

Los estándares IEEE 802.11n/ac/ad usan la tecnología MIMO para aumentar el ancho de banda disponible. Específicamente, MIMO usa varias antenas para intercambiar más datos de los que sería posible intercambiar mediante una única antena. Se pueden usar hasta cuatro antenas para aumentar el rendimiento.

**Nota:** no todos los routers inalámbricos son iguales. Por ejemplo, los routers 802.11n básicos admiten un ancho de banda de 150 Mb/s mediante el alcance Wi-Fi y una antena conectada a la unidad. Para admitir velocidades de datos superiores, los routers 802.11n requieren más radios y antenas para administrar más canales de datos en paralelo. Por ejemplo, dos radios y dos antenas en un router 802.11n admiten hasta 300 Mb/s, mientras que para las velocidades de 450 Mb/s y 600 Mb/s se requieren tres y cuatro radios y antenas, respectivamente.

Capítulo 4: LAN inalámbricas 4.1.2.9 Actividad: Identificar la terminología de los componentes

de WLAN

**Actividad: Identificar la terminología de los componentes de WLAN**  
Arrastra cada término relacionado con la tecnología de LAN inalámbrica hasta la definición correspondiente.



#### Capítulo 4: LAN inalámbricas 4.1.2.10 Práctica de laboratorio: Investigación de

#### implementaciones inalámbricas

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: Explorar los routers inalámbricos integrados
- Parte 2: Explorar los puntos de acceso inalámbrico

#### Práctica de laboratorio: Investigación de implementaciones inalámbricas

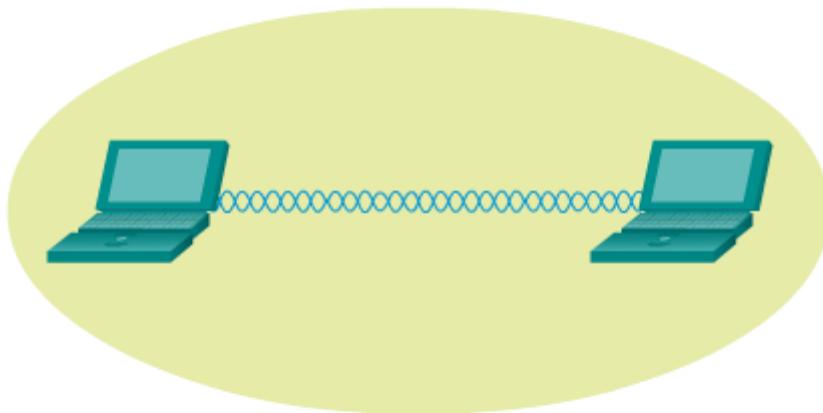
#### Capítulo 4: LAN inalámbricas 4.1.3.1 Modos de topología inalámbrica 802.11

Las LAN inalámbricas pueden utilizar diferentes topologías de red. El estándar 802.11 identifica dos modos principales de topología inalámbrica:

- Modo ad hoc:** cuando dos dispositivos se conectan de manera inalámbrica sin la ayuda de un dispositivo de infraestructura, como un router o un AP inalámbrico. Los ejemplos incluyen Bluetooth y Wi-Fi Direct.
- Modo de infraestructura:** cuando los clientes inalámbricos se conectan mediante un router o un AP inalámbrico, como en las WLAN. Los AP se conectan a la infraestructura de la red mediante el sistema de distribución (DS) conectado por cable, como Ethernet.

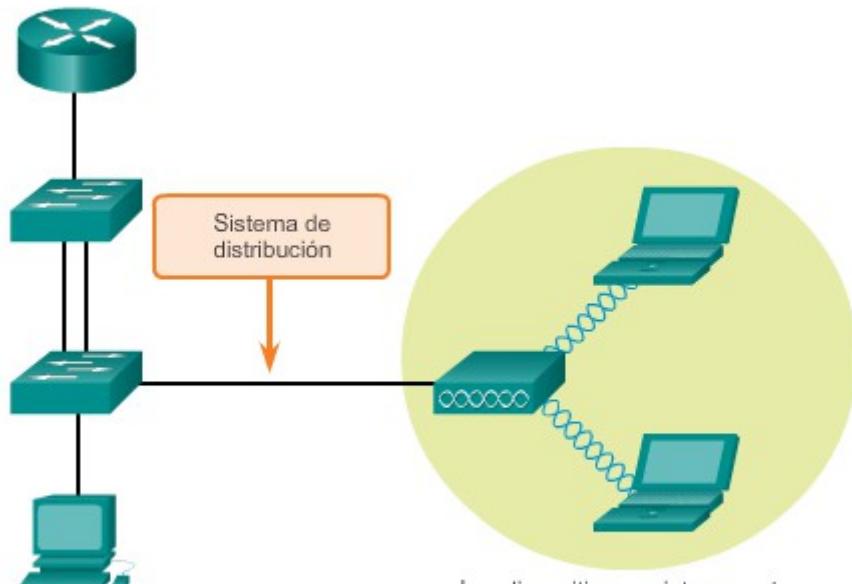
En la figura 1, se muestra un ejemplo de modo ad hoc, y en la figura 2, se muestra un ejemplo de modo de infraestructura.

### Modo ad hoc



Los dispositivos se interconectan directamente sin el uso de un AP o router inalámbrico.

### Modo infraestructura



Los dispositivos se interconectan mediante los servicios de un AP o router inalámbrico.

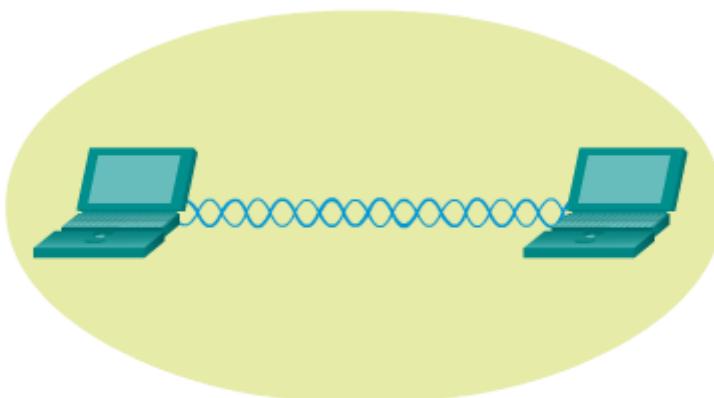
Existe una red inalámbrica ad hoc cuando dos dispositivos inalámbricos se comunican de manera peer-to-peer (P2P) sin usar AP o routers inalámbricos. Por ejemplo, se puede configurar la estación de trabajo de un cliente con capacidad inalámbrica para que funcione en modo ad hoc, lo que permite que se conecte otro dispositivo a la estación. Bluetooth y Wi-Fi Direct son ejemplos de modo ad hoc.

**Nota:** el estándar IEEE 802.11 denomina a las redes ad hoc “conjunto de servicios básicos independientes” (IBSS).

En la ilustración, se muestra un resumen del modo ad hoc.

Existe una variación de la topología ad hoc cuando se permite que un smartphone o una tablet PC con acceso celular a datos cree una zona de cobertura inalámbrica personal. En ocasiones, esta característica se denomina “anclaje a red”. Por lo general, una zona de cobertura inalámbrica es una solución temporal rápida que permite que un smartphone proporcione los servicios inalámbricos de un router Wi-Fi. Otros dispositivos se asocian y autentican con el smartphone para usar la conexión a Internet. El iPhone de Apple denomina a esta característica “Compartir Internet”, mientras que los dispositivos con Android la denominan “Anclaje a red y zona de cobertura portátil”.

#### Resumen del modo ad hoc



#### Resumen de IBSS

Modo de topología WLAN	Ad hoc
Topología inalámbrica 802.11	BSS independiente
Cantidad de AP	Ninguno
Área de cobertura de 802.11	Área de servicios básicos (BSA)

#### Capítulo 4: LAN inalámbricas 4.1.3.3 Modo infraestructura

La arquitectura IEEE 802.11 consta de varios componentes que interactúan para proporcionar una WLAN que admite clientes. Define dos componentes básicos de la topología del modo de infraestructura: un conjunto de servicios básicos (BSS) y un conjunto de servicios extendidos (ESS).

#### Conjunto de servicios básicos

Un BSS consta de un único AP que interconecta todos los clientes inalámbricos asociados. En la figura 1, se muestran dos BSS. Los círculos representan el área de cobertura dentro de la que los clientes inalámbricos del BSS pueden permanecer comunicados. Esta área se denomina “área de servicios básicos” (BSA). Si un cliente inalámbrico sale de su BSA, ya no se puede comunicar directamente con otros clientes inalámbricos dentro de la BSA. El BSS es el componente básico de la topología, mientras que la BSA es el área de cobertura real (los términos BSA y BSS a menudo se usan de manera indistinta).

La dirección MAC de capa 2 del AP se usa para identificar de forma exclusiva cada BSS y se denomina “identificador del conjunto de servicios básicos” (BSSID). Por lo tanto, el BSSID es el nombre formal del BSS y siempre se asocia a un único AP.

### **Conjunto de servicios extendidos**

Cuando un único BSS proporciona una cobertura de RF insuficiente, se pueden unir dos o más BSS a través de un sistema de distribución (DS) común para formar un ESS. Como se muestra en la figura 2, un ESS es la unión de dos o más BSS interconectados mediante un DS por cable. Los clientes inalámbricos en una BSA ahora se pueden comunicar con los clientes inalámbricos en otra BSA dentro del mismo ESS. Los clientes con conexión inalámbrica móvil se pueden trasladar de una BSA a otra (dentro del mismo ESS) y se pueden conectar sin inconvenientes.

El área rectangular representa el área de cobertura dentro de la que los miembros de un ESS se pueden comunicar. Esta área se denomina “área de servicios extendidos” (ESA). Una ESA a menudo involucra varios BSS en configuraciones superpuestas o separadas.

Cada ESS se identifica mediante un SSID y, en un ESS, cada BSS se identifica mediante su BSSID. Por motivos de seguridad, se pueden propagar SSID adicionales a través del ESS para segregar el nivel de acceso a la red.

**Nota:** el estándar 802.11 denomina IBSS al modo ad hoc.

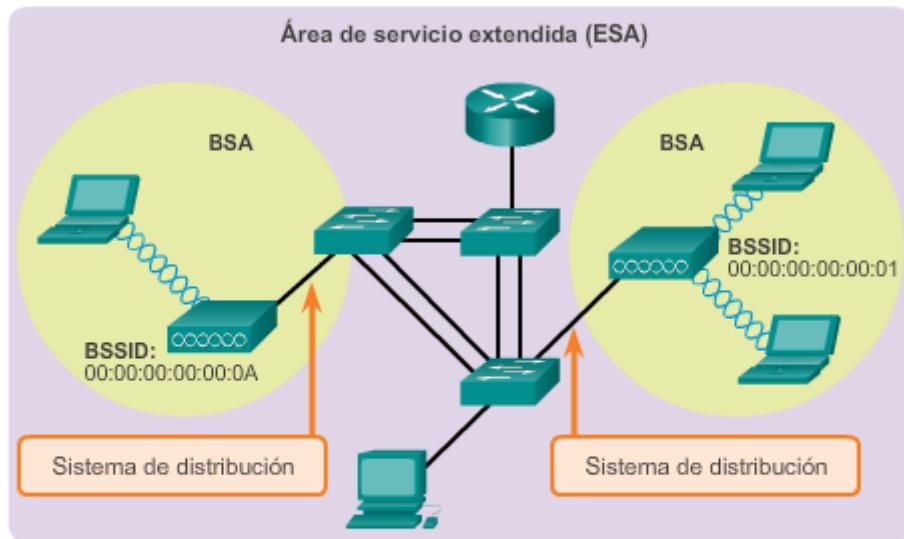
## Resumen del conjunto de servicios básicos



### Resumen de BSS

Modo de topología WLAN	Infraestructura
Topología inalámbrica 802.11	conjunto de servicios básicos (BSS)
Cantidad de AP	1
Área de cobertura de 802.11	Área de servicios básicos (BSA)

## Resumen del conjunto de servicios extendidos



### Resumen de ESS

Modo de topología WLAN	Infraestructura
Topología inalámbrica 802.11	conjunto de servicios extendidos (ESS)
Cantidad de AP	2 o más
Área de cobertura de 802.11	Área de servicio extendida (ESA)

#### Capítulo 4: LAN inalámbricas 4.1.3.4 Actividad: Identificar la terminología de la topología WLAN

##### **Actividad: Unir los términos relacionados con la topología 802.11**

Arrastre los términos relacionados con WLAN hasta los campos correspondientes para completar la tabla. Algunas respuestas se pueden usar más de una vez.

Componente básico de la topología WLAN	Modo	Cantidad de puntos de acceso (AP)	Área de cobertura inalámbrica
Conjunto de servicios extendidos (ESS)	Infraestructura	2 o más	Área de servicio extendida (ESA)
conjunto de servicios básicos (BSS)	Infraestructura	1	Área de servicios básicos (BSA)
Conjunto de servicios básicos independientes (IBSS)	Ad hoc	0	Área de servicios básicos (BSA)

#### Capítulo 4: LAN inalámbricas 4.2.1.1 Trama 802.11 inalámbrica

Todas las tramas de capa 2 constan de un encabezado, un contenido y una sección FCS, como se muestra en la figura 1. El formato de la trama 802.11 es similar al formato de la trama de Ethernet, con la excepción de que contiene más campos.

Como se muestra en la figura 2, todas las tramas 802.11 inalámbricas contienen los siguientes campos:

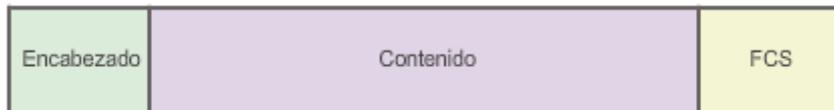
- **Control de trama:** identifica el tipo de trama inalámbrica y contiene subcampos para la versión del protocolo, el tipo de trama, el tipo de dirección, la administración de energía y la configuración de seguridad.
- **Duración:** en general, se usa para indicar la duración restante necesaria para recibir la siguiente transmisión de tramas.
- **Dirección 1:** normalmente, contiene la dirección MAC del dispositivo o AP receptor inalámbrico.
- **Dirección 2:** normalmente, contiene la dirección MAC del dispositivo o AP transmisor inalámbrico.
- **Dirección 3:** en ocasiones, contiene la dirección MAC del destino, como la interfaz del router (gateway predeterminado) a la que se conecta el AP.
- **Control de secuencia:** contiene los subcampos Número de secuencia y Número de fragmento. El Número de secuencia indica el número de secuencia de cada trama. El Número de fragmento indica el número de cada trama que se envió de una trama fragmentada.
- **Dirección 4:** suele faltar, ya que se usa solo en el modo ad hoc.
- **Contenido:** contiene los datos para la transmisión.

- **FCS:** es la Secuencia de verificación de trama, usada para el control de errores de capa 2.

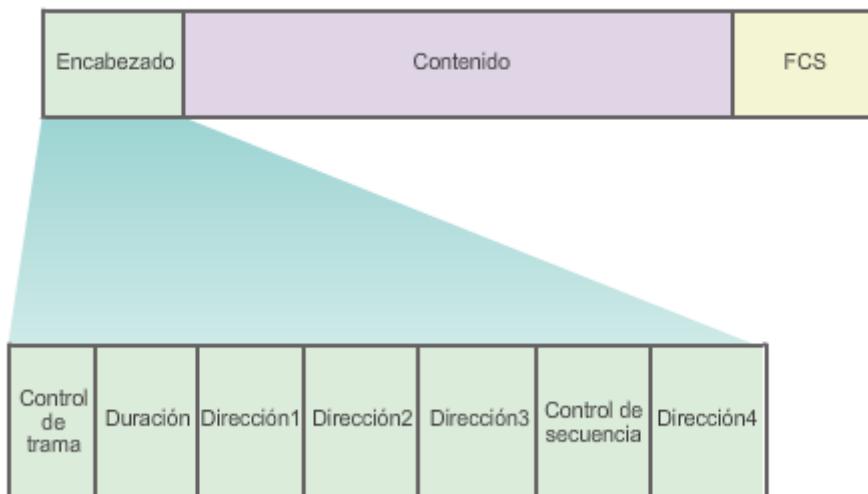
En la figura 3, se muestra una captura de Wireshark de una trama de señal WLAN. Observe que el campo Control de trama también se expandió para mostrar sus subcampos.

**Nota:** el contenido de los campos Dirección varía según la configuración en el campo Control de trama.

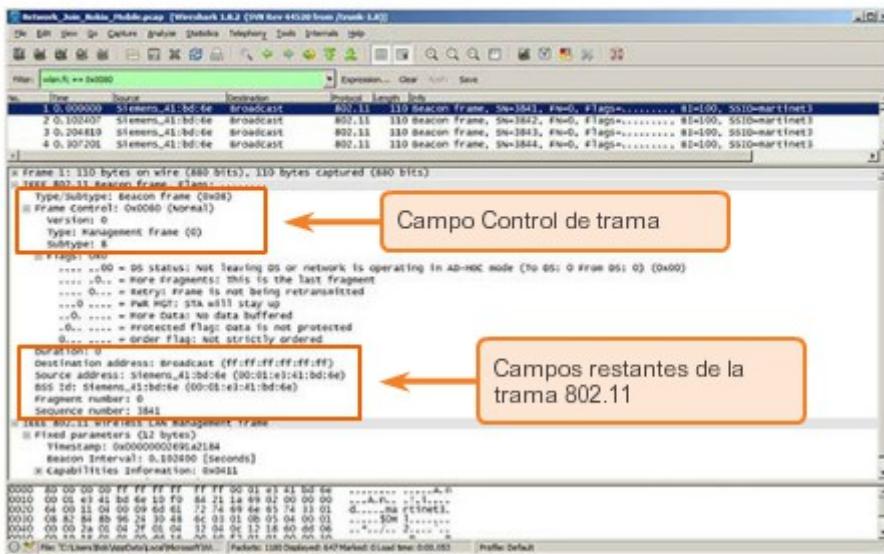
### Trama genérica



### Contenido del encabezado de la trama 802.11 inalámbrica



## Captura de Wireshark de una trama 802.11



### Capítulo 4: LAN inalámbricas 4.2.1.2 Campo Control de trama

El campo Control de trama contiene varios subcampos, como se muestra en la figura 1.

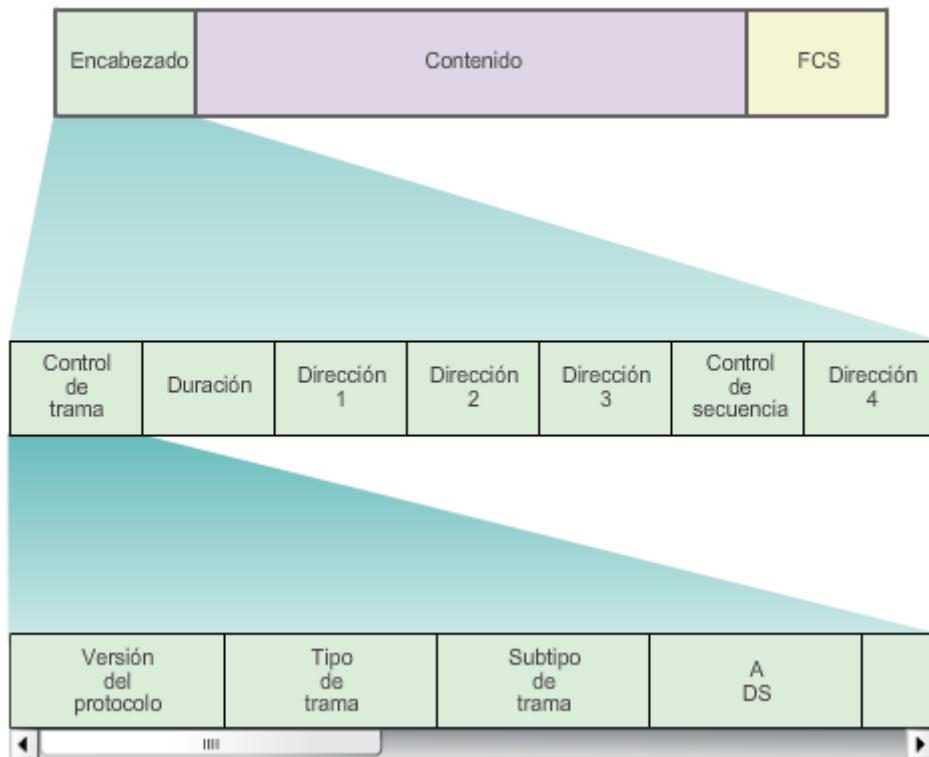
Especificamente, el campo Control de trama contiene los siguientes subcampos:

- **Versión del protocolo:** proporciona la versión actual del protocolo 802.11 que se usa. Los dispositivos receptores usan este valor para determinar si se admite la versión del protocolo de la trama recibida.
- **Tipo de trama y Subtipo de trama:** determinan la función de la trama. Una trama inalámbrica puede ser una trama de control, una trama de datos o una trama de administración. Existen varios campos de subtipos para cada tipo de trama. Cada subtipo determina la función específica que debe realizar el tipo de trama asociado.
- **A DS y De DS:** indican si la trama entra al DS o sale de este, y solo se usan en las tramas de datos de los clientes inalámbricos asociados a un AP.
- **Más fragmentos:** indica si existen más fragmentos de la trama para recibir, ya sean del tipo de datos o de administración.
- **Reintentar:** indica si la trama se vuelve a transmitir o no, ya sean tramas de datos o de administración.
- **Administración de energía:** indica si el dispositivo emisor está en modo activo o en modo de ahorro de energía.

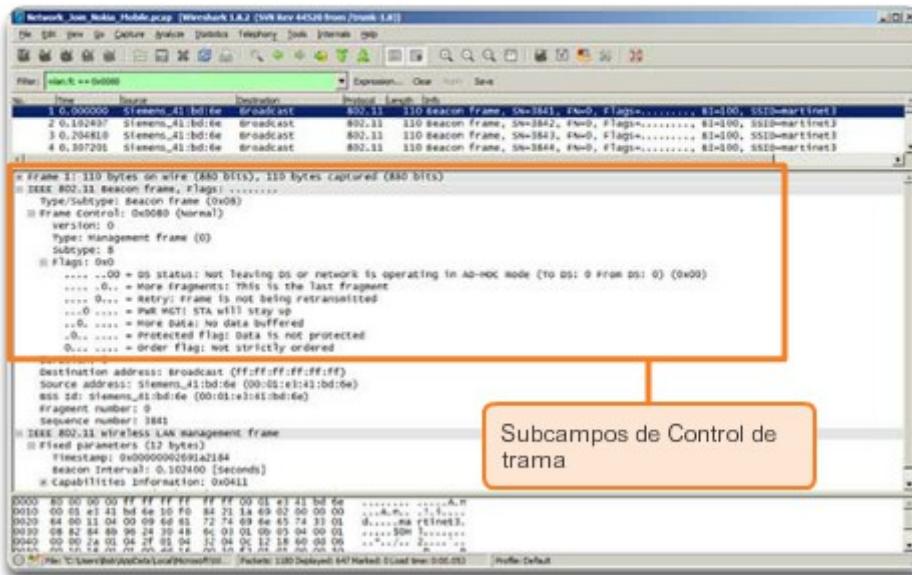
- **Más datos:** indica a un dispositivo en modo de ahorro de energía que el AP tiene más tramas para enviar. Se usa también para que los AP indiquen que existen tramas adicionales de difusión y multidifusión.
- **Seguridad:** indica si se usan el cifrado y la autenticación en la trama. Se puede establecer para todas las tramas de datos y de administración que tienen el subtipo establecido en autenticación.
- **Reservado:** puede indicar que todas las tramas de datos recibidas se deben procesar en orden.

En la figura 2, se muestra una captura de Wireshark de una trama de señal de WLAN. Observe que los campos Tipo de trama y Subtipo de trama identifican si la trama es de administración, de control o de datos. En el ejemplo, el Tipo de trama es “0x0”, lo que la identifica como una trama de administración. El valor de subtipo “8” la identifica como una trama de señal. La trama se identifica específicamente como “0x08”.

#### Contenido del campo Control de trama



## Captura de Wireshark de una trama 802.11

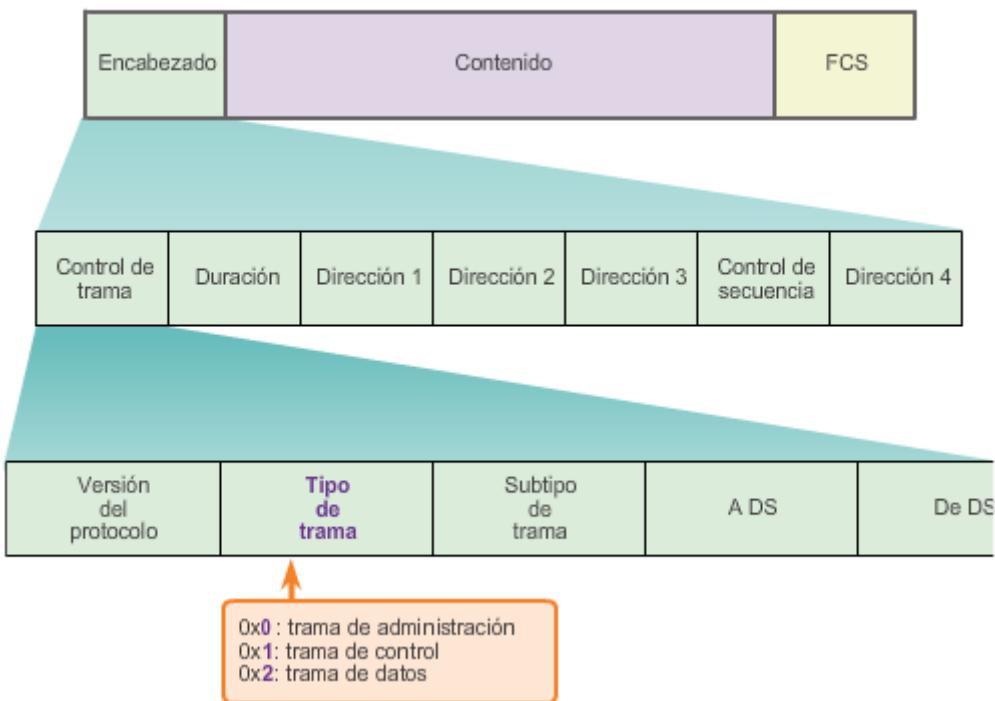


### Capítulo 4: LAN inalámbricas 4.2.1.3 Tipo de trama inalámbrica

ama se usan para identificar el tipo de transmisión inalámbrica. Como se muestra en la ilustración, una trama inalámbrica puede ser uno de tres tipos de trama:

- **Trama de administración:** se utiliza para el mantenimiento de la comunicación, como la detección de un AP, la autenticación de este y la asociación a dicho AP.
- **Trama de control:** se utiliza para facilitar el intercambio de tramas de datos entre clientes inalámbricos.
- **Trama de datos:** se utiliza para transportar la información de contenido, como páginas web y archivos.

### Contenido del campo Control de trama



#### Capítulo 4: LAN inalámbricas 4.2.1.4 Tramas de administración

Las tramas de administración se usan exclusivamente para buscar un AP, autenticarlo y asociarse a este.

En la figura 1, se muestra el valor de campo de las tramas de administración comunes, incluidas las siguientes:

- **Trama de solicitud de asociación:**(0x00) se envía desde un cliente inalámbrico, permite que el AP asigne los recursos y sincronice. La trama transporta información sobre la conexión inalámbrica, incluso las velocidades de datos admitidas y el SSID de la red a la que se quiere asociar el cliente inalámbrico. Si se acepta la solicitud, el AP reserva memoria y establece una ID de asociación para el dispositivo.
- **Trama de respuesta de asociación:**(0x01) se envía desde un AP hasta un cliente inalámbrico, contiene la aceptación o el rechazo de la solicitud de asociación. Si es una aceptación, la trama contiene información como una ID de asociación y las velocidades de datos admitidas.
- **Trama de solicitud de reasociación:**(0x02) un dispositivo envía una solicitud de reasociación cuando sale del alcance del AP al que está asociado actualmente y encuentra otro AP con una señal más intensa. El nuevo AP coordina el reenvío de toda la información que todavía pueda contener el búfer del AP anterior.
- **Trama de respuesta de reasociación:**(0x03) se envía desde un AP, contiene la aceptación o el rechazo de una trama de solicitud de reasociación de un dispositivo. La trama incluye la información requerida para la asociación, como la ID de asociación y las velocidades de datos admitidas.

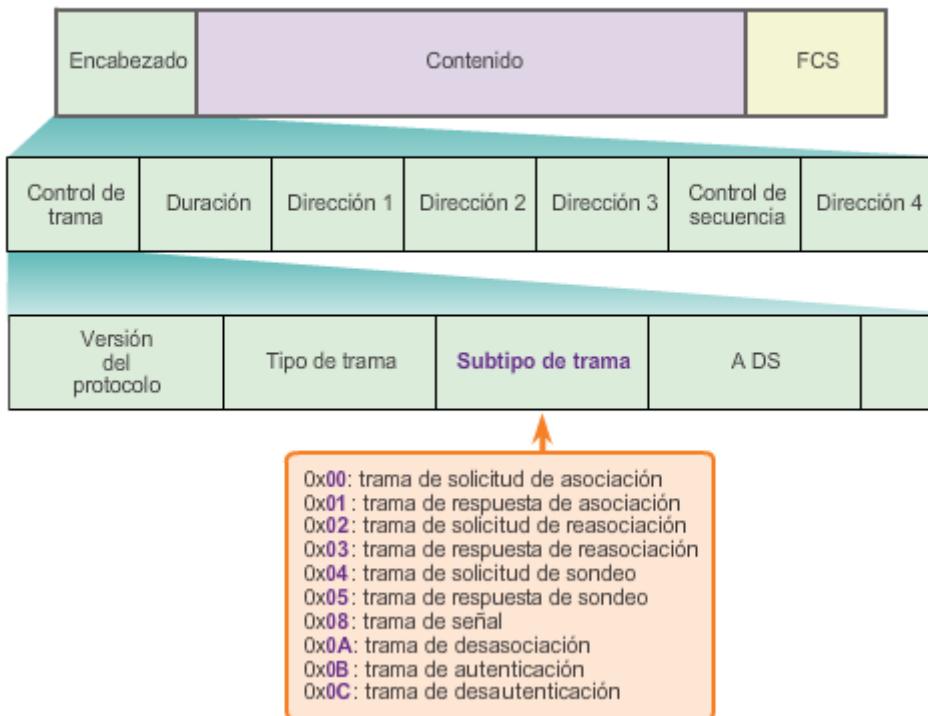
- **Trama de solicitud de sondeo:** (0x04) se envía desde un cliente inalámbrico cuando este requiere información de otro cliente inalámbrico.
- **Trama de respuesta de sondeo:** (0x05) se envía desde un AP después de recibir una trama de solicitud de sondeo y contiene la información de capacidad, como las velocidades de datos admitidas.
- **Trama de señal:** (0x08) se envía periódicamente desde un AP para anunciar su presencia y proporcionar el SSID y otros parámetros configurados con anterioridad.
- **Trama de desasociación:** (0x0A) se envía desde un dispositivo que desea finalizar una conexión. Permite que el AP detenga la asignación de memoria y quite el dispositivo de la tabla de asociación.
- **Trama de autenticación:** (0x0B) el dispositivo emisor envía al AP una trama de autenticación que contiene su identidad.
- **Trama de desautenticación:** (0x0C) se envía desde un cliente inalámbrico que desea finalizar la conexión de otro cliente inalámbrico.

Las señales son las únicas tramas de administración que un AP puede transmitir en forma regular. Todas las demás tramas de sondeo, autenticación y asociación se usan solo durante el proceso de asociación (o reasociación).

En la figura 2, se muestra un ejemplo de una captura de pantalla de Wireshark de una trama de administración. Los valores de campo cambian para reflejar el propósito de la trama.

**Nota:** el ejemplo proporcionado se capturó mediante Wireshark. Sin embargo, Wireshark se debe configurar específicamente para capturar el tráfico de WLAN. La capacidad para capturar el tráfico varía entre los sistemas operativos y puede requerir una NIC inalámbrica especial.

### Contenido de los campos de administración



#### Capítulo 4: LAN inalámbricas 4.2.1.5 Tramas de control

Las tramas de control se usan para administrar el intercambio de información entre un cliente inalámbrico y un AP. Ayudan a evitar las colisiones en un medio inalámbrico.

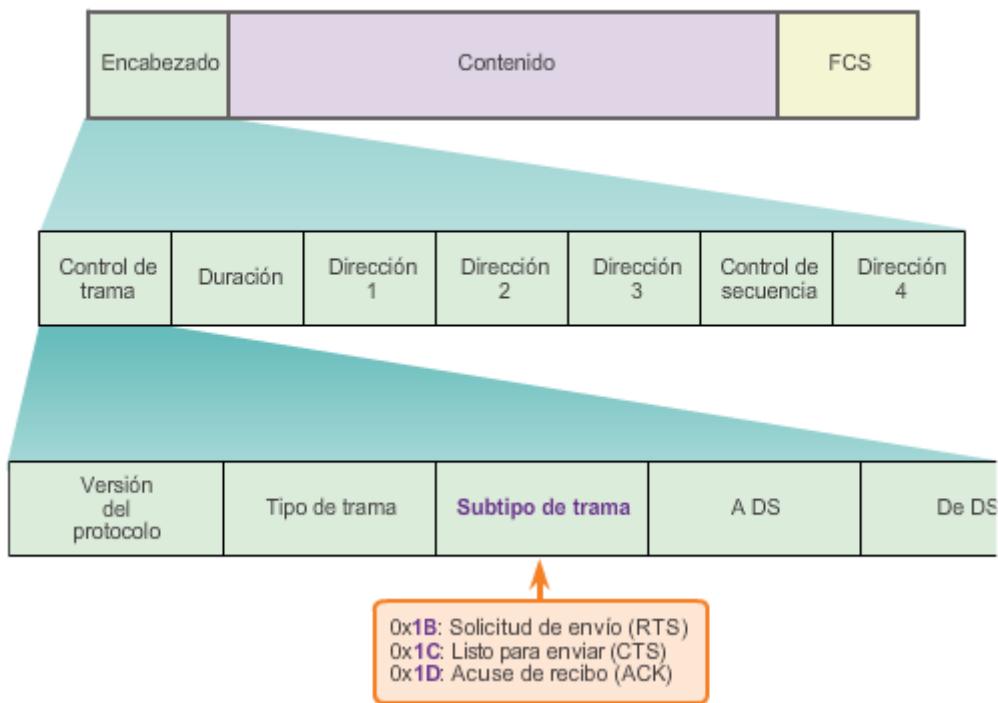
En la ilustración, se muestra el valor de campo de las tramas de control comunes, incluidas las siguientes:

- **Trama de Solicitud de envío (RTS):** las tramas RTS y CTS proporcionan un esquema optativo de reducción de colisiones para los AP con clientes inalámbricos ocultos. Un cliente inalámbrico envía una trama RTS como primer paso en el enlace de dos vías, lo cual se requiere antes de enviar tramas de datos.
- **Trama de Listo para enviar (CTS):** un AP inalámbrico responde a una trama RTS con una trama CTS. Proporciona autorización para que el cliente inalámbrico que realizó la solicitud envíe tramas de datos. La trama CTS contribuye a la administración del control de colisiones al incluir un valor de tiempo. Este retraso minimiza la probabilidad de que otros clientes transmitan mientras lo hace el cliente que realizó la solicitud.
- **Trama de Acuse de recibo (ACK):** después de recibir una trama de datos, el cliente inalámbrico receptor envía una trama ACK al cliente emisor si no se encuentran errores. Si el cliente emisor no recibe una trama ACK en un plazo predeterminado, reenvía la trama.

Las tramas de control son fundamentales para la transmisión inalámbrica y desempeñan una función importante en el método de contienda de los medios que usan las tecnologías

inalámbricas, conocido como “acceso múltiple por detección de portadora y prevención de colisiones” (CSMA/CA).

### Contenido del campo Control de trama

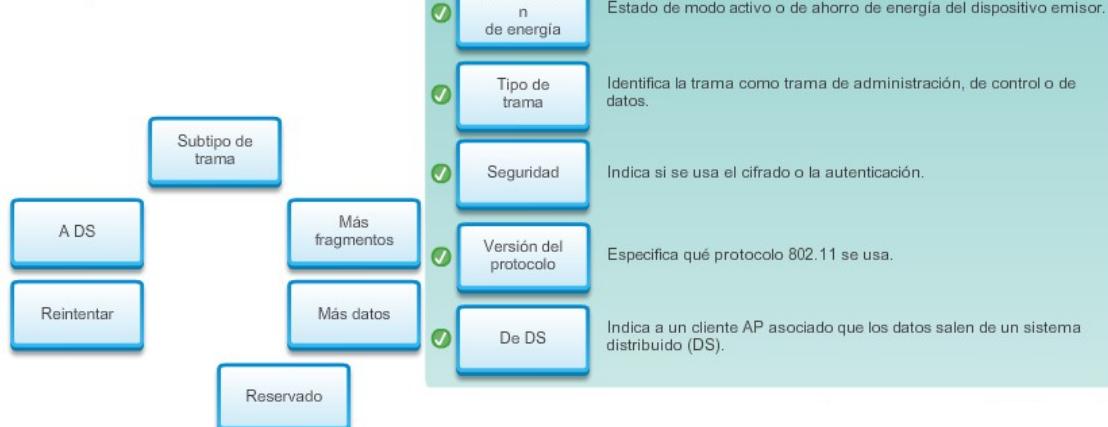


#### Capítulo 4: LAN inalámbricas 4.2.1.6 Actividad: Identificar los campos de Control de

#### trama 802.11

Actividad: Identificar los subcampos de Control de trama 802.11

Arrastra los nombres del subcampo de Control de trama 802.11 hasta las descripciones correspondientes en la tabla. No se utilizan todos los subcampos.



#### Capítulo 4: LAN inalámbricas 4.2.2.1 Acceso múltiple por detección de portadora y prevención

##### de colisiones

Recuerde que el método de contienda de los medios es el método mediante el cual los dispositivos determinan cómo y cuándo acceder a los medios cuando se debe reenviar el tráfico a través de la red. Las WLAN IEEE 802.11 usan el protocolo MAC CSMA/CA. Si bien el nombre es similar al del método CSMA/CD de Ethernet, el concepto operativo es completamente diferente.

Los sistemas Wi-Fi son configuraciones de medios compartidos half-duplex; por lo tanto, los clientes inalámbricos pueden transmitir y recibir en el mismo canal de radio. Esto crea un problema, ya que un cliente inalámbrico no puede oír mientras envía; por lo tanto, no es posible detectar una colisión. Para abordar este problema, el IEEE desarrolló un mecanismo adicional para la prevención de colisiones denominado “función de coordinación distribuida” (DCF). Mediante DCF, un cliente inalámbrico transmite solo si el canal está libre. Todas las transmisiones se confirman; por ello, si un cliente inalámbrico no recibe un acuse de recibo, supone que ocurrió una colisión y lo vuelve a intentar después de un intervalo de espera aleatorio.

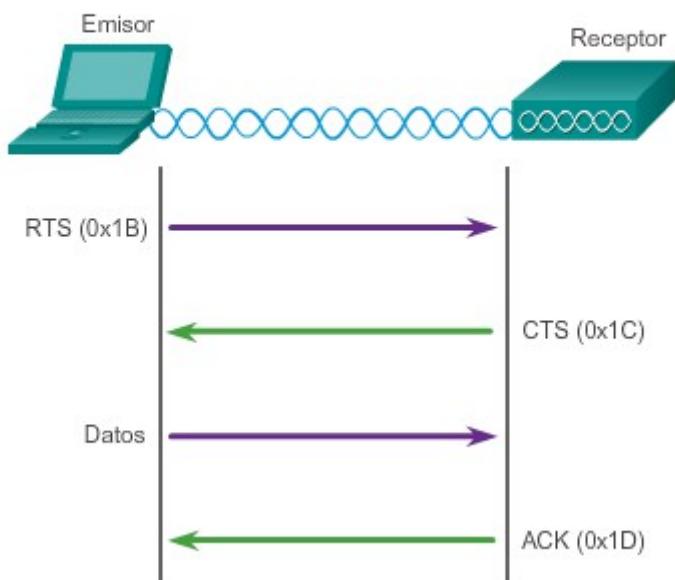
Los clientes inalámbricos y los AP usan las tramas de control RTS y CTS para facilitar la transferencia de datos propiamente dicha.

Como se muestra en la figura 1, cuando un cliente inalámbrico envía datos, primero evalúa los medios para determinar si otros dispositivos los están usando para transmitir. De lo contrario, envía una trama RTS al AP. Esta trama se usa para solicitar acceso dedicado al medio de RF durante un período específico. El AP recibe la trama y, si está disponible, otorga al cliente inalámbrico acceso al medio de RF mediante el envío de una trama CTS de la misma duración. Todos los demás dispositivos inalámbricos que observan la trama CTS ceden los medios al nodo transmisor para la transmisión.

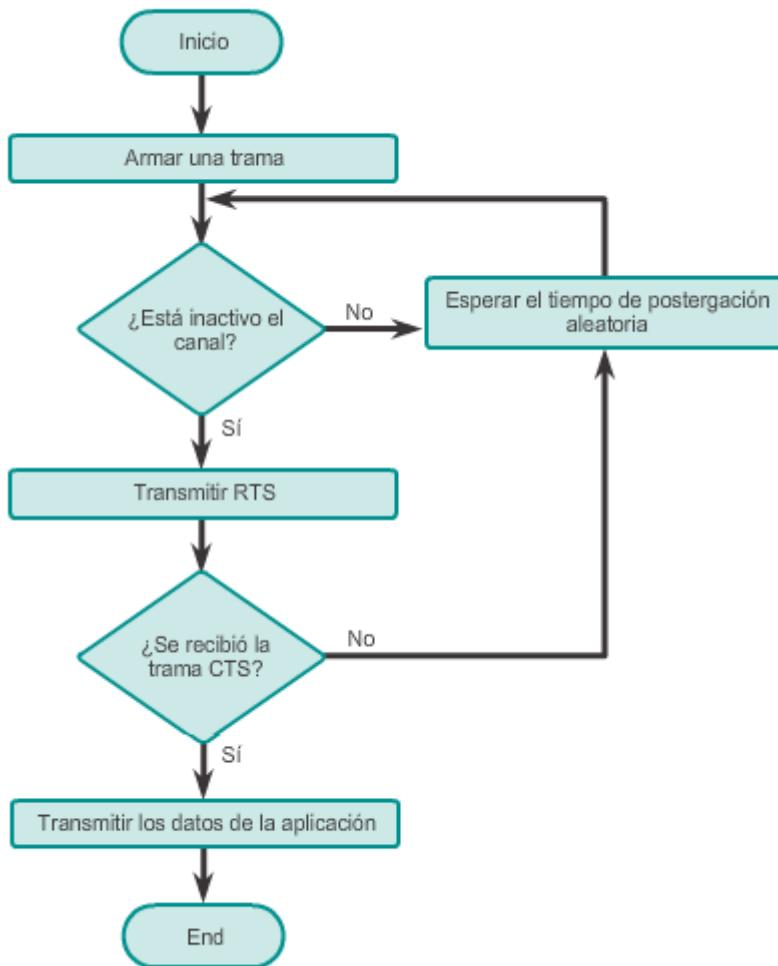
La trama de control CTS incluye el período durante el que se le permite transmitir al nodo transmisor. Otros clientes inalámbricos retienen las transmisiones durante, por lo menos, el período especificado.

En la figura 2, se muestra un diagrama de flujo que detalla el proceso CSMA/CA.

## Uso de las tramas de control para la transferencia de datos



### Diagrama de flujo de CSMA/CA



#### Capítulo 4: LAN inalámbricas 4.2.2.2 Asociación de puntos de acceso y clientes inalámbricos

Para que los dispositivos inalámbricos se comuniquen a través de una red, primero se deben asociar a un AP o un router inalámbrico. Una parte importante del proceso 802.11 es descubrir una WLAN y conectarse a esta.

Los dispositivos inalámbricos usan las tramas de administración para completar el siguiente proceso de tres etapas:

- Descubrir nuevos AP inalámbricos.
- Autenticar con el AP.
- Asociarse al AP.

Para asociarse, un cliente inalámbrico y un AP deben acordar parámetros específicos. Para permitir la negociación de estos procesos, se deben configurar los parámetros en el AP y posteriormente en el cliente.

#### Capítulo 4: LAN inalámbricas 4.2.2.3 Parámetros de asociación

En la figura 1, se muestra la configuración inalámbrica en un router inalámbrico Linksys EA6500. Los parámetros inalámbricos configurables comunes incluyen lo siguiente:

- **SSID:** un SSID es un identificador único que usan los clientes inalámbricos para distinguir entre varias redes inalámbricas en la misma área. El nombre del SSID aparece en la lista de redes inalámbricas disponibles en un cliente. Según la configuración de la red, varios AP en una red pueden compartir un SSID. En general, los nombres tienen una longitud de 2 a 32 caracteres.
- **Password (Contraseña):** el cliente inalámbrico la necesita para autenticarse con el AP. Las contraseñas a veces se denominan “clave de seguridad”. Evita que los intrusos y otros usuarios no deseados accedan a la red inalámbrica.
- **Network mode (Modo de red):** se refiere a los estándares de WLAN 802.11a/b/g/n/ac/ad. Los AP y los routers inalámbricos pueden funcionar en modo Mixed (Mixto), lo que implica que pueden usar varios estándares a la vez.
- **Security mode (Modo de seguridad):** se refiere a la configuración de los parámetros de seguridad, como WEP, WPA o WPA2. Habilite siempre el nivel más alto de seguridad que se admita.
- **Channel settings (Configuración de canales):** se refiere a las bandas de frecuencia que se usan para transmitir datos inalámbricos. Los routers y los AP inalámbricos pueden elegir la configuración de canales, o esta se puede establecer manualmente si existe interferencia con otro AP o dispositivo inalámbrico.

Observe que Linksys EA6500 admite alcances de 2,4 GHz y 5 GHz.

En la figura 2, se muestran las opciones para el modo de red con un alcance de 2,4 GHz. Observe que puede admitir los modos Mixed (Mixto), Wireless-N Only (Solo Wireless-N) o Wireless-G Only (Solo Wireless-G). La configuración Mixed proporciona más flexibilidad, pero también puede lentificar la comunicación. Por ejemplo, si todos los clientes inalámbricos que se conectan al router usan 802.11n, todos disfrutan de las mejores velocidades de datos que se proporcionan. Si un cliente inalámbrico 802.11g se asocia al AP, todos los clientes inalámbricos más rápidos que compiten por el canal deben esperar a que los clientes 802.11g despejen el canal antes de transmitir. Sin embargo, si todos los clientes inalámbricos admiten 802.11n, seleccione Wireless-N Only para lograr el mejor rendimiento.

En la figura 3, se muestran las opciones de Network mode para el alcance de 5 GHz. Observe que también admite la configuración Mixed, junto con la configuración de Wireless-N Only y Wireless-AC Only (Solo Wireless-AC).

Observe que Linksys EA6500 no admite 802.11ad.

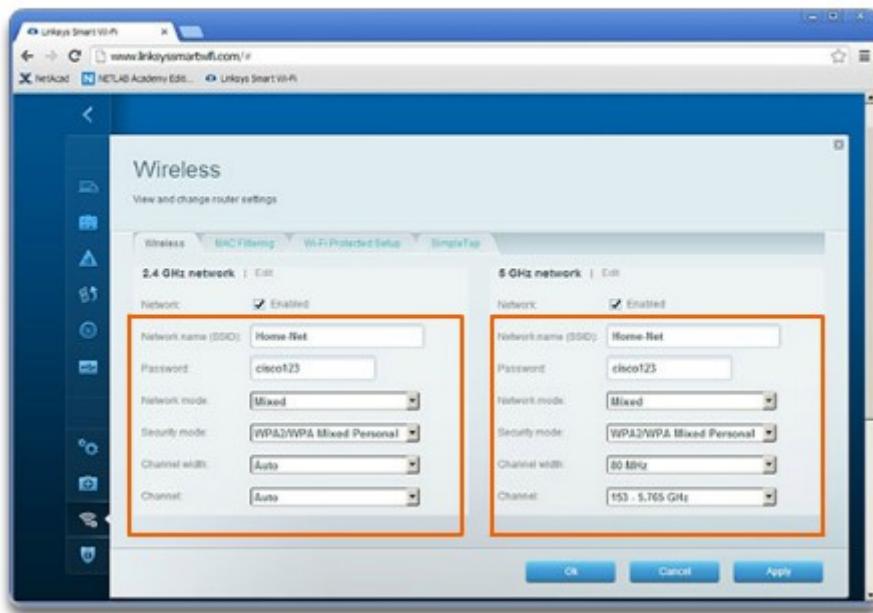
Las opciones de Security que se indican en la figura 4 son opciones de protocolos de seguridad disponibles en el router inalámbrico Linksys EA6500. Los usuarios domésticos deben elegir WPA2/WPA Mixed Personal (WPA2/WPA personal combinado), mientras que los usuarios empresariales normalmente eligen WPA2/WPA Mixed Enterprise (WPA2/WPA empresarial

combinado). El alcance de 5 GHz ofrece las mismas opciones. La terminal inalámbrica también debe admitir la opción de seguridad seleccionada para asociarse.

**Nota:** todos los routers y los AP inalámbricos se deben proteger con la configuración más alta disponible. Se deben evitar las opciones None (Ninguno) o WEP, que solo se deben usar en situaciones en las que la seguridad no es un motivo de preocupación.

En la figura 5, se muestran las opciones de Channel settings para el alcance de 2,4 GHz. La opción preferida es Auto (Automático); sin embargo, si hubiera otros AP u otros dispositivos cercanos que interfirieran en el canal seleccionado por el router, se podría seleccionar un canal específico. Si bien el alcance de 5 GHz también tiene la opción Auto, en el ejemplo, se indica un canal (153) y un ancho de canal específicos.

#### Ventana de configuración inalámbrica



#### Capítulo 4: LAN inalámbricas 4.2.2.4 Detección de AP

Los dispositivos inalámbricos deben detectar un AP o un router inalámbrico y se deben conectar a este. Los clientes inalámbricos se conectan al AP mediante un proceso de análisis (sondeo). Este proceso puede realizarse de los siguientes modos:

- **Modo pasivo:** el AP anuncia abiertamente su servicio al enviar periódicamente tramas de señal de difusión que contienen el SSID, los estándares admitidos y la configuración de seguridad. El propósito principal de la señal es permitir que los clientes inalámbricos descubran qué redes y qué AP existen en un área determinada, de modo que puedan elegir qué red y qué AP usar.
- **Modo activo:** los clientes inalámbricos deben conocer el nombre del SSID. El cliente inalámbrico inicia el proceso al transmitir por difusión una trama de solicitud de sondeo en varios canales. La solicitud de sondeo incluye el nombre del SSID y los estándares

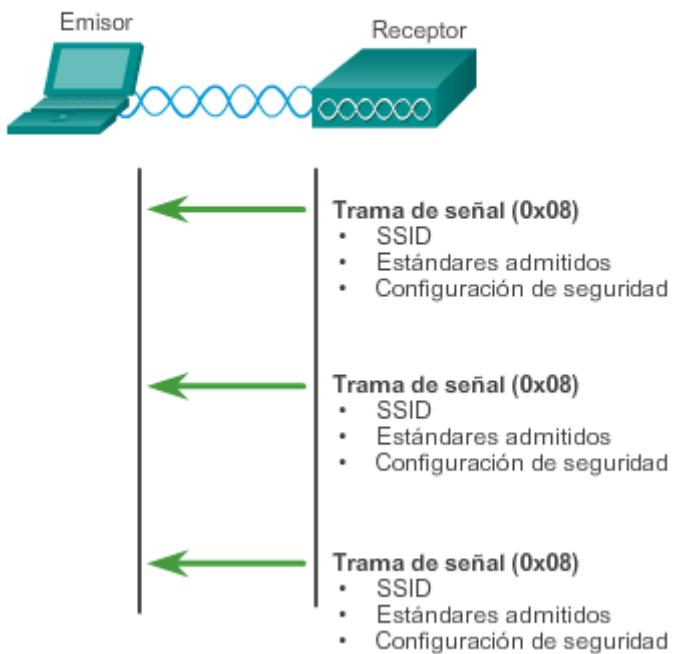
admitidos. Si un AP o un router inalámbrico se configuran para que no transmitan por difusión las tramas de señal, es posible que se requiera el modo activo.

En la figura 1, se muestra cómo funciona el modo pasivo con el AP que transmite por difusión una trama de señal con determinada frecuencia.

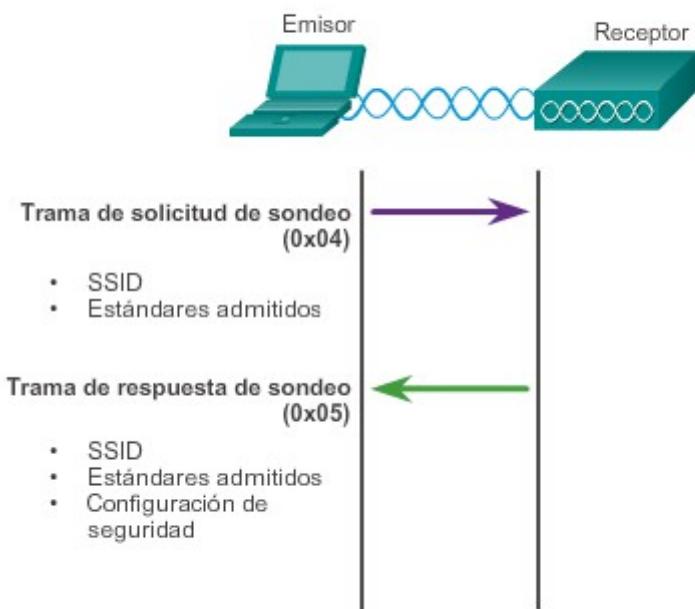
En la figura 2, se muestra cómo funciona el modo activo con un cliente inalámbrico que transmite por difusión una solicitud de sondeo para un SSID específico. El AP con ese SSID responde con una trama de respuesta de sondeo.

Para descubrir las redes WLAN cercanas, un cliente inalámbrico también podría enviar una solicitud de sondeo sin un nombre de SSID. Los AP configurados para transmitir por difusión tramas de señal responderían al cliente inalámbrico con una respuesta de sondeo y proporcionarían el nombre del SSID. Los AP con la característica de transmisión del SSID por difusión deshabilitada no responden.

### **Los dispositivos cliente escuchan un AP**



El AP transmite tramas de señal periódicas por difusión



Capítulo 4: LAN inalámbricas 4.2.2.5 Autenticación

El estándar 802.11 se desarrolló originariamente con dos mecanismos de autenticación:

- **Autenticación abierta:** fundamentalmente, una autenticación NULA donde el cliente inalámbrico dice “autentíqueme” y el AP responde “sí”. La autenticación abierta proporciona conectividad inalámbrica a cualquier dispositivo inalámbrico y se debe usar solo en situaciones donde la seguridad no es un motivo de preocupación.
- **Autenticación de clave compartida:** es una técnica que se basa en una clave previamente compartida entre el cliente y el AP.

En la figura 1, se proporciona una descripción general simple del proceso de autenticación. Sin embargo, en la mayoría de las instalaciones con autenticación mediante clave compartida, el intercambio es el siguiente:

1. El cliente inalámbrico envía una trama de autenticación al AP.
2. El AP responde con un texto de desafío al cliente.
3. El cliente cifra el mensaje mediante la clave compartida y devuelve el texto cifrado al AP.
4. A continuación, el AP descifra el texto cifrado mediante la clave compartida.
5. Si el texto descifrado coincide con el texto de desafío, el AP autentica el cliente. Si los mensajes no coinciden con el texto de desafío, no se autentica el cliente inalámbrico y se deniega el acceso inalámbrico.

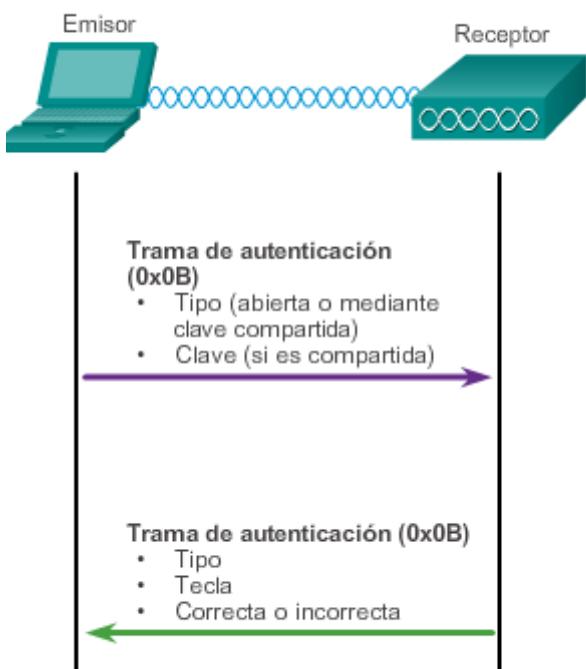
Una vez que se autenticó un cliente inalámbrico, el AP continúa con la etapa de asociación. Como se muestra en la figura 2, la etapa de asociación finaliza la configuración y establece el enlace de datos entre el cliente inalámbrico y el AP.

Como parte de esta etapa:

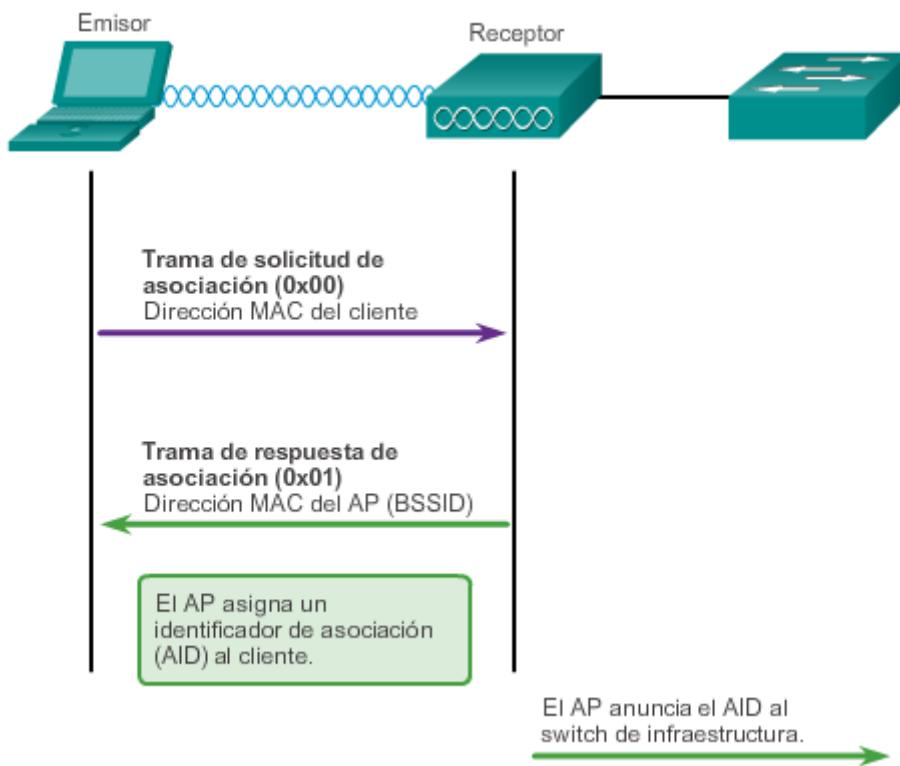
- El cliente inalámbrico reenvía una trama de solicitud de asociación que incluye su dirección MAC.
- El AP responde con una respuesta de asociación que incluye el BSSID del AP, que es la dirección MAC del AP.
- El AP asigna un puerto lógico conocido como “identificador de asociación” (AID) al cliente inalámbrico. El AID equivale a un puerto en un switch y permite que el switch de infraestructura mantenga un registro de las tramas destinadas a que el cliente inalámbrico las reenvíe.

Una vez que un cliente inalámbrico se asocia a un AP, el tráfico entre el cliente y el AP puede fluir.

### El cliente y el AP se autentican



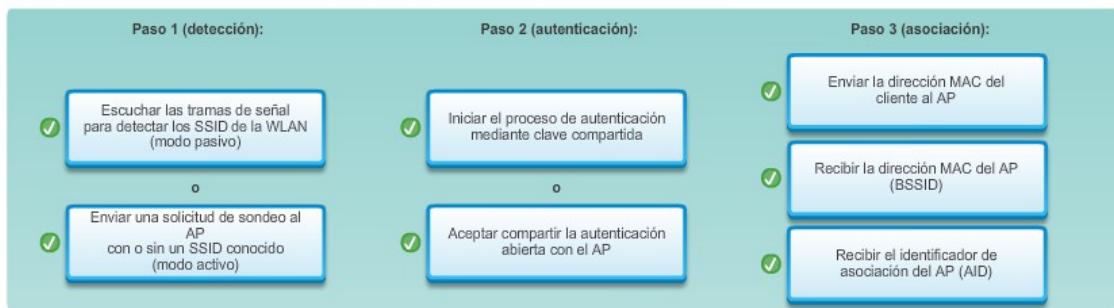
### El cliente y el AP se asocian



Capítulo 4: LAN inalámbricas 4.2.2.6 Actividad: Ordenar los pasos del proceso de asociación

del cliente y el AP

**Actividad: Ordenar los pasos en el proceso de asociación del cliente y el AP**  
Arrastra el cliente WLAN hasta los pasos de asociación de AP en el orden correcto en el diagrama proporcionado.



#### Capítulo 4: LAN inalámbricas 4.3.1.1 Protección de redes inalámbricas

Las dificultades para mantener segura una red conectada por cable se multiplican con una red inalámbrica. La seguridad debe ser una prioridad para cualquiera que utilice o administre redes.

Una WLAN está abierta a cualquier persona dentro del alcance de un AP con las credenciales correspondientes para asociarse a él. Con una NIC inalámbrica y conocimientos de técnicas de decodificación, un atacante no tendrá que entrar físicamente al espacio de trabajo para obtener acceso a una WLAN.

Las preocupaciones de seguridad son aún más importantes cuando se lida con redes empresariales, ya que el sustento de la empresa depende de la protección de su información. En estos casos, las violaciones a la seguridad pueden tener graves repercusiones, sobre todo si la empresa guarda información financiera relacionada con sus clientes. Cada vez se implementan más redes inalámbricas en las empresas y, en muchos casos, estas redes evolucionaron de ser una conveniencia a ser una parte de la red imprescindible para cumplir con los objetivos. Si bien las WLAN siempre fueron un blanco de los ataques, debido al aumento constante de su popularidad, ahora son un blanco principal.

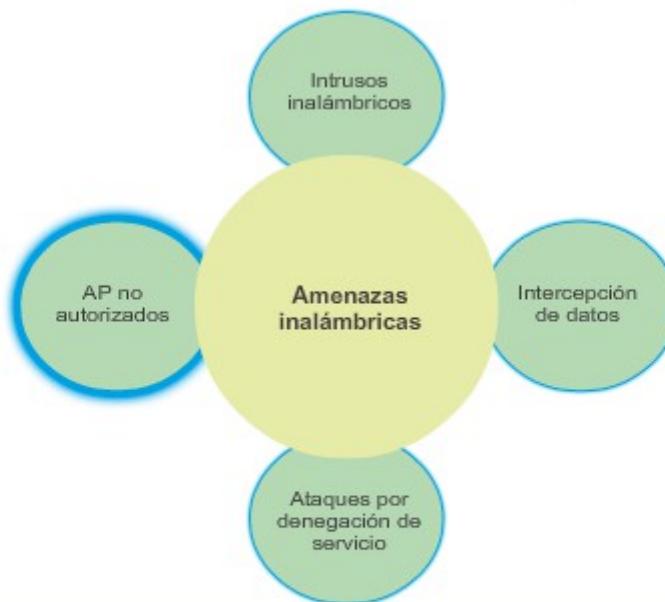
Las personas ajenas a la empresa, los empleados insatisfechos e incluso otros empleados, involuntariamente, pueden generar los ataques. Las redes inalámbricas son específicamente vulnerables a varias amenazas, incluido lo siguiente:

- Intrusos inalámbricos
- Aplicaciones no autorizadas
- Intercepción de datos
- Ataques DoS

En la ilustración, haga clic en cada amenaza para obtener más información.

**Nota:** otras amenazas, como los ataques de suplantación de direcciones MAC de un AP o un cliente inalámbrico, los ataques de decodificación y los ataques de infraestructura están fuera del ámbito de este capítulo.

### Amenazas inalámbricas comunes



#### AP no autorizados



Un usuario con buenas o malas intenciones instala AP no autorizados. Use un software de administración inalámbrica para detectar AP no autorizados.

#### Capítulo 4: LAN inalámbricas 4.3.1.2 Ataque de DoS

Los ataques DoS inalámbricos pueden ser el resultado de lo siguiente:

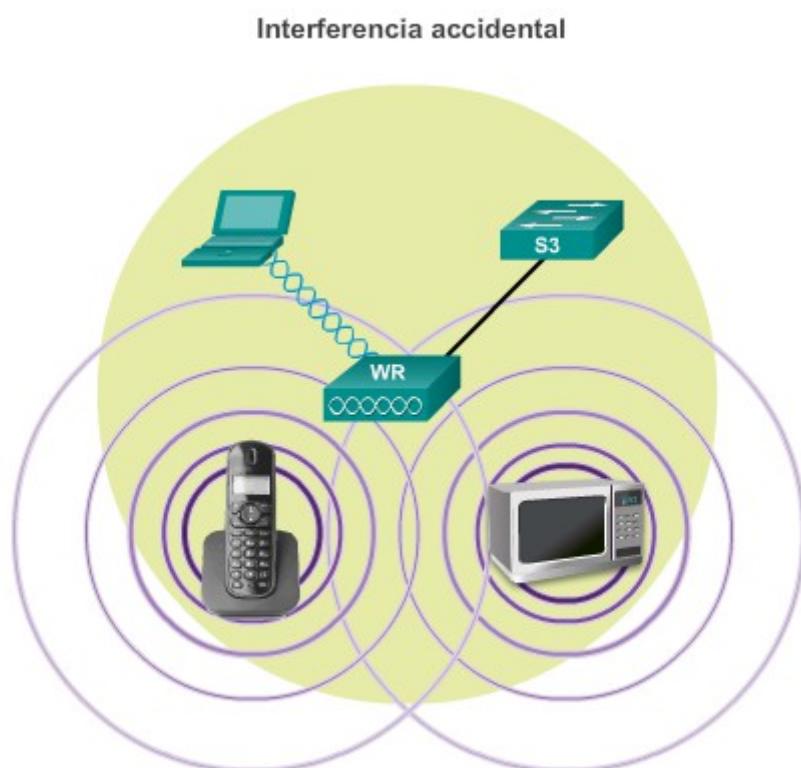
- **Dispositivos mal configurados:** los errores de configuración pueden deshabilitar la WLAN. Por ejemplo, un administrador puede modificar accidentalmente una configuración y deshabilitar la red, o un intruso con privilegios de administrador puede deshabilitar una WLAN intencionalmente.
- **Un usuario malintencionado interfiere en la comunicación inalámbrica intencionalmente:** su objetivo es deshabilitar la red inalámbrica por completo o a tal punto que ningún dispositivo legítimo pueda acceder al medio.
- **Interferencia accidental:** las WLAN operan en las bandas de frecuencia sin licencia y, por lo tanto, todas las redes inalámbricas, independientemente de las características de seguridad, pueden sufrir la interferencia de otros dispositivos inalámbricos. La interferencia accidental puede provenir de dispositivos como los hornos de microondas, los teléfonos inalámbricos, los monitores para bebés, entre otros. La banda de 2,4 GHz es más proclive a la interferencia que la banda de 5 GHz.

Para minimizar el riesgo de un ataque DoS debido a dispositivos mal configurados o ataques malintencionados, proteja todos los dispositivos y las contraseñas, cree copias de seguridad y asegúrese de que todos los cambios de configuración se incorporen fuera del horario de operación.

La interferencia accidental solo ocurre cuando se agrega otro dispositivo inalámbrico. La mejor solución consiste en controlar la WLAN para detectar cualquier problema de interferencia y abordarlo cuando aparezca. Debido a que la banda de 2,4 GHz es más proclive a la interferencia, la banda de 5 GHz se podría usar en áreas con tendencia a la interferencia. Algunas soluciones de WLAN permiten que los AP ajusten automáticamente los canales y usen la banda de 5 GHz para compensar la interferencia. Por ejemplo, algunas soluciones 802.11n/ac/ad se ajustan de manera automática para contrarrestar la interferencia.

En la ilustración, se muestra cómo un teléfono inalámbrico o incluso un horno de microondas pueden interferir con la comunicación WLAN.

La tecnología Cisco CleanAir permite que los dispositivos identifiquen y ubiquen las fuentes de interferencia que no son 802.11. Crea una red que tiene la capacidad de ajustarse de forma automática a los cambios en el entorno.



Los dispositivos comerciales comunes pueden interferir con los dispositivos WLAN causando una denegación del servicio.

#### Capítulo 4: LAN inalámbricas 4.3.1.3 Ataques DoS a las tramas de administración

Si bien es poco probable, un usuario malintencionado podría iniciar intencionalmente un ataque DoS mediante bloqueadores de RF que producen interferencia accidental. Es más probable que intenten manipular las tramas de administración para consumir los recursos del AP y mantener los canales demasiado ocupados como para admitir el tráfico de usuarios legítimos.

Las tramas de administración se pueden manipular para crear varios tipos de ataque DoS. Los dos tipos de ataques comunes a las tramas de administración incluyen lo siguiente:

- **Un ataque de desconexión suplantada:** esto ocurre cuando un atacante envía una serie de comandos de “desasociación” a los clientes inalámbricos dentro de un BSS. Estos comandos hacen que todos los clientes se desconecten. Al desconectarse, los clientes inalámbricos inmediatamente intentan volver a asociarse, lo que crea un estallido de tráfico. El atacante continúa enviando tramas de desasociación, y el ciclo se repite.
- **Una saturación con CTS:** esto ocurre cuando un atacante aprovecha el método de contienda CSMA/CA para monopolizar el ancho de banda y denegar el acceso de todos los demás clientes inalámbricos al AP. Para lograr esto, el atacante satura repetidamente el BSS con tramas de Listo para enviar (CTS) a una STA falsa. Todos los demás clientes inalámbricos que comparten el medio de RF reciben las CTS y retienen sus transmisiones hasta que el atacante deja de transmitir las tramas CTS.

En la figura 1, se muestra cómo un cliente inalámbrico y un AP usan CSMA/CA normalmente para acceder al medio.

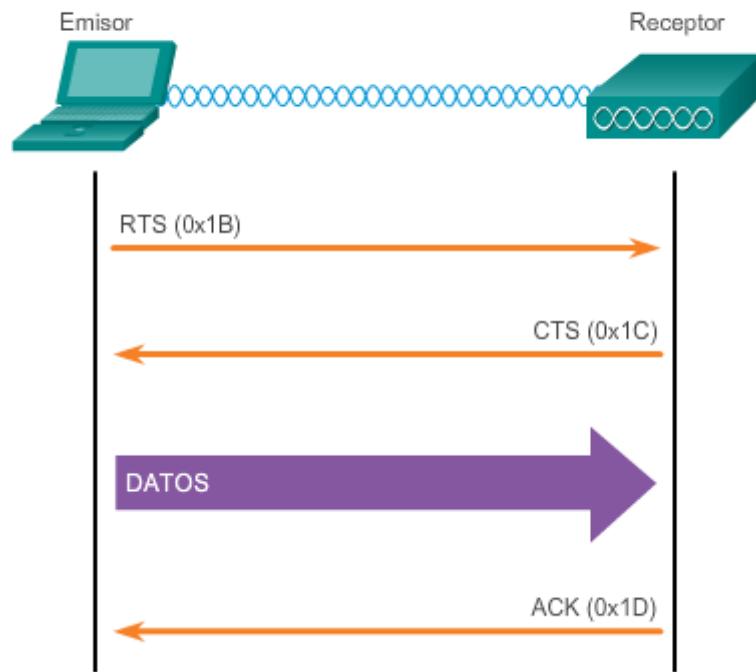
En la figura 2, se muestra cómo un atacante satura con CTS al enviar este tipo de tramas a un cliente inalámbrico falso. Todos los demás clientes ahora deben esperar la duración especificada en la trama CTS. Sin embargo, el atacante continúa enviando tramas CTS; por lo tanto, los demás clientes esperan indefinidamente. El atacante ahora controla el medio.

**Nota:** este es solo un ejemplo de ataque a las tramas de administración. Existen muchos otros tipos de ataques.

Para mitigar muchos de estos ataques, Cisco desarrolló una variedad de soluciones, incluida la característica de protección de tramas de administración (MFP) de Cisco, que también proporciona protección proactiva y completa contra la suplantación de tramas y dispositivos. El Cisco Adaptive Wireless IPS contribuye a esta solución mediante un sistema de detección temprana en el que se comparan las firmas del atacante.

El comité del IEEE 802.11 también lanzó dos estándares en relación con la seguridad inalámbrica. El estándar 802.11i, que se basa en la característica MFP de Cisco, especifica los mecanismos de seguridad para las redes inalámbricas, mientras que el estándar de protección de tramas de administración 802.11w aborda el problema de la manipulación de estas tramas.

### Funcionamiento normal con CSMA/CA



### Un atacante crea un ataque DoS de saturación con CTS



Un AP no autorizado es un AP o un router inalámbrico que:

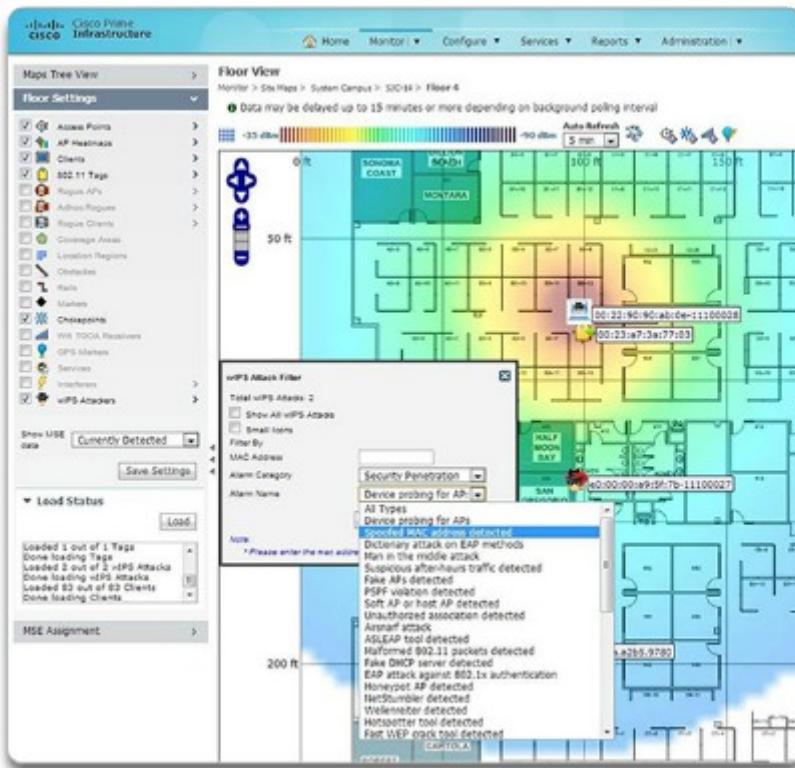
- Se conectó a una red empresarial sin autorización explícita o en contra de la política de la empresa. Cualquier persona con acceso a las instalaciones puede instalar (malintencionadamente o no) un router inalámbrico económico que puede permitir el acceso a los recursos de red protegidos.
- Un atacante lo conectó o habilitó para capturar datos de clientes, como las direcciones MAC de los clientes (inalámbricos y cableados), o para capturar y camuflar paquetes de datos, obtener acceso a los recursos de la red o iniciar un ataque man-in-the-middle (intermediario).

Otra consideración es determinar con qué facilidad se crea una zona de cobertura de red inalámbrica personal. Por ejemplo, un usuario con acceso seguro a la red habilita su host de Windows autorizado para que se convierta en un AP Wi-Fi. Al hacer esto, se evaden las medidas de seguridad, y otros dispositivos no autorizados ahora pueden acceder a los recursos de la red, como un dispositivo compartido.

Para evitar la instalación de AP no autorizados, las organizaciones deben usar software de supervisión para supervisar activamente el espectro de radio en busca de AP no autorizados. En el ejemplo de la captura de pantalla del software de administración de redes Cisco Prime Infrastructure de la ilustración, se muestra un mapa de RF en el que se identifica la ubicación de un intruso con una dirección MAC suplantada.

**Nota:** Cisco Prime es un software de administración de redes que funciona con otros softwares de administración para proporcionar una mirada común y la ubicación central de toda la información de la red. Normalmente, se implementa en organizaciones muy grandes.

## Captura de pantalla de ejemplo de la detección de un AP no autorizado



### Capítulo 4: LAN inalámbricas 4.3.1.5 Ataque man-in-the-middle

Uno de los ataques más sofisticados que un usuario malintencionado puede usar se denomina “ataque man-in-the-middle” (MITM, intermediario). Existen varias maneras de crear un ataque MITM.

Un popular ataque MITM inalámbrico se denomina “ataque con AP de red intrusa”, en el que un atacante introduce un AP no autorizado y lo configura con el mismo SSID que el de un AP legítimo. Las ubicaciones que ofrecen Wi-Fi gratuito, como los aeropuertos, los cafés y los restaurantes, son focos para este tipo de ataque, debido a la autenticación abierta.

Los clientes que se conectan a una red inalámbrica verán dos AP que ofrecen acceso inalámbrico. Aquellos que están cerca del AP no autorizado detectan la señal más intensa y es más probable que se asocien a este AP de red intrusa. El tráfico de usuarios ahora se envía al AP no autorizado, que a su vez captura los datos y los reenvía al AP legítimo. El tráfico de retorno del AP legítimo se envía al AP no autorizado, se captura y se reenvía a la STA desprevinida. El atacante puede robar la contraseña del usuario y su información personal, obtener acceso a la red y comprometer el sistema del usuario.

Por ejemplo, en la figura 1, un usuario malintencionado está en la Cafetería de Juan y desea capturar el tráfico de los clientes inalámbricos desprevinidos. El atacante lanza un software que le permite a su computadora portátil convertirse en un AP de red intrusa con el mismo SSID y el mismo canal que el router inalámbrico legítimo.

En la figura 2, un usuario ve dos conexiones inalámbricas disponibles, pero elige el AP no autorizado y se asocia a este. El atacante captura los datos del usuario y los reenvía al AP legítimo, que a su vez dirige el tráfico de retorno al AP de red intrusa. El AP de red intrusa captura el tráfico de retorno y reenvía la información al usuario desprevenido.

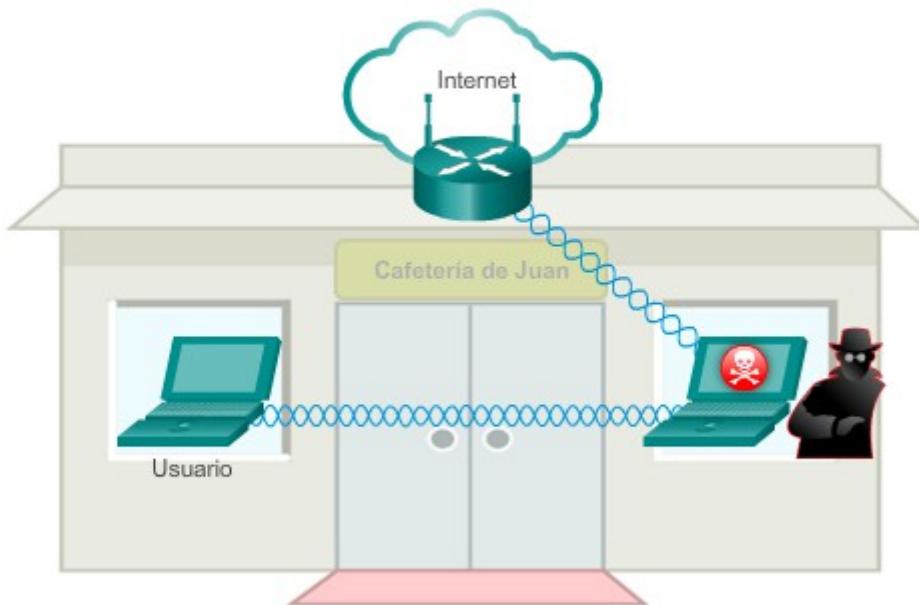
Vencer un ataque MITM depende de la sofisticación de la infraestructura WLAN y la vigilancia de la actividad de monitoreo de red. El proceso comienza con la identificación de los dispositivos legítimos en la WLAN. Para hacer esto, se deben autenticar los usuarios. Una vez que se conocen todos los dispositivos legítimos, se puede monitorear la red para detectar los dispositivos o el tráfico anormales.

Las WLAN de empresas que utilizan dispositivos WLAN de tecnología avanzada proveen herramientas a los administradores que trabajan juntas como un sistema de prevención de intrusión inalámbrica (IPS). Estas herramientas incluyen escáneres que identifican las redes ad hoc y los AP no autorizados, así como la administración de recursos de radio (RRM), que controla la banda de RF para vigilar la actividad y la carga de AP. Un AP que está más ocupado de lo normal advierte al administrador sobre posible tráfico no autorizado.

**Un usuario malintencionado inicia un ataque con un AP de red intrusa**



### Ataque con AP de red intrusa exitoso



#### Capítulo 4: LAN inalámbricas 4.3.2.1 Descripción general de la seguridad inalámbrica

La seguridad siempre fue un motivo de preocupación con la tecnología Wi-Fi, debido a que se movió el límite de la red. Las señales inalámbricas pueden trasladarse a través de la materia sólida, como los techos, los pisos, las paredes, fuera del hogar o de la oficina. Sin medidas de seguridad estrictas, instalar una WLAN equivale a colocar puertos Ethernet en todas partes, incluso en exteriores.

Para abordar las amenazas relacionadas con mantener alejados a los intrusos inalámbricos y proteger los datos, en un principio se usaron dos características de seguridad:

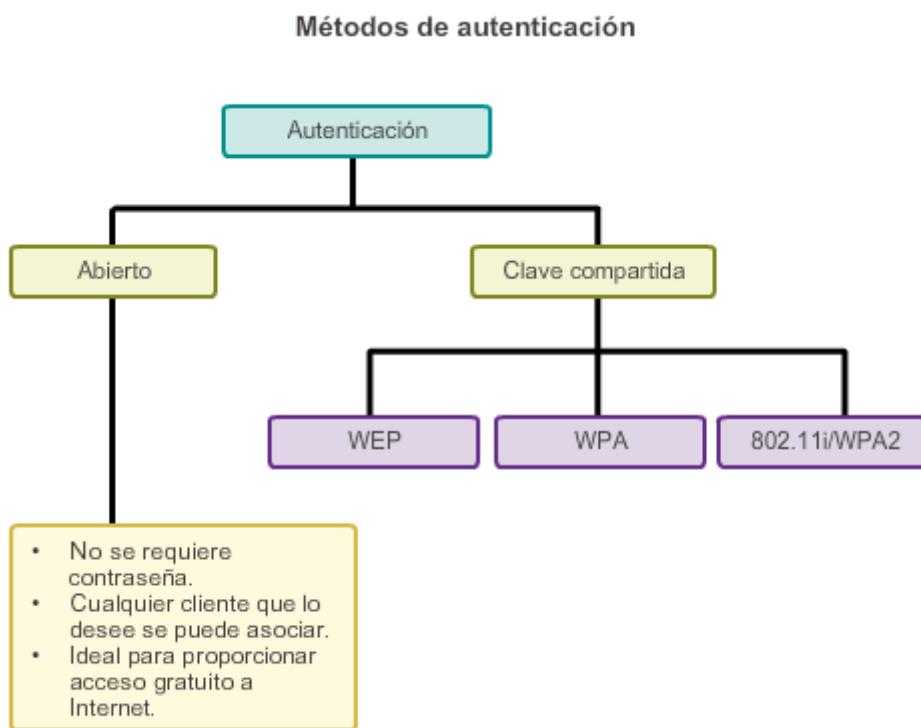
- **Ocultamiento del SSID:** los AP y algunos routers inalámbricos permiten que se deshabilite la trama de señal del SSID. Los clientes inalámbricos deben identificar manualmente el SSID para conectarse a la red.
- **Filtrado de direcciones MAC:** un administrador puede permitir o denegar el acceso inalámbrico a los clientes de forma manual según la dirección MAC del hardware físico.

Si bien estas dos características pueden disuadir a la mayoría de los usuarios, la realidad es que ni el ocultamiento del SSID ni el filtrado de direcciones MAC podrían disuadir a un intruso hábil. Los SSID se descubren con facilidad, incluso si los AP no los transmiten por difusión, y las direcciones MAC se pueden suplantar. La mejor manera de proteger una red inalámbrica es usar sistemas de autenticación y cifrado, como se muestra en la figura 1.

Se introdujeron dos tipos de autenticación con el estándar 802.11 original:

- **Autenticación de sistema abierto:** cualquier cliente inalámbrico se debe poder conectar con facilidad, y este método solo se debe usar en situaciones en las que la seguridad no es motivo de preocupación, como en los lugares que proporcionan acceso gratuito a Internet, como cafés, hoteles y áreas remotas.
- **Autenticación mediante clave compartida:** proporciona mecanismos como WEP, WPA o WPA2 para autenticar y cifrar datos entre un cliente y un AP inalámbricos. Sin embargo, la contraseña se debe compartir previamente entre las dos partes para que estas se conecten.

En el gráfico de la figura 2, se resumen los distintos tipos de autenticación.



#### Capítulo 4: LAN inalámbricas 4.3.2.2 Métodos de autenticación mediante clave compartida

Como se muestra en la figura 1, existen tres técnicas de autenticación mediante clave compartida:

- **Privacidad equiparable a la de redes cableadas (WEP):** especificación 802.11 original, diseñada para proporcionar una privacidad similar a la de conectarse a una red mediante una conexión por cable. Los datos se protegen mediante el método de cifrado RC4 con una clave estática. Sin embargo, la clave nunca cambia al intercambiar paquetes, por lo que es fácil de descifrar.
- **Acceso protegido Wi-Fi (WPA):** un estándar de Wi-Fi Alliance que usa WEP, pero protege los datos con un algoritmo de cifrado del protocolo de integridad de clave temporal (TKIP), que es mucho más seguro. TKIP cambia la clave para cada paquete, lo que hace que sea mucho más difícil de descifrar.

- **IEEE 802.11i/WPA2:** IEEE 802.11i es un estándar del sector para proteger las redes inalámbricas. La versión de Wi-Fi Alliance se denomina WPA2. Tanto 802.11i como WPA2 usan el estándar de cifrado avanzado (AES). En la actualidad, se considera que AES es el protocolo de cifrado más seguro.

Ya no se recomienda WEP. Se comprobó que las claves WEP compartidas presentan errores y, por lo tanto, no se lo debe usar nunca. Para contrarrestar la debilidad de las claves WEP compartidas, el primer enfoque de las empresas fue probar técnicas, como el ocultamiento de los SSID y el filtrado de las direcciones MAC. Se comprobó que estas técnicas también son demasiado débiles.

Luego de las debilidades de una seguridad basada en WEP, hubo un período de medidas de seguridad interinas. Los proveedores como Cisco, que quieren responder a la demanda de mejor seguridad, desarrollaron sus propios sistemas y, al mismo tiempo, ayudaron con la evolución del estándar 802.11i. En el camino hacia 802.11i, se creó el algoritmo de cifrado TKIP, que se unió al método de seguridad WPA de Wi-Fi Alliance.

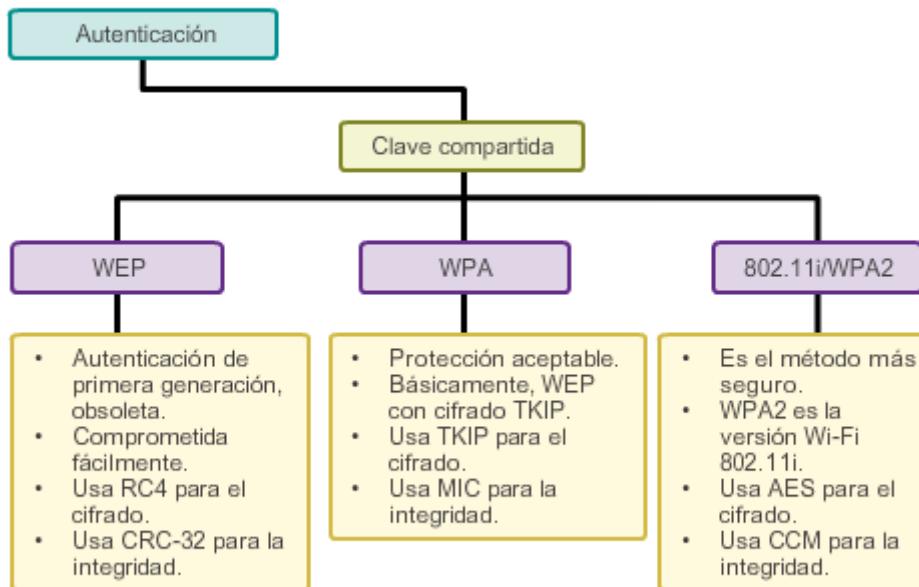
Las redes inalámbricas modernas siempre deben usar el estándar 802.11i/WPA2. WPA2 es la versión Wi-Fi de 802.11i y, por lo tanto, los términos WPA2 y 802.11i se suelen usar de manera indistinta.

Desde 2006, cualquier dispositivo que tenga el logo Wi-Fi Certified tiene la certificación WPA2.

**Nota:** las redes Wireless-N deben usar el modo de seguridad WPA2-Personal para obtener un mejor rendimiento.

En la tabla de la figura 2, se resumen los tres tipos de métodos de autenticación mediante clave compartida.

## Métodos de autenticación



### Métodos de autenticación mediante clave compartida

	WEP	WPA	802.11i/WPA2
Método de autenticación	Clave pre-compartida	PSK o 802.1x	PSK o 802.1x
Cifrado	RC4	TKIP	AES
Integridad del mensaje	CRC-32	MIC	CCMP
Seguridad	Débil	Fuerte	Más seguro

#### Capítulo 4: LAN inalámbricas 4.3.2.3 Métodos de cifrado

El cifrado se usa para proteger datos. Si un intruso captura datos cifrados, no podrá descifrarlos durante un período razonable.

El estándar IEEE 802.11i y los estándares WPA y WPA2 de Wi-Fi Alliance usan los siguientes protocolos de cifrado:

- Protocolo de integridad de clave temporal (TKIP):** es el método de cifrado que usa WPA. Provee apoyo para el equipo WLAN heredado que atiende las fallas originales asociadas con el método de encriptación WEP 802.11. Usa WEP, pero cifra el contenido de capa 2 mediante TKIP y realiza una comprobación de integridad de los mensajes (MIC) en el paquete cifrado para asegurar que no se alteró el mensaje.
- Estándar de cifrado avanzado (AES):** es el método de cifrado que usa WPA2. Es el método preferido, ya que se alinea con el estándar del sector IEEE 802.11i. AES realiza las mismas funciones que TKIP, pero es un método de cifrado más seguro. Usa el protocolo Counter Mode Cipher Block Chaining Message Authentication Code Protocol

(CCMP), que permite que los hosts de destino reconozcan si se alteraron los bits cifrados y no cifrados.

**Nota:** siempre que sea posible, elija WPA2 con AES.

#### Capítulo 4: LAN inalámbricas 4.3.2.4 Autenticación de un usuario doméstico

En la ilustración, se muestran las opciones del modo de seguridad del router inalámbrico Linksys EA6500. Observe cómo el **Security mode (Modo de seguridad)** para la red de 2,4 GHz usa autenticación abierta (es decir, None [Ninguna]) y no requiere una contraseña, mientras que la opción de **Security mode** para la red de 5 GHz usa una autenticación WPA2/WPA Mixed Personal (WPA2/WPA personal combinado) y requiere una contraseña.

**Nota:** normalmente, las redes de 2,4 GHz y 5 GHz se configurarían con los mismos modos de seguridad. El ejemplo de la ilustración se usa solo con fines de demostración.

En la lista desplegable de **Security mode** de la red de 2,4 GHz, se muestran los métodos de seguridad disponibles en el router Linksys EA6500. Se indica desde el método más débil (es decir, None) al más seguro (es decir, WPA2/WPA Mixed Enterprise [WPA2/WPA empresarial combinado]). La red de 5 GHz incluye la misma lista desplegable.

WPA y WPA2 admiten dos tipos de autenticación:

- **Personal:** diseñada para las redes domésticas o de oficinas pequeñas; los usuarios se autentican mediante una clave previamente compartida (PSK). Los clientes inalámbricos se autentican con el AP mediante una contraseña previamente compartida. No se requiere ningún servidor de autenticación especial.
- **Enterprise (Empresarial):** diseñada para las redes empresariales, pero requiere un servidor de servicio de autenticación remota telefónica de usuario (RADIUS). Si bien su configuración es más complicada, proporciona seguridad adicional. El servidor RADIUS debe autenticar el dispositivo y, a continuación, se deben autenticar los usuarios mediante el estándar 802.1X, que usa el protocolo de autenticación extensible (EAP).

#### Capítulo 4: LAN inalámbricas 4.3.2.5 Autenticación en la empresa

En las redes que tienen requisitos de seguridad más estrictos, se requiere una autenticación o un inicio de sesión adicionales para otorgar acceso a los clientes inalámbricos. Las opciones del modo de seguridad Enterprise requieren un servidor RADIUS con autenticación, autorización y contabilidad (AAA).

Consulte el ejemplo de la ilustración. Observe los nuevos campos que se muestran al elegir la versión Enterprise de WPA o WPA2. Estos campos son necesarios para proporcionar al AP la información requerida para contactar al servidor AAA:

- **Dirección IP del servidor RADIUS:** esta es la dirección del servidor RADIUS a la que se puede llegar.

- **Números de puerto UDP:** los números de puerto UDP asignados oficialmente son 1812 para la autenticación RADIUS y 1813 para la contabilidad RADIUS, pero también pueden funcionar mediante los números de puerto UDP 1645 y 1646.
- **Clave compartida:** se usa para autenticar el AP con el servidor RADIUS.

La clave compartida no es un parámetro que se debe configurar en una STA. Solo se requiere en el AP para autenticar con el servidor RADIUS.

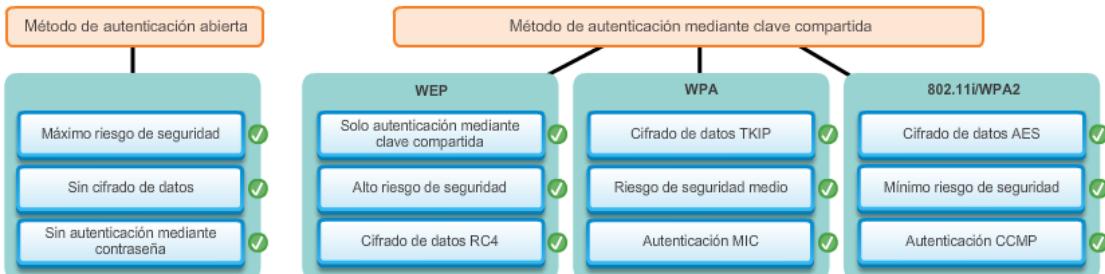
**Nota:** no se indica ningún campo de contraseña, debido a que la autenticación y la autorización del usuario propiamente dichas se manejan mediante el estándar 802.1X, que proporciona a los usuarios finales una autenticación centralizada basada en servidores.

El proceso de inicio de sesión 802.1X usa EAP para comunicarse con el AP y el servidor RADIUS. El EAP es una estructura para autenticar el acceso a la red. Puede proporcionar un mecanismo de autenticación seguro y negociar una clave privada segura que después se puede usar para una sesión de cifrado inalámbrico mediante el cifrado TKIP o AES.

#### Capítulo 4: LAN inalámbricas 4.3.2.6 Actividad: Identificar las características de autenticación

##### de WLAN

**Actividad: Identificar las características de autenticación de WLAN**  
Arrastra cada característica de seguridad de WLAN hasta el campo del método de autenticación abierta o mediante clave abierta correspondiente.



#### Capítulo 4: LAN inalámbricas 4.4.1.1 Configuración de un router inalámbrico

Los routers inalámbricos modernos ofrecen una variedad de características, y la mayoría se diseñó para funcionar sin ninguna configuración adicional aparte de la configuración predeterminada. Sin embargo, es aconsejable cambiar la configuración predeterminada inicial.

Los routers inalámbricos domésticos se configuran mediante una interfaz web GUI.

Un enfoque básico a la implementación inalámbrica, como en cualquier trabajo de red básico, es configurar y probar progresivamente. Por ejemplo, antes de implementar un dispositivo inalámbrico, verifique que la red conectada por cable existente funcione y que los hosts conectados por cable puedan acceder a los servicios de Internet.

Una vez que se confirma el funcionamiento de la red conectada por cable, el plan de implementación consta de lo siguiente:

**Paso 1.** Comience el proceso de implementación de WLAN con un único AP y un único cliente inalámbrico, sin habilitar la seguridad inalámbrica.

**Paso 2.** Verifique que el cliente recibió una dirección IP de DHCP y puede hacer ping al router predeterminado local conectado por cable, y luego explore Internet externo.

**Paso 3.** Configure la seguridad inalámbrica con WPA2/WPA Mixed Personal. Nunca use WEP, a menos que no existan otras opciones.

**Paso 4.** Realice una copia de seguridad de la configuración.

Antes de instalar un router inalámbrico, tenga en cuenta la siguiente configuración:

- **Nombre de SSID:** nombre de la red WLAN.
- **Contraseña de red (si se requiere):** si el sistema lo solicita, esta es la contraseña requerida para asociarse y acceder al SSID.
- **Contraseña del router:** esta es la contraseña de administración del router, equivalente a la contraseña **deenable secret** del modo EXEC privilegiado.
- **Nombre del SSID de la red para invitados:** por motivos de seguridad, se puede aislar a los invitados con un SSID diferente.
- **Contraseña de la red para invitados:** esta es la contraseña para acceder al SSID para invitados.
- **Nombre de usuario de Linksys Smart Wi-Fi:** cuenta de Internet requerida para acceder al router de manera remota a través de Internet.
- **Contraseña de Linksys Smart Wi-Fi:** contraseña para acceder al router de manera remota.

En la tabla de la ilustración, se describe el ejemplo de configuración usado para configurar el router inalámbrico Linksys EA6500.

## Parámetros y configuración de administración para tener en cuenta

Parámetros de administración	Configuración
Nombre de la red (SSID)	Red-hogar
Contraseña de red	cisco123
Contraseña del router	clase123
Nombre de la red para invitados (SSID)	Red-invitados-hogar
Contraseña de la red para invitados	cisco
Nombre de usuario de Linksys Smart Wi-Fi	Mi-nombre
Contraseña de Linksys Smart Wi-Fi	clase12345

### Capítulo 4: LAN inalámbricas 4.4.1.2 Configuración e instalación iniciales de Linksys EA6500

El router inalámbrico Linksys EA6500 viene con un CD de configuración.

Para configurar e instalar el software del router Linksys EA6500, siga estos pasos:

**Paso 1.** Introduzca el CD en la unidad de CD o DVD, y la instalación debería comenzar automáticamente. Si el CD de instalación no está disponible, descargue el programa de instalación de <http://Linksys.com/support>.

En la figura 1, se muestra la ventana inicial Connect your Linksys EA6500 (Conecte el Linksys EA6500) con las instrucciones para conectar la alimentación del router y la conexión a Internet.

**Nota:** en nuestro ejemplo, el router inalámbrico no se conecta a Internet.

**Paso 2.** Haga clic en **Next** (Siguiente) para iniciar la instalación.

El programa inicia la instalación y muestra una ventana de estado (figura 2). Durante este tiempo, el programa de instalación intenta configurar y habilitar la conexión a Internet. En el ejemplo, la conexión a Internet no está disponible y, después de algunas solicitudes para conectarse a Internet, se muestra la opción para omitir este paso.

Se muestra la ventana de la configuración del router Linksys (figura 3). Aquí es donde se configuran el SSID, la contraseña inalámbrica y la contraseña administrativa.

**Paso 3.** Haga clic en **Next** para mostrar la pantalla de resumen de configuración del router (figura 4). Registre esta configuración si no se completó previamente la tabla inicial.

**Paso 4.** Haga clic en **Next** para mostrar la ventana de configuración de la cuenta de Linksys Smart Wi-Fi (figura 5).

Esta ventana le permite administrar el router de manera remota a través de Internet. En este ejemplo, no se configura la cuenta de Linksys Smart Wi-Fi debido a que no hay acceso a Internet.

**Paso 5.** Haga clic en **Continue** (Continuar) para mostrar la ventana Sign In (Inicio de sesión, figura 6). Debido a que no se configuró la conexión a Internet, se requiere la contraseña administrativa del router.

**Paso 6.** Después de introducir la contraseña, haga clic en **Log In** (Iniciar sesión) para mostrar la página de inicio de Linksys Smart Wi-Fi (figura 7).

#### Capítulo 4: LAN inalámbricas 4.4.1.3 Configuración de la página de inicio de Linksys Smart Wi-Fi

Como se muestra en las figuras 1 a 3, la página de inicio de Linksys Smart Wi-Fi se divide en las tres secciones principales siguientes:

- **Router Settings (Configuración del router):** use esta sección para modificar la configuración de conectividad, resolución de problemas, tecnología inalámbrica y seguridad.
- **Smart Wi-Fi Tools (Herramientas de Smart Wi-Fi):** use esta sección para ver quién está conectado actualmente a la red, crear una red separada para los invitados, configurar el control parental para proteger a sus hijos, priorizar el ancho de banda para aplicaciones y dispositivos específicos, probar la velocidad de la conexión a Internet y controlar el acceso a los archivos compartidos.
- **Widgets de Smart Wi-Fi:** proporciona un resumen rápido de la sección Smart Wi-Fi Tools.

Haga clic en el botón Reproducir de la figura 4 para ver un video breve sobre la interfaz de Smart Wi-Fi.

#### Capítulo 4: LAN inalámbricas 4.4.1.4 Configuración de Smart Wi-Fi.

Como se muestra en las figuras 1 a 4, la configuración de Smart Wi-Fi le permite hacer lo siguiente:

- Configurar los parámetros básicos del router para la red local. Esta herramienta se puede usar para configurar una reserva de DHCP, cambiar la contraseña de administración del router, cambiar la dirección IP del router Linksys, configurar los routers Linksys con una ruta estática, configurar el router con un servicio de Internet por cable y configurar los parámetros de MTU del router Linksys.
- Diagnosticar y resolver problemas de conectividad de la red. Contiene el estado actual del router y los dispositivos conectados. También se puede usar para realizar una prueba de ping y de traceroute, realizar una copia de seguridad y restaurar la configuración actual

del router, revisar la dirección IP de la WAN, reiniciar y restablecer el router a la configuración predeterminada de fábrica, y mantener el estado del router.

- Proteger y personalizar la red inalámbrica. También se puede usar para habilitar y configurar el filtro de MAC inalámbrico y conectar dispositivos con facilidad mediante WPS.
- Mantener la red protegida contra las amenazas de Internet mediante la configuración de la característica DMZ.
- Ver las computadoras y los dispositivos conectados en la red, y configurar el reenvío de puertos.

#### Capítulo 4: LAN inalámbricas 4.4.1.5 Herramientas de Smart Wi-Fi

Como se muestra en las figuras 1 a 6, las herramientas de Smart Wi-Fi proporcionan servicios adicionales que incluyen lo siguiente:

- **Device List (Lista de dispositivos):**vea quién está conectado a la WLAN. Se pueden personalizar los nombres y los íconos de los dispositivos. También se pueden conectar dispositivos mediante este servicio.
- **Guest Access (Acceso de invitados):**cree una red separada para hasta 50 invitados en el hogar y, al mismo tiempo, proteja los archivos de la red con la herramienta Guest Access.
- **Parental Controls (Controles parentales):** proteja a los niños y a los integrantes de la familia mediante la restricción del acceso a sitios web potencialmente perjudiciales. Esta herramienta se usa para restringir el acceso a Internet en dispositivos específicos, controlar la hora y los días en los que estos dispositivos pueden acceder a Internet, bloquear sitios web específicos para ciertos dispositivos, deshabilitar las restricciones de acceso a Internet y deshabilitar la característica Parental Controls.
- **Media Prioritization (Priorización de medios):** prioriza el ancho de banda para aplicaciones y dispositivos específicos. Con esta herramienta, se optimiza la experiencia en línea al priorizar el ancho de banda en las aplicaciones y los dispositivos que más lo necesitan. Esta herramienta se puede usar para emplear la característica Settings (Configuración) de la herramienta Media Prioritization, agregar más aplicaciones para asignarles un ancho de banda específico y asignar un ancho de banda más alto para una aplicación, un dispositivo o un juego en línea al establecer la prioridad del ancho de banda.
- **Speed Test (Prueba de velocidad):**esta herramienta se usa para probar la velocidad de subida y descarga del enlace a Internet. Es útil para establecer la línea de base.
- **USB Storage (Almacenamiento USB):** controla el acceso a los archivos compartidos. Configura cómo los usuarios pueden acceder a los archivos compartidos. Con esta herramienta, los usuarios pueden acceder al almacenamiento USB en la red local, crear recursos compartidos en un dispositivo de almacenamiento USB, configurar los parámetros de Folder Access (Acceso a las carpetas), configurar la forma en que los

dispositivos y las computadoras dentro de la red pueden acceder al servidor FTP y configurar el acceso a un servidor de medios.

#### Capítulo 4: LAN inalámbricas 4.4.1.6 Realización de copias de seguridad de una configuración

De la misma manera que el IOS de un router Cisco debe tener una copia de seguridad en caso de falla, la configuración de un router doméstico también la debe tener. Si un router doméstico queda con su configuración predeterminada, entonces la copia de seguridad de la configuración no se justifica realmente. Sin embargo, si se personalizaron muchas de las herramientas de Smart Wi-Fi, puede ser beneficioso realizar una copia de seguridad de la configuración:

Hacer una copia de seguridad de la configuración es fácil con el router inalámbrico Linksys EA6500.

**Paso 1.** Inicie sesión en la página de inicio de Smart Wi-Fi. Haga clic en el ícono de **Troubleshooting** (Resolución de problemas) para mostrar la ventana Status (Estado) de la resolución de problemas (figura 1).

**Paso 2.** Haga clic en la ficha **Diagnostics** (Diagnóstico) para abrir la ventana Diagnostics de la sección Troubleshooting (figura 2).

**Paso 3.** Bajo el título Router configuration (Configuración del router), haga clic en **Backup** (Realizar copia de seguridad) y guarde el archivo en una carpeta adecuada.

**Nota:** para subir una copia de seguridad guardada previamente, haga clic en **Restore** (Restaurar), ubique el archivo y comience el proceso de restauración.

#### Capítulo 4: LAN inalámbricas 4.4.2.1 Conexión de clientes inalámbricos

Una vez que se configuró el AP o el router inalámbrico, se debe configurar la NIC inalámbrica en el cliente para permitir que se conecte a la WLAN. El usuario también debe verificar que el cliente se conectó correctamente a la red inalámbrica correspondiente, en especial porque es probable que existan muchas WLAN disponibles a las que se pueda conectar.

Haga clic en el botón Reproducir de la figura 1 para ver un video breve sobre cómo conectar un equipo Windows a la WLAN.

Haga clic en el botón Reproducir de la figura 2 para ver un video breve sobre la conexión de un iPod, un iPhone y un iPad a la WLAN.

#### Capítulo 4: LAN inalámbricas 4.4.2.2 Packet Tracer: Configuración del acceso a una LAN

inalámbrica

Información básica/situación

En esta actividad, configurará un router inalámbrico Linksys para permitir el acceso remoto desde las computadoras, así como la conectividad inalámbrica con seguridad WPA2. Configurará la conectividad inalámbrica de las computadoras de forma manual mediante la introducción del SSID y la contraseña del router Linksys.

[Packet Tracer: Configuración del acceso a una LAN inalámbrica \(instrucciones\)](#)

[Packet Tracer: Configuración del acceso a una LAN inalámbrica \(PKA\)](#)

Capítulo 4: LAN inalámbricas 4.4.2.3 Práctica de laboratorio: Configuración de un cliente y un

router inalámbricos

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: Configurar parámetros básicos en un router Linksys serie EA
- Parte 2: Proteger la red inalámbrica
- Parte 3: Revisar las características adicionales en un router Linksys serie EA
- Parte 4: Conectar un cliente inalámbrico

[Práctica de laboratorio: Configuración de un cliente y un router inalámbricos](#)

Capítulo 4: LAN inalámbricas 4.4.3.1 Métodos de resolución de problemas

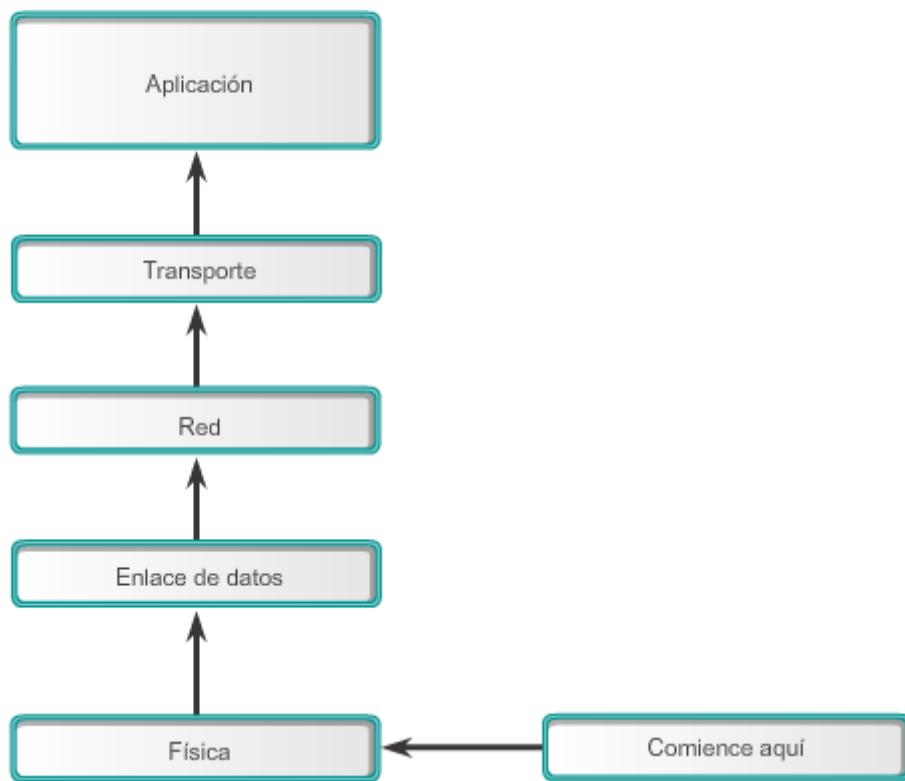
La resolución de cualquier tipo de problemas de red debe seguir un método sistemático. Los modelos lógicos de tecnología de redes, como los modelos OSI y TCP/IP, dividen la funcionalidad de la red en capas modulares.

Cuando se realiza la resolución de problemas, se pueden aplicar estos modelos en capas a la red física para aislar los problemas de la red. Por ejemplo, si los síntomas sugieren un problema de conexión física, el técnico de red puede concentrarse en la resolución de problemas del circuito que funciona en la capa física. Si ese circuito funciona correctamente, el técnico observa las áreas en otra capa que podrían estar causando el problema.

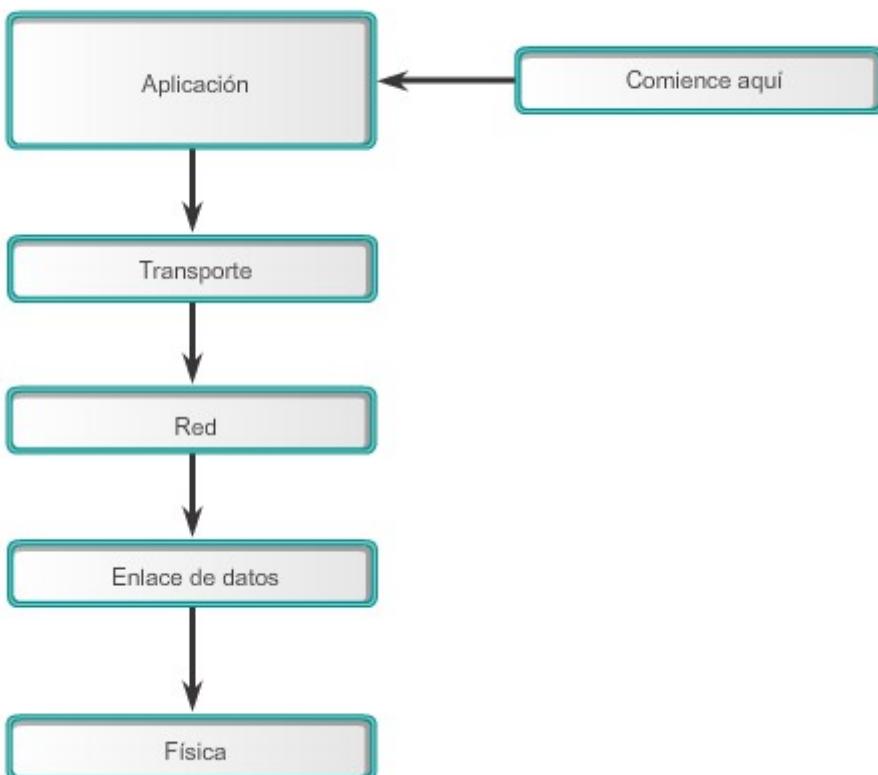
Existen tres métodos principales de resolución de problemas para solucionar los problemas de una red:

- **Ascendente:** comenzar por la capa 1 y continuar en sentido ascendente (figura 1).
- **Descendente:** comenzar en la capa superior y continuar en sentido descendente (figura 2).
- **Divide y vencerás:** hacer ping al destino. Si los pings fallan, verificar las capas inferiores. Si los pings se realizan correctamente, verificar las capas superiores (figura 3).

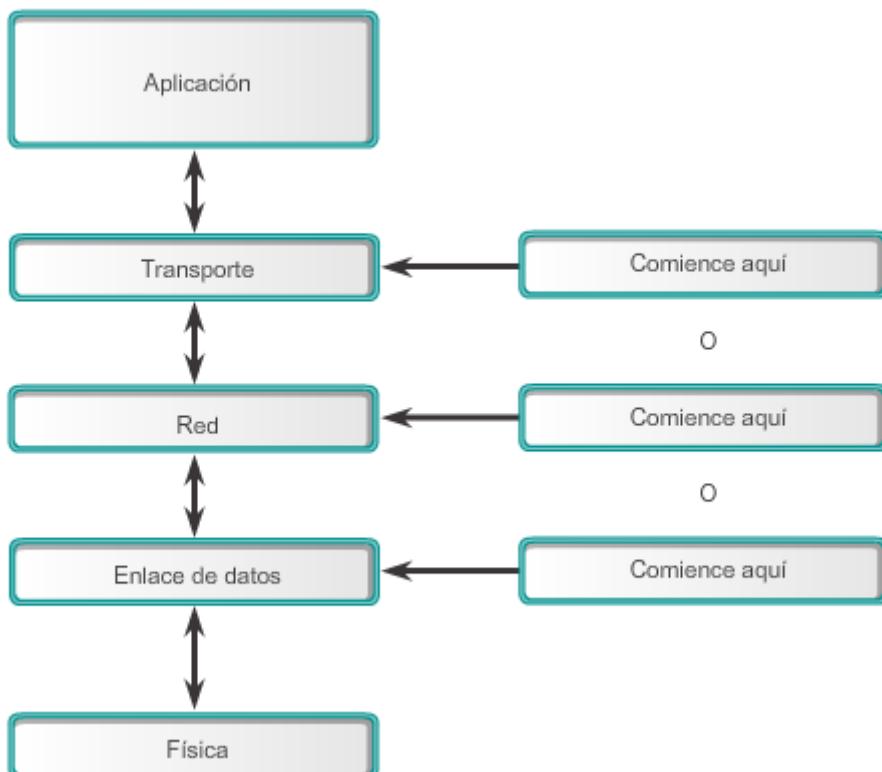
### Método de resolución de problemas: ascendente



### Método descendente



### Método divide y vencerás



Cuando se realiza la resolución de problemas de una WLAN, se recomienda un proceso de eliminación.

En la ilustración, un cliente inalámbrico no se conecta a la WLAN. Si no hay conectividad, compruebe lo siguiente:

- Confirme la configuración de red en la computadora mediante el comando **ipconfig**. Verifique que la PC recibió una dirección IP a través de DHCP o está configurada con una dirección IP estática.
- Confirme que el dispositivo puede conectarse a una red conectada por cable. Conecte el dispositivo a la LAN conectada por cable y haga **ping** a una dirección IP conocida.
- Si es necesario, vuelva a cargar los controladores para el cliente, según corresponda. Puede ser necesario intentar una NIC inalámbrica diferente.
- Si la NIC inalámbrica del cliente funciona, compruebe el modo seguridad y la configuración de encriptación en el cliente. Si la configuración de seguridad no coincide, el cliente no puede acceder a la WLAN.

Si la computadora funciona pero la conexión inalámbrica funciona de manera deficiente, revise lo siguiente:

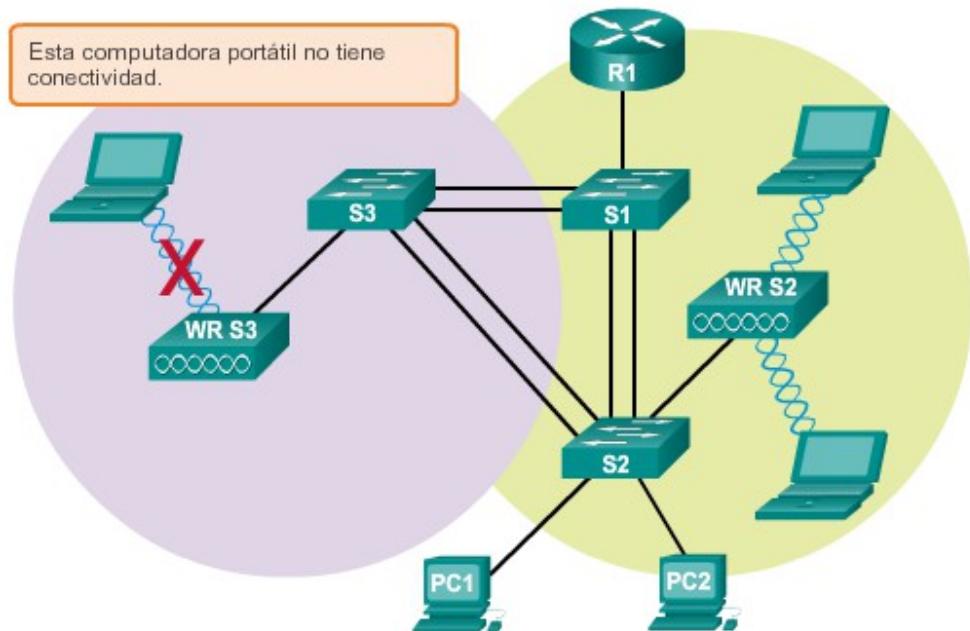
- ¿A qué distancia se encuentra la computadora del AP? ¿La computadora está fuera del área de cobertura planificada (BSA)?
- Revise la configuración de canales en el cliente inalámbrico. El software cliente debe detectar el canal apropiado siempre y cuando el SSID sea correcto.
- Revise la presencia de otros dispositivos en el área que puedan interferir en la banda de 2,4 GHz. Ejemplos de estos dispositivos son los teléfonos inalámbricos, los monitores para bebés, los hornos de microondas, los sistemas de seguridad inalámbrica y los AP potencialmente no autorizados. Los datos de estos dispositivos pueden causar interferencia en la WLAN y problemas de conexión intermitente entre el cliente inalámbrico y el AP.

A continuación, asegúrese de que todos los dispositivos estén realmente en su lugar. Considere un posible problema de seguridad física. ¿Hay alimentación para todos los dispositivos, y estos están encendidos?

Por último, inspeccione los enlaces entre los dispositivos conectados por cable para detectar conectores defectuosos o dañados o cables faltantes. Si la planta física está en su lugar, haga ping a los dispositivos, incluido el AP, para verificar la LAN conectada por cable. Si la conectividad sigue fallando en este momento, tal vez haya algún error en el AP o en su configuración.

Cuando se descarte la computadora del usuario como origen del problema y se confirme el estado físico de los dispositivos, comience a investigar el rendimiento del AP. Revise el estado de la alimentación del AP.

## Problema de conectividad



### Capítulo 4: LAN inalámbricas 4.4.3.3 Resolución de problemas en una red lenta

Para optimizar y aumentar el ancho de banda de los routers 802.11n/ac de banda dual, realice lo siguiente:

- **Actualice sus clientes inalámbricos:** los dispositivos anteriores a 802.11b e incluso 802.11g pueden hacer que toda la WLAN sea más lenta. Para lograr el mejor rendimiento, todos los dispositivos inalámbricos deben admitir el mismo estándar más alto aceptable.
- **Divida el tráfico:** la manera más fácil de mejorar el rendimiento inalámbrico es dividir el tráfico inalámbrico entre las bandas 802.11n de 2,4 GHz y de 5 GHz. Por lo tanto, IEEE 802.11n (o superior) puede usar las dos bandas como dos redes inalámbricas separadas para ayudar a administrar el tráfico. Por ejemplo, use la red de 2,4 GHz para las tareas de Internet básicas, como la navegación web, el correo electrónico y las descargas, y use la banda de 5 GHz para la transmisión de multimedios, como se muestra en la figura 1.

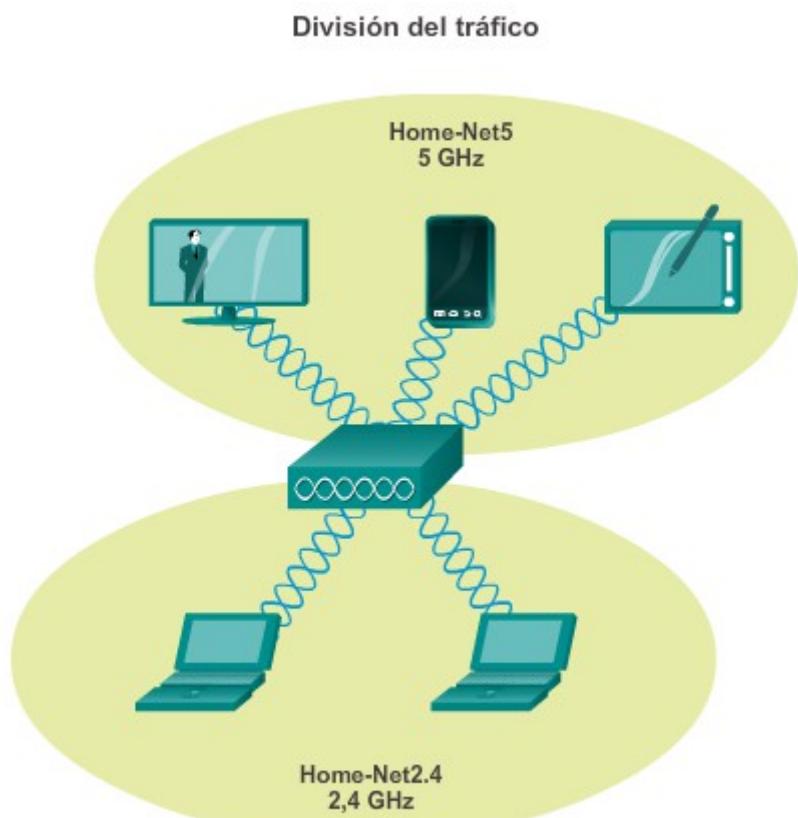
Existen varios motivos para usar un método de división del tráfico:

- La banda de 2,4 GHz puede ser adecuada para el tráfico de Internet básico que no depende del factor tiempo.
- El ancho de banda aún se puede compartir con otras WLAN cercanas.
- La banda de 5 GHz está mucho menos poblada que la banda de 2,4 GHz, ideal para la transmisión de multimedios.

- La banda de 5 GHz tiene más canales; por lo tanto, es más probable que el canal que se elija no tenga interferencia.

De manera predeterminada, los routers de banda dual usan el mismo nombre de red en las bandas de 2,4 GHz y de 5 GHz. La manera más simple de segmentar el tráfico es cambiar el nombre de una de las redes inalámbricas, como se muestra en la figura 2. Con un nombre descriptivo y separado, es más fácil conectarse a la red correcta.

Para mejorar el alcance de una red inalámbrica, asegúrese de que la ubicación física del router inalámbrico no presente obstrucciones, como muebles, elementos fijos y aparatos altos. Estos bloquean la señal, lo que reduce el alcance de la WLAN. Si esto tampoco resuelve el problema, se puede usar un extensor de alcance de Wi-Fi o la tecnología inalámbrica de red por línea eléctrica.



#### Capítulo 4: LAN inalámbricas 4.4.3.4 Actualización de firmware

El IOS del router Linksys EA6500 se denomina “firmware”. Es probable que se necesite actualizar el firmware si existe un problema con el dispositivo o si se incluye una nueva característica en la nueva actualización de firmware. Independientemente del motivo, la mayoría de los routers domésticos inalámbricos modernos ofrecen firmware actualizable.

Puede actualizar fácilmente el firmware de router Linksys EA6500 Smart Wi-Fi mediante los siguientes pasos:

**Paso 1.** Acceda a la página de inicio de Linksys Smart Wi-Fi.

**Paso 2.** Haga clic en el ícono **Connectivity**(Conectividad) para abrir la ventana de Connectivity (figura 1).

**Paso 3.** Bajo la etiqueta Firmware Update (Actualización de firmware), haga clic en**Check for Updates** (Buscar actualizaciones).

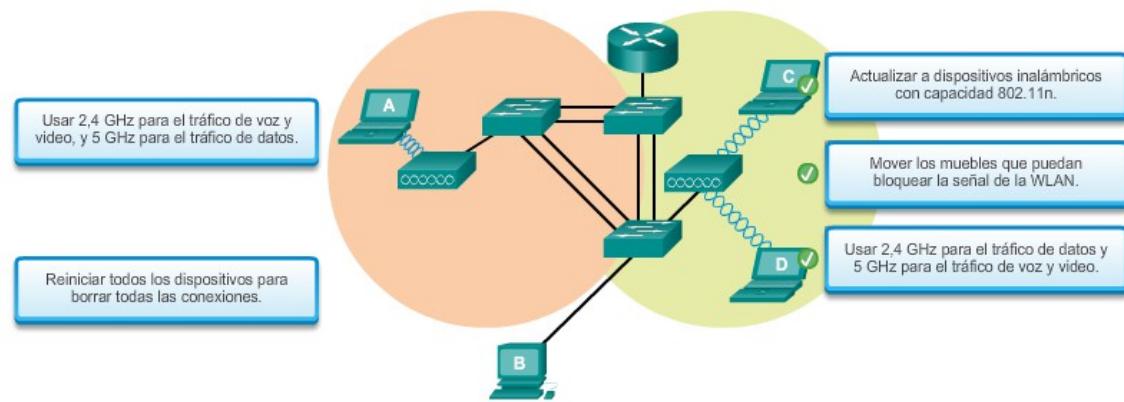
El router responde No updates found(No se encontraron actualizaciones) o solicita que se descargue e instale el nuevo firmware.

**Nota:** algunos routers requieren que el archivo del firmware se descargue antes y que después se cargue manualmente. Para esto, elija **Choose File** (Seleccionar archivo). Si una actualización de firmware falla o empeora la situación, el router puede cargar el firmware anterior al hacer clic en**Troubleshooting, Diagnostics** y, a continuación, **Restore previous firmware**(Restaurar firmware anterior, figura 2).

**Precaución:** no actualice el firmware a menos que existan problemas con el AP o que el nuevo firmware tenga una característica que desee.

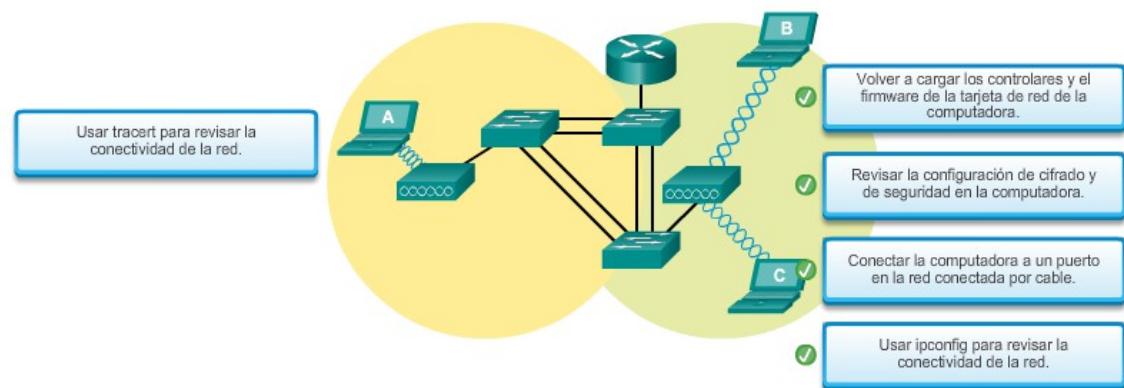
#### Capítulo 4: LAN inalámbricas 4.4.3.5 Actividad: Identificar la solución de la resolución de problemas

**Actividad (parte 1): Identificar la solución de la resolución de problemas**  
En el diagrama que se muestra, todas las computadoras se pueden conectar a la red, pero esta es lenta. Arrastre las tres soluciones que proporcionan el mejor resultado de rendimiento hasta los campos proporcionados. Haga clic en el botón 2 para continuar la actividad.

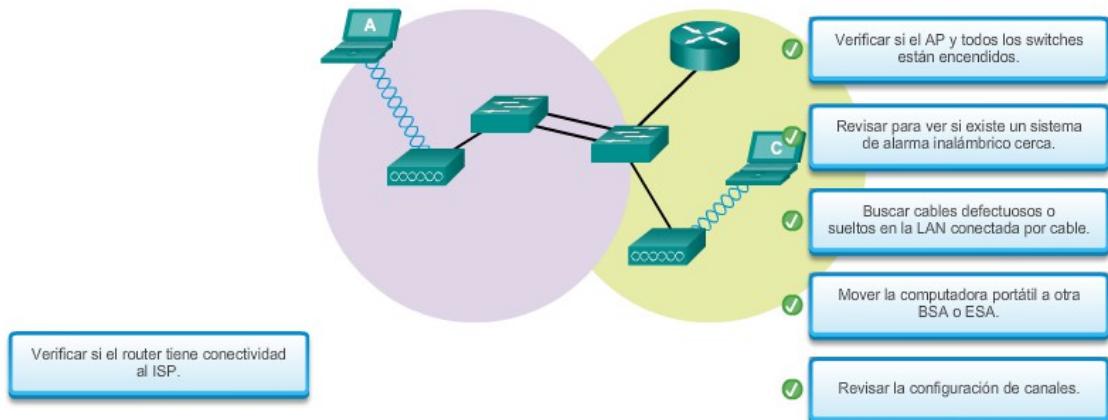


**Actividad (parte 2): Identificar la solución de la resolución de problemas**

En el diagrama que se muestra, el cliente inalámbrico B no se puede conectar a la WLAN. Arrastra las cuatro mejores soluciones que ayudarían a resolver los problemas de conectividad de la WLAN hasta los campos proporcionados. Haga clic en el botón 3 para continuar la actividad.

**Actividad (parte 3): Identificar la solución de la resolución de problemas**

En el diagrama que se muestra, la PC-A se puede conectar a la WLAN. La conexión es muy lenta y a veces se cae completamente. Arrastra las cinco soluciones que proporcionan información para corregir estos problemas hasta los campos proporcionados.



## Capítulo 4: LAN inalámbricas 4.5.1.1 Actividad de clase: Control interno y externo

### Control interno y externo

Se completó una evaluación que valida la necesidad de actualizar la red inalámbrica de su pequeña a mediana empresa. Se aprueba la compra de puntos de acceso para interiores y exteriores, y de un controlador inalámbrico. Debe comparar los modelos de equipos y las especificaciones antes de realizar la compra.

Por lo tanto, visite el sitio web “[Wireless Compare Products and Services](#)” y vea el gráfico de características para los puntos de acceso inalámbrico y los controladores para interiores y exteriores. Después de revisar el gráfico, advierte que hay términos que desconoce:

- Estándar federal de procesamiento de la información (FIPS)
- MIMO
- Tecnología Cisco CleanAir

- Cisco FlexConnect
- Band Select

Investigue los términos indicados anteriormente. Prepare un gráfico propio con los requisitos más importantes que indica la empresa para comprar los puntos de acceso inalámbrico para interiores y exteriores, y el controlador inalámbrico. Este gráfico lo ayudará a que el gerente de finanzas y el director validen la orden de compra.

#### [Actividad de clase: Control interno y externo](#)

#### Capítulo 4: LAN inalámbricas 4.5.1.2 Packet Tracer: desafío de integración de habilidades

##### **Información básica/situación**

En esta actividad del desafío, configurará las VLAN y el routing entre VLAN, DHCP, y PVST+ rápido. También se requiere que configure la seguridad inalámbrica en un router Linksys para obtener conectividad inalámbrica. Al final de la actividad, las computadoras no podrán hacer ping entre sí, pero deberán poder hacer ping al host externo.

##### [Packet Tracer: desafío de habilidades de integración \(instrucciones\)](#)

##### [Packet Tracer: desafío de integración de habilidades \(PKA\)](#)

#### Capítulo 4: LAN inalámbricas 4.5.1.3 Resumen

Las WLAN se suelen implementar en entornos domésticos, de oficina y de campus. Solo las frecuencias de 2,4 GHz, 5,0 GHz y 60 GHz se usan para las WLAN 802.11. El ITU-R regula la asignación del espectro de RF, mientras que el IEEE proporciona los estándares 802.11 para definir cómo se usan estas frecuencias para la subcapa física y MAC de las redes inalámbricas. Wi-Fi Alliance certifica que los productos de los proveedores cumplen con los estándares y las normas del sector.

Los clientes inalámbricos usan una NIC inalámbrica para conectarse a un dispositivo de infraestructura, como un router o un AP inalámbrico. Los clientes inalámbricos se conectan mediante un SSID. Los AP se pueden implementar como dispositivos independientes, en pequeños clústeres o en una red más grande basada en controladores.

Un AP Cisco Aironet puede usar una antena omnidireccional, una antena direccional o una antena Yagi para dirigir las señales. Los estándares IEEE 802.11n/ac/ad usan la tecnología MIMO para mejorar el rendimiento y admitir hasta cuatro antenas a la vez.

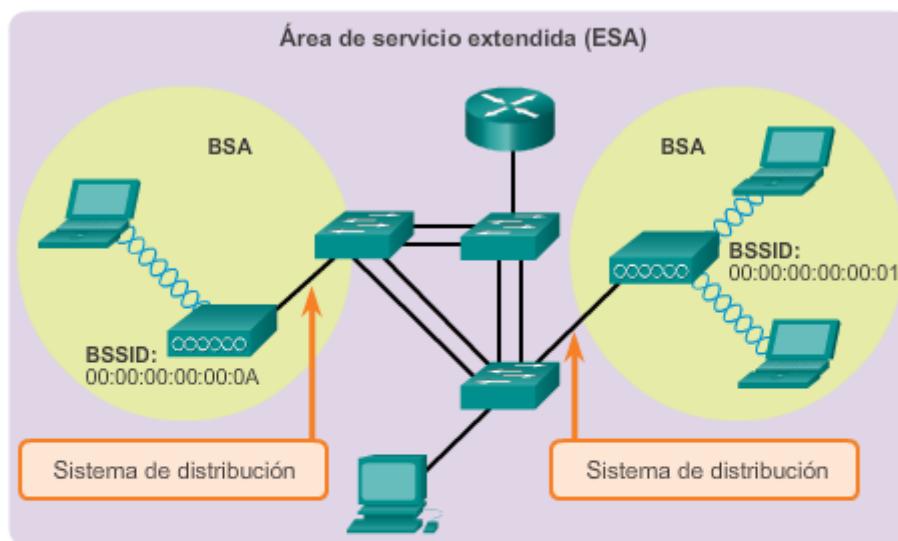
En el modo ad hoc o IBSS, dos dispositivos inalámbricos se conectan entre sí de manera P2P.

En el modo de infraestructura, los AP se conectan a la infraestructura de la red mediante un DS conectado por cable. Cada AP define un BSS y se identifica de forma exclusiva mediante su BSSID. Se pueden unir varios BSS para formar un ESS. El uso de un SSID específico en un ESS proporciona capacidad móvil sin inconvenientes entre los BSS en el ESS. Se pueden usar SSID adicionales para segregar el nivel de acceso a la red, definido por el SSID en uso.

Un cliente inalámbrico primero se autentica con un AP y después se asocia a ese AP. Se debe usar el estándar de autenticación 802.11i/WPA2. AES es el método de cifrado que se debe usar con WPA2.

Cuando se planifica una red inalámbrica, se deben usar canales no superpuestos al implementar varios AP para abarcar un área en particular. Debe existir una superposición de entre un 10 % y un 15 % entre las BSA en un ESS. Los AP Cisco admiten alimentación por Ethernet para simplificar la instalación.

Las redes inalámbricas son específicamente vulnerables a las amenazas, como los intrusos inalámbricos, los AP no autorizados, la intercepción de datos y los ataques DoS. Cisco desarrolló un conjunto de soluciones para mitigar este tipo de amenazas.



Resumen de ESS	
Modo de topología WLAN	Infraestructura
Topología inalámbrica 802.11	conjunto de servicios extendidos (ESS)
Cantidad de AP	2 o más
Área de cobertura de 802.11	Área de servicio extendida (ESA)

#### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.0.1.1 Introducción

OSPF es un protocolo de routing de estado de enlace popular que se puede ajustar de muchas maneras. Algunos de los métodos de ajuste más comunes incluyen la manipulación del proceso de elección del router designado/router designado de respaldo (DR/BDR), la propagación de rutas predeterminadas, el ajuste de las interfaces OSPFv2 y OSPFv3 y la habilitación de la autenticación.

En este capítulo sobre OSPF, se describen las características de estos ajustes, los comandos del modo de configuración que se utilizan para implementar estas características para IPv4 e IPv6, y los componentes y comandos que se usan para resolver problemas de OSPFv2 y OSPFv3.

**Después de completar este capítulo, podrá hacer lo siguiente:**

- Modificar la prioridad de interfaz OSPF para influenciar la elección del DR/BDR.
- Configurar un router para propagar una ruta predeterminada en una red OSPF.
- Modificar la configuración de las interfaces OSPF para mejorar el rendimiento de la red.
- Configurar la autenticación de OSPF para asegurar que las actualizaciones de routing sean seguras.
- Explicar el proceso y las herramientas que se usan para resolver problemas en una red OSPF de área única.
- Resolver problemas de entradas de rutas faltantes en una tabla de rutas OSPFv2 de área única.
- Resolver problemas de entradas de rutas faltantes en una tabla de rutas OSPFv3 de área única.

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.0.1.2 Actividad de clase:

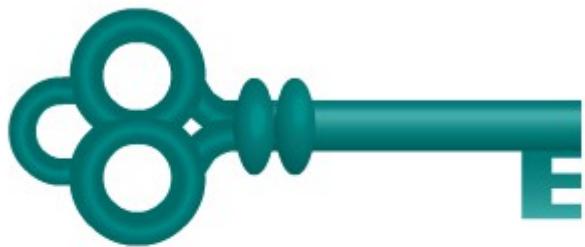
#### Elección del DR y el BDR

Usted intenta decidir cómo influir en la selección del router designado y del router designado de respaldo para la red OSPF. En esta actividad, se simula ese proceso.

Se presentan tres situaciones distintas sobre la elección del router designado. El enfoque se centra en la elección de un DR y un BDR para su grupo. Consulte el PDF correspondiente a esta actividad para obtener el resto de las instrucciones.

Si se dispone de tiempo adicional, se pueden combinar dos grupos para simular la elección del DR y el BDR.

[Actividad de clase: Elección del DR y el BDR](#)



*Ahora que aprendió los aspectos básicos, modifique los parámetros OSPF para influir en el resultado.*

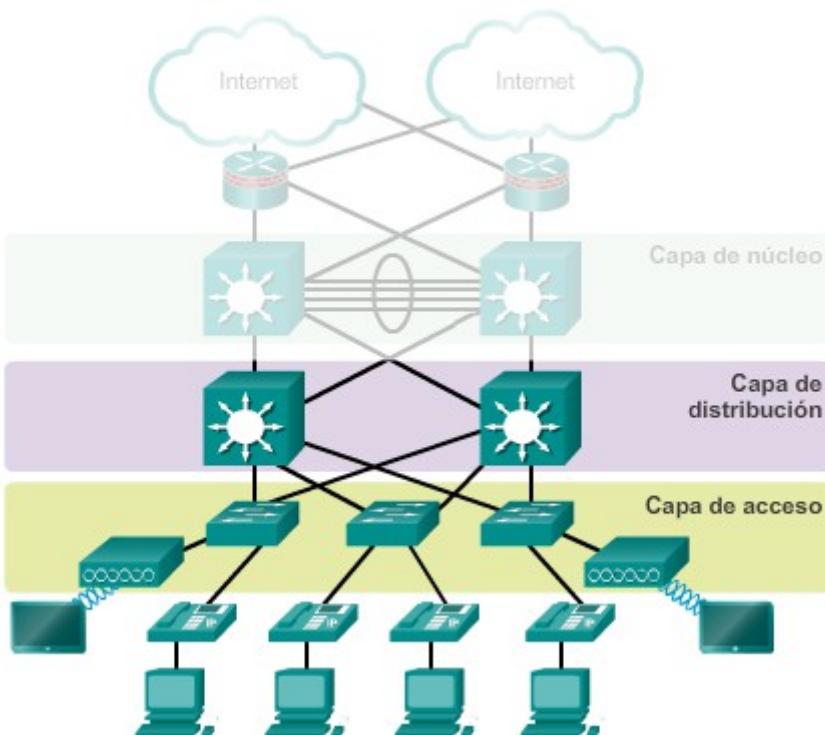
## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.1 Comparación entre routing y switching

Las redes escalables requieren un diseño de red jerárquico. El eje central de los capítulos anteriores fueron las capas de acceso y de distribución. Como se muestra en la figura 1, los switches de capa 2, la agregación de enlaces, la redundancia LAN y las LAN inalámbricas son tecnologías que le proporcionan al usuario acceso a los recursos de la red o mejoran dicho acceso.

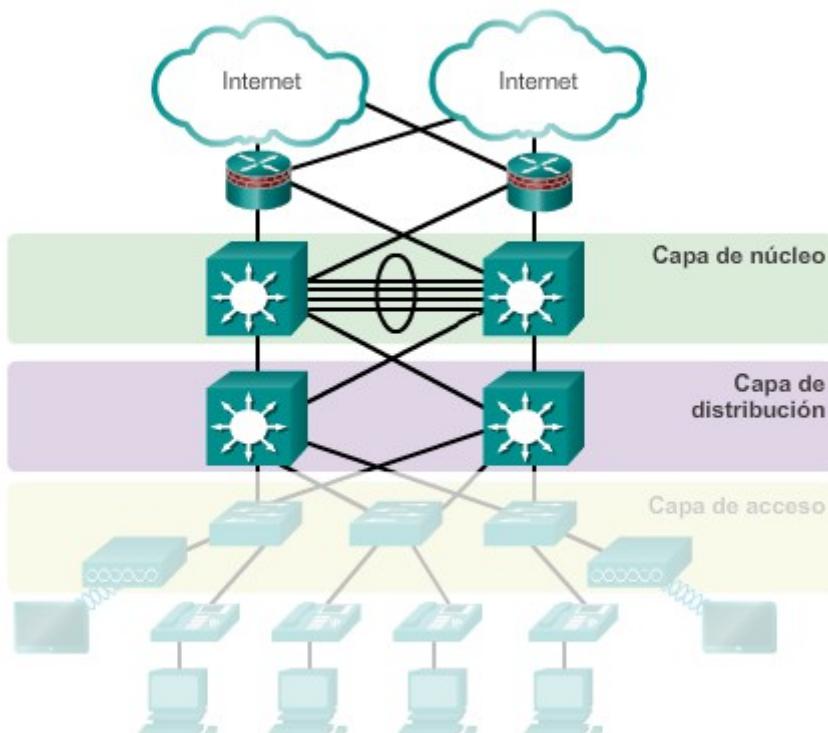
Las redes escalables también requieren que la posibilidad de conexión entre sitios sea óptima. La posibilidad de conexión de una red remota es proporcionada por los routers y los switches de capa 3 que operan en las capas de distribución y de núcleo, como se muestra en la figura 2. Los routers y los switches de capa 3 descubren las redes remotas de una de las dos maneras siguientes:

- **Manualmente:** las redes remotas se introducen manualmente en la tabla de rutas por medio de rutas estáticas.
- **Dinámicamente:** las rutas remotas se descubren automáticamente por medio de un protocolo de routing dinámico, como el protocolo de routing de gateway interior mejorado (EIGRP) o el protocolo OSPF (Open Shortest Path First).

## Tecnologías de capas de acceso y de distribución



## Routing en las capas de distribución y de núcleo



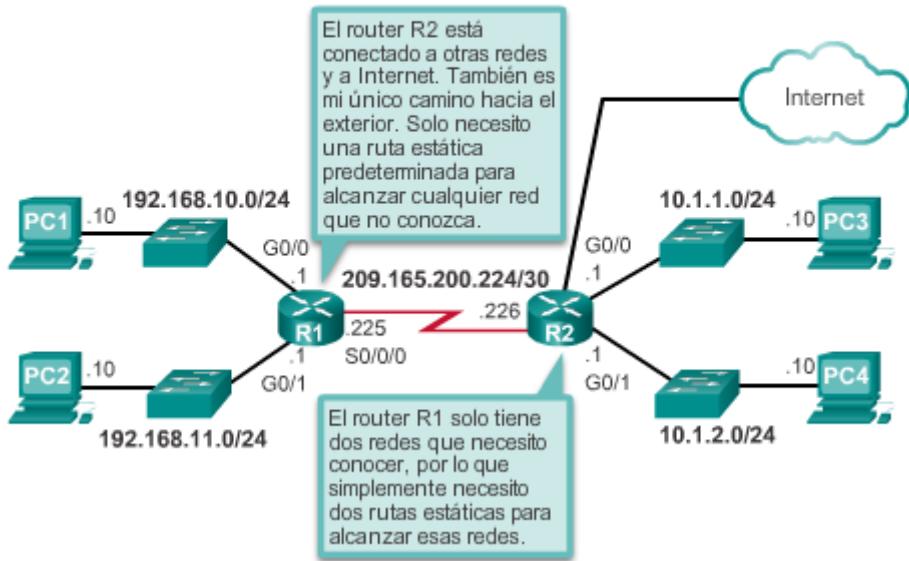
## Routing estático

En la ilustración, se proporciona una situación de ejemplo de routing estático. Un administrador de red puede configurar una ruta estática manualmente para alcanzar una red específica. A diferencia de un protocolo de routing dinámico, las rutas estáticas no se actualizan automáticamente, y se deben volver a configurar manualmente cada vez que cambia la topología de la red. Una ruta estática no cambia hasta que el administrador la vuelve a configurar en forma manual.

El routing estático tiene tres usos principales:

- Facilita el mantenimiento de la tabla de routing en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
- Proporciona routing hacia las redes de rutas internas y desde estas. Una red de rutas internas es aquella a la cual se accede a través de una única ruta y cuyo router tiene solo un vecino.
- Utiliza una única ruta predeterminada para representar una ruta hacia cualquier red que no tenga una coincidencia más específica con otra ruta en la tabla de routing. Las rutas predeterminadas se utilizan para enviar tráfico a cualquier destino que esté más allá del próximo router ascendente.

### Situación de rutas estáticas y predeterminadas



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.3 Protocolos de routing dinámico

## Enrutamiento dinámico

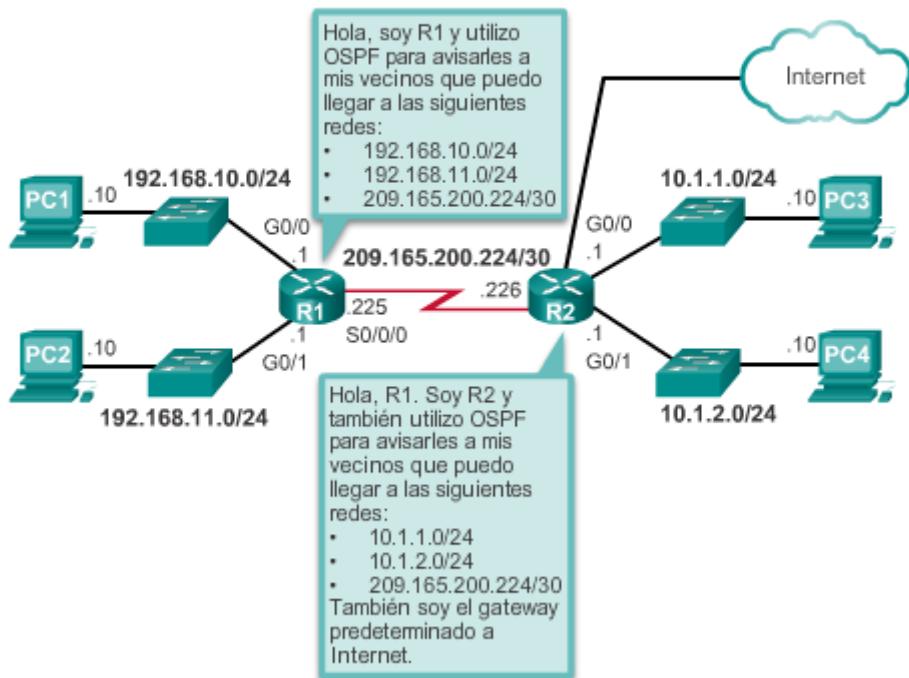
Los protocolos de routing permiten que los routers compartan información sobre redes remotas de forma dinámica, como se muestra en la ilustración. Los routers que reciben la actualización agregan esa información automáticamente a sus propias tablas de routing. A continuación, los protocolos de routing determinan la mejor ruta hacia cada red. Uno de los beneficios principales de los protocolos de routing dinámico es que los routers intercambian información de routing cuando se produce un cambio en la topología. Este intercambio permite a los routers obtener automáticamente información 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, usar protocolos de routing dinámico implica el costo de dedicar parte de los recursos de un router a la operación del protocolo, incluidos tiempo de CPU y 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. Sin embargo, es importante comprender que el routing estático y el routing dinámico no son mutuamente excluyentes. En cambio, la mayoría de las redes utilizan una combinación de protocolos de routing dinámico y rutas estáticas.

Los dos protocolos de routing dinámico más comunes son EIGRP y OSPF. Este capítulo se centra en OSPF.

**Nota:** todos los protocolos de routing dinámico tienen capacidad para anunciar y propagar rutas estáticas en las actualizaciones de routing.

### Situación de protocolo de routing dinámico



## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.4 Open Shortest

### Path First

OSPF es un protocolo de routing de estado de enlace que se implementa con frecuencia y se desarrolló como un reemplazo para el protocolo de routing vector distancia RIP. Sin embargo, OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.

Las características de OSPF, que se muestran en la ilustración, incluyen lo siguiente:

- **Sin clase:** fue concebido como un protocolo sin clase, de modo que admite VLSM y CIDR.
- **Eficaz:** los cambios de routing desencadenan actualizaciones de routing (no hay actualizaciones periódicas). Usa el algoritmo SPF para elegir la mejor ruta.
- **Convergencia rápida:** propaga rápidamente los cambios que se realizan a la red.
- **Escalable:** funciona bien en redes pequeñas y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.
- **Seguro:** admite la autenticación de síntesis del mensaje 5 (MD5). Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de routing cifradas de peers con la misma contraseña compartida previamente.

**Características de OSPF**



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.5 Configuración de OSPF de área única

Este capítulo se centra en ajustes y resolución de problemas de OSPF. Sin embargo, se recomienda revisar una implementación básica del protocolo de routing OSPF.

En el ejemplo de la figura 1, se muestra la topología que se usa para configurar OSPFv2. Los routers en la topología tienen una configuración inicial, que incluye direcciones de interfaz habilitadas. En este momento, ninguno de los routers tiene configurado routing estático o routing dinámico. Todas las interfaces en los routers R1, R2 y R3 (excepto la interfaz loopback en el R2) se encuentran dentro del área de red troncal de OSPF. El router ISP se usa como gateway del dominio de routing a Internet.

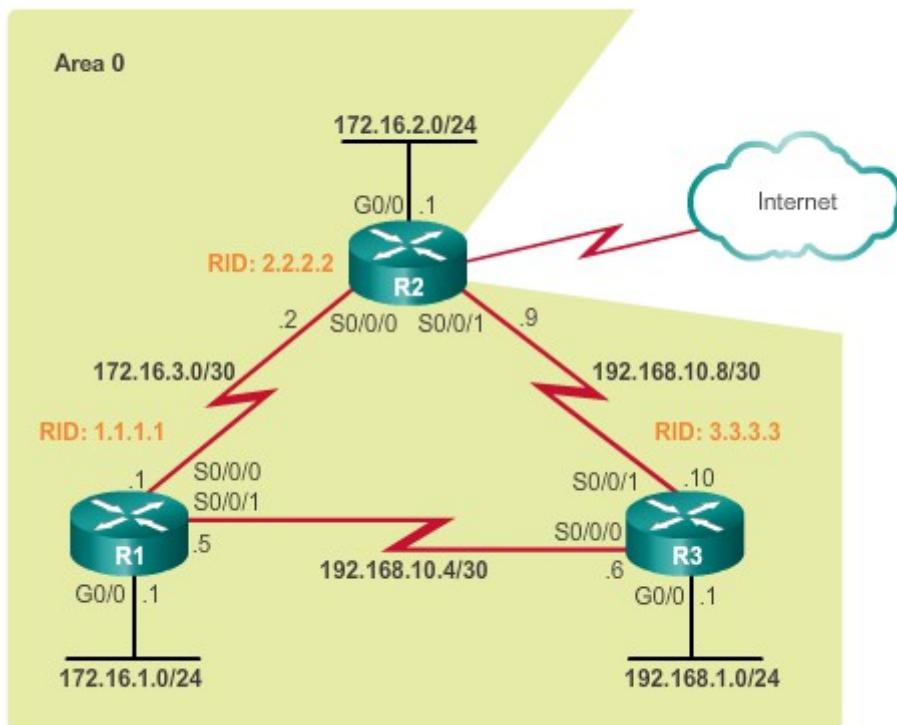
En la figura 2, la interfaz Gigabit Ethernet 0/0 del R1 se configura para reflejar su ancho de banda real de 1 000 000 kilobits (es decir, 1 000 000 000 b/s). Luego en el modo de configuración del router OSPF, se asigna la ID del router, se ajusta el ancho de banda de referencia para las interfaces rápidas y se anuncian las tres redes conectadas al R1. Observe la forma en que se usa la máscara wildcard para identificar las redes específicas.

En la figura 3, la interfaz Gigabit Ethernet 0/0 del R2 también se configura para reflejar su ancho de banda real, se asigna la ID del router, se ajusta el ancho de banda de referencia para las interfaces rápidas y se anuncian las tres redes conectadas al R2. Observe la forma en que se puede evitar el uso de la máscara wildcard al identificar la interfaz del router propiamente dicha con una máscara de cuádruple cero. Esto hace que OSPF use la máscara de subred asignada a la interfaz del router como la máscara de red anunciada.

Utilice el verificador de sintaxis de la figura 4 para ajustar el ancho de banda en la interfaz G0/0 del R3, ingresar al modo de configuración del router OSPF, asignar la ID del router correcta, ajustar el ancho de banda de referencia y anunciar las tres redes conectadas directamente mediante las interfaces del router y la máscara wildcard de cuádruple cero.

Observe los mensajes informativos que muestran que el R3 estableció una plena adyacencia de vecino con el R1 con la ID de router 1.1.1.1 y con el R2 con la ID de router 2.2.2.2. Se produjo la convergencia de la red OSPF.

## Topología OSPF de referencia



### Configuración de OSPF de área única en el R1

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# exit
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent
across all routers.
R1(config-router)# network 172.16.1.0 0.0.0.255 area 0
R1(config-router)# network 172.16.3.0 0.0.0.3 area 0
R1(config-router)# network 192.168.10.4 0.0.0.3 area 0
R1(config-router)#
R1(config-router)# passive-interface g0/0
R1(config-router)#[/pre>
```

## Configuración de OSPF de área única en el R2

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# exit
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent
across all routers.
R2(config-router)# network 172.16.2.1 0.0.0.0 area 0
R2(config-router)# network 172.16.3.2 0.0.0.0 area 0
R2(config-router)# network 192.168.10.9 0.0.0.0 area 0
R2(config-router)#
R2(config-router)# passive-interface g0/0
R2(config-router)#

```

## Configuración de OSPF de área única en el R3

**Configure el ancho de banda de GigabitEthernet0/0 en 1 000 000 y vuelva al modo de configuración global.**

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# bandwidth 1000000
R3(config-if)# exit
```

**Configure lo siguiente para OSPF con la ID de proceso 10:**

- Establezca la ID del router en 3.3.3.3.
- Establezca el ancho de banda de referencia de costo en 1000 para que se corresponda con gigabit.
- Anuncie las interfaces 192.168.1.1, 192.168.10.6 y 192.168.10.10 para el área 0.
- Establezca la interfaz g0/0 como pasiva.

```
R3(config)# router ospf 10
R3(config-router)# router-id 3.3.3.3
R3(config-router)# auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all
routers.

R3(config-router)# network 192.168.1.1 0.0.0.0 area 0
R3(config-router)# network 192.168.10.6 0.0.0.0 area 0
R3(config-router)# network 192.168.10.10 0.0.0.0 area 0
R3(config-router)# passive-interface g0/0
*Aug 28 17:15:26.547: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
*Aug 28 17:15:26.863: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config-router)#

```

**Configuró correctamente OSPF de área única en el R3.**

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.6 Verificación de

### OSPF de área única

Algunos de los comandos útiles para verificar OSPF son los siguientes:

- **show ip ospf neighbor**: comando para verificar que el router formó una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.
- **show ip protocols**: comando que proporciona una manera rápida de verificar información fundamental de configuración de OSPF. Esta incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es de 110.
- **show ip ospf**: comando que se usa para mostrar la ID del proceso OSPF y la ID del router, así como el SPF de OSPF y la información de área OSPF.
- **show ip ospf interface**: comando que proporciona una lista detallada de cada interfaz con OSPF habilitado y es muy útil para determinar si las instrucciones **network** se compusieron correctamente.
- **show ip ospf interface brief**: comando útil para mostrar un resumen y el estado de las interfaces con OSPF habilitado.

En las figuras 1 a 5, se muestra el resultado correspondiente a cada comando de verificación que se introdujo en el R1.

Utilice el verificador de sintaxis de la figura 6 para verificar la adyacencia de vecino y la información fundamental de configuración de OSPF, y para mostrar un resumen de las interfaces con OSPF habilitado en el R2.

Utilice el verificador de sintaxis de la figura 7 para verificar la adyacencia de vecino y la información fundamental de configuración de OSPF, y para mostrar un resumen de las interfaces con OSPF habilitado en el R3.

```
R1# show ip ospf neighbor

Neighbor ID      Pri  State        Dead Time     Address          Interface
3.3.3.3           0    FULL/        - 00:00:32    192.168.10.6   Serial0/0/1
2.2.2.2           0    FULL/        - 00:00:38    172.16.3.2     Serial0/0/0
R1#
```

### Verificación de la información de configuración de OSPF en el R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.255 area 0
    172.16.3.0 0.0.0.3 area 0
    192.168.10.4 0.0.0.3 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          00:12:14
    2.2.2.2           110          00:12:46
  Distance: (default is 110)

R1#
```

### Verificación de la información de algoritmo y de ID de OSPF en el R1

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
Start time: 00:06:18.952, Time elapsed: 00:39:56.400

<resultado omitido>

Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 1000 mbps
Area BACKBONE(0)
  Number of interfaces in this area is 3
  Area has no authentication
  SPF algorithm last executed 00:15:21.436 ago
  SPF algorithm executed 6 times
  Area ranges are
    Number of LSA 3. Checksum Sum 0x023523
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

R1#
```

### Verificación de la interfaz OSPF en el R1

```
R1# show ip ospf interface
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 172.16.1.1/24, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
    0            1        no          no          Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 172.16.1.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  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)
Serial0/0/1 is up, line protocol is up
  Internet Address 192.168.10.5/30, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
Cost: 647

<resultado omitido>
```

### Visualización de un resumen de las interfaces OSPF configuradas en el R1

```
R1# show ip ospf interface brief
Interface    PID    Area    IP Address/Mask    Cost    State Nbrs F/C
Gi0/0        10     0        172.16.1.1/24      1       DR      0/0
Se0/0/1      10     0        192.168.10.5/30    647     P2P     1/1
Se0/0/0      10     0        172.16.3.1/30      647     P2P     1/1
R1#
```

## Verificación de la configuración de OSPF de área única en el R2

### Muestre la tabla de vecinos OSPF.

```
R2# show ip ospf neighbor  
  
Neighbor ID Pri State      Dead Time Address          Interface  
3.3.3.3       0 FULL/    - 00:00:39  192.168.10.10  Serial0/0/1  
1.1.1.1       0 FULL/    - 00:00:32  172.16.3.1    Serial0/0/0
```

### Muestre los protocolos IP configurados en el R2.

```
R2# show ip protocols  
*** IP Routing is NSF aware ***  
  
Routing Protocol is "ospf 10"  
  Outgoing update filter list for all interfaces is not set  
  Incoming update filter list for all interfaces is not set  
  Router ID 2.2.2.2  
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa  
  Maximum path: 4  
  Routing for Networks:  
    172.16.2.1 0.0.0.0 area 0  
    172.16.3.2 0.0.0.0 area 0  
    192.168.10.9 0.0.0.0 area 0  
  Passive Interface(s):  
    GigabitEthernet0/0  
  Routing Information Sources:  
    Gateway          Distance      Last Update  
    3.3.3.3           110          00:34:32  
    1.1.1.1           110          00:35:05  
  Distance: (default is 110)
```

### Muestre la lista resumida de interfaces OSPF.

```
R2# show ip ospf interface brief  
Interface  PID  Area  IP Address/Mask   Cost  State Nbrs F/C  
Gi0/0     10    0     172.16.2.1/24     1     DR    0/0  
Se0/0/1   10    0     192.168.10.9/30   647   P2P   1/1  
Se0/0/0   10    0     172.16.3.2/30     647   P2P   1/1  
R2#
```

Verificó correctamente la configuración de OSPF de área única en el R2.

## Verificación de la configuración de OSPF de área única en el R

### Muestre la tabla de vecinos OSPF.

```
R3# show ip ospf neighbor

Neighbor ID  Pri  State      Dead Time   Address          Interface
2.2.2.2       0    FULL/ -  00:00:35   192.168.10.9  Serial0/0/1
1.1.1.1       0    FULL/ -  00:00:35   192.168.10.5  Serial0/0/0
```

### Muestre los protocolos IP configurados en el R3.

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.1 0.0.0.0 area 0
    192.168.10.6 0.0.0.0 area 0
    192.168.10.10 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    2.2.2.2           110          00:35:41
    1.1.1.1           110          00:35:41
  Distance: (default is 110)
```

### Muestre la lista resumida de interfaces OSPF.

```
R3# show ip ospf interface brief
Interface  PID  Area  IP Address/Mask     Cost  State Nbrs F/C
Gi0/0      10   0     192.168.1.1/24      1     DR    0/0
Se0/0/1    10   0     192.168.10.10/30    647   P2P   1/1
Se0/0/0    10   0     192.168.10.6/30    647   P2P   1/1
R3#
```

Verificó correctamente la configuración de OSPF de área única en el R3.

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.7 Configuración de OSPFv3 de área única

A continuación, se presenta un repaso de una implementación básica del protocolo de routing OSPFv3 para IPv6.

En el ejemplo de la figura 1, se muestra la topología que se usa para configurar OSPFv3. Los routers en la topología tienen una configuración inicial, que incluye direcciones de interfaz IPv6 habilitadas. En este momento, ninguno de los routers tiene configurado routing estático o routing dinámico. Todas las interfaces en los routers R1, R2 y R3 (excepto la interfaz loopback en el R2) se encuentran dentro del área de red troncal de OSPF.

En la figura 2, en el modo de configuración del router OSPFv3 del R1, la ID del router se asigna manualmente y el ancho de banda de referencia se ajusta para las interfaces rápidas. A continuación, se configuran las interfaces que participan en OSPFv3. También se configura la

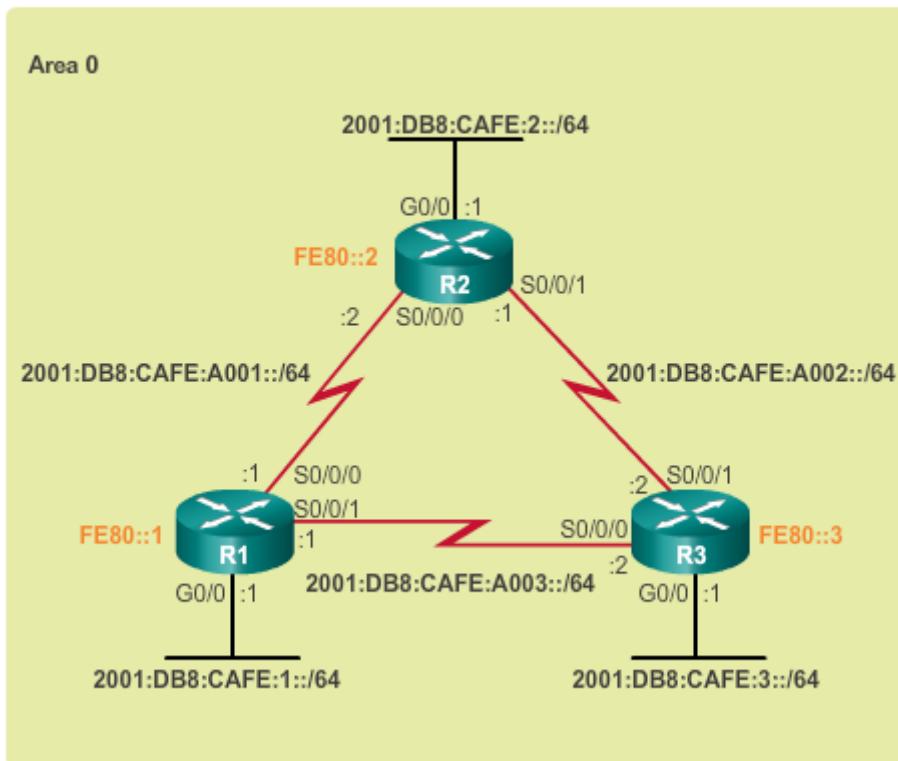
interfaz Gigabit Ethernet 0/0 para reflejar su ancho de banda real. Observe que, cuando se configura OSPFv3, no se requiere una máscara wildcard.

En la figura 3, en el modo de configuración del router OSPFv3 del R2, la ID del router se asigna manualmente y el ancho de banda de referencia se ajusta para las interfaces rápidas. A continuación, se configuran las interfaces que participan en OSPFv3. Aquí también se configura la interfaz Gigabit Ethernet 0/0 para reflejar su ancho de banda real.

Utilice el verificador de sintaxis de la figura 4 para asignar manualmente la ID del router y ajustar el ancho de banda de referencia. A continuación, configure las interfaces según corresponda, empezando por la interfaz Gigabit Ethernet 0/0. También asigne el ancho de banda real a esa interfaz.

Observe los mensajes informativos que muestran que el R3 estableció una plena adyacencia de vecino con el R1 con la ID de router 1.1.1.1 y con el R2 con la ID de router 2.2.2.2. Se produjo la convergencia de la red OSPFv3.

#### Topología de referencia de OSPFv3 de área única



### Configuración de OSPFv3 de área única en el R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all
routers.
R1(config-rtr)#
R1(config-rtr)# interface GigabitEthernet 0/0
R1(config-if)# bandwidth 1000000
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

### Configuración de OSPFv3 de área única en el R2

```
R2(config)# ipv6 router ospf 10
R2(config-rtr)# router-id 2.2.2.2
R2(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all
routers.
R2(config-rtr)#
R2(config-rtr)# interface GigabitEthernet 0/0
R2(config-if)# bandwidth 1000000
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)#
R2(config-if)# interface Serial0/0/0
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)#
R2(config-if)# interface Serial0/0/1
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)# end
R2#
*Aug 28 19:02:47.991: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
GigabitEthernet0/0 from LOADING to FULL, Loading Done
*Aug 28 19:02:48.423: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
*Aug 28 19:02:48.959: %SYS-5-CONFIG_I: Configured from console by
console
R2#
```

## Configuración de OSPF de área única en el R3

Configure lo siguiente para OSPFv3 con la ID de proceso 10:

- Establezca la ID del router en 3.3.3.3.
- Establezca el ancho de banda de referencia de costo en 1000 para que se corresponda con gigabit.
- Establezca el ancho de banda en la interfaz GigabitEthernet0/0 en 1 000 000.
- Habilite OSPFv3 para el área 0 de la ID de proceso 10 en GigabitEthernet0/0, Serial0/0/0 y Serial0/0/1.
- Vuelva directamente al modo EXEC privilegiado.

```
R3(config)# ipv6 router ospf 10
R3(config-rtr)# router-id 3.3.3.3
R3(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-10-IPv6: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all
routers.
R3(config-rtr)# interface GigabitEthernet0/0
R3(config-if)# bandwidth 1000000
R3(config-if)# ipv6 ospf 10 area 0
R3(config-if)# interface Serial0/0/0
R3(config-if)# ipv6 ospf 10 area 0
R3(config-if)# interface Serial0/0/1
R3(config-if)# ipv6 ospf 10 area 0
R3(config-if)# end
R3#
*Aug 28 19:07:34.723: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1
on GigabitEthernet0/0 from LOADING to FULL, Loading Done
*Aug 28 19:07:34.723: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2
on GigabitEthernet0/0 from LOADING to FULL, Loading Done
*Aug 28 19:07:35.163: %OSPFv3-5-ADJCHG: Process 10, Nbr 1.1.1.1
on Serial0/0/0 from LOADING to FULL, Loading Done
*Aug 28 19:07:35.547: %OSPFv3-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/1 from LOADING to FULL, Loading Done
R3#
```

Configuró correctamente OSPFv3 de área única en el R3.

### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.8 Verificación de

#### OSPFv3 de área única

Algunos de los comandos útiles para verificar OSPFv3 son los siguientes:

- **show ipv6 ospf neighbor**: comando para verificar que el router formó una adyacencia con los routers vecinos. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL, los dos routers no formaron una adyacencia OSPF.
- **show ipv6 protocols**: este comando proporciona una manera rápida de verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.

- **show ipv6 route ospf:** este comando proporciona datos específicos sobre rutas OSPFv3 en la tabla de routing.
- **show ipv6 ospf interface brief:** comando útil para mostrar un resumen y el estado de las interfaces con OSPFv3 habilitado.

En las figuras 1 a 4, se muestra el resultado correspondiente a cada comando de verificación que se introdujo en el R1.

#### **Verificación de las adyacencias de vecinos del R1**

```
R1# show ipv6 ospf neighbor
OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

Neighbor ID Pri State      Dead Time Interface ID Interface
3.3.3.3    0 FULL/ -      00:00:31  6             Serial0/0/1
2.2.2.2    0 FULL/ -      00:00:37  6             Serial0/0/0
2.2.2.2    1 FULL/BDR    00:00:38  3             GigabitEthernet0/0
3.3.3.3    1 FULL/DROTHER 00:00:32  3             GigabitEthernet0/0
R1#
```

#### **Verificación de la información de configuración de OSPFv3 en el R1**

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

## Verificación de las rutas OSPFv3 en la tabla de routing IPv6 en el R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static,
       U - Per-user Static route
       B - BGP, R - RIP, N - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
       D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
       DCE - Destination
       Ndr - Redirect, O - OSPF Intra, OI - OSPF Inter,
       OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1,
       ON2 - OSPF NSSA ext 2
O  2001:DB8:CAFE:2::/64 [110/1]
  via GigabitEthernet0/0, directly connected
O  2001:DB8:CAFE:3::/64 [110/1]
  via GigabitEthernet0/0, directly connected
O  2001:DB8:CAFE:A002::/64 [110/648]
  via FE80::2, GigabitEthernet0/0
  via FE80::3, GigabitEthernet0/0
R1#
```

## Visualización de un resumen de las interfaces con OSPFv3 habilitado en el R1

```
R1# show ipv6 ospf interface brief
Interface    PID   Area          Intf ID     Cost  State Nbrs F/C
Se0/0/1      10    0             7           647   P2P   1/1
Se0/0/0      10    0             6           647   P2P   1/1
Gi0/0        10    0             3           1     DR    2/2
R1#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.1.9 Práctica de laboratorio: configuración de OSPFv2 básico de área única

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar y verificar el routing OSPF
- Parte 3: cambiar las asignaciones de ID del router
- Parte 4: configurar interfaces OSPF pasivas
- Parte 5: cambiar las métricas de OSPF

## [Práctica de laboratorio: configuración de OSPFv2 básico de área única](#)

### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.1 Tipos de redes

#### OSPF

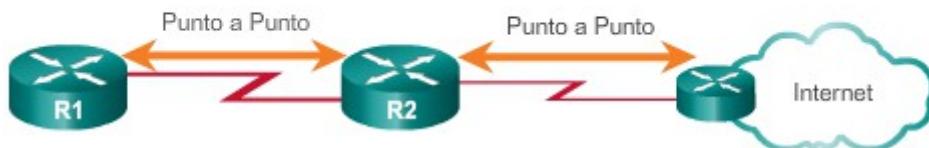
Para configurar los ajustes de OSPF, empiece por una implementación básica del protocolo de routing OSPF.

OSPF define cinco tipos de redes, como se muestra en las figuras 1 a 5:

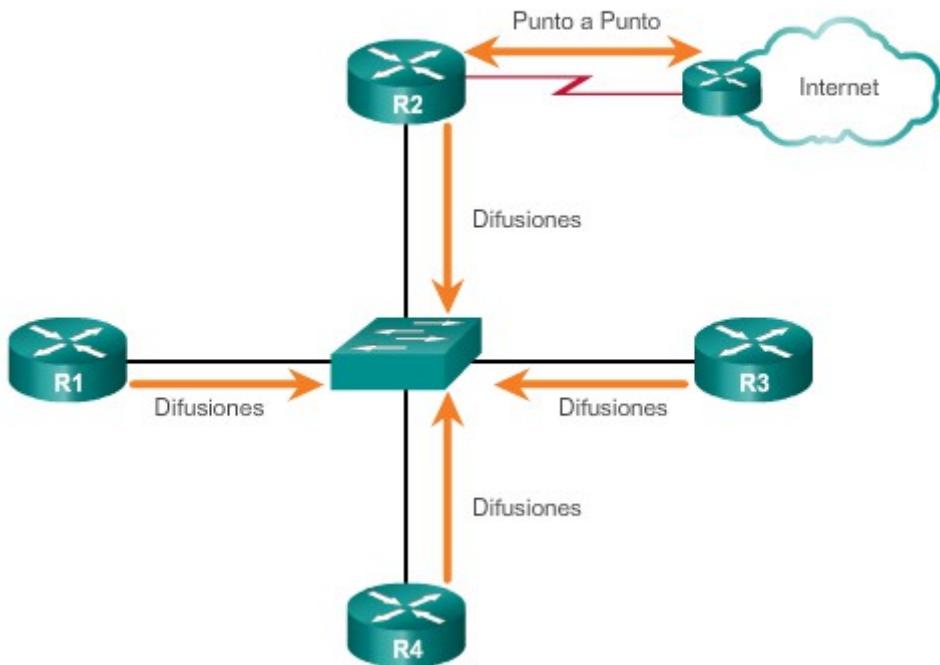
- **Punto a punto:** dos routers interconectados por medio de un enlace común. No hay otros routers en el enlace. Con frecuencia, esta es la configuración en los enlaces WAN (figura 1).
- **Multiacceso con difusión:** varios routers interconectados por medio de una red Ethernet (figura 2).
- **Multiacceso sin difusión (NBMA):** varios routers interconectados en una red que no permite transmisiones por difusión, como Frame Relay (figura 3).
- **Punto a multipunto:** varios routers interconectados en una topología hub-and-spoke por medio de una red NBMA. Con frecuencia, se usa para conectar sitios de sucursal (spokes, que significa “rayo”) a un sitio central (hub, que significa “concentrador”) (figura 4).
- **Enlaces virtuales:** una red OSPF especial que se usa para interconectar áreas OSPF distantes al área de red troncal (figura 5)

Una red de accesos múltiples es una red con varios dispositivos en los mismos medios compartidos, que comparten comunicaciones. Las LAN Ethernet son el ejemplo más común de redes multiacceso con difusión. En las redes de difusión, todos los dispositivos en la red pueden ver todas las tramas de difusión y de multidifusión. 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.

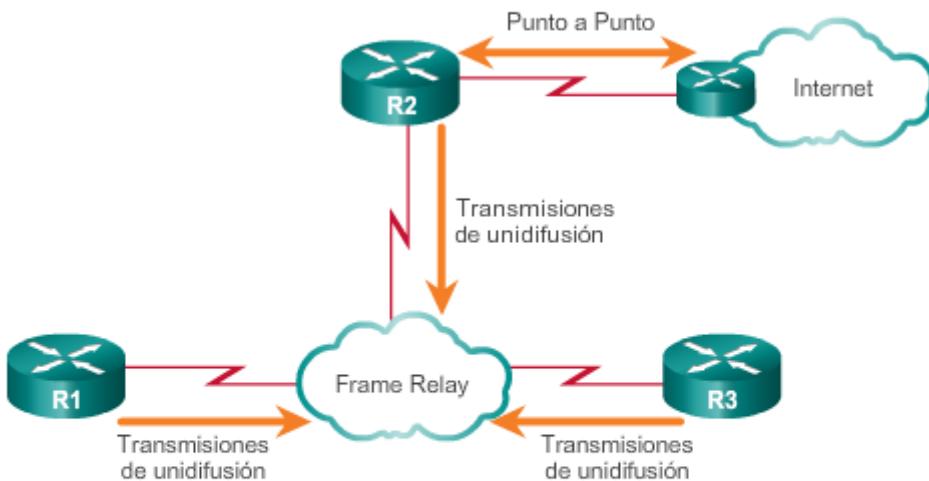
#### **Redes OSPF punto a punto**



### Red OSPF de accesos múltiples

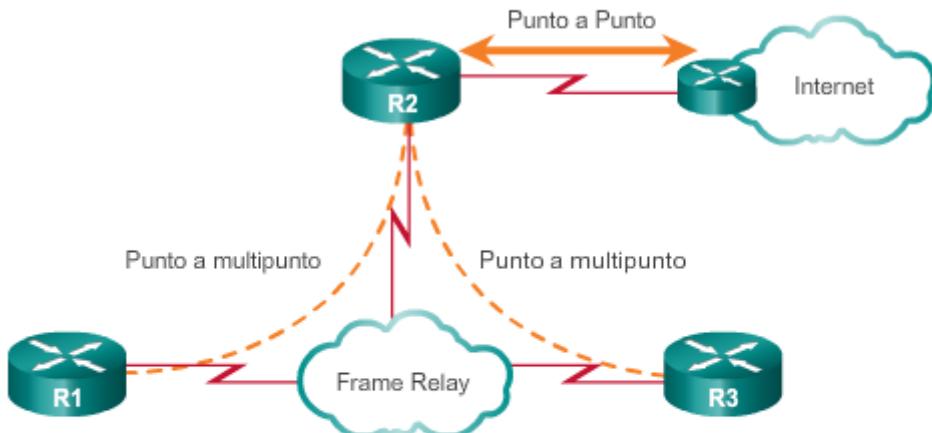


### Red OSPF multiacceso sin difusión



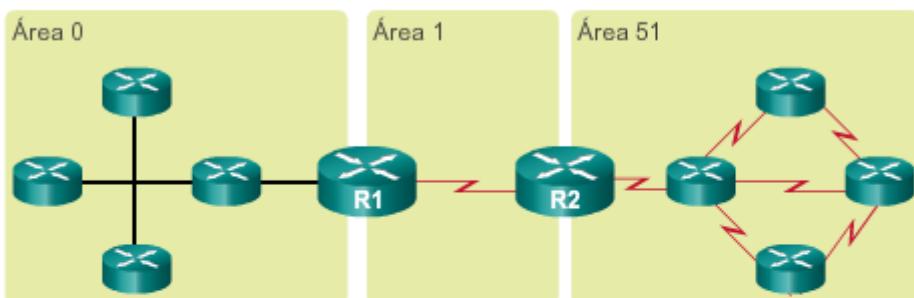
- En esta situación, el R1, el R2 y el R3 se interconectan mediante una red Frame Relay.
- Frame relay no permite las difusiones.
- OSPF se debe configurar según corresponda para crear adyacencias de vecinos.

### Red OSPF punto a multipunto



- En esta situación, el R1, el R2 y el R3 se interconectan mediante una red Frame Relay.
- Frame relay no permite las difusiones.
- OSPF se debe configurar según corresponda para crear adyacencias de vecinos.

### Red OSPF de enlace virtual



- En esta situación, el área 51 no puede conectarse directamente al área 0.
- Debe configurarse un área OSPF especial para conectar el área 51 al área 0.
- El área 1 del R2 y el R1 debe configurarse como un enlace virtual.

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.2 Desafíos en redes de accesos múltiples

Las redes de accesos múltiples pueden crear dos retos para OSPF en relación con la saturación de las LSA:

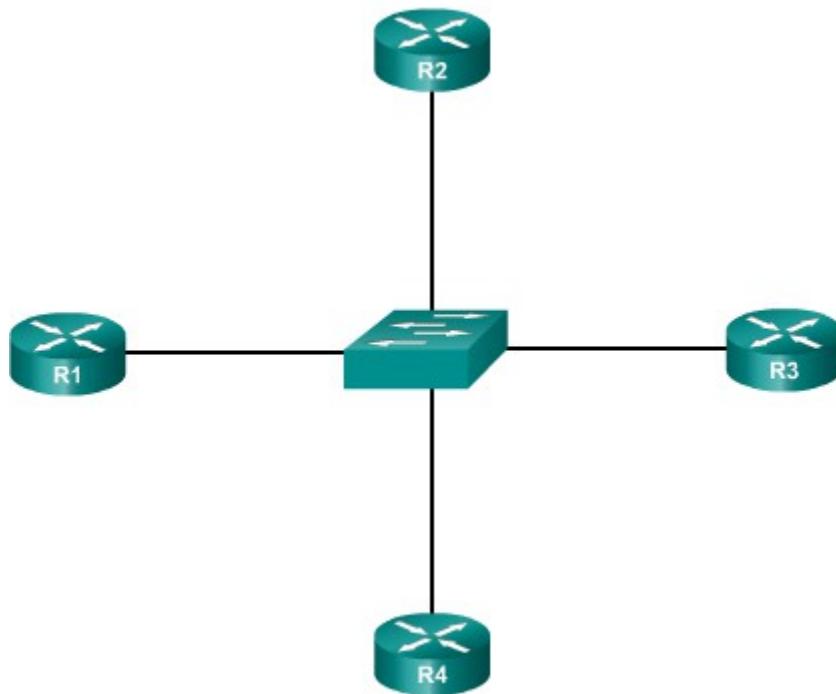
- **Creación de varias adyacencias:** las redes Ethernet podrían interconectar muchos routers OSPF con un enlace común. La creación de adyacencias con cada router es innecesaria y no se recomienda, ya que conduciría al intercambio de una cantidad excesiva de LSA entre routers en la misma red.
- **Saturación intensa con LSA:** los routers de estado de enlace saturan con sus paquetes de estado de enlace cuando se inicializa OSPF o cuando se produce un cambio en la topología. Esta saturación puede llegar a ser excesiva.

Para calcular la cantidad de adyacencias requeridas, se puede usar la siguiente fórmula. La cantidad de adyacencias requeridas para cualquier cantidad de routers (designada como  $n$ ) en una red de accesos múltiples es la siguiente:

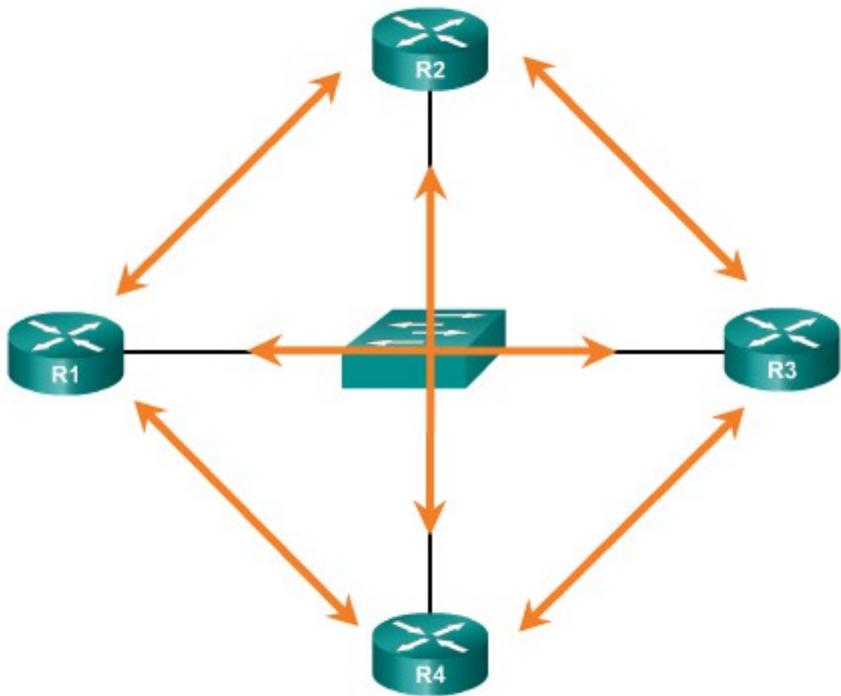
$$n(n - 1) / 2$$

En la figura 1, se muestra una topología simple de cuatro routers, los cuales están conectados a la misma red Ethernet de accesos múltiples. Sin algún tipo de mecanismo para reducir el número de adyacencias, colectivamente estos routers formarían seis adyacencias:  $4(4 - 1) / 2 = 6$ , como se muestra en la figura 2. En la figura 3, se muestra que, a medida que se agregan routers a la red, el número de adyacencias aumenta drásticamente.

**Red OSPF de accesos múltiples**



### Establecimiento de seis adyacencias de vecinos



Más routers = más adyacencias

Routers n	Adyacencias $n(n-1)/2$
4	6
5	10
10	45
20	190
50	1225

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.3 Router designado

### OSPF

La solución para administrar la cantidad de adyacencias y la saturación con LSA en una red de accesos múltiples es el DR. En las redes de accesos múltiples, OSPF elige un DR para que funcione como punto de recolección y distribución de las LSA enviadas y recibidas. También se elige un BDR en caso de que falle el DR. El BDR escucha este intercambio en forma pasiva y mantiene una relación con todos los routers. Si el DR deja de producir paquetes de saludo, el BDR se asciende a sí mismo y asume la función de DR.

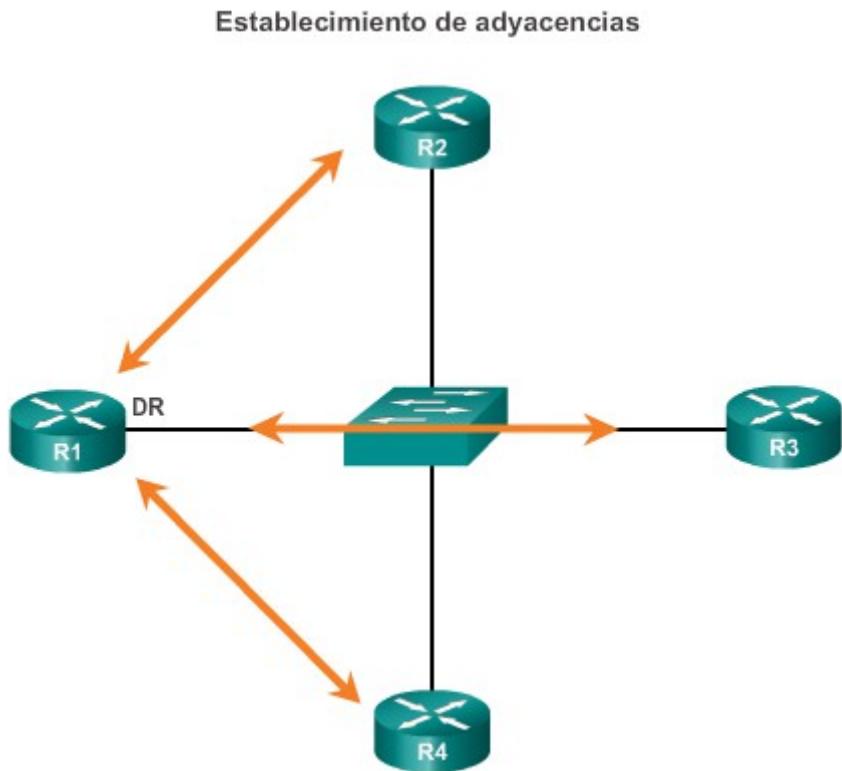
Todos los otros routers que no son DR ni BDR se convierten en DROthers.

En la figura 1, se seleccionó al R1 como router designado de la LAN Ethernet que interconecta al R2, el R3 y el R4. Observe la manera en que el número de adyacencias se redujo a tres.

Los routers de una red de accesos múltiples eligen un DR y un BDR. Los DROthers solo crean adyacencias completas con el DR y el BDR de la red. En vez de saturar todos los routers de la red con LSA, los DROthers solo envían sus LSA al DR y el BDR mediante la dirección de multidifusión 224.0.0.6 (todos los routers DR).

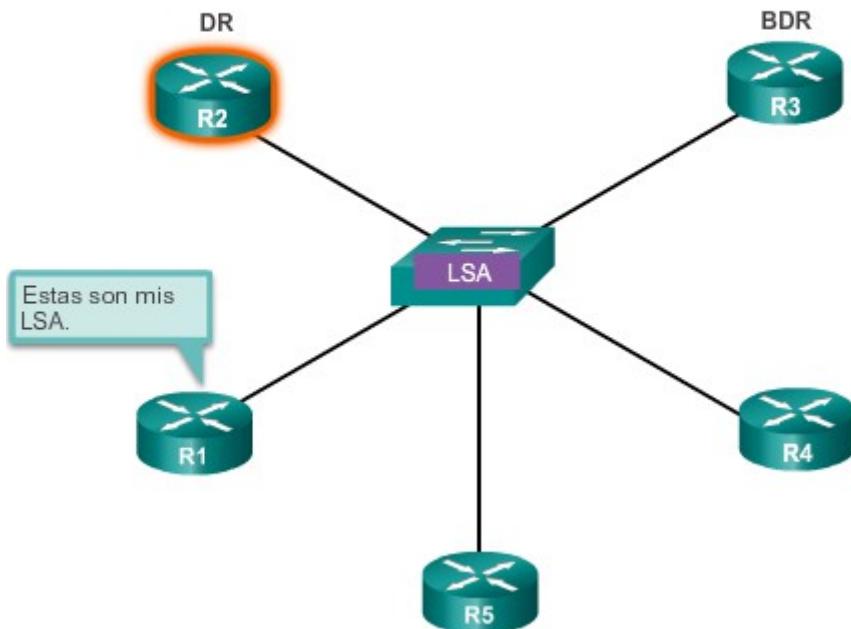
Haga clic en el botón Reproducir que aparece en la figura 2 para ver la animación de la función del DR. En la animación, el R1 envía LSA al DR. El BDR también escucha. El DR es responsable de reenviar todas las LSA desde R1 hasta todos los demás routers. El DR usa la dirección de multidifusión 224.0.0.5 (todos los routers OSPF). El resultado final es que sólo hay un router que realiza la saturación completa de todas las LSA en la red de accesos múltiples.

**Nota:** la elección de DR/BDR solo se producen en las redes de accesos múltiples y no en las redes punto a punto.



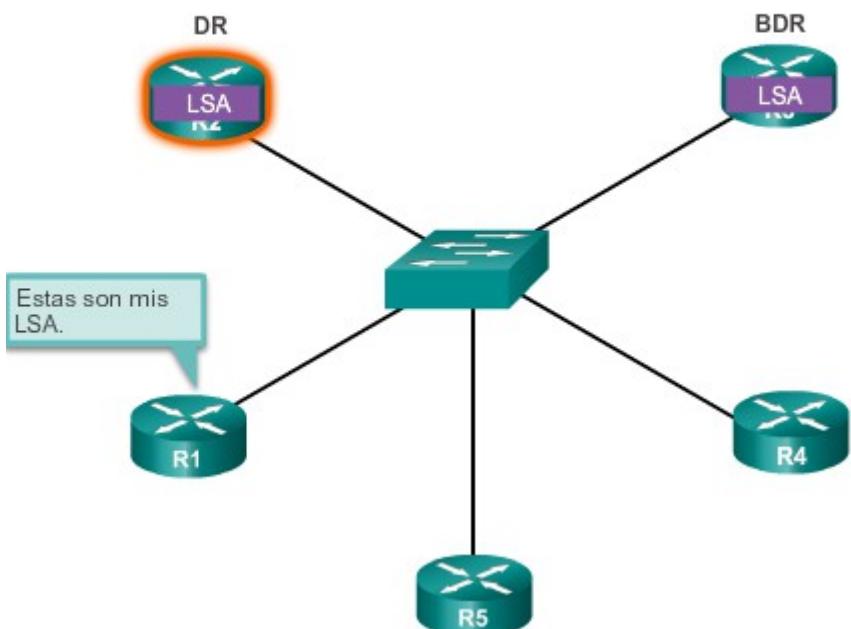
### Función del DR

Las adyacencias solo se forman con el DR y el BDR.



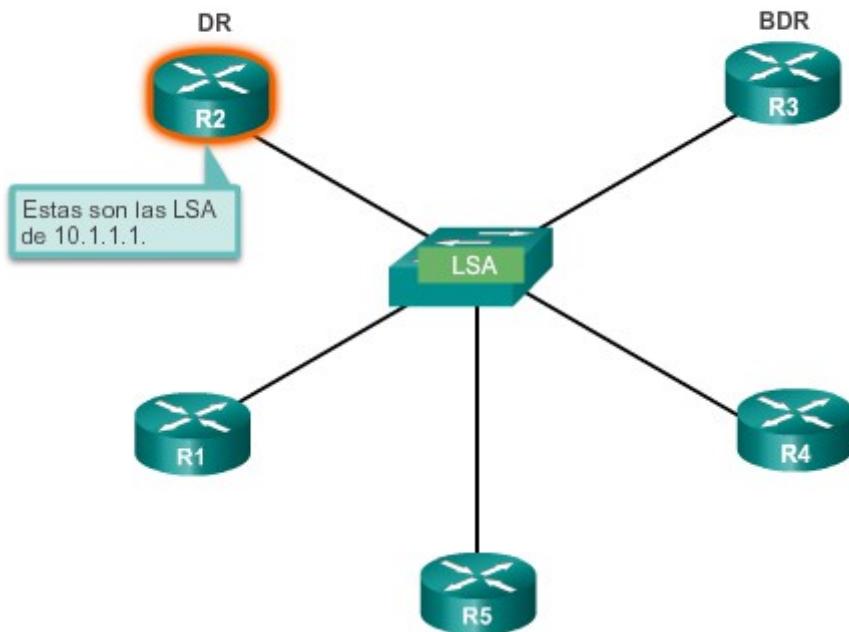
### Función del DR

Las adyacencias solo se forman con el DR y el BDR.



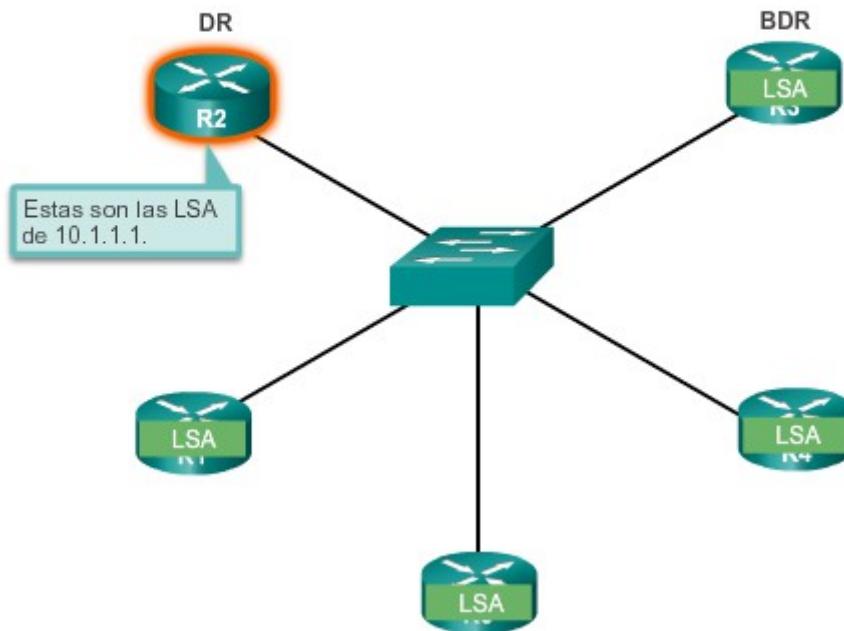
### Función del DR

El DR envía LSA a todos los otros routers.



### Función del DR

El DR envía LSA a todos los otros routers.



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.4 Verificación de las

funciones del DR/BDR

En la topología de accesos múltiples que se muestra en la figura 1, hay tres routers interconectados por medio de una red de accesos múltiples Ethernet común, 192.168.1.0/28. Cada router está configurado con la dirección IP indicada en la interfaz Gigabit Ethernet 0/0.

Debido a que los routers están conectados por medio de una red multiacceso con difusión común, OSPF seleccionó automáticamente un DR y un BDR. En este ejemplo, se eligió al R3 como el DR porque la ID del router es 3.3.3.3, que es la más alta en la red. El R2 es el BDR porque tiene la segunda ID del router más alta en la red.

Para verificar las funciones del router, utilice el comando **show ip ospf interface** (figura 2). El resultado que genera el R1 confirma lo siguiente:

- El R1 no es el DR ni el BDR, sino un DROther con una prioridad predeterminada de 1. (1)
- El DR es el R3 con la ID de router 3.3.3.3 en la dirección IP 192.168.1.3, mientras que el BDR es el R2 con la ID de router 2.2.2.2 en la dirección IP 192.168.1.2. (2)
- El R1 tiene dos adyacencias: una con el BDR y otra con el DR. (3)

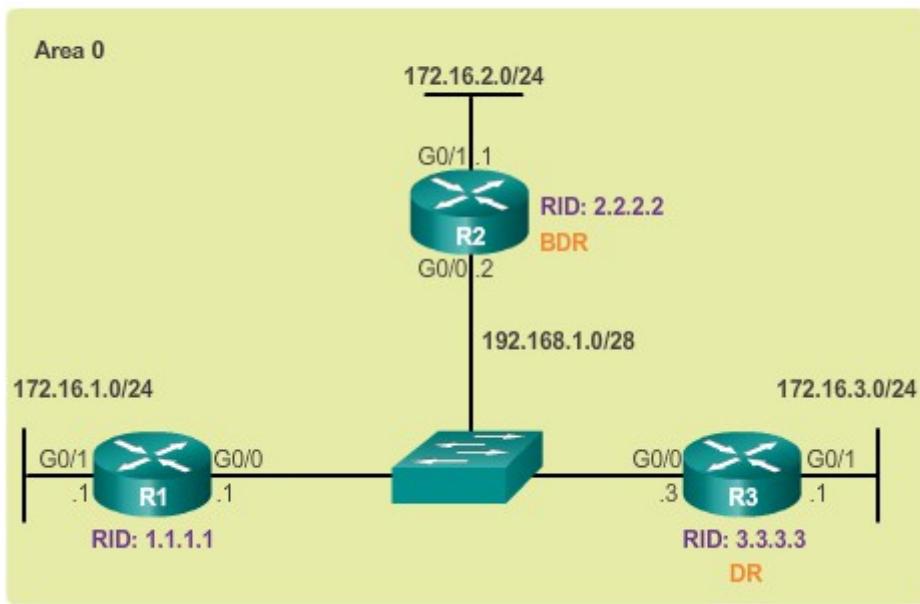
El resultado que genera el R2, en la figura 3, confirma lo siguiente:

- El R2 es el BDR, con una prioridad predeterminada de 1. (1)
- El DR es el R3 con la ID de router 3.3.3.3 en la dirección IP 192.168.1.3, mientras que el BDR es el R2 con la ID de router 2.2.2.2 en la dirección IP 192.168.1.2. (2)
- El R2 tiene dos adyacencias, una con un vecino que tiene la ID de router 1.1.1.1 (R1) y la otra con el DR. (3)

El resultado que genera el R3, en la figura 4, confirma lo siguiente:

- El R3 es el DR, con una prioridad predeterminada de 1. (1)
- El DR es el R3 con la ID de router 3.3.3.3 en la dirección IP 192.168.1.3, mientras que el BDR es el R2 con la ID de router 2.2.2.2 en la dirección IP 192.168.1.2. (2)
- El R3 tiene dos adyacencias, una con un vecino que tiene la ID de router 1.1.1.1 (R1) y la otra con el BDR. (3)

## Topología OSPF de referencia de difusión de accesos múltiples



### Verificación de la función del R1

```
R1# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/28,Area 0,Attached via Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTUID      Cost      Disabled      Shutdown      Topology Name
          0          1        no        no        Base
  1 Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  2 Backup Designated router (ID) 2.2.2.2, 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)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
  3   Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
      Adjacent with neighbor 3.3.3.3 (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

## Verificación de la función del R2

```
R2# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.2/28,Area 0,Attached via Network Statement
  Process ID 10, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
          0        1        no         no         Base
  1 Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  2 Backup Designated router (ID) 2.2.2.2, 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)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
  3   Adjacent with neighbor 1.1.1.1
      Adjacent with neighbor 3.3.3.3 (Designated Router)
  Suppress hello for 0 neighbor(s)
R2#
```

## Verificación de la función del R3

```
R3# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.3/28,Area 0,Attached via Network Statement
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
          0        1        no         no         Base
  1 Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  2 Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 3, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
  3   Adjacent with neighbor 1.1.1.1
      Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R3#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.5 Verificación de las adyacencias del DR/BDR

Para verificar las adyacencias OSPF, utilice el comando **show ip ospf neighbor**, como se muestra en la figura 1.

A diferencia de los enlaces seriales que solo muestran un estado de FULL/-, el estado de los vecinos en redes de accesos múltiples puede ser uno de los siguientes:

- FULL/DROTHER: se trata de un router DR o BDR que tiene plena adyacencia con un router que no es DR ni BDR. Estos dos vecinos pueden intercambiar paquetes de salud, actualizaciones, consultas, respuestas y acuses de recibo.
- FULL/DR: el router tiene plena adyacencia con el vecino DR indicado. Estos dos vecinos pueden intercambiar paquetes de salud, actualizaciones, consultas, respuestas y acuses de recibo.
- FULL/BDR: el router tiene plena adyacencia con el vecino BDR indicado. Estos dos vecinos pueden intercambiar paquetes de salud, actualizaciones, consultas, respuestas y acuses de recibo.
- 2-WAY/DROTHER: el router que no es DR ni BDR tiene una relación de vecino con otro router que no es DR ni BDR. Estos dos vecinos intercambian paquetes de salud.

En general, el estado normal de un router OSPF es FULL. Si un router está atascado en otro estado, es un indicio de que existen problemas en la formación de adyacencias. La única excepción a esto es el estado 2-WAY, que es normal en una red multiacceso con difusión.

En redes de accesos múltiples, los DROthers solo forman adyacencias FULL con el DR y el BDR. Sin embargo, forman adyacencias de vecino 2-WAY con cualquier otro DROther que se una a la red. Esto significa que todos los routers DROther en la red de accesos múltiples siguen recibiendo paquetes de salud de todos los otros routers DROther. De esta manera, éstos conocen a todos los routers de la red. Cuando dos routers DROther forman una adyacencia de vecino, el estado de vecino aparece como 2-WAY/DROTHER.

El resultado que genera el R1 confirma que este tiene adyacencias con el router:

- El R2 con la ID de router 2.2.2.2 está en estado Full y cumple la función de BDR. (1)
- El R3 con la ID de router 3.3.3.3 está en estado Full y cumple la función de DR. (2)

El resultado que genera el R2, en la figura 2, confirma que este tiene adyacencias con el router:

- El R1 con la ID de router 1.1.1.1 está en estado Full, y su función no es la de DR ni la de BDR. (1)
- El R3 con la ID de router 3.3.3.3 está en estado Full y cumple la función de DR. (2)

El resultado que genera el R3, en la figura 3, confirma que este tiene adyacencias con el router:

- El R1 con la ID de router 1.1.1.1 está en estado Full, y su función no es la de DR ni la de BDR. (1)
- El R2 con la ID de router 2.2.2.2 está en estado Full y cumple la función de BDR. (2)

### Verificación de las adyacencias de vecinos del R1

```
R1# show ip ospf neighbor

Neighbor ID Pri State      Dead Time   Address      Interface
1 2.2.2.2      1  FULL/BDR    00:00:36  192.168.1.2 GigabitEthernet0/0
2 3.3.3.3      1  FULL/DR     0:00:35   192.168.1.3 GigabitEthernet0/0

R1#
```

### Verificación de las adyacencias de vecinos del R2

```
R2# show ip ospf neighbor

Neighbor ID Pri State      Dead Time   Address      Interface
1 1.1.1.1      1  FULL/DROTHER 00:00:31  192.168.1.1 GigabitEthernet0/0
2 3.3.3.3      1  FULL/DR     00:00:39  192.168.1.3 GigabitEthernet0/0

R2#
```

### Verificación de las adyacencias de vecinos del R3

```
R3# show ip ospf neighbor

Neighbor ID Pri State      Dead Time   Address      Interface
1 1.1.1.1      1  FULL/DROTHER 00:00:34  192.168.1.1 GigabitEthernet0/0
2 2.2.2.2      1  FULL/BDR    00:00:39  192.168.1.2 GigabitEthernet0/0

R3#
```

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.6 Proceso de

### elección del DR/BDR predeterminado

¿Cómo se seleccionan el DR y el BDR? La decisión de elección del DR y el BDR OSPF se hace según los siguientes criterios, en orden secuencial:

1. Los routers en la red seleccionan como DR al router con la prioridad de interfaz más alta. El router con la segunda prioridad de interfaz más alta se elige como BDR. La prioridad puede configurarse para que sea cualquier número entre 0 y 255. Cuanto mayor sea la prioridad, más probabilidades hay de que se elija al router como DR. Si la prioridad se establece en 0, el router no puede convertirse en el DR. La prioridad predeterminada de las interfaces de difusión de accesos múltiples es 1. Por lo tanto, a menos que se configuren de otra manera, todos los routers tienen un mismo valor de prioridad y deben depender de otro método de diferenciación durante la elección del DR/BDR.
2. Si las prioridades de interfaz son iguales, se elige al router con la ID más alta como DR. El router con la segunda ID de router más alta es el BDR.

Recuerde que la ID del router se determina de tres maneras:

- La ID del router se puede configurar manualmente.
- Si no hay una ID de router configurada, la ID del router la determina la dirección IP de loopback más alta.
- Si no hay interfaces loopback configuradas, la ID del router la determina la dirección IPv4 activa más alta.

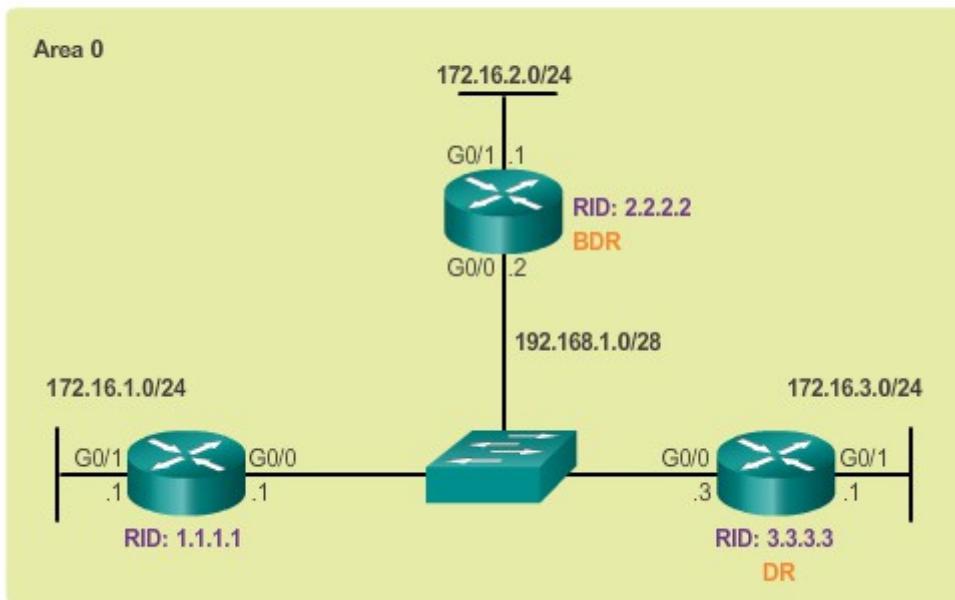
**Nota:** si en una red IPv6 no hay direcciones IPv4 configuradas en el router, la ID del router debe configurarse manualmente con el comando **router-id id-router**; de lo contrario, OSPFv3 no se inicia.

En la ilustración, todas las interfaces Ethernet del router tienen una prioridad determinada de 1. Como resultado, según los criterios de selección descritos anteriormente, para seleccionar el DR y el BDR se usa la ID del router OSPF. El R3, con la ID de router más alta, se convierte en el DR, y el R2, que tiene la segunda ID de router más alta, se convierte en el BDR.

**Nota:** las interfaces seriales tienen la prioridad predeterminada establecida en 0; por eso, no seleccionan DR ni BDR.

El proceso de elección del DR y el BDR ocurre en cuanto el primer router con una interfaz con OSPF habilitado se activa en la red de accesos múltiples. Esto puede ocurrir cuando se encienden los routers o cuando se configura el comando de OSPF**network** para esa interfaz. El proceso de elección sólo toma unos pocos segundos. Si no terminaron de arrancar todos los routers en la red de accesos múltiples, es posible que un router con una ID de router más baja se convierta en el DR. (Puede ser un router más económico que demore menos en arrancar).

## Topología OSPF de referencia de difusión de accesos múltiples



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.7 Proceso de elección de DR/BDR

La elección del DR y el BDR OSPF no se basa en prelación. Si se agregan a la red un router nuevo con una prioridad más alta o una ID de router más alta después de la elección del DR y el BDR, el router agregado no se apropiará de la función de DR o BDR. Esto se debe a que esas funciones ya se asignaron. La incorporación de un nuevo router no inicia un nuevo proceso de elección.

Una vez que se elige el DR, permanece como tal hasta que se produce una de las siguientes situaciones:

- El DR falla.
- El proceso OSPF en el DR falla o se detiene.
- La interfaz de accesos múltiples en el DR falla o se apaga.

Si el DR falla, el BDR se asciende automáticamente a DR. Esto ocurre así incluso si se agrega otro DROther con una prioridad o ID de router más alta a la red después de la elección inicial de DR/BDR. Sin embargo, después del ascenso de un BDR a DR, se lleva a cabo otra elección de BDR y se elige al DROther con la prioridad o la ID de router más alta como el BDR nuevo.

En las figuras 1 a 4, se muestran las diferentes situaciones relacionadas con el proceso de elección de DR y BDR.

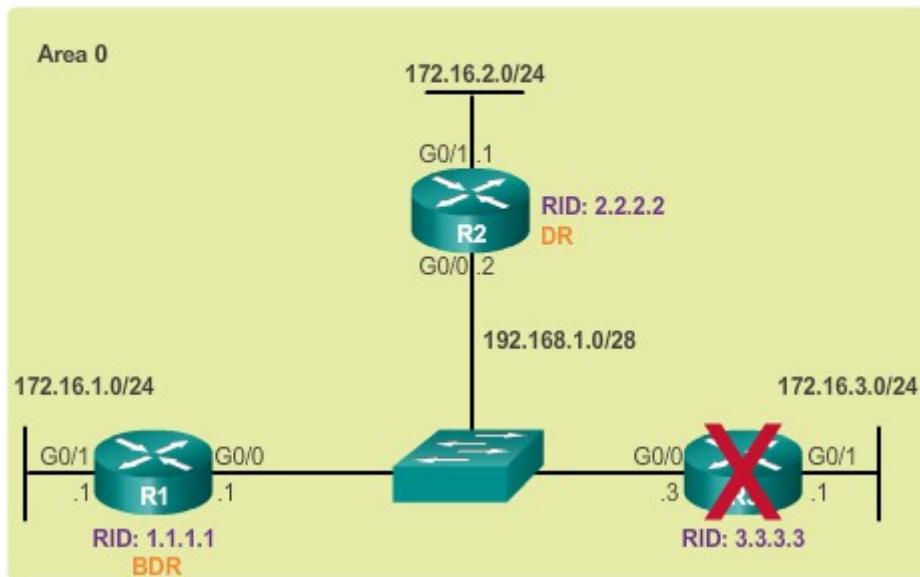
En la figura 1, el DR actual (R3) falla, por lo tanto, el BDR preseleccionado (R2) asume la función de DR. A continuación, se hace la elección del BDR nuevo. Debido a que el R1 es el único DROther, se lo selecciona como BDR.

En la figura 2, el R3 vuelve a unirse a la red, después de varios minutos de no estar disponible. Debido a que el DR y el BDR ya existen, el R3 no ocupa ninguna de las dos funciones. En cambio, se convierte en un DROther.

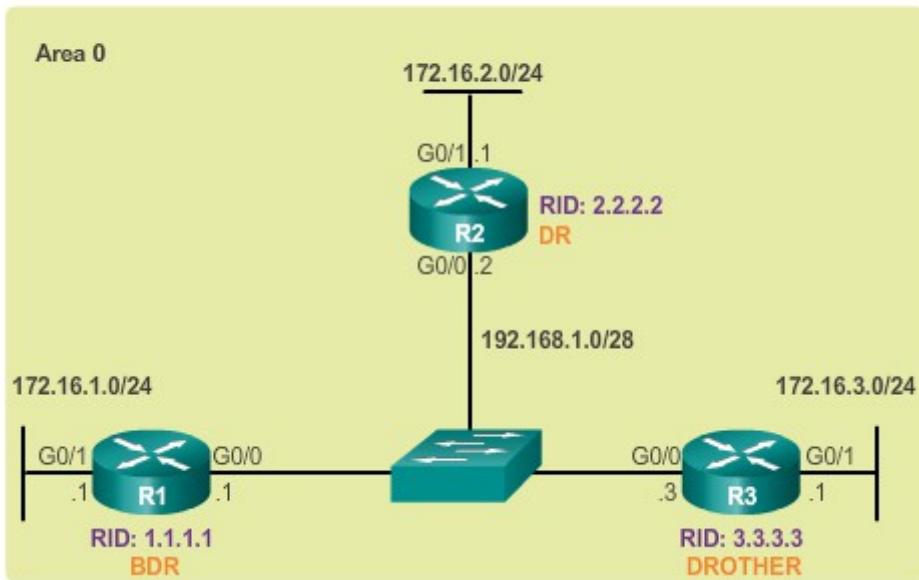
En la figura 3, se agrega a la red un nuevo router (R4) con una ID de router más alta. El DR (R2) y el BDR (R1) retienen sus funciones de DR y BDR. El R4 se convierte automáticamente en DROther.

En la figura 4, el R2 falla. El BDR (R1) se convierte automáticamente en el DR, y un proceso de elección selecciona al R4 como el BDR, ya que tiene la ID de router más alta.

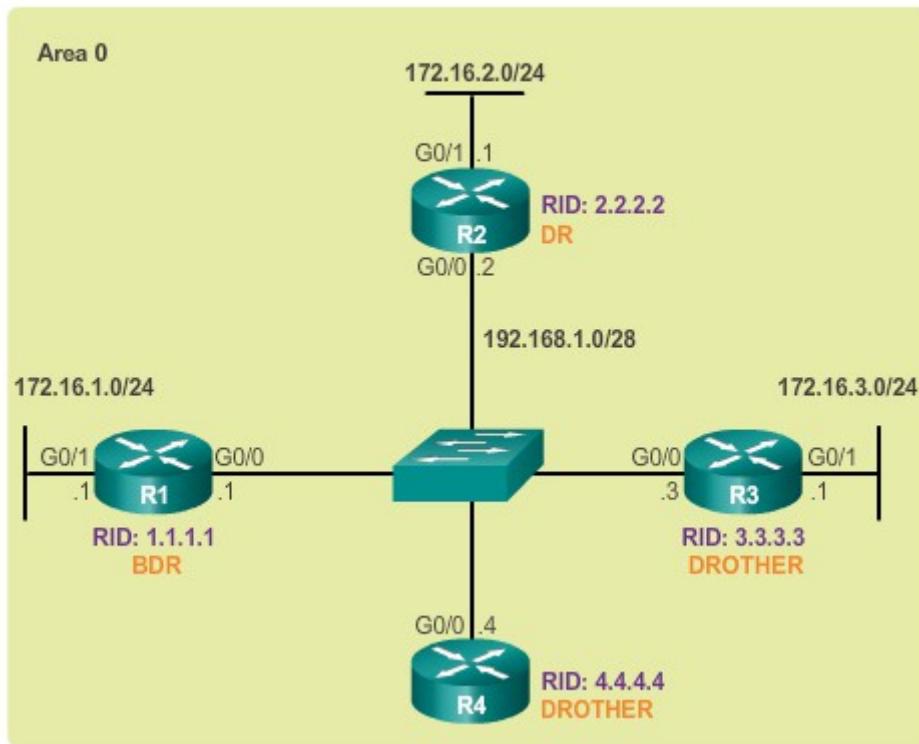
## El R3 falla



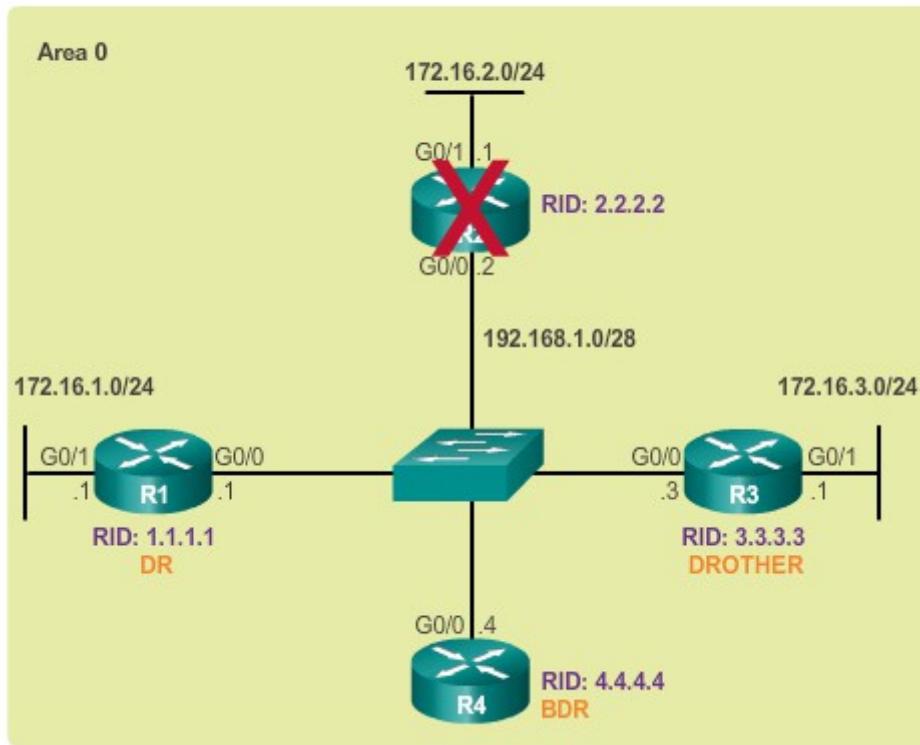
### El R3 vuelve a unirse a la red



### El R4 se une a la red



## El R2 falla



### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.8 La prioridad OSPF

El DR se convierte en el centro de la recopilación y distribución de LSA, por lo tanto, dicho router debe contar con suficiente capacidad de memoria y de CPU para manejar la carga de trabajo. Es posible influenciar el proceso de elección de DR/BDR mediante configuraciones.

Si las prioridades de interfaz son iguales en todos los routers, se elige al router con la ID más alta como DR. Es posible configurar la ID del router para manipular la elección de DR/BDR. Sin embargo, el proceso solo funciona si hay un plan riguroso para establecer la ID de router de todos los routers. En las redes grandes, esto puede ser engoroso.

En vez de depender de la ID del router, es mejor controlar la elección mediante el establecimiento de prioridades de interfaz. Las prioridades son un valor específico de cada interfaz, lo que significa que proporcionan un mejor control en una red de accesos múltiples. Esto también permite que un router sea el DR en una red y un DROther en otra.

Para establecer la prioridad de una interfaz, use los siguientes comandos:

- **ip ospf priority *valor*** - comando de interfaz OSPFv2
- **ipv6 ospf priority *valor*** - comando de interfaz OSPFv3

El *valor* puede ser uno de los siguientes:

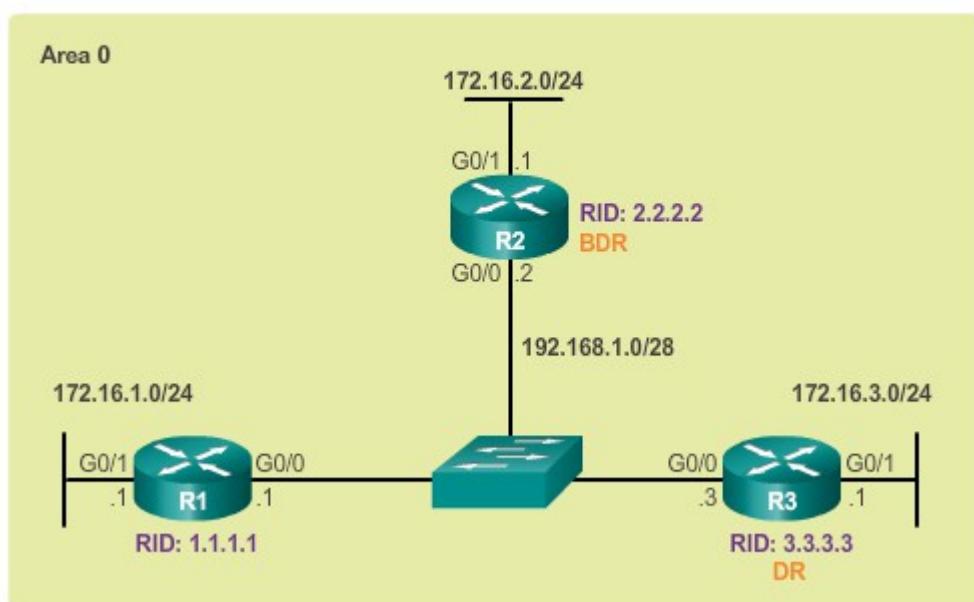
- **0:** no se convierte en DR ni en BDR.

- **1 a 255:** cuanto más alto sea el valor de la prioridad, habrá más probabilidades de que el router se convierta en el DR o el BDR de la red.

En la ilustración, todos los routers tienen la misma prioridad OSPF, porque el valor de la prioridad se establece de manera predeterminada en 1 para todas las interfaces de router. Por esta razón, para determinar el DR (R3) y el BDR (R2), se usa la ID del router. Si se cambia el valor de la prioridad en una interfaz de 1 a un valor más alto, se habilita el router para que se convierta en un router DR o BDR durante la siguiente elección.

Si la prioridad de la interfaz se configura después de habilitar OSPF, el administrador debe desactivar el proceso OSPF en todos los routers y, luego, volver a habilitarlo para forzar una nueva elección de DR/BDR.

### Topología OSPF de referencia de difusión de accesos múltiples



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.9 Cambio de la prioridad OSPF

En la topología de la figura 1, el R3 es el DR y el R2 es el BDR. Se decidió lo siguiente:

- El R1 debe ser el DR y se configura con una prioridad de 255.
- El R2 debe ser el BDR y se le deja la prioridad predeterminada de 1.
- El R3 nunca debe ser un DR ni BDR y se configura con una prioridad de 0.

En la figura 2, se cambia la prioridad de la interfaz Gigabit 0/0 del R1 de 1 a 255.

En la figura 3, se cambia la prioridad de la interfaz Gigabit 0/0 del R3 de 1 a 0.

Los cambios no tienen efecto automáticamente, debido a que el DR y el BDR ya fueron seleccionados. Por lo tanto, la elección de OSPF se debe negociar mediante uno de los siguientes métodos:

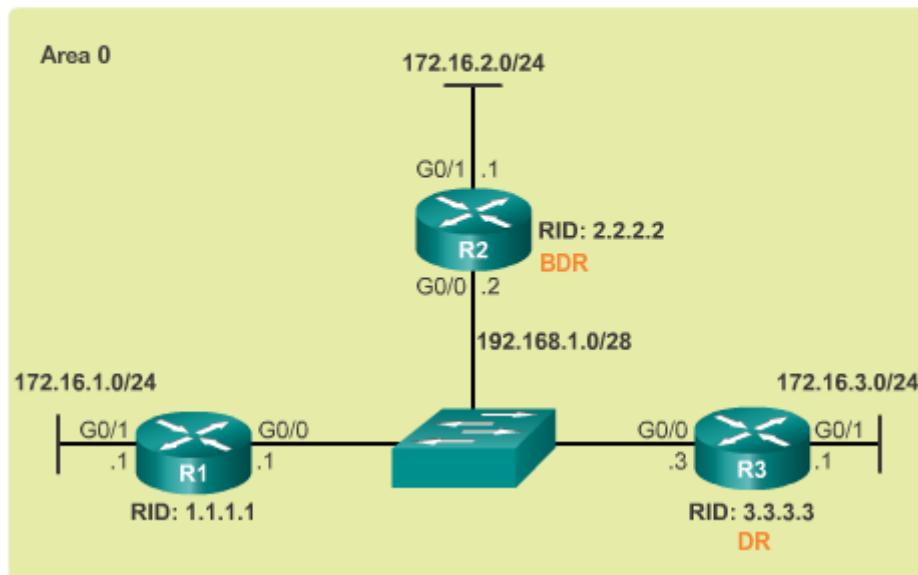
- Desactivar las interfaces del router y volver a habilitarlas de a una: primero el DR, luego el BDR y después todos los demás routers.
- Restablecer el proceso OSPF mediante el comando **clear ip ospf process** del modo EXEC privilegiado en todos los routers.

En la figura 4, se muestra cómo borrar el proceso OSPF en el R1. Suponga que el comando **clear ip ospf process** del modo EXEC privilegiado también se configuró en el R2 y el R3. Observe la información del estado de OSPF que se genera.

El resultado que se muestra en la figura 5 confirma que el R1 ahora es el DR, con una prioridad de 255, e identifica las nuevas adyacencias de vecinos del R1.

Utilice el verificador de sintaxis de la figura 6 para verificar la función y las adyacencias del R2 y el R3.

#### Topología OSPF de referencia de difusión de accesos múltiples



#### Cambio de la prioridad de la interfaz G0/0 del R1

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1#
```

### Cambio de la prioridad de la interfaz G0/0 del R3

```
R3(config)# interface GigabitEthernet 0/0
R3(config-if)# ip ospf priority 0
R3(config-if)# end
R3#
```

### Eliminación del proceso OSPF en el R1

```
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: yes
R1#
*Apr  6 16:00:44.282: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on GigabitEthernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached
*Apr  6 16:00:44.282: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on GigabitEthernet0/0 from FULL to DOWN, Neighbor
Down: Interface down or detached
R1#
```

### Verificación de la función y las adyacencias del R1

```
R1# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/28, Area 0, Attached via Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost      Disabled     Shutdown   Topology Name
    0          1        no        no        Base
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next Rx0(0)/Tx0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
R1#
R1# show ip ospf neighbor

Neighbor ID  Pri  State      Dead Time Address      Interface
2.2.2.2      1  FULL/BDR    00:00:30  192.168.1.2 GigabitEthernet0/0
3.3.3.3      0  FULL/DROTHER 00:00:38  192.168.1.3 GigabitEthernet0/0
R1#
```

## Verificación de la función y las adyacencias

Muestre la configuración y las adyacencias OSPF para la interfaz GigabitEthernet 0/0 en el R2.

```
R2# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.2/28, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
    0            1        no          no          Base
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    cob-resync timeout 40
    Hello due in 00:00:09
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 1.1.1.1 (Designated Router)
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
R2#
```

Muestre la tabla de vecinos OSPF para el R2.

```
R2# show ip ospf neighbor
Neighbor ID      Pri  State           Dead Time     Address          Interface
1.1.1.1          255  FULL/DR        00:00:35     192.168.1.1    GigabitEthernet0/0
3.3.3.3           0    FULL/DROTHER  00:00:38     192.168.1.3    GigabitEthernet0/0
R2#
```

Ahora, inició sesión en el R3. Muestre la configuración y las adyacencias OSPF para la interfaz GigabitEthernet 0/0 en el R3.

```
R3# show ip ospf interface GigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.3/28, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown    Topology Name
    0            1        no          no          Base
  Transmit Delay is 1 sec, State DROTHER, Priority 0
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    cob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 3
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 1.1.1.1 (Designated Router)
    Adjacent with neighbor 2.2.2.2 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R3#
```

Muestre la tabla de vecinos OSPF para el R3.

```
R3# show ip ospf neighbor
Neighbor ID      Pri  State           Dead Time     Address          Interface
1.1.1.1          255  FULL/DR        00:00:32     192.168.1.1    GigabitEthernet0/0
2.2.2.2           1    FULL/BDR       00:00:39     192.168.1.2    GigabitEthernet0/0
R3#
```

Verificó correctamente las funciones y las adyacencias para el R2 y el R3.

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.10 Actividad:

### Identificar la terminología de los tipos de redes OSPF

#### **Actividad (parte 1): Identificar los tipos de red**

En la tabla figuran características de diferentes tipos de redes OSPF. Una el tipo de red OSPF con la característica adecuada. No se utilizan todos los tipos de red. Haga clic en el botón 2 para continuar la actividad.

Tipo de red OSPF	Características de la red OSPF
✓ Broadcast de accesos múltiples	Conecta varios routers mediante tecnología Ethernet.
✓ Punto a multipunto	Conecta sitios de sucursal (spokes, "rayos") a un sitio central (hub)
✓ Multiacceso sin difusión	Conecta sitios de sucursal a un sitio central.
✓ Punto a Punto	Conecta dos routers directamente mediante una sola red WAN.

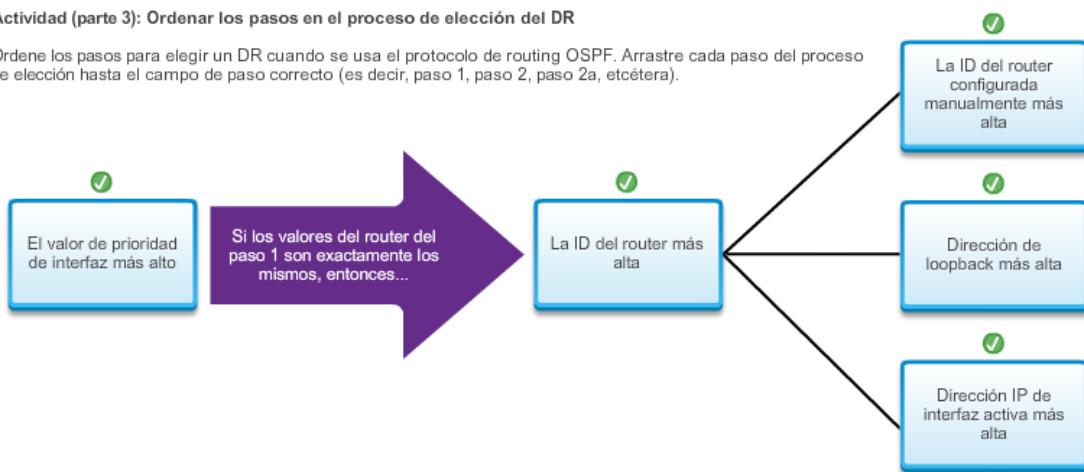
#### **Actividad (parte 2): Identificar las características del DR, el BDR y los DRothers**

A continuación, figuran las características de los routers configurados con el protocolo de routing OSPF en una red de accesos múltiples. Una la característica del router OSPF con el tipo adecuado de router OSPF. Haga clic en el botón 3 para continuar.

	DR	BDR	DRother
1. Usa multidifusión 224.0.0.5 para escuchar las LSA.			✓
2. Satura con LSA a todos los routers participantes.	✓		
3. Escucha pasivamente las LSA.		✓	
4. Si el DR deja de producir paquetes de saludo, se asciende a si mismo.		✓	
5. No satura con LSA a todos los routers dentro de la red.			✓
6. Usa multidifusión 224.0.0.6 para enviar LSA.			✓

#### Actividad (parte 3): Ordenar los pasos en el proceso de elección del DR

Ordene los pasos para elegir un DR cuando se usa el protocolo de routing OSPF. Arrastre cada paso del proceso de elección hasta el campo de paso correcto (es decir, paso 1, paso 2, paso 2a, etcétera).

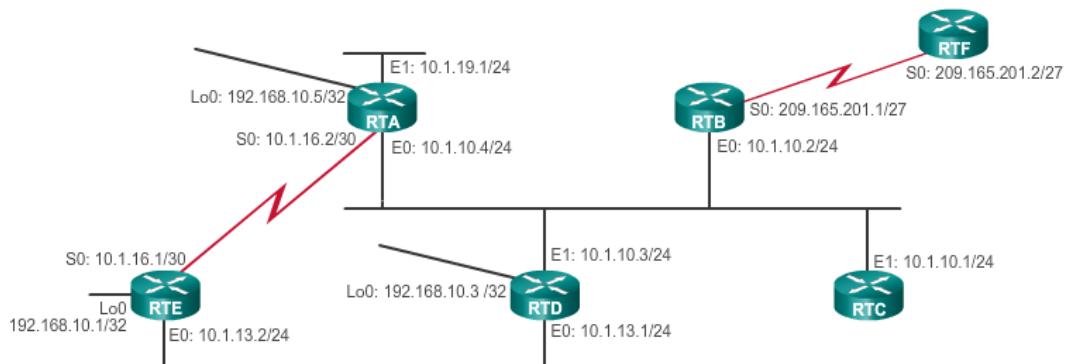


#### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.11 Actividad:

##### Seleccionar el router designado

###### Actividad: Topología

Use la topología de esta página para determinar la ID de cada router para la parte 1 y el router designado para la parte 2. Haga clic en el botón 2 para continuar la actividad.



###### Actividad (parte 1): Seleccionar la ID del router

Arrastre el número de ID del router hasta el campo junto al nombre de host del router adecuado. Haga clic en el botón 1 para consultar la topología. Haga clic en el botón 3 para continuar la actividad.

Nombre de host del router	Id. de router	Números de ID del router
Router A	192.168.10.5	10.1.16.2
Router B	209.165.201.1	10.1.13.1
Router C	10.1.10.1	10.1.13.2
Router D	192.168.10.3	10.1.10.4
Router E	192.168.10.1	10.1.19.1
Router F	209.165.201.2	10.1.10.3

**Actividad (parte 2): Seleccionar el router designado**

En la actividad 1, identificó la ID del router para los nombres de host incluidos en el diagrama de la topología. En esta actividad, usará el mismo diagrama de topología y las mismas ID de los routers y reglas para la selección del router designado por OSPF.

Determine el router designado para las redes especificadas. Arrastre el router designado hasta el campo junto a la ID de la red adecuada. Las respuestas se pueden usar más de una vez. Haga clic en el botón 1 para consultar la topología.

Identificación de red	Nombre de host
10.1.10.0	<input checked="" type="checkbox"/> Router B
10.1.13.0	<input checked="" type="checkbox"/> Router D
10.1.16.0	<input checked="" type="checkbox"/> Ninguno
10.1.19.0	<input checked="" type="checkbox"/> Router A
209.165.201.0	<input checked="" type="checkbox"/> Ninguno

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.12 Packet Tracer:Determinación del DR y el BDR**Información básica/situación**

En esta actividad, examinará las funciones del DR y el BDR, y observará cómo estas cambian cuando se modifica la red. A continuación, modificará la prioridad para controlar las funciones y forzará una nueva elección. Por último, verificará que los routers cumplan las funciones deseadas.

[Packet Tracer: Determinación del DR y el BDR \(instrucciones\)](#)

[Packet Tracer: Determinación del DR y el BDR \(PKA\)](#)

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.2.13 Práctica delaboratorio: Configuración de OSPFv2 en una red de accesos múltiples**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar y verificar OSPFv2 en el DR, el DBR y el DROther
- Parte 3: Configurar la prioridad de interfaz OSPFv2 para determinar el DR y el BDR

## [Práctica de laboratorio: Configuración de OSPFv2 en una red de accesos múltiples](#)

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.3.1 Propagación de una ruta estática predeterminada en OSPFv2

### **Propagación de una ruta estática predeterminada**

Con OSPF, el router conectado a Internet se utiliza para propagar una ruta predeterminada a otros routers en el dominio de routing OSPF. Este router a veces se denomina router perimetral, de gateway o de entrada. Sin embargo, en la terminología de OSPF, el router ubicado entre un dominio de routing OSPF y una red que no es OSPF también se denomina “router limítrofe del sistema autónomo” (ASBR).

En la figura 1, el R2 tiene conexión simple a un proveedor de servicios. Por lo tanto, todo lo que se requiere para que el R2 llegue a Internet es una ruta estática predeterminada al proveedor de servicios.

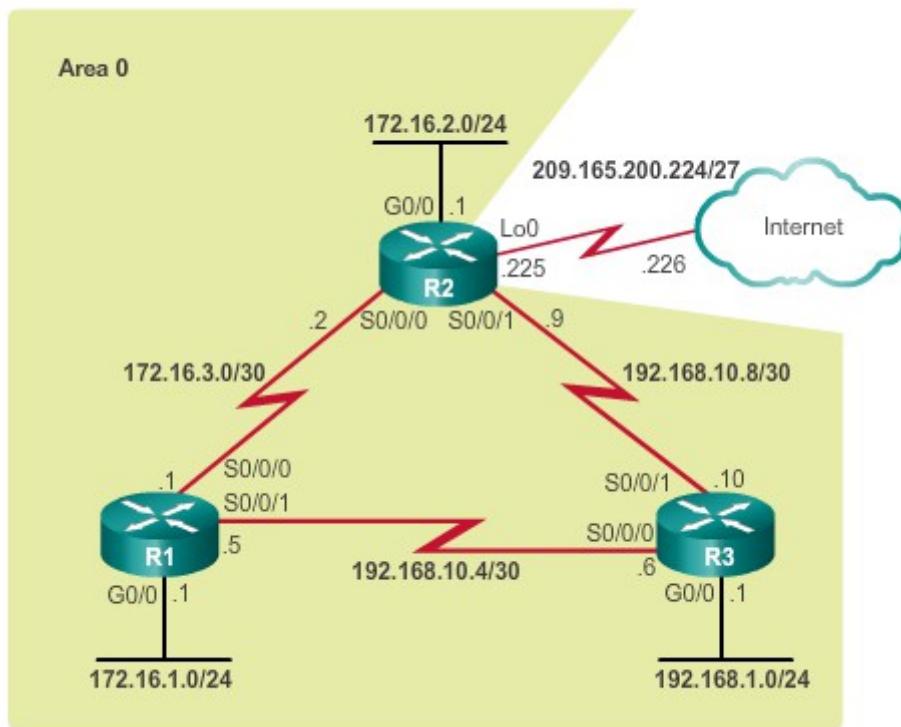
**Nota:** en este ejemplo, para simular la conexión al proveedor de servicios, se usa una interfaz loopback con la dirección IP 209.165.200.225.

Para propagar una ruta predeterminada, el router perimetral (R2) debe configurarse con lo siguiente:

- Una ruta estática predeterminada, mediante el comando **ip route 0.0.0.0 0.0.0.0 {dirección-ip | interfaz-salida}**.
- El comando **default-information originate** del modo de configuración del router. Esto ordena al R2 que sea el origen de la información de la ruta predeterminada y que propague la ruta estática predeterminada en las actualizaciones OSPF.

En la figura 2, se muestra cómo configurar una ruta estática predeterminada completamente especificada al proveedor de servicios.

## Propagación de una ruta predeterminada en el R2



## Configuración de una ruta predeterminada en el R2

```
R2(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.226
R2(config)#
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.3.2 Verificación de la

ruta predeterminada propagada

Verifique la configuración de la ruta predeterminada en el R2 mediante el comando **show ip route**, como se muestra en la figura 1.

Utilice el verificador de sintaxis de la figura 2 para verificar que la ruta predeterminada se haya propagado al R1 y al R3. Observe que el origen de la ruta es **O\*E2**, lo que especifica que se

descubrió mediante OSPF. El asterisco indica que esa ruta es una buena candidata para la ruta predeterminada. La designación “E2” indica que se trata de una ruta externa.

Las rutas externas pueden ser externa de tipo 1 o externa de tipo 2. La diferencia entre ambos tipos es la manera en que se calcula el costo (métrica) de la ruta. El costo de una ruta de tipo 2 siempre es el costo externo, independientemente del costo interno para llegar a esa ruta. El costo de tipo 1 es la suma del costo externo y del costo interno necesario para llegar a esa ruta. Para el mismo destino, siempre se prefiere una ruta de tipo 1 a una ruta de tipo 2.

#### Verificación de una ruta predeterminada en el R2

```
R2# show ip route | begin Gateway
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 209.165.200.226, Loopback0
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O  172.16.1.0/24 [110/65] via 172.16.3.1, 00:01:44,
    Serial0/0/0
C  172.16.2.0/24 is directly connected, GigabitEthernet0/0
L  172.16.2.1/32 is directly connected, GigabitEthernet0/0
C  172.16.3.0/30 is directly connected, Serial0/0/0
L  172.16.3.2/32 is directly connected, Serial0/0/0
O  192.168.1.0/24 [110/65] via 192.168.10.10, 00:01:12,
    Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2
    masks
O  192.168.10.4/30 [110/128] via 192.168.10.10, 00:01:12,
    Serial0/0/1
        [110/128] via 172.16.3.1, 00:01:12, Serial0/0/0
C  192.168.10.8/30 is directly connected, Serial0/0/1
L  192.168.10.9/32 is directly connected, Serial0/0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2
    masks
C  209.165.200.224/30 is directly connected, Loopback0
L  209.165.200.225/32 is directly connected, Loopback0
R2#
```

## Verificación de una ruta predeterminada propagada en el R1 y el R3

Muestre la tabla de routing en el R1 para ver la ruta predeterminada propagada desde el R2.

```
R1# show ip route
Codes: L - local, 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 - CDR, P - periodic downloaded static route, H - NHOP, l - LISP
      + - replicated route, # - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:19:37, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
      C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
      L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
      O        172.16.2.0/24 [110/65] via 172.16.3.2, 00:21:19, Serial0/0/0
      C        172.16.3.0/30 is directly connected, Serial0/0/0
      L        172.16.3.1/32 is directly connected, Serial0/0/0
      O        192.168.1.0/24 [110/65] via 192.168.10.6, 00:20:49, Serial0/0/1
              192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
      C        192.168.10.4/30 is directly connected, Serial0/0/1
      L        192.168.10.5/32 is directly connected, Serial0/0/1
      O        192.168.10.8/30 [110/128] via 192.168.10.6, 00:20:49, Serial0/0/1
              [110/128] via 172.16.3.2, 00:20:49, Serial0/0/0
R1#
```

Ahora, inició sesión en el R3. Muestre la tabla de routing en el R3 para ver la ruta predeterminada propagada desde el R2.

```
R3# show ip route
Codes: L - local, 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 - CDR, P - periodic downloaded static route, H - NHOP, l - LISP
      + - replicated route, # - next hop override

Gateway of last resort is 192.168.10.9 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 192.168.10.9, 00:18:22, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
      O        172.16.1.0/24 [110/65] via 192.168.10.5, 00:19:36, Serial0/0/0
      O        172.16.2.0/24 [110/65] via 192.168.10.9, 00:19:36, Serial0/0/1
      O        172.16.3.0/30 [110/128] via 192.168.10.9, 00:19:36, Serial0/0/1
              [110/128] via 192.168.10.5, 00:19:36, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
      C        192.168.1.0/24 is directly connected, GigabitEthernet0/0
      L        192.168.1.1/32 is directly connected, GigabitEthernet0/0
      192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
      C        192.168.10.4/30 is directly connected, Serial0/0/0
      L        192.168.10.6/32 is directly connected, Serial0/0/0
      C        192.168.10.8/30 is directly connected, Serial0/0/1
      L        192.168.10.10/32 is directly connected, Serial0/0/1
R3#
```

Verificó correctamente las rutas predeterminadas propagadas desde el R2 hasta el R1 y el R3.

El proceso de propagación de una ruta estática predeterminada en OSPFv3 es casi idéntico al de OSPFv2.

En la figura 1, el R2 tiene conexión simple a un proveedor de servicios. Por lo tanto, todo lo que se requiere para que el R2 llegue a Internet es una ruta estática predeterminada al proveedor de servicios.

**Nota:** en este ejemplo, para simular la conexión al proveedor de servicios, se usa una interfaz loopback con la dirección IP 2001:DB8:FEED:1::1/64.

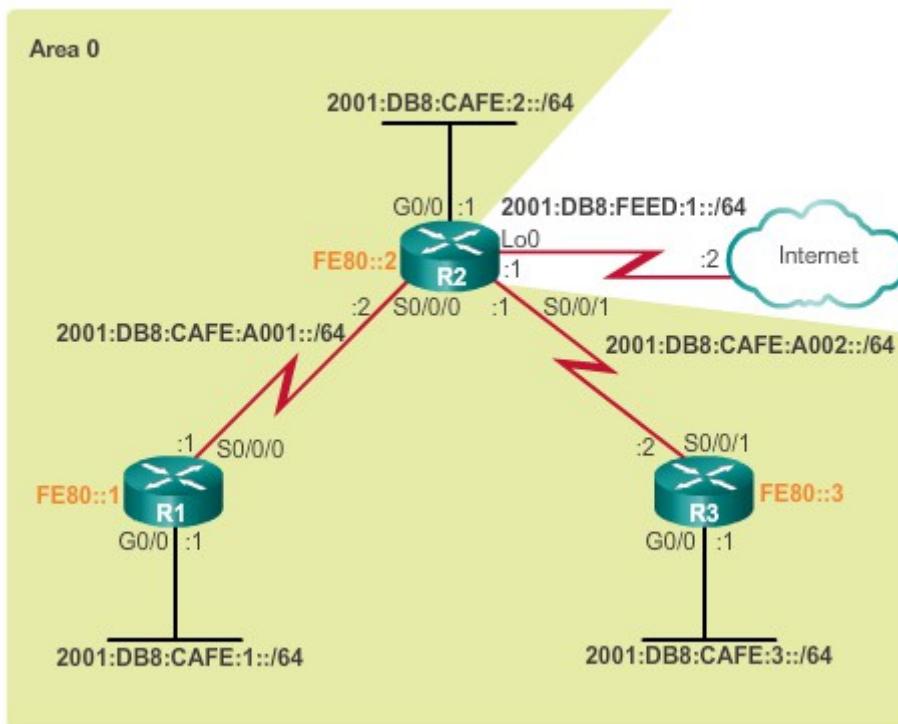
En la figura 2, se muestra la tabla de routing IPv6 actual del R1. Observe que en dicha tabla no hay registro de que se conozca la ruta a Internet.

Para propagar una ruta predeterminada, el router perimetral (R2) debe configurarse con lo siguiente:

- Una ruta estática predeterminada, mediante el comando **ipv6 route ::/0 {dirección-ipv6 |interfaz-salida}**.
- El comando **default-information originate** del modo de configuración del router. Esto ordena al R2 que sea el origen de la información de la ruta predeterminada y que propague la ruta estática predeterminada en las actualizaciones OSPF.

En el ejemplo de la figura 3, se configura una ruta estática predeterminada completamente especificada al proveedor de servicios.

### Topología OSPFv3



### Verifique la tabla de routing IPv6 en el R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
Codes:
  C - Connected, L - Local, S - Static, U - Per-user Static route
  B - BGP, R - RIP, N - NHRP, I1 - ISIS L1
  I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
  EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE -
    Destination
  NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
  OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O  2001:DB8:CAFE:2::/64 [110/648]
  via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:3::/64 [110/648]
  via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:A002::/64 [110/1294]
  via FE80::2, Serial0/0/0
R1#
```

### Habilitación de OSPFv3 en las interfaces del R1

```
R2(config)# ipv6 route ::/0 2001:DB8:FEED:1::2
R2(config)#
R2(config)# ipv6 router ospf 10
R2(config-rtr)# default-information originate
R2(config-rtr)# end
R2#
*Apr 10 11:36:21.995: %SYS-5-CONFIG_I: Configured from console by
console
R2#
```

#### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.3.4 Verificación de la

#### ruta predeterminada IPv6 propagada

Verifique la configuración de la ruta estática predeterminada en el R2 mediante el comando **show ipv6 route**, como se muestra en la figura 1.

Utilice el verificador de sintaxis de la figura 2 para verificar que la ruta predeterminada se haya propagado al R1 y al R3. Observe que el origen de la ruta es **OE2**, lo que especifica que se descubrió mediante OSPFv3. La designación “E2” indica que se trata de una ruta externa.

A diferencia de la tabla de routing IPv4, IPv6 no usa el asterisco para indicar que la ruta es una buena candidata para la ruta predeterminada.

## Verificación de una ruta predeterminada en el R2

```
R2# show ipv6 route static
IPv6 Routing Table - default - 12 entries
Codes:C -Connected, L - Local, S - Static, U - Per-user Static route
      B -BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 -ISIS L2, IA - ISIS interarea, IS-ISIS summary,D-EIGRP
      EX -EIGRP external, ND-ND Default,NDp-ND Prefix,
      DCE-Destination, NDr -Redirect, O - OSPF Intra,OI-OSPF Inter
      OE1-OSPF ext 1, OE2 -OSPF ext 2, ON1 - OSPF NSSA ext 1
      ON2 - OSPF NSSA ext 2
S    ::/0 [1/0]
      via 2001:DB8:FEED:1::2, Loopback0
R2#
```

### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.3.5 Packet Tracer:

#### Propagación de una ruta predeterminada en OSPFv2

##### **Información básica/situación**

En esta actividad, configurará una ruta predeterminada IPv4 a Internet y propagará esa ruta predeterminada a otros routers OSPF. A continuación, verificará que la ruta predeterminada esté en las tablas de routing descendente y que los hosts puedan acceder a un servidor web en Internet.

[Packet Tracer: Propagación de una ruta predeterminada en OSPFv2 \(instrucciones\)](#)

[Packet Tracer: Propagación de una ruta predeterminada en OSPFv2 \(PKA\)](#)

### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.4.1 Intervalos de

#### saludo y muerto de OSPF

Los intervalos de saludo y muerto de OSPF pueden configurarse por interfaz. Los intervalos de OSPF deben coincidir, de lo contrario, no se crea una adyacencia de vecino.

Para verificar los intervalos de la interfaz configurados actualmente, use el comando **show ip ospf interface**, como se muestra en la figura 1. Los intervalos de saludo y muerto de la interfaz Serial 0/0/0 están establecidos en los valores predeterminados: 10 segundos y 40 segundos, respectivamente.

En la figura 2, se presenta un ejemplo de uso de una técnica de filtrado para mostrar los intervalos de OSPF de la interfaz Serial 0/0/0 con OSPF habilitado en el R1.

En la figura 3, se usa el comando **show ip ospf neighbor** en el R1 para verificar que el R1 es adyacente al R2 y el 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.

## Verificación de los intervalos de OSPF en el R1

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via
Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 64
  Topology-MTID  Cost  Disabled   Shutdown   Topology Name
    0        64      no        no        Base
  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 00:00:03
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  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 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R1#
```

## Verificación de los intervalos de OSPF en el R1 con filtro

```
R1# show ip ospf interface serial 0/0/0 | include Timer
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
R1#
```

## Verificación de la actividad del temporizador de OSPF

```
R1# show ip ospf neighbor
Neighbor ID  Pri  State     Dead Time   Address       Interface
3.3.3.3       0    FULL/-  00:00:35  192.168.10.6  Serial0/0/1
2.2.2.2       0    FULL/-  00:00:33  172.16.3.2    Serial0/0/0
R1#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.4.2 Modificación de los intervalos de OSPFv2

Quizá se deseen cambiar los temporizadores de OSPF para que los routers detecten fallas en las redes en menos tiempo. Esto incrementa el tráfico, pero a veces la necesidad de convergencia rápida es más importante que el tráfico adicional que genera.

**Nota:** los intervalos de saludo y muerto predeterminados se basan en prácticas recomendadas y solo deben alterarse en situaciones excepcionales.

Los intervalos de saludo y muerto de OSPF pueden modificarse manualmente mediante los siguientes comandos del modo de configuración de interfaz:

- **ip ospf hello-intervalsegundos**
- **ip ospf dead-intervalsegundos**

Utilice los comandos **no ip ospf hello-interval** y **no ip ospf dead-interval** para restablecer los intervalos al valor predeterminado.

En el ejemplo de la figura 1, el intervalo de saludo se cambia a 5 segundos. Inmediatamente después de cambiar el intervalo de saludo, el IOS de Cisco modifica de forma automática el intervalo muerto a un valor equivalente al cuádruple del 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. Por lo tanto, el intervalo muerto también se establece manualmente en 20 segundos en la interfaz Serial 0/0/0 del R1.

Como se muestra en el mensaje de adyacencia OSPFv2 destacado en la figura 1, cuando el temporizador de tiempo muerto en el R1 caduca, el R1 y el R2 pierden la adyacencia. Esto se debe a que los valores solo se cambiaron en un lado del enlace serial entre el R1 y el R2. Recuerde que los intervalos de saludo y muerto de OSPF deben coincidir entre los vecinos.

Use el comando **show ip ospf neighbor** en el R1 para verificar las adyacencias de vecinos, como se muestra en la figura 2. Observe que el único vecino que se incluye es el router 3.3.3.3 (R3) y que el R1 ya no es adyacente al vecino 2.2.2.2 (R2). Los temporizadores establecidos en Serial 0/0/0 no afectan la adyacencia de vecinos con R3.

Para restaurar la adyacencia entre el R1 y el R2, el intervalo de saludo de la interfaz Serial 0/0/0 del R2 se establece en **5segundos**, como se muestra en la figura 3. Casi de inmediato, el IOS muestra un mensaje que indica que se estableció la adyacencia con un estado **FULL**.

Verifique los intervalos de la interfaz mediante el comando **show ip ospf interface**, como se muestra en la figura 4. Observe que el tiempo de saludo es de 5 segundos y el tiempo muerto se estableció automáticamente en 20 segundos en lugar de los 40 segundos predeterminados. Recuerde que OSPF establece automáticamente el intervalo muerto en cuatro veces el intervalo de saludo.

### Modificación de los intervalos de OSPF en la interfaz Serial 0/0/0 del 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
R1#
R1#
*Apr  7 17:28:21.529: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1#
```

### Verificación de las adyacencias de vecinos OSPF en el R1

```
R1# show ip ospf neighbor

Neighbor ID  Pri  State      Dead Time   Address          Interface
3.3.3.3       0    FULL/-  00:00:37   192.168.10.6  Serial0/0/1
R1#
```

### Modificación de los intervalos de OSPF en la interfaz Serial 0/0/0 del R2

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip ospf hello-interval 5
R2(config-if)#
*Apr  7 17:41:49.001: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1
on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)# end
R2#
```

### Verificación de las adyacencias de vecinos OSPF en el R2

```
R2# show ip ospf interface s0/0/0 | include Timer
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
  Retransmit 5
R2#
R2# show ip ospf neighbor

Neighbor ID  Pri  State      Dead Time   Address          Interface
3.3.3.3       0    FULL/-  00:00:35   192.168.10.10  Serial0/0/1
1.1.1.1       0    FULL/-  00:00:17   172.16.3.1    Serial0/0/0
R2#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.4.3 Modificación de los intervalos de OSPFv3

Al igual que en OSPFv2, los intervalos de OSPFv3 también pueden ajustarse.

Los intervalos de saludo y muerto de OSPFv3 pueden modificarse manualmente mediante los siguientes comandos del modo de configuración de interfaz:

- **ipv6 ospf hello-interval segundos**
- **ipv6 ospf dead-interval segundos**

**Nota:** utilice los comandos **no ipv6 ospf hello-interval** y **no ipv6 ospf dead-interval** para restablecer los intervalos al valor predeterminado.

Consulte la topología IPv6 de la figura 1. Suponga que se produjo la convergencia de la red mediante OSPFv3.

En el ejemplo de la figura 2, se cambia el intervalo de saludo de OSPFv3 a 5segundos. Inmediatamente después de cambiar el intervalo de saludo, el IOS de Cisco modifica de forma automática el intervalo muerto a un valor equivalente al cuádruple del intervalo de saludo. Sin embargo, al igual que con OSPFv2, siempre es aconsejable modificar explícitamente el temporizador en lugar de depender de la función automática del IOS para que las modificaciones queden documentadas en la configuración. Por lo tanto, el intervalo muerto también se establece manualmente en 20 segundos en la interfaz Serial 0/0/0 del R1.

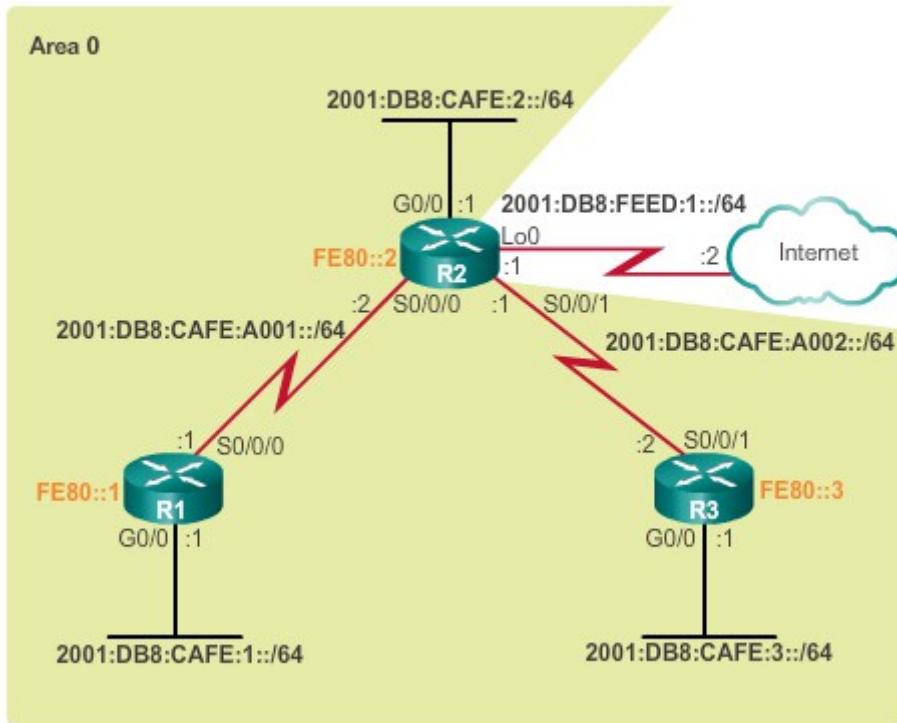
Cuando el temporizador de tiempo muerto en el R1 caduca, el R1 y el R2 pierden la adyacencia (como se muestra en el mensaje de adyacencia de OSPFv3 destacado en la figura 2) debido a que los valores solo se alteraron en un lado del enlace serial entre el R1 y el R2. Recuerde que los intervalos de saludo y muerto de OSPFv3 deben ser iguales entre los vecinos.

Use el comando **show ipv6 ospf neighbor** en el R1 para verificar las adyacencias de vecinos (figura 3). Observe que el R1 ya no es adyacente al vecino 2.2.2.2 (R2).

Para restaurar la adyacencia entre el R1 y el R2, el intervalo de saludo de la interfaz Serial 0/0/0 del R2 se establece en 5segundos (figura 4). Casi de inmediato, el IOS muestra un mensaje que indica que se estableció la adyacencia con un estado**FULL**.

Verifique los intervalos de la interfaz mediante el comando **show ipv6 ospf interface** (figura 5). Observe que el tiempo de saludo es de 5 segundos y el tiempo muerto se estableció automáticamente en 20 segundos en lugar de los 40 segundos predeterminados. Recuerde que OSPF establece automáticamente el intervalo muerto en cuatro veces el intervalo de saludo.

## Topología OSPFv3



Modificación de los intervalos de OSPFv3 en la interfaz Serial 0/0/0 del R1

```
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 ospf hello-interval 5
R1(config-if)# ipv6 ospf dead-interval 20
R1(config-if)# end
R1#
*Apr 10 15:03:51.175: %OSPFV3-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Dead timer expired
R1#
```

Verificación de las adyacencias de vecinos OSPFv3 en el R1

```
R1# show ipv6 ospf neighbor
R1#
```

## Modificación de los intervalos de OSPFv3 en la interfaz Serial 0/0/0 del R2

```
R2(config)# interface serial 0/0/0
R2(config-if)# ipv6 ospf hello-interval 5
R2(config-if)#
*Apr 10 15:07:28.815: %OSPFV3-5-ADJCHG: Process 10, Nbr
1.1.1.1 on Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)# end
R2#
```

## Verificación de las adyacencias de vecinos OSPFv3 en el R2

```
R2# show ipv6 ospf interface s0/0/0 | include Timer
    Timer intervals configured, Hello 5, Dead 20, Wait 20,
    Retransmit 5
R2#
R2# show ipv6 ospf neighbor

        OSPFv3 Router with ID (2.2.2.2) (Process ID 10)

Neighbor ID  Pri  State     Dead Time   Interface ID  Interface
3.3.3.3      0    FULL/-  00:00:38    7             Serial0/0/1
1.1.1.1      0    FULL/-  00:00:19    6             Serial0/0/0
R2#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.1 Los routers son un blanco

La función de los routers en una red es tan importante que, con frecuencia, son el blanco de ataques de red. Los administradores de red deben tener en cuenta que los routers corren el mismo riesgo de sufrir ataques que los sistemas para usuarios finales.

En general, se puede atacar a los sistemas de routing mediante la perturbación de los peers de routing o la falsificación de los datos que se transportan en el protocolo de routing. En general, la información de routing falsificada se puede usar para causar que los sistemas intercambien información errónea (se mientan), provoquen un ataque por denegación de servicio (DoS) u occasionen que el tráfico tome una ruta que normalmente no seguiría. Las consecuencias de falsificar información de routing son las siguientes:

- Redireccionamiento del tráfico para crear bucles de routing
- Redireccionamiento del tráfico para que se lo pueda controlar en un enlace no seguro
- Redireccionamiento del tráfico para descartarlo

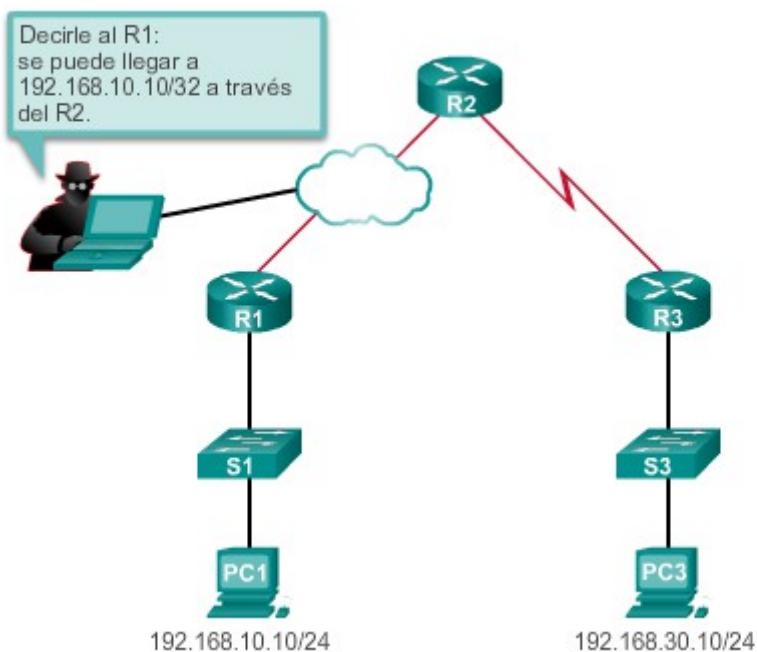
Haga clic en el botón Reproducir en la animación para ver un ejemplo de un ataque que genera un bucle de routing. Un atacante pudo conectarse directamente al enlace entre los routers R1 y

R2. El atacante inserta información de routing falsa destinada solo al router R1, que indica que el R2 es el destino preferido a la ruta de host 192.168.10.10/32. Aunque el R1 tiene una entrada en la tabla de routing a la red 192.168.10.0/24 conectada directamente, agrega la ruta insertada a su tabla de routing debido a la máscara de subred más larga. Una ruta con una máscara de subred coincidente más larga se considera superior a una ruta con una máscara de subred más corta. En consecuencia, cuando un router recibe un paquete, selecciona la máscara de subred más larga, debido a que se trata de una ruta más precisa hacia el destino.

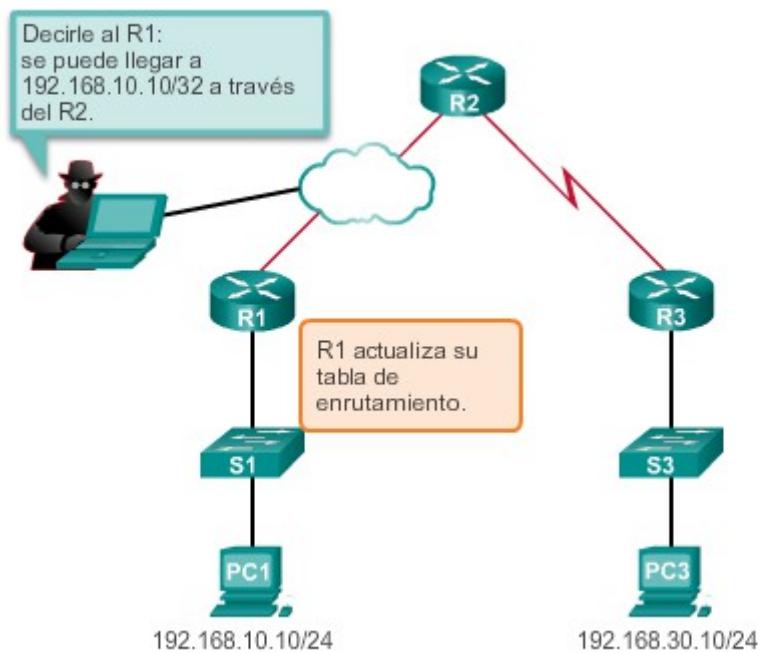
Cuando la PC3 envía un paquete a la PC1 (192.168.10.10/24), el R1 no reenvía el paquete a la PC1 host. En cambio, dirige el paquete al router R2, porque la aparente mejor ruta a 192.168.10.10/32 pasa a través del R2. Cuando el R2 recibe el paquete, analiza la tabla de routing y reenvía el paquete nuevamente al R1, lo que ocasiona un bucle.

Para mitigar los ataques a los protocolos de routing, puede configurar la autenticación de OSPF.

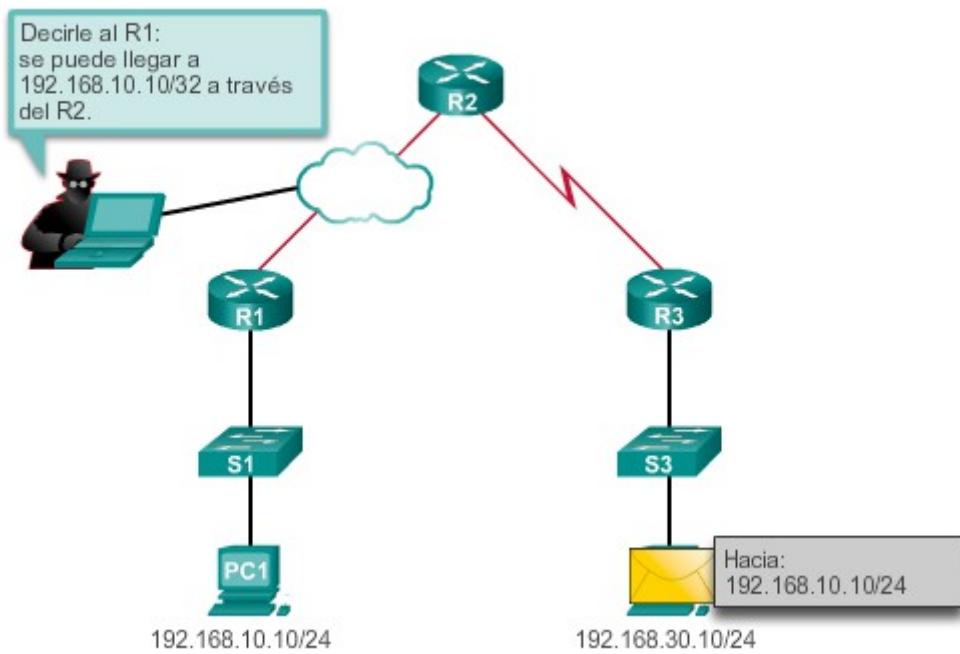
#### Descripción general de la autenticación del protocolo de enrutamiento



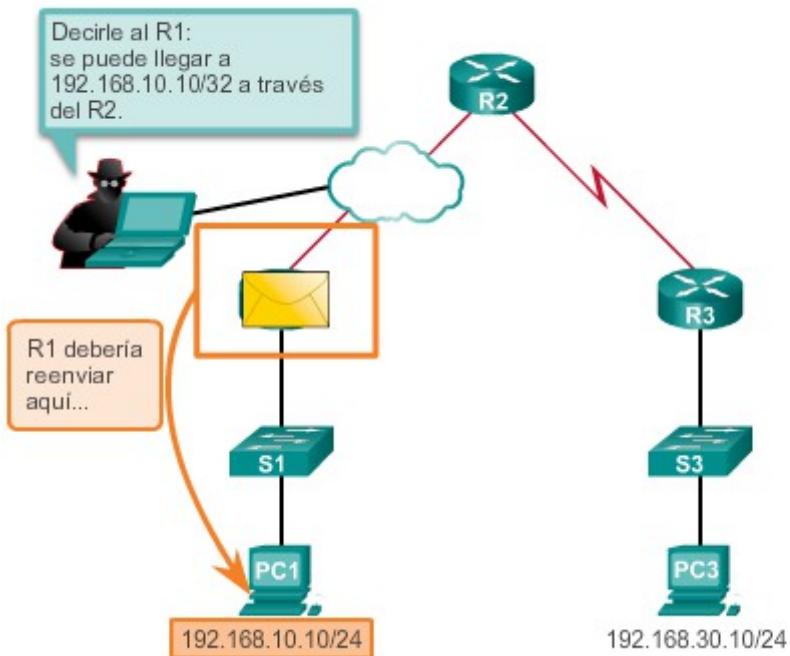
### Descripción general de la autenticación del protocolo de enrutamiento



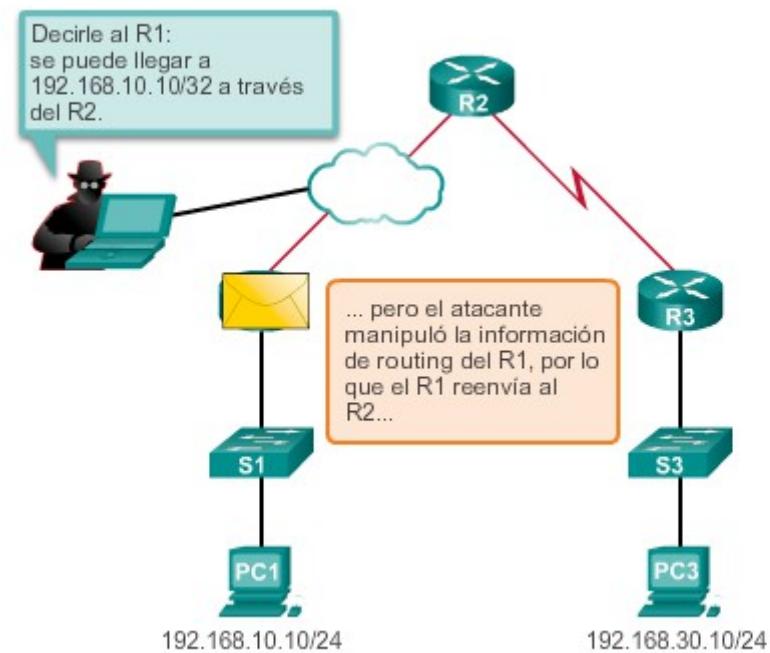
### Descripción general de la autenticación del protocolo de enrutamiento



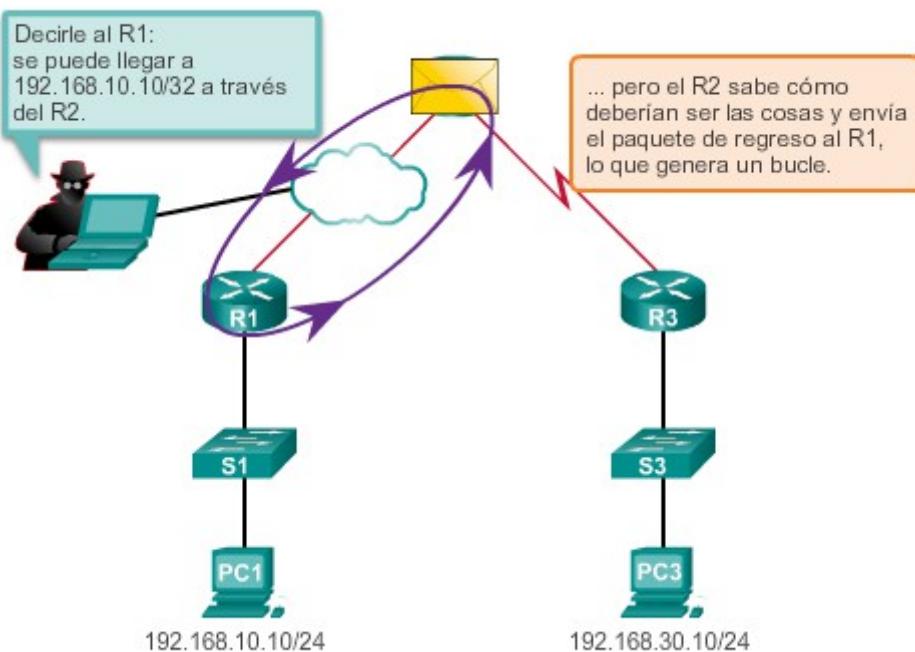
### Descripción general de la autenticación del protocolo de enrutamiento



### Descripción general de la autenticación del protocolo de enrutamiento



## Descripción general de la autenticación del protocolo de enrutamiento



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.2 Actualizaciones de routing seguras

Cuando en un router está configurada la autenticación de vecinos, el router autentica el origen de cada paquete de actualización de routing que recibe. Esto se logra mediante el intercambio de una clave de autenticación (a veces llamada “contraseña”) que conocen tanto el router que envía el paquete como el que lo recibe.

Para intercambiar información de actualización de routing de manera segura, se debe habilitar la autenticación de OSPF. La autenticación de OSPF puede ser ninguna (nula), sencilla o de síntesis del mensaje 5 (MD5).

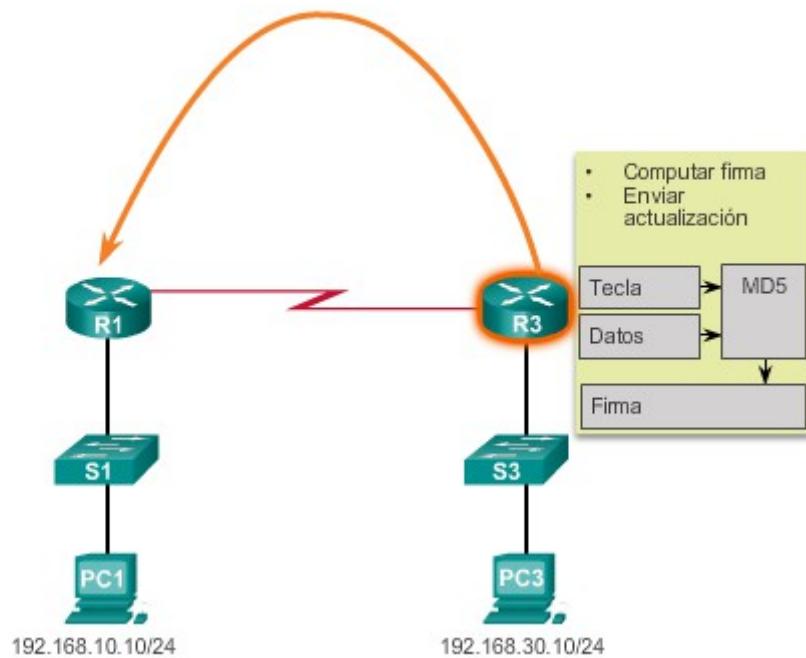
OSPF admite tres tipos de autenticación:

- **Null (nula):** este es el método predeterminado y significa que no se usa ninguna autenticación para OSPF.
- **Simple password authentication (autenticación por contraseña simple):** también se conoce como “autenticación con texto no cifrado”, porque la contraseña en la actualización se envía como texto no cifrado a través de la red. Este método se considera un método antiguo de autenticación de OSPF.
- **MD5 authentication (autenticación MD5):** se trata del método de autenticación más seguro y recomendado. La autenticación MD5 proporciona mayor seguridad, dado que la contraseña nunca se intercambia entre peers. En cambio, se calcula mediante el algoritmo MD5. La coincidencia de los resultados autentica al emisor.

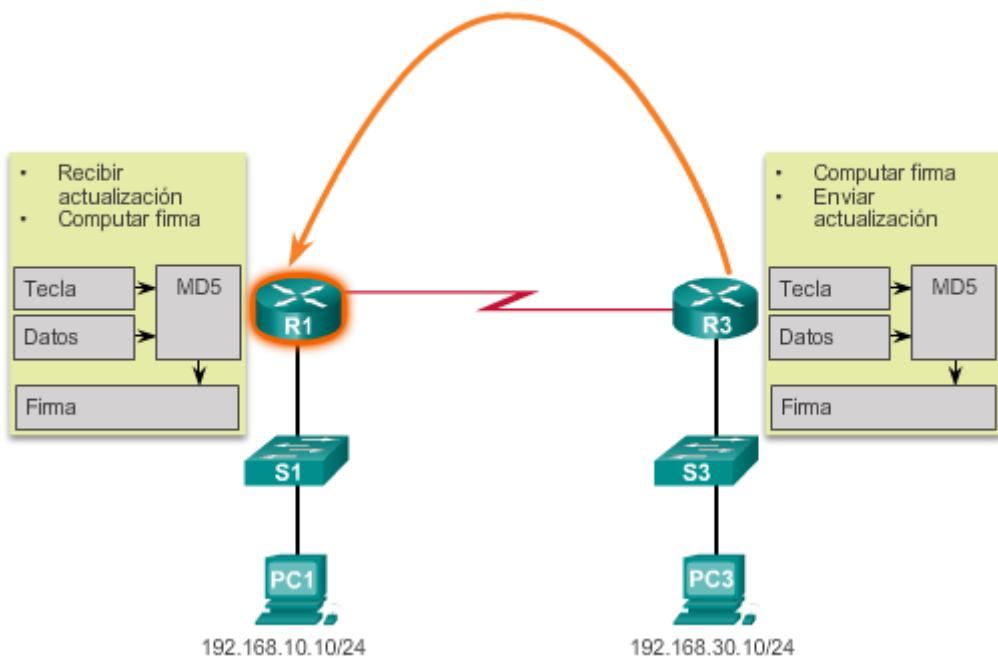
Haga clic en el botón Reproducir en la animación para ver cómo se usa la autenticación MD5 para autenticar mensajes de peer vecinos.

**Nota:** RIPv2, EIGRP, OSPF, IS-IS y BGP admiten varias formas de autenticación MD5.

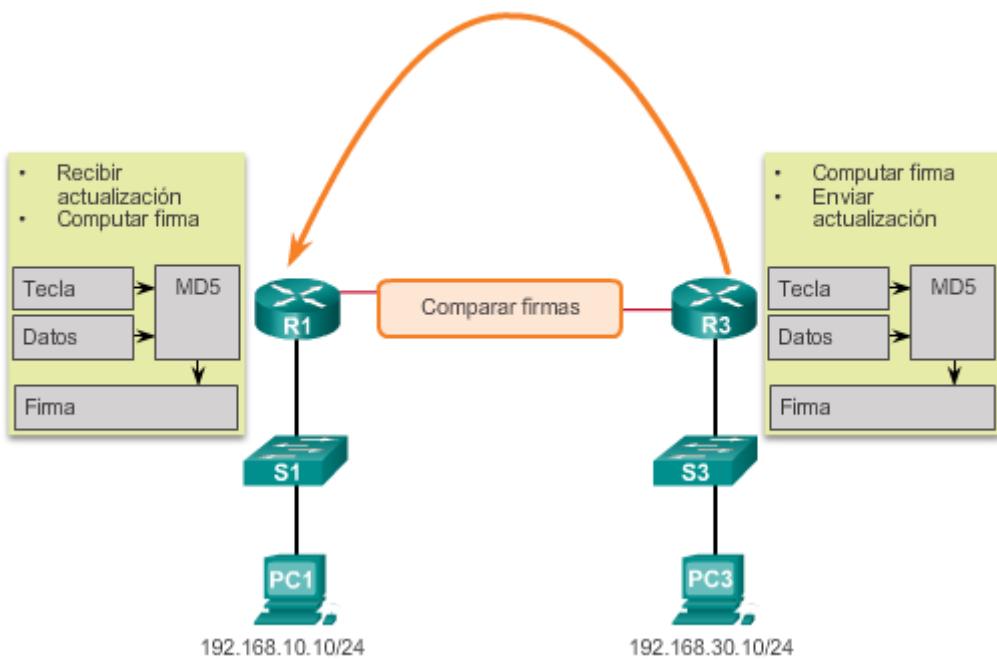
#### Autenticación mediante MD5



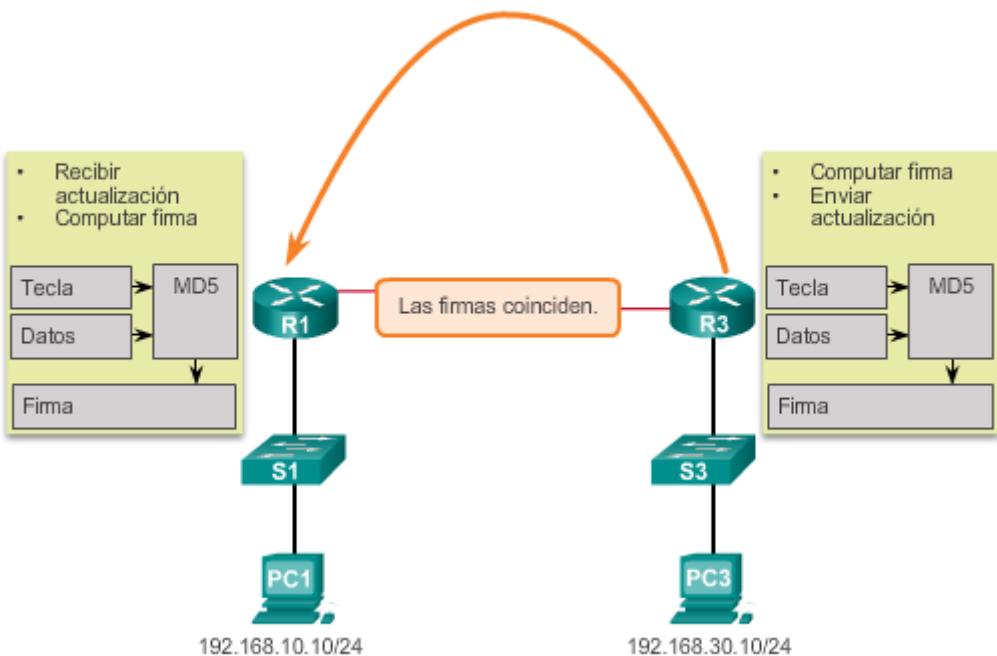
#### Autenticación mediante MD5



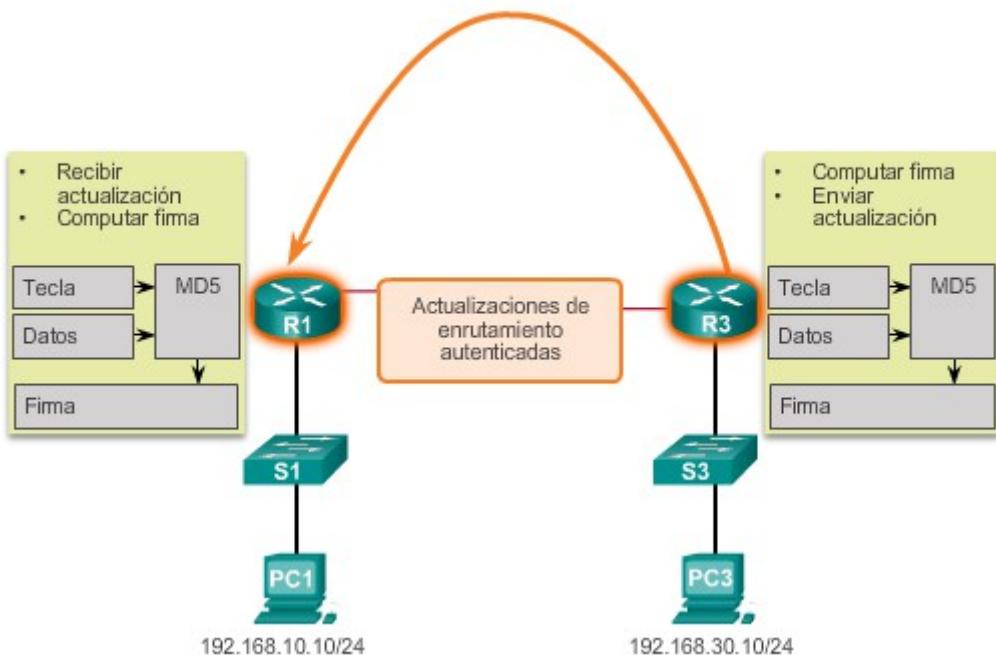
### Autenticación mediante MD5



### Autenticación mediante MD5



## Autenticación mediante MD5



### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.3 Autenticación MD5

En el siguiente ejemplo, se muestra cómo se usa la autenticación MD5 para autenticar dos routers OSPF vecinos.

En la figura 1, el R1 combina el mensaje de routing con la clave secreta previamente compartida y calcula la firma con el algoritmo MD5. La firma también se conoce como “valor de hash”.

En la figura 2, el R1 agrega la firma al mensaje de routing y lo envía al R2.

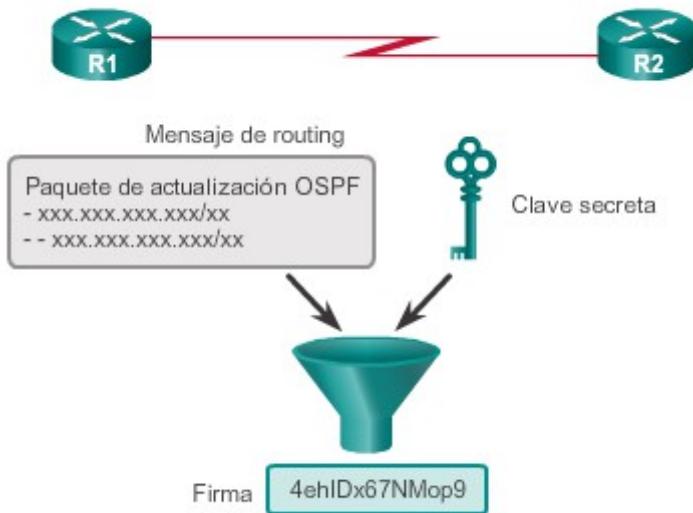
MD5 no cifra el mensaje; por eso, el contenido se puede leer fácilmente.

En la figura 3, el R2 abre el paquete, combina el mensaje de routing con la clave secreta previamente compartida y calcula la firma con el algoritmo MD5.

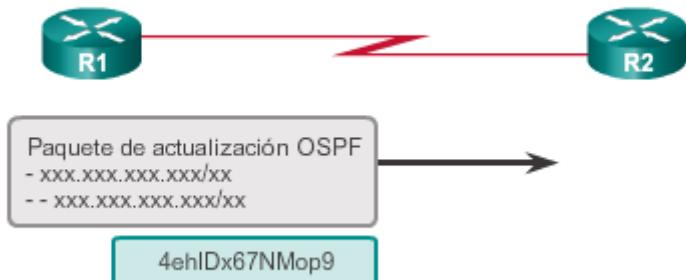
- Si las firmas coinciden, el R2 acepta la actualización de routing.
- Si las firmas no coinciden, el R2 descarta la actualización.

OSPFv3 (OSPF para IPv6) no incluye ninguna capacidad de autenticación propia. En cambio, depende por completo de IPsec para proteger las comunicaciones entre vecinos con el comando **ipv6 ospf authentication ipsec spi** del modo de configuración de interfaz. Esto resulta beneficioso, ya que simplifica el protocolo OSPFv3 y estandariza su mecanismo de autenticación.

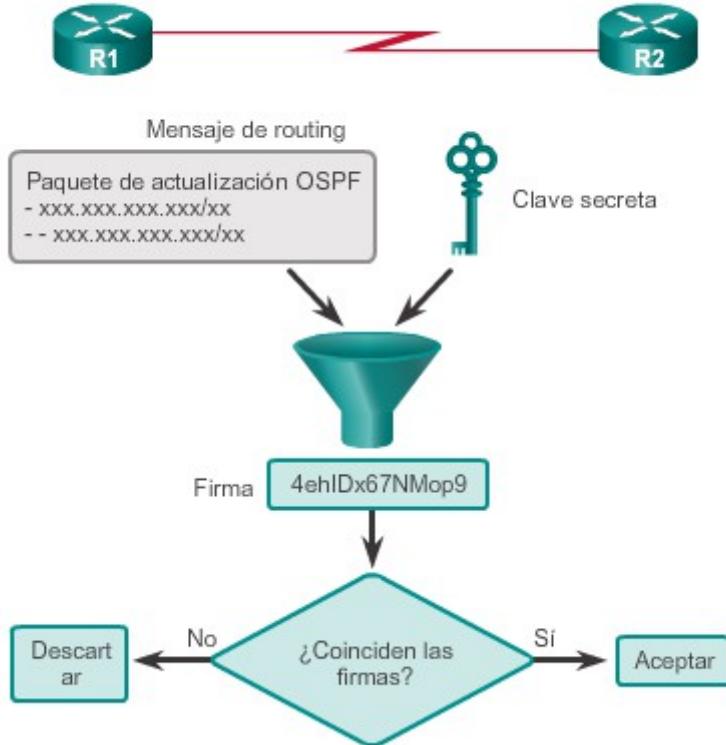
## Funcionamiento del algoritmo MD5



El R1 envía un mensaje de routing con autenticación MD5



## Funcionamiento del algoritmo MD5



### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.4 Configuración de la autenticación MD5 de OSPF

OSPF admite la autenticación de protocolos de routing mediante MD5. La autenticación MD5 se puede habilitar globalmente para todas las interfaces o para cada interfaz deseada.

Para habilitar la autenticación MD5 de OSPF globalmente, configure lo siguiente:

- **ip ospf message-digest-keykey md5 password** (comando del modo de configuración de interfaz)
- **area area-id authentication message-digest** (comando del modo de configuración del router)

Este método impone la autenticación en todas las interfaces con OSPF habilitado. Si una interfaz no está configurada con el comando **ip ospf message-digest-key**, no podrá establecer adyacencias con otros vecinos OSPF.

Para proporcionar más flexibilidad, ahora se admite la autenticación por interfaz. Para habilitar la autenticación MD5 por interfaz, configure lo siguiente:

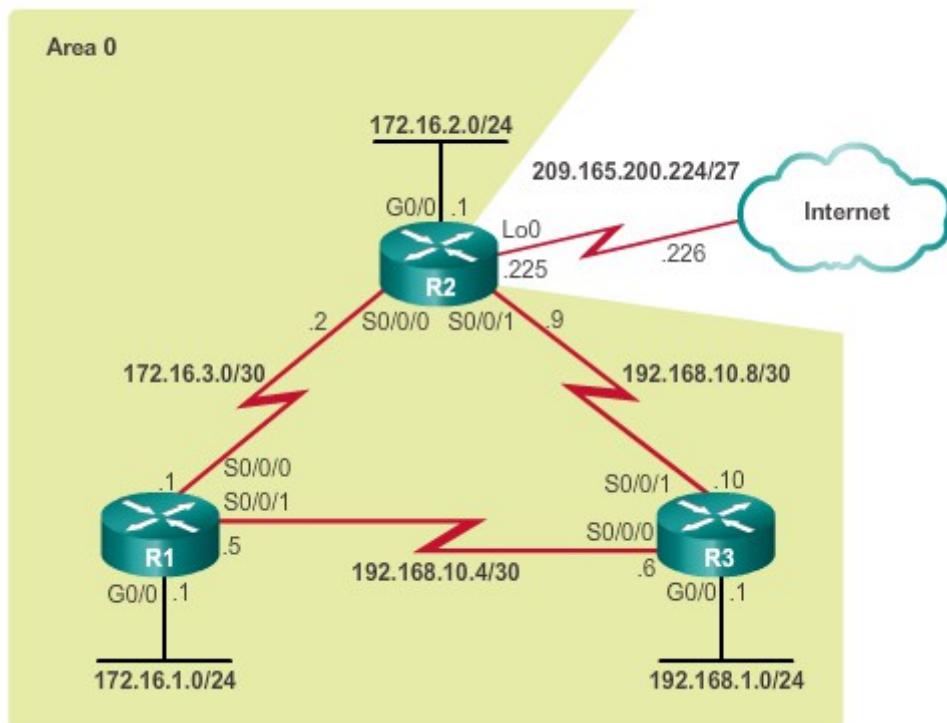
- **ip ospf message-digest-keykey md5 password** (comando del modo de configuración de interfaz)

- **ip ospf authentication message-digest** (comando del modo de configuración de interfaz)

Los métodos de autenticación MD5 de OSPF global y por interfaz pueden usarse en el mismo router. Sin embargo, la configuración por interfaz reemplaza la configuración global. Las contraseñas de autenticación MD5 no tienen que ser las mismas en toda un área; sin embargo, tienen que ser las mismas entre vecinos.

Por ejemplo, suponga que todos los routers en la ilustración convergieron mediante OSPF y que el routing funciona correctamente. La autenticación de OSPF se implementará en todos los routers.

**Topología OSPF**



#### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.5 Ejemplo de autenticación MD5 de OSPF

En el ejemplo de la figura 1, se muestra cómo configurar el R1 para habilitar la autenticación MD5 de OSPF en todas las interfaces. Observe que los mensajes informativos indican que las adyacencias de vecinos OSPF con el R2 y el R3 cambiaron al estado Down (inactivo), porque todavía no se configuraron el R2 ni el R3 para que admitan autenticación MD5.

Como una alternativa a la habilitación global de la autenticación MD5, en el ejemplo de la figura 2 se muestra cómo configurar el R1 para habilitar la autenticación MD5 de OSPF por interfaz. Observe que, también en este caso, las adyacencias de vecinos OSPF cambiaron al estado Down.

Utilice el verificador de sintaxis de la figura 3 para habilitar la autenticación MD5 de OSPF globalmente en el R2 y por interfaz en el R3.

Aquí también aparecen mensajes informativos. El primer mensaje se debe a que se volvió a establecer la adyacencia de vecino con el R1. Sin embargo, la adyacencia con el R3 cambió al estadoDown, porque todavía no se configuró el R3.

Después de configurar el R3, se volvieron a establecer todas las adyacencias de vecinos.

#### **Habilitación de la autenticación MD5 de OSPF en forma global en el R1**

```
R1(config)# router ospf 10
R1(config-router)# area 0 authentication message-digest
R1(config-router)# exit
R1(config)#
*Apr  8 09:58:09.899: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
*Apr  8 09:58:28.627: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)#

```

## Habilitación de la autenticación MD5 de OSPF en las interfaces del R1

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
R1(config)# interface Serial 0/0/1
R1(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# exit
R1(config)#
*Apr  8 10:20:10.647: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2
on Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#
*Apr  8 10:20:50.007: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3
on Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer
expired
R1(config)#

```

## Habilitación de la autenticación MD5 de OSPF

Use CISCO-123 como la clave MD5 de OSPF y realice los siguientes pasos en orden:

- Habilite la autenticación MD5 en forma global para el área OSPF 0, ID de proceso 10.
- Configure la clave MD5 de OSPF en la interfaz GigabitEthernet 0/0.
- Configure la clave MD5 de OSPF en la interfaz Serial 0/0/0.
- Configure la clave MD5 de OSPF en la interfaz Serial 0/0/1.
- Vuelva al modo EXEC privilegiado.

```
R2(config)# router ospf 10
R2(config-router)# area 0 authentication message-digest
R2(config-router)# interface GigabitEthernet 0/0
R2(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R2(config-if)# interface Serial 0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R2(config-if)# interface Serial 0/0/1
R2(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R2(config-if)# end
R2(config)#
*Apr 8 10:26:46.783: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
R2#
```

Ahora configure el R3. Con CISCO-123 como la clave MD5 de OSPF, configure la clave y habilite la autenticación MD5 de OSPF en cada interfaz, en orden:

- GigabitEthernet 0/0
- Serial 0/0/0
- Serial 0/0/1
- Vuelva al modo EXEC privilegiado.

```
R3(config)# interface GigabitEthernet 0/0
R3(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# interface Serial 0/0/0
R3(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# interface Serial 0/0/1
R3(config-if)# ip ospf message-digest-key 1 md5 CISCO-123
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# end
R3#
*Apr 8 10:29:21.859: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
*Apr 8 10:29:27.315: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R3#
```

Habilitó correctamente la autenticación MD5 de OSPF, tanto en forma global como por interfaz.

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.6 Verificación de la

autenticación MD5 de OSPF

Para verificar que la autenticación MD5 de OSPF esté habilitada, use el comando **show ip ospf interface** del modo EXEC privilegiado. Al verificar que la tabla de routing está completa, se puede confirmar que la autenticación se realizó correctamente.

En la figura 1, se muestra la verificación de la autenticación MD5 de OSPF en la interfaz serial 0/0/0 en el R1.

En la figura 2, se confirma que la autenticación se realizó correctamente.

Utilice el verificador de sintaxis de la figura 3 para verificar la autenticación MD5 de OSPF en el R2 y el R3.

## Verificación de los parámetros de la autenticación MD5 de OSPF del R1

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
    Internet Address 172.16.3.1/30, Area 0, Attached via
Network Statement
    Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 64
Topology-MTID  Cost  Disabled  Shutdown      Topology Name
              0       64        no        no          Base
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 5, Dead 20, Wait 20,
Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
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 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
```

## Verificación de la tabla de routing en el R1

```
R1# show ip route ospf
Codes: L - local, 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
       H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O     172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17, Serial0/0/0
O     192.168.1.0/24 [110/65] via 192.168.10.6, 00:30:43, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O     192.168.10.8/30 [110/128] via 192.168.10.6, 00:30:43, Serial0/0/1
                                [110/128] via 172.16.3.2, 00:33:17, Serial0/0/0
R1#
```

## Verificación de la autenticación MD5 de OSPF en el R2

Verifique la habilitación de la autenticación MD5 de OSPF en el R2 por medio del filtrado del comando "show ip ospf interface" para que se muestre solamente la porción "Message" del resultado.

```
R2# show ip ospf interface | include Message
  Message digest authentication enabled
  Message digest authentication enabled
  Message digest authentication enabled
```

R2#

Verifique que la tabla de routing esté completa mostrando solo las rutas OSPF.

```
R2# show ip route ospf
```

```
Codes: L - local, 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 - CDR, P - periodic downloaded static route, H - NHRP,
L - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.226 to network 0.0.0.0
```

```
    172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O         172.16.1.0/24 [110/65] via 172.16.3.1, 00:46:13,
Serial0/0/0
O         192.168.1.0/24 [110/65] via 192.168.10.10, 00:43:50,
Serial0/0/1
          192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O             192.168.10.4/30 [110/128] via 192.168.10.10, 00:43:50,
Serial0/0/1
          [110/128] via 172.16.3.1, 00:46:13,
Serial0/0/0
```

R2#

Ahora, inició sesión en el R3. Verifique la habilitación de la autenticación MD5 de OSPF por medio del filtrado del comando "show ip ospf interface" para que se muestre solamente la porción "Message" del resultado.

```
R3# show ip ospf interface | include Message
  Message digest authentication enabled
  Message digest authentication enabled
  Message digest authentication enabled
```

R3#

Verifique que la tabla de routing esté completa mostrando solo las rutas OSPF.

```
R3# show ip route ospf
```

```
Codes: L - local, 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 - CDR, P - periodic downloaded static route, H - NHRP,
L - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 209.165.200.226 to network 0.0.0.0
```

```
O*E2  0.0.0.0/0 [110/1] via 192.168.10.9, 00:01:54,
Serial0/0/1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
O         172.16.1.0/24 [110/65] via 192.168.10.5, 00:01:59,
Serial0/0/0
O         172.16.2.0/24 [110/65] via 192.168.10.9, 00:01:54,
Serial0/0/1
O             172.16.3.0/30 [110/128] via 192.168.10.9, 00:01:54,
Serial0/0/1
          [110/128] via 192.168.10.5, 00:01:59,
Serial0/0/0
```

R3#

Verificó correctamente la autenticación MD5 de OSPF en el R2 y el R3.

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.7 Packet Tracer:

### Configuración de las características avanzadas de OSPFv2

#### **Información básica/situación**

En esta actividad, ya se configuró OSPF, y todas las terminales actualmente tienen plena conectividad. Modificará la configuración predeterminada de routing OSPF mediante la modificación de los temporizadores de saludo y de muerto, el ajuste del ancho de banda de un enlace y la habilitación de la autenticación de OSPF. A continuación, verificará que se haya restaurado la plena conectividad para todas las terminales.

[Packet Tracer: Configuración de las características avanzadas de OSPF \(instrucciones\)](#)

[Packet Tracer: Configuración de las características avanzadas de OSPF \(PKA\)](#)

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.1.5.8 Práctica de

### laboratorio: Configuración de las características avanzadas de OSPFv2

#### **En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar y verificar el routing OSPF
- Parte 3: cambiar las métricas de OSPF
- Parte 4: Configurar y propagar una ruta estática predeterminada
- Parte 5: Configurar la autenticación de OSPF

[Práctica de laboratorio: Configuración de las características avanzadas de OSPFv2](#)

## Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.1.1 Descripción

### general

OSPF es un protocolo de routing de frecuente implementación que se utiliza en redes empresariales grandes. La resolución de problemas relacionados con el intercambio de información de routing es una de las habilidades más indispensables para un profesional de redes dedicado a la implementación y el mantenimiento de grandes redes empresariales enrutadas que usan OSPF como IGP.

En la ilustración, se indican los problemas que pueden surgir durante el establecimiento de adyacencias OSPF.

## Adyacencias OSPF



### Si ocurre lo siguiente, no se forman adyacencias OSPF:

- Las interfaces no están en la misma red.
- Los tipos de redes OSPF no coinciden.
- Los temporizadores muerto y de saludo de OSPF no coinciden.
- La interfaz al vecino está configurada incorrectamente como pasiva.
- Hay un comando **network** de OSPF faltante o incorrecto.
- La autenticación está mal configurada.

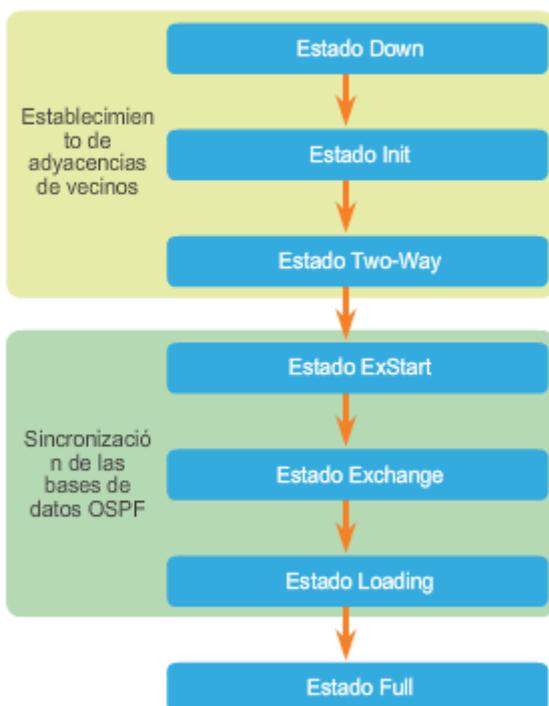
### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.1.2 Estados de OSPF

Para resolver problemas de OSPF, es importante comprender la manera en que los routers OSPF atraviesan distintos estados de OSPF cuando se establecen las adyacencias.

En la ilustración, se indican los estados de OSPF y se proporciona un resumen de las funciones de cada estado.

Cuando se realiza la resolución de problemas de vecinos OSPF, tenga en cuenta que los estados FULL o 2WAY son normales. Todos los otros estados son temporales, es decir, el router no debería permanecer en esos estados durante períodos extendidos.

## Transición a través de los estados OSPF



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.1.3 Comandos para solución de problemas de OSPF

Existen muchos comandos de OSPF distintos que se pueden usar para facilitar el proceso de resolución de problemas. A continuación, se resumen los comandos más comunes:

- **show ip protocols** (figura 1): se utiliza para verificar información fundamental de configuración de OSPF, como la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.
- **show ip ospf neighbor**(figura 2): se usa para verificar si el router formó una adyacencia con los routers vecinos. Muestra la ID del router vecino, la prioridad del vecino, el estado de OSPF, el temporizador de tiempo muerto, la dirección IP de la interfaz vecina y la interfaz mediante la cual se puede acceder al vecino. Si no se muestra la ID del router vecino o este no se muestra en el estado FULL o 2WAY, los dos routers no formaron una adyacencia OSPF. Si dos routers no establecieron adyacencia, no se intercambiará la información de link-state. Las bases de datos de link-state incompletas pueden crear árboles SPF y tablas de enrutamiento imprecisos. Es posible que no existan rutas hacia las redes de destino o que estas no representen la ruta más óptima.
- **show ip ospf interface**(figura 3): se usa para mostrar los parámetros de OSPF que se configuraron en una interfaz, como la ID del proceso OSPF a la que se asignó la interfaz, el área en la que están las interfaces, el costo de la interfaz y los intervalos de saludo y muerto. Si se agrega el nombre y el número de interfaz al comando, se muestra el resultado para una interfaz específica.

- **show ip ospf** (figura 4): se utiliza para examinar la ID del proceso OSPF y la ID del router. Además, este comando muestra información de área OSPF y la última vez que se calculó el algoritmo SPF.
- **show ip route ospf** (figura 5): se utiliza para mostrar solo las rutas OSPF descubiertas en la tabla de routing. El resultado muestra que el R1 descubrió alrededor de cuatro redes remotas mediante OSPF.
- **clear ip ospf [ id-proceso ] process**: se usa para restablecer las adyacencias de vecinos OSPFv2.

#### Verificación de la configuración de OSPF en el R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.1 0.0.0.0 area 0
    172.16.3.1 0.0.0.0 area 0
    192.168.10.5 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          00:08:35
    2.2.2.2           110          00:08:35
  Distance: (default is 110)

R1#
```

#### Verificación de las adyacencias de vecinos OSPF en el R1

```
R1# show ip ospf neighbor

Neighbor ID Pri State          Dead Time Address      Interface
2.2.2.2      1 FULL/BDR      00:00:30  192.168.1.2 GigabitEthernet0/0
3.3.3.3      0 FULL/BROTHER  00:00:38  192.168.1.3 GigabitEthernet0/0
R1#
```

### Verificación de la configuración de la interfaz OSPF de S0/0/0 en el R1

```
R1# show ip ospf interface Serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via Network
Statement
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
Cost: 64
  Topology-MTID      Cost      Disabled      Shutdown      Topology Name
          0           64         no            no            Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    cob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  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 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
R1#
```

## Visualización de los parámetros de OSPF

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
  Start time: 00:02:19.116, Time elapsed: 00:01:00.796
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Supports area transit capability
  Supports NSSA (compatible with RFC 3101)
  Event-log enabled, Maximum number of events: 1000, Mode: cyclic
  Router is not originating router-LSAs with maximum metric
  Initial SPF schedule delay 5000 msec
  Minimum hold time between two consecutive SPFs 10000 msec
  Maximum wait time between two consecutive SPFs 10000 msec
  Incremental-SPF disabled
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msec
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msec
  Retransmission pacing timer 66 msec
  Number of external LSA 1. Checksum Sum 0x00A1FF
  Number of opaque AS LSA 0. Checksum Sum 0x000000
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Number of areas transit capable is 0
  External flood list length 0
  IETF NSF helper support enabled
  Cisco NSF helper support enabled
  Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
      Number of interfaces in this area is 3
  Area has no authentication
  SPF algorithm last executed 00:00:36.936 ago
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x016D60
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0

R1#
```

## Verificación de las rutas OSPF en la tabla de routing del R1

```
R1# show ip route ospf
Codes:L - local,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, H - NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
      O     172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17,Serial0/0/0
      O     192.168.1.0/24 [110/65] via 192.168.10.6, 00:30:43,Serial0/0/1
            192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
      O     192.168.10.8/30[110/128] via 192.168.10.6,00:30:43,Serial0/0/1
            [110/128] via 172.16.3.2,00:33:17,Serial0/0/0
R1#
```

### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.1.4 Componentes de la resolución de problemas de OSPF

Como se muestra en la ilustración, en general, los problemas de OSPF se relacionan con uno de los siguientes aspectos:

- Adyacencias de vecinos
- Rutas faltantes
- Selección de rutas

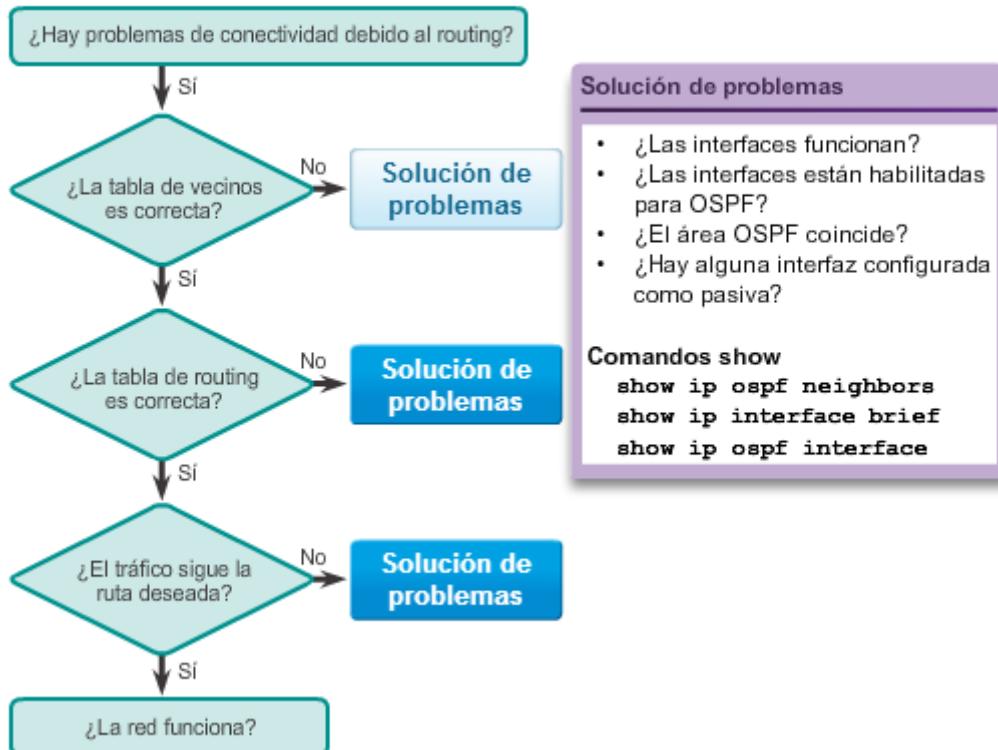
Cuando resuelva problemas de vecinos, verifique si el router estableció adyacencias con routers vecinos mediante el comando **show ip ospf neighbors**. Si no hay adyacencias, los routers no pueden intercambiar rutas. Verifique si las interfaces funcionan y están habilitadas para OSPF mediante los comandos **show ip interface brief** y **show ip ospf interface**. Si las interfaces funcionan y están habilitadas para OSPF, asegúrese de que las interfaces en ambos routers estén configuradas para la misma área OSPF y que no estén configuradas como interfaces pasivas.

Si la adyacencia entre los dos routers está establecida, verifique que haya rutas OSPF en la tabla de routing mediante el comando **show ip route ospf**. Si no hay rutas OSPF, verifique que no haya otros protocolos de routing con distancias administrativas más bajas en ejecución en la red. Verifique si todas las redes requeridas se anuncian en OSPF. También verifique si hay una

lista de acceso configurada en un router que podría filtrar las actualizaciones de routing entrantes o salientes.

Si todas las rutas requeridas están en la tabla de routing pero la ruta que el tráfico toma es incorrecta, verifique el costo de OSPF de las interfaces en la ruta. Además, preste especial atención en los casos en que las interfaces tienen una velocidad superior a 100 Mb/s, ya que todas las interfaces por encima de este ancho de banda tienen el mismo costo de OSPF de manera predeterminada.

### Resolución de problemas de OSPF



Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.1.5 Actividad:

Identificar el comando para la resolución de problemas

**Actividad (situación 1): Identificar el comando para la resolución de problemas**

En esta actividad, se incluyen cinco situaciones que muestran resultados de comandos habituales para la resolución de problemas de OSPF. En cada situación, identifique el comando de resolución de problemas indicado por el resultado. Haga clic en el círculo junto al comando correspondiente para indicar su respuesta. Haga clic en el botón 2 para continuar la actividad.

```
Routing Process "ospf 10" with ID 1.1.1.1
  Start time: 00:02:19.116, Time elapsed: 00:01:00.796
<resultado omitido>
  Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
      Number of interfaces in this area is 3
  Area has no authentication
  SPF algorithm last executed 00:00:36.936 ago
  SPF algorithm executed 3 times
  Area ranges are
  Number of LSA 3. Checksum Sum 0x016D60
<resultado omitido>
```

- |  |   |
|--|---|
| <input type="radio"/> show ip ospf interface | <input checked="" type="radio"/> show ip ospf |
| <input type="radio"/> show ip route ospf     | <input type="radio"/> show ip ospf neighbor   |
| <input type="radio"/> show ip protocols      | <input type="radio"/> show ip interface brief |

**Actividad (situación 2): Identificar el comando para la resolución de problemas de OSPF**

Identifique cuál es el comando para la resolución de problemas de OSPF que produjo el resultado que se muestra. Haga clic en el círculo junto al comando correspondiente para indicar su respuesta. Haga clic en el botón 3 para continuar.

```
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.0 0.0.0.0 area 0
    172.16.3.1 0.0.0.0 area 0
    192.168.10.5 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          00:08:35
    2.2.2.2           110          00:08:35
  Distance: (default is 110)
```

- |  |   |
|--|---|
| <input type="radio"/> show ip ospf interface       | <input type="radio"/> show ip ospf            |
| <input type="radio"/> show ip route ospf           | <input type="radio"/> show ip ospf neighbor   |
| <input checked="" type="radio"/> show ip protocols | <input type="radio"/> show ip interface brief |

**Actividad (situación 3): Identificar el comando para la resolución de problemas de OSPF**

Identifique cuál es el comando para la resolución de problemas de OSPF que produjo el resultado que se muestra. Haga clic en el círculo junto al comando correspondiente para indicar su respuesta. Haga clic en el botón 4 para continuar.

```
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 64
  Topology-MTID   Cost   Disabled   Shutdown   Topology Name
  0              64     no        no        Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:02
  Supports Link-local Signaling (LLS)
<resultado omitido>
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
    Suppress hello for 0 neighbor(s)
  Message digest authentication enabled
    Youngest key id is 1
```

- |   |   |
|---|---|
| <input checked="" type="radio"/> show ip ospf interface | <input type="radio"/> show ip ospf            |
| <input type="radio"/> show ip route ospf                | <input type="radio"/> show ip ospf neighbor   |
| <input type="radio"/> show ip protocols                 | <input type="radio"/> show ip interface brief |

**Actividad (situación 4): Identificar el comando para la resolución de problemas de OSPF**

Identifique cuál es el comando para la resolución de problemas de OSPF que produjo el resultado que se muestra. Haga clic en el círculo junto al comando correspondiente para indicar su respuesta. Haga clic en el botón 5 para continuar.

Codes: L - local, 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, H - NHRP, l - LISP  
+ - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

```
O*E2 0.0.0.0/0 [110/1] via 172.16.3.2, 00:33:17, Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
O       172.16.2.0/24 [110/65] via 172.16.3.2, 00:33:17, Serial0/0/0
O       192.168.10.8/30 [110/128] via 192.168.10.6, 00:30:43, Serial0/0/1
                  [110/128] via 172.16.3.2, 00:33:17, Serial0/0/0
```

- |   |   |
|---|---|
| <input type="radio"/> show ip ospf interface        | <input type="radio"/> show ip ospf            |
| <input checked="" type="radio"/> show ip route ospf | <input type="radio"/> show ip ospf neighbor   |
| <input type="radio"/> show ip protocols             | <input type="radio"/> show ip interface brief |

**Actividad (situación 5): Identificar el comando para la resolución de problemas de OSPF**

Identifique cuál es el comando para la resolución de problemas de OSPF que produjo el resultado que se muestra. Haga clic en el círculo junto al comando correspondiente para indicar su respuesta.

Neighbor ID	Pri	State	Dead Time	Address	Interface
2.2.2.2	1	FULL/BDR	00:00:30	192.168.1.2	GigabitEthernet0/0
3.3.3.3	0	FULL/DROTHER	00:00:38	192.168.1.3	GigabitEthernet0/0

- |  |  |
|--|--|
| <input type="radio"/> show ip ospf interface | <input type="radio"/> show ip ospf                     |
| <input type="radio"/> show ip route ospf     | <input checked="" type="radio"/> show ip ospf neighbor |
| <input type="radio"/> show ip protocols      | <input type="radio"/> show ip interface brief          |

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.2.1 Resolución de problemas de vecinos

En este ejemplo, se demostrará cómo resolver problemas de vecinos. En la topología de la figura 1, todos los routers se configuraron para admitir el routing OSPF.

Un vistazo a la tabla de routing del R1, que se muestra en la figura 2, nos permite saber que no agrega rutas OSPF. Existen varios posibles motivos para esto. Sin embargo, un requisito para que se forme una relación de vecinos entre dos routers es la conectividad de capa 3 del modelo OSI.

El resultado de la figura 3 confirma que la interfaz S0/0/0 está activa y en funcionamiento. El ping correcto también confirma que la interfaz serial del R2 está activa. Un ping correcto no significa que se formará una adyacencia, porque es posible que haya subredes superpuestas. Todavía debe verificar que las interfaces en los dispositivos conectados comparten la misma subred. Si el ping no fue correcto, revise el cableado y verifique que las interfaces en los dispositivos conectados estén configuradas correctamente y funcionen.

Para habilitar una interfaz para OSPF, se debe configurar un comando **network** que coincida durante el proceso de routing OSPF. Las interfaces OSPF activas pueden verificarse mediante el comando **show ip ospf interface**. El resultado de la figura 4 verifica que la interfaz Serial 0/0/0 está habilitada para OSPF. Si las interfaces conectadas en dos routers no están habilitadas para OSPF, los vecinos no formarán una adyacencia.

Verifique la configuración de OSPF mediante el comando **show ip protocols**. El resultado que se muestra en la figura 5 verifica que OSPF está habilitado y también enumera las redes que se anuncian como habilitadas por medio del comando **network**. Si una dirección IP en una interfaz está incluida en una red habilitada para OSPF, la interfaz está habilitada para OSPF.

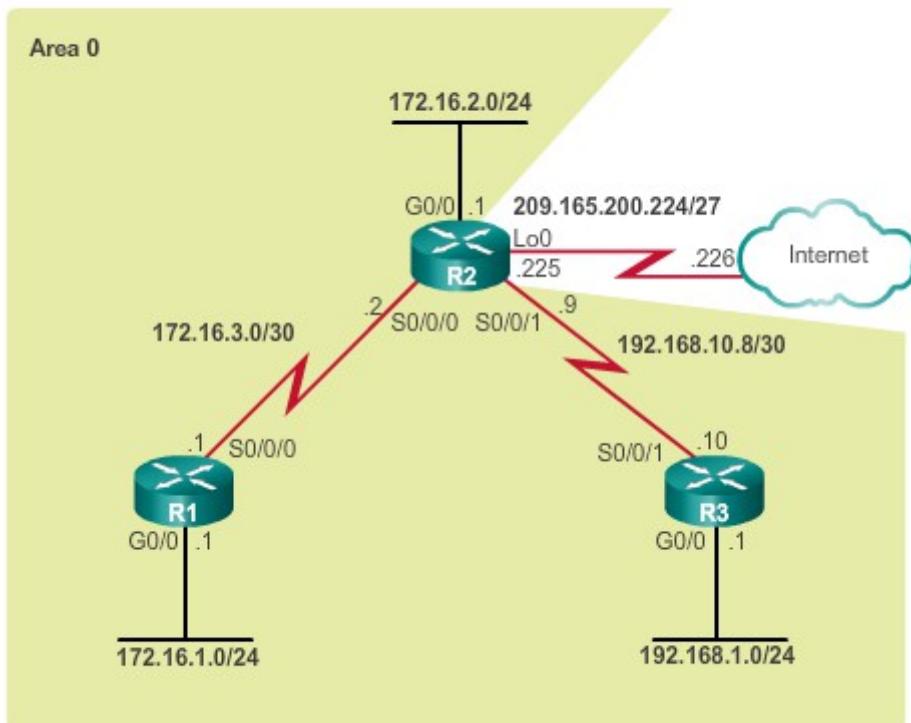
Sin embargo, observe que la interfaz Serial 0/0/0 figura como pasiva. Recuerde que el comando **passive-interface** detiene las actualizaciones de routing entrantes y salientes, debido a que el efecto del comando ocasiona que el router deje de enviar y recibir paquetes de saludo a través de una interfaz. Por esta razón, los routers no formarán una relación de vecinos.

Para deshabilitar la interfaz como pasiva, use el comando **no passive-interface** del modo de configuración del router, como se muestra en la figura 6. Después de deshabilitar la interfaz pasiva, los routers establecen una adyacencia, como lo indica el mensaje de información generado automáticamente.

Una verificación rápida de la tabla de routing, que se muestra de la figura 7, confirma que OSPF ahora intercambia información de routing.

Otro problema que puede surgir es que dos routers vecinos tengan tamaños de MTU incompatibles en las interfaces conectadas. El tamaño de MTU es el paquete de capa de red más grande que el router reenvía por cada interfaz. De manera predeterminada, los routers tienen un tamaño de MTU de 1500 bytes. Sin embargo, este valor puede cambiarse para paquetes IPv4 mediante el comando de configuración de interfaz **ip mtu size** o el comando de interfaz **ipv6 mtu size** para paquetes IPv6. Si dos routers conectados tuvieran valores de MTU incompatibles, igualmente intentarían formar una adyacencia, pero no intercambiarían sus LSDB y la relación de vecinos fallaría.

## Topología OSPF



### Verificación de rutas OSPF en la tabla de routing del R1

```
R1# show ip route
Codes: L - local, 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, H -
            NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0
C        172.16.3.0/30 is directly connected, Serial0/0/0
L        172.16.3.1/32 is directly connected, Serial0/0/0
R1#
```

### Verificación de conectividad de capa 3 al R2

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
Embedded-Service-Engine0/0 unassigned    YES  unset  administratively down down
GigabitEthernet0/0     172.16.1.1    YES  manual up           up
GigabitEthernet0/1     unassigned    YES  unset  administratively down down
Serial0/0/0            172.16.3.1    YES  manual up           up
Serial0/0/1            unassigned    YES  TFTP   up           up
R1#
R1# ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/14/16 ms
R1#
```

### Verificación de habilitación de OSPF en la interfaz Serial 0/0/0 del R1

```
R1# show ip ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Internet Address 172.16.3.1/30, Area 0, Attached via
  Network Statement
  Process ID 10, Router ID 1.1.1.1, Network Type
  POINT_TO_POINT, Cost: 64
  Topology-MTID    Cost  Disabled Shutdown Topology Name
                  0       64      no        no      Base
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20,
  Retransmit 5
  oob-resync timeout 40
  No Hellos (Passive interface)
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  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)
  Message digest authentication enabled
  Youngest key id is 1
```

### Verificación de la configuración de OSPF en el R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.16.1.1 0.0.0.0 area 0
    172.16.3.1 0.0.0.0 area 0
  Passive Interface(s):
    GigabitEthernet0/0
    Serial0/0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          00:50:03
    2.2.2.2           110          04:27:25
  Distance: (default is 110)

R1#
```

### Deshabilitación de la interfaz pasiva en la interfaz S0/0/0 del R1

```
R1(config)# router ospf 10
R1(config-router)# no passive-interface s0/0/0
R1(config-router)#
*Apr  9 13:14:15.454: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
R1(config-router)# end
R1#
```

## Verificación de rutas OSPF en la tabla de routing del R1

```
R1# show ip route ospf
Codes: L - local, 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, H -
           NHRP, l - LIS
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:00:18,
Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
O     172.16.2.0/24 [110/65] via 172.16.3.2, 00:00:18,
      Serial0/0/0
O     192.168.1.0/24 [110/129] via 172.16.3.2, 00:00:18,
      Serial0/0/0
      192.168.10.0/30 is subnetted, 1 subnets
O     192.168.10.8 [110/128] via 172.16.3.2, 00:00:18,
      Serial0/0/0
R1#
```

### Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.2.2 Resolución de problemas de la tabla de routing OSPF

En la topología de la figura 1, todos los routers se configuraron para admitir el routing OSPF.

Un vistazo a la tabla de routing del R1 (figura 2) nos permite saber que recibe información de la ruta predeterminada, la LAN del R2 (172.16.2.0/24) y el enlace entre el R2 y el R3 (192.168.10.8/30). Sin embargo, no recibe la ruta OSPF LAN del R3.

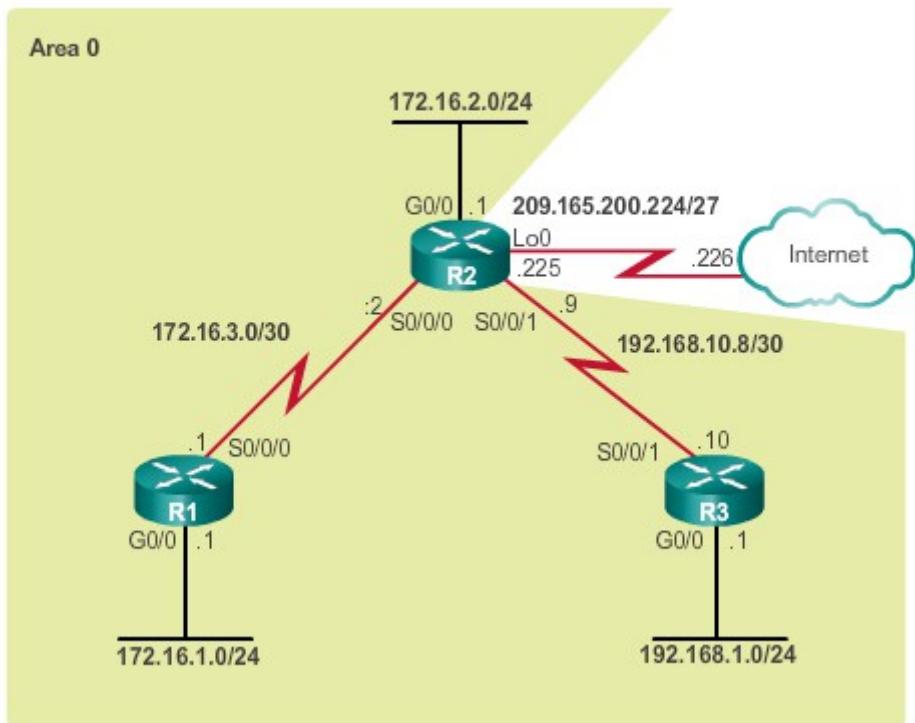
El resultado de la figura 3 verifica la configuración de OSPF en el R3. Observe que el R3 solo anuncia el enlace entre el R3 y el R2, pero no anuncia la LAN del R3 (192.168.1.0/24).

Para habilitar una interfaz para OSPF, se debe configurar un comando **network** que coincida durante el proceso de routing OSPF. El resultado de la figura 4 confirma que la LAN del R3 no se anuncia en OSPF.

En el ejemplo de la figura 5, se agrega un comando **network** para la LAN del R3. Ahora el R3 debería anunciar la LAN del R3 a sus vecinos OSPF.

El resultado de la figura 6 verifica que la LAN del R3 ahora esté en la tabla de routing del R1.

Topología OSPF



## Verificación de rutas OSPF en la tabla de routing del R1

```
R1# show ip route
Codes: L - local, 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, H -
           NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:05:26,
      Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
      masks
C        172.16.1.0/24 is directly connected,
      GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
      GigabitEthernet0/0
O        172.16.2.0/24 [110/65] via 172.16.3.2, 00:05:26,
      Serial0/0/0
C        172.16.3.0/30 is directly connected, Serial0/0/0
L        172.16.3.1/32 is directly connected, Serial0/0/0
      192.168.10.0/30 is subnetted, 1 subnets
O        192.168.10.8 [110/128] via 172.16.3.2, 00:05:26,
      Serial0/0/0

R1#
```

### Verificación de la configuración de OSPF en el R3

```
R3# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0
    nssa
  Maximum path: 4
  Routing for Networks:
    192.168.10.8 0.0.0.3 area 0
  Passive Interface(s):
    Embedded-Service-Engine0/0
    GigabitEthernet0/0
    GigabitEthernet0/1
    GigabitEthernet0/3
    RG-AR-IF-INPUT1
  Routing Information Sources:
    Gateway          Distance      Last Update
    1.1.1.1           110          00:02:48
    2.2.2.2           110          00:02:48
  Distance: (default is 110)

R3#
```

### Verificación de la configuración del router OSPF en el R3

```
R3# show running-config | section router ospf
router ospf 10
  router-id 3.3.3.3
  passive-interface default
  no passive-interface Serial0/0/1
  network 192.168.10.8 0.0.0.3 area 0
R3#
```

### Anuncio de la LAN del R3 en OSPF

```
R3# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# router ospf 10
R3(config-router)# network 192.168.1.0 0.0.0.255 area 0
R3(config-router)# end
R3#
*Apr 10 11:03:11.115: %SYS-5-CONFIG_I: Configured from
console by console
R3#
```

## Verificación de rutas OSPF en la tabla de routing del R1

```
R1# show ip route ospf
Codes: L - local, 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, H -
           NHRP, l - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 172.16.3.2 to network 0.0.0.0

O*E2  0.0.0.0/0 [110/1] via 172.16.3.2, 00:08:38,
      Serial0/0/0
      172.16.0.0/16 is variably subnetted, 5 subnets, 3
      masks
O      172.16.2.0/24 [110/65] via 172.16.3.2, 00:08:38,
      Serial0/0/0
O      192.168.1.0/24 [110/129] via 172.16.3.2, 00:00:37,
      Serial0/0/0
      192.168.10.0/30 is subnetted, 1 subnets
O      192.168.10.8 [110/128] via 172.16.3.2, 00:08:38,
      Serial0/0/0
R1#
```

[Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.2.3 Packet Tracer:](#)

[Resolución de problemas de OSPFv2 de área única](#)

**Información básica/situación**

En esta actividad, resolverá problemas de routing OSPF mediante los comandos **ping** y **show** para identificar errores en la configuración de red. A continuación, registrará los errores que detecte e implementará una solución apropiada. Por último, verificará que se haya restaurado la conectividad de extremo a extremo.

[Packet Tracer: Resolución de problemas de OSPFv2 de área única \(instrucciones\)](#)

[Packet Tracer: Resolución de problemas de OSPFv2 de área única \(PKA\)](#)

[Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.3.1 Comandos para la resolución de problemas de OSPFv3](#)

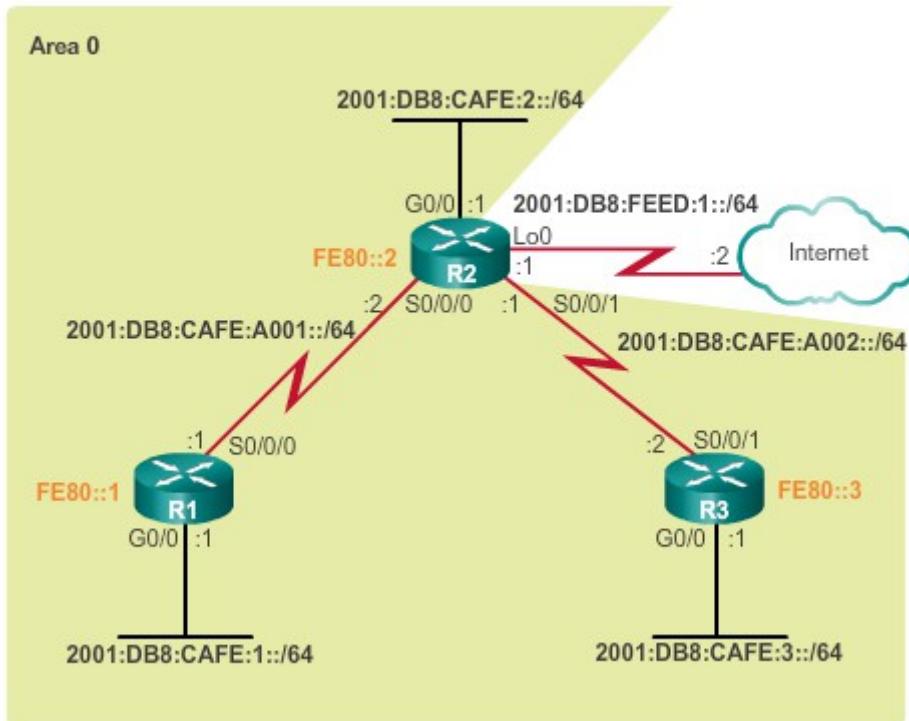
Consulte la figura 1 para ver la topología de referencia OSPFv3.

La resolución de problemas de OSPFv3 es casi idéntica a la de OSPFv2; por eso, muchos comandos y criterios de resolución de problemas de OSPFv3 también se aplican a OSPFv3.

Por ejemplo, los siguientes son los comandos equivalentes que se utilizan con OSPFv3:

- **show ipv6 protocols** (figura 2): este comando se utiliza para verificar información fundamental de configuración de OSPFv3, incluidas la ID del proceso OSPFv3, la ID del router y las interfaces de las que el router recibe actualizaciones.
- **show ipv6 ospf neighbor**(figura 3): se usa para verificar que el router formó una adyacencia con los routers vecinos. Este resultado muestra la ID del router vecino, la prioridad del vecino, el estado de OSPFv3, el temporizador de tiempo muerto, la ID de la interfaz vecina y la interfaz mediante la cual se puede acceder al vecino. Si no se muestra la ID del router vecino o este no se muestra en el estado **FULL** o **2WAY**, los dos routers no formaron una adyacencia OSPFv3. Si dos routers no establecieron adyacencia, no se intercambiará la información de link-state. Las bases de datos de link-state incompletas pueden crear árboles SPF y tablas de enrutamiento imprecisos. Es posible que no existan rutas hacia las redes de destino o que estas no constituyan las mejores rutas.
- **show ipv6 ospf interface**(figura 4): se usa para mostrar los parámetros de OSPFv3 que se configuraron en una interfaz, como la ID del proceso OSPFv3 a la que se asignó la interfaz, el área en la que están las interfaces, el costo de la interfaz y los intervalos de saludo y muerto. Si se agrega el nombre y el número de interfaz al comando, se muestra el resultado para una interfaz específica.
- **show ipv6 ospf** (figura 5): se usa para examinar la ID del proceso OSPF y la ID del router, así como la información sobre las transmisiones de LSA.
- **show ipv6 route ospf** (figura 6): se utiliza para mostrar solo las rutas OSPFv3 descubiertas en la tabla de routing. El resultado muestra que el R1 descubrió alrededor de cuatro redes remotas mediante OSPFv3.
- **clear ipv6 ospf [ id-proceso] process**: se usa para restablecer las adyacencias de vecinos OSPFv3.

## Topología OSPFv3



### Verificación de la configuración de OSPFv3 en el R1

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/0
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

### Verificación de las adyacencias de vecinos OSPFv3 en el R1

```
R1# show ipv6 ospf neighbor  
  
Neighbor ID      Pri  State      Dead Time   Interface ID  Interface  
2.2.2.2          0    FULL/-    00:00:33     7           Serial0/0/0  
R1#
```

### Visualización de los parámetros de OSPFv3

```
R1# show ipv6 ospf interface s0/0/0  
Serial0/0/0 is up, line protocol is up  
  Link Local Address FE80::1, Interface ID 6  
  Area 0, Process ID 10, Instance ID 0, Router ID 1.1.1.1  
  Network Type POINT_TO_POINT, Cost: 647  
  Transmit Delay is 1 sec, State POINT_TO_POINT  
  Timer intervals configured, Hello 10, Dead 40, Wait 40,  
  Retransmit 5  
    Hello due in 00:00:08  
  Graceful restart helper support enabled  
  Index 1/2/2, flood queue length 0  
  Next 0x0(0)/0x0(0)/0x0(0)  
  Last flood scan length is 2, maximum is 6  
  Last flood scan time is 0 msec, maximum is 0 msec  
  Neighbor Count is 1, Adjacent neighbor count is 1  
    Adjacent with neighbor 2.2.2.2  
    Suppress hello for 0 neighbor(s)  
R1#
```

**Verificación de la configuración de la interfaz OSPFv3 de S0/0/0 en R1**

```
R1# show ipv6 ospf
Routing Process "ospfv3 10" with ID 1.1.1.1
Event-log enabled, Maximum number of events: 1000, Mode:
cyclic
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPFs 10000 msec
Maximum wait time between two consecutive SPFs 10000 msec
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 1. Checksum Sum 0x0017E9
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Graceful restart helper support enabled
Reference bandwidth unit is 1000 mbps
RFC1583 compatibility enabled
    Area BACKBONE(0)
Number of interfaces in this area is 2
SPF algorithm executed 8 times
Number of LSA 13. Checksum Sum 0x063D5D
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0

R1#
```

**Verificación de las rutas OSPFv3 en la tabla de routing del R1**

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
    B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
    I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
        summary, D - EIGRP
    EX - EIGRP external, ND - ND Default, NDp - ND
        Prefix, DCE - Destination
    NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1
        - OSPF ext 1
    OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
        NSSA ext 2
OE2 ::/0 [110/1], tag 10
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:2::/64 [110/648]
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:3::/64 [110/648]
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:A002::/64 [110/1294]
    via FE80::2, Serial0/0/0

R1#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.3.2 Resolución de problemas de OSPFv3

En la topología de la figura 1, todos los routers se configuraron para admitir el routing OSPFv3.

Un vistazo a la tabla de routing IPv6 del R1 (figura 2) nos permite saber que recibe la ruta predeterminada, la LAN del R2 (2001:DB8:CAFE:2::/64) y el enlace entre el R2 y el R3 (2001:DB8:CAFE:A002::/64). Sin embargo, no recibe la ruta OSPFv3 LAN del R3 (2001:DB8:CAFE:3::/64).

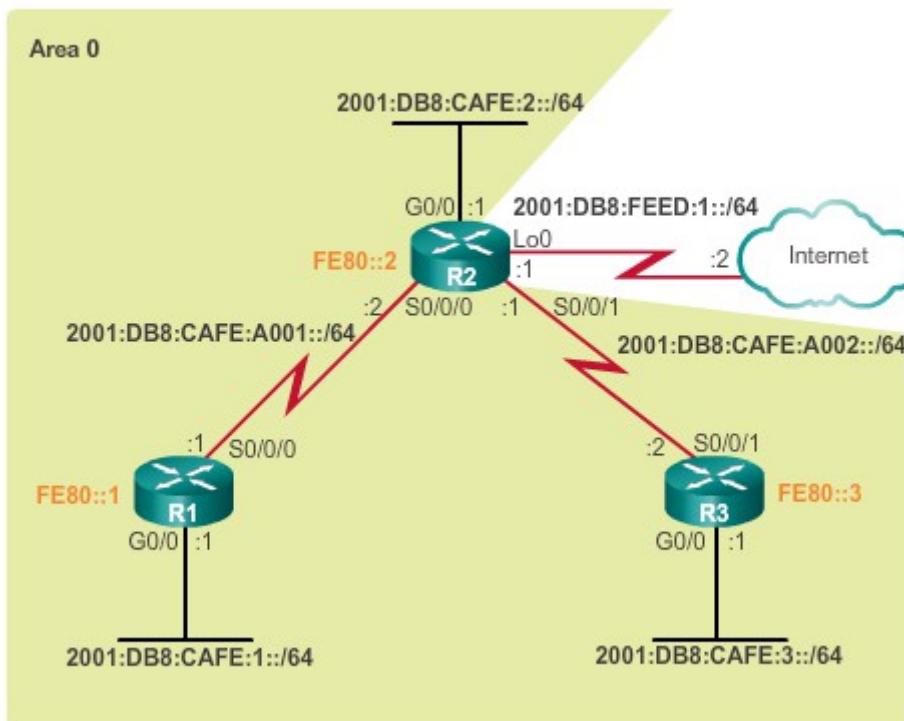
El resultado de la figura 3 verifica la configuración de OSPFv3 en el R3. Observe que OSPF solo está habilitado en la interfaz Serial 0/0/1. Al parecer, no está habilitado en la interfaz G0/0 del R3.

A diferencia de OSPFv2, en OSPFv3 no se usa el comando **network**. En cambio, OSPFv3 se habilita directamente en la interfaz. El resultado de la figura 4 confirma que la interfaz del R3 no está habilitada para OSPFv3.

En el ejemplo de la figura 5, se habilita OSPFv3 en la interfaz Gigabit Ethernet 0/0 del R3. Ahora el R3 debería anunciar la LAN del R3 a sus vecinos OSPFv3.

El resultado de la figura 6 verifica que la LAN del R3 ahora esté en la tabla de routing del R1.

**Topología OSPFv3**



### Verificación de rutas OSPFv3 en la tabla de routing del R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
      Static route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary,
            D - EIGRP
      EX - EIGRP external, ND - ND Default, NDp - ND
            Prefix, DCE - Destination
      NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1
            - OSPF ext 1
      OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
            NSSA ext 2
OE2 ::/0 [110/1], tag 10
  via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:2::/64 [110/648]
  via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:A002::/64 [110/1294]
  via FE80::2, Serial0/0/0
R1#
```

### Verificación de la configuración de OSPFv3 en el R3

```
R3# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 3.3.3.3
  Number of areas: 1 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/1
  Redistribution:
    None
R3#
```

### Verificación de la configuración del router OSPFv3 en el R3

```
R3# show running-config interface g0/0
Building configuration...

Current configuration : 196 bytes
!
interface GigabitEthernet0/0
description R3 LAN
no ip address
duplex auto
speed auto
ipv6 address FE80::3 link-local
ipv6 address 2001:DB8:CAFE:3::1/64
end

R3#
```

### Habilitación de OSPFv3 en la LAN del R3

```
R3# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)# interface g0/0
R3(config-if)# ipv6 ospf 10 area 0
R3(config-if)# end
R3#
```

### Verificación de rutas OSPFv3 en la tabla de routing del R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 9 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
    B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
    I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D
        - EIGRP
    EX - EIGRP external, ND - ND Default, NDp - ND Prefix,
        DCE - Destination
    NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 -
        OSPF ext 1
    OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF
        NSSA ext 2
OE2 ::/0 [110/1], tag 10
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:2::/64 [110/648]
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:3::/64 [110/1295]
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:A002::/64 [110/1294]
    via FE80::2, Serial0/0/0
R1#
```

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.3.3 Práctica de

laboratorio: Resolución de problemas de OSPFv2 y OSPFv3 básico de área única

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de conectividad de capa 3
- Parte 3: Resolver problemas de OSPFv2
- Parte 4: Resolver problemas de OSPFv3

[Práctica de laboratorio: Resolución de problemas de OSPFv2 y OSPFv3 básico de área única](#)

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.2.3.4 Práctica de

laboratorio: Resolución de problemas de OSPFv2 avanzado de área única

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de OSPF

[Práctica de laboratorio: Resolución de problemas de OSPFv2 avanzado de área única](#)

Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.3.1.1 Actividad de clase:

Dominio de la resolución de problemas de OSPF

### **Dominio de la resolución de problemas de OSPF**

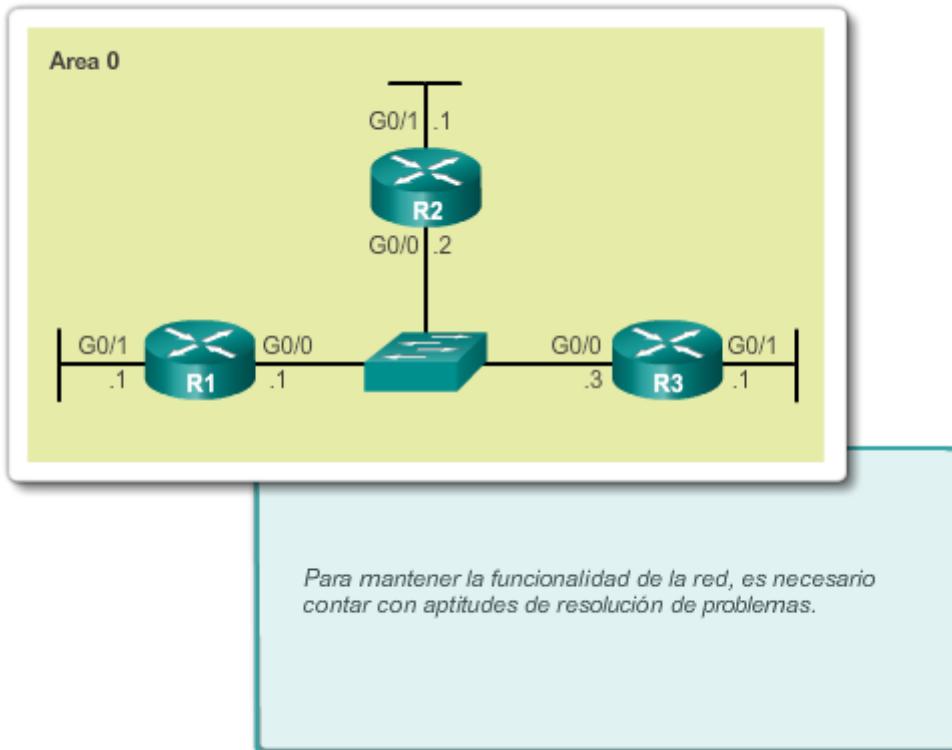
Decidió cambiar el protocolo de routing RIPv2 por OSPFv2. No se cambiará la configuración física original de la topología de la red de su pequeña a mediana empresa. Para esta actividad, use el diagrama del PDF como el diseño de red para pequeñas o medianas empresas de su compañía.

El diseño de direccionamiento está completo y, a continuación, usted configura los routers con IPv4 y VLSM. Se aplicó OSPF como protocolo de routing. Sin embargo, algunos routers comparten información de routing entre sí y otros no.

Abra el archivo PDF que acompaña esta actividad de creación de modelos y siga las instrucciones para completar la actividad.

Cuando se completen los pasos de las instrucciones, vuelva a agrupar la clase y compare los tiempos de reparación que se registraron en la actividad. El grupo que haya tardado menos en detectar y corregir el error de configuración será el ganador solo después de explicar correctamente cómo se detectó y se reparó el error, y de demostrar que la topología funciona.

[Actividad de clase: Dominio de la resolución de problemas de OSPF](#)



[Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.3.1.2 Packet Tracer:](#)

[desafío de integración de habilidades](#)

**Información básica/situación**

En este desafío de integración de habilidades, debe concentrarse en las configuraciones avanzadas de OSPFv2. Ya se configuró el direccionamiento IP para todos los dispositivos. Configurará el routing OSPFv2 con interfaces pasivas y la propagación de rutas predeterminadas. Modificará la configuración OSPFv2 mediante el ajuste de los temporizadores y el establecimiento de la autenticación MD5. Por último, verificará las configuraciones y probará la conectividad entre las terminales.

[Packet Tracer: Reto de habilidades de integración \(instrucciones\)](#)

[Packet Tracer: desafío de integración de habilidades \(PKA\)](#)

[Capítulo 5: Ajuste y resolución de problemas de OSPF de área única 5.3.1.3 Resumen](#)

OSPF define cinco tipos de red: punto a punto, multiacceso con difusión, multiacceso sin difusión, punto a multipunto y enlaces virtuales.

Las redes de accesos múltiples pueden suponer dos desafíos para OSPF en relación con la saturación con LSA: la creación de varias adyacencias y la saturación intensa con LSA. La solución para administrar la cantidad de adyacencias y la saturación con LSA en una red de accesos múltiples son el DR y el BDR. Si el DR deja de producir paquetes de saludo, el BDR se asciende a sí mismo y asume la función de DR.

Los routers en la red seleccionan como DR al router con la prioridad de interfaz más alta. El router con la segunda prioridad de interfaz más alta se elige como BDR. Cuanto mayor sea la prioridad, más probabilidades hay de que se elija al router como DR. Si se establece en 0, el router no puede convertirse en el DR. La prioridad predeterminada de las interfaces de difusión de accesos múltiples es 1. Por lo tanto, a menos que se configuren de otra manera, todos los routers tienen un mismo valor de prioridad y deben depender de otro método de diferenciación durante la elección del DR/BDR. Si las prioridades de interfaz son iguales, se elige al router con la ID más alta como DR. El router con la segunda ID de router más alta es el BDR. La incorporación de un nuevo router no inicia un nuevo proceso de elección.

Para propagar una ruta predeterminada en OSPF, el router debe estar configurado con una ruta estática predeterminada y se debe agregar el comando **default-information originate** a la configuración. Verifique las rutas mediante el comando **show ip route** o **show ipv6 route**.

Para ayudar a OSPF a determinar la ruta correcta, se debe cambiar el ancho de banda de referencia a un valor superior, a fin de admitir redes con enlaces más rápidos que 100 Mb/s. Para ajustar el ancho de banda de referencia, use el comando **auto-cost reference-bandwidthMbps** del modo de configuración del router. Para ajustar el ancho de banda de la interfaz, utilice el comando **bandwidthkilobits** del modo de configuración de interfaz. Es posible configurar el costo manualmente en una interfaz con el comando **ip ospf cost valor** del modo de configuración de interfaz.

Los Intervalos de saludo y muerto de OSPF deben coincidir, de lo contrario, no se crea una adyacencia de vecino. Para modificar estos intervalos, use los siguientes comandos de interfaz:

- **ip ospf hello-intervalsegundos**
- **ip ospf dead-intervalsegundos**
- **ipv6 ospf hello-intervalsegundos**
- **ipv6 ospf dead-intervalsegundos**

OSPF admite tres tipos de autenticación: nula, autenticación por contraseña simple y autenticación MD5. La autenticación MD5 de OSPF se puede configurar globalmente o por interfaz. Para verificar que la autenticación MD5 de OSPF esté habilitada, use el comando **show ip ospf interface** del modo EXEC privilegiado.

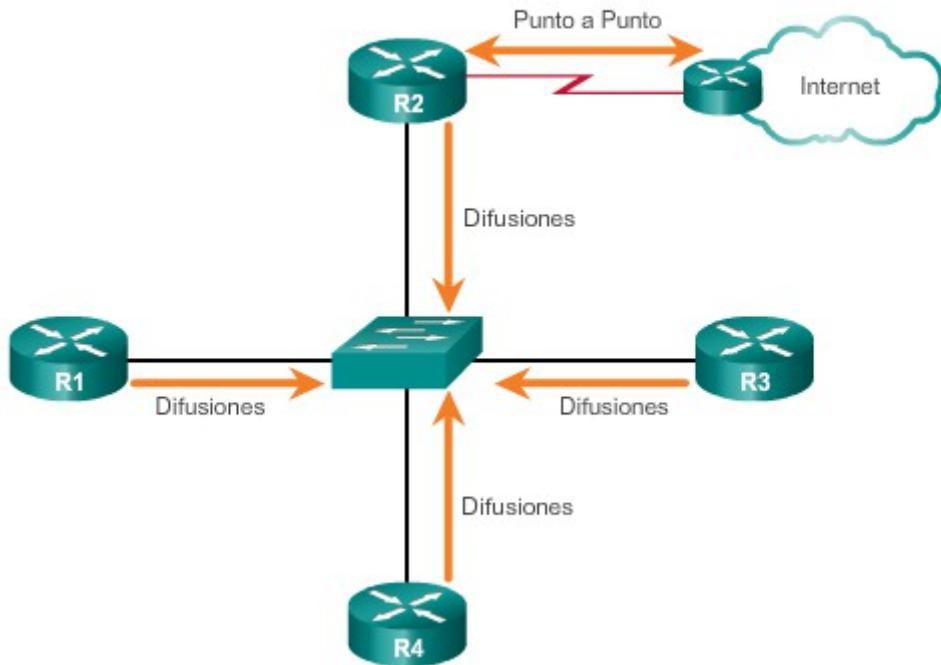
Cuando se realiza la resolución de problemas de vecinos OSPF, tenga en cuenta que los estados FULL o 2WAY son normales. Los siguientes comandos resumen la resolución de problemas de OSPF para IPv4:

- **show ip protocols**

- **show ip ospf neighbor**
- **show ip ospf interface**
- **show ip ospf**
- **show ip route ospf**
- **clear ip ospf [ id-proceso ]proceso**

La resolución de problemas de OSPFv3 es similar a la de OSPFv2. Los siguientes comandos son los comandos equivalentes que se usan con OSPFv3: **show ipv6 protocols**, **show ipv6 ospf neighbor**, **show ipv6 ospf interface**, **show ipv6 ospf**, **show ipv6 route ospf** y **clear ipv6 ospf[id-proceso] process**.

**Red OSPF de accesos múltiples**



#### Capítulo 6: OSPF multiárea 6.0.1.1 Introducción

OSPF multiárea se utiliza para dividir redes OSPF grandes. Si hubiera demasiados routers en un área, se incrementaría la carga en la CPU y se crearía una base de datos de estado de enlace muy grande. En este capítulo, se proporcionan instrucciones para dividir un área única grande en varias áreas eficazmente. El área 0 que se utiliza en OSPF de área única se conoce como “área de red troncal”.

El análisis se centra en las LSA que se intercambian entre áreas. Además, se proporcionan actividades para configurar OSPFv2 y OSPFv3. El capítulo concluye con los comandos **show** que se utilizan para verificar las configuraciones OSPF.

**Después de completar este capítulo, podrá hacer lo siguiente:**

- Explicar para qué se utiliza OSPF multiárea.
- Explicar la forma en que OSPF multiárea utiliza las notificaciones de estado de enlace para mantener las tablas de routing.
- Explicar la forma en que OSPF establece las adyacencias de vecinos en una implementación de OSPF multiárea.
- Configurar OSPFv2 multiárea en una red enrutada.
- Configurar la sumarización de rutas multiárea en una red enrutada.
- Verificar las operaciones de OSPFv2 multiárea.

#### Capítulo 6: OSPF multiárea 6.0.1.2 Actividad de clase: Como viajar en un avión de reacción

##### **Como viajar en un avión de reacción**

Usted y un compañero de clase inician una nueva línea aérea que brinda servicios en el continente.

Además del aeropuerto central de la empresa, ubican y asignan cuatro áreas de servicio de aeropuerto intracontinental y un área de servicio de aeropuerto transcontinental que se pueden utilizar como puntos de origen y destino adicionales.

Utilice el planisferio en blanco proporcionado para diseñar las ubicaciones de los aeropuertos. En el PDF correspondiente a esta actividad, podrá encontrar instrucciones adicionales para completar esta actividad.

#### [Actividad de clase: Como viajar en un avión de reacción](#)

#### Capítulo 6: OSPF multiárea 6.1.1.1 OSPF de área única

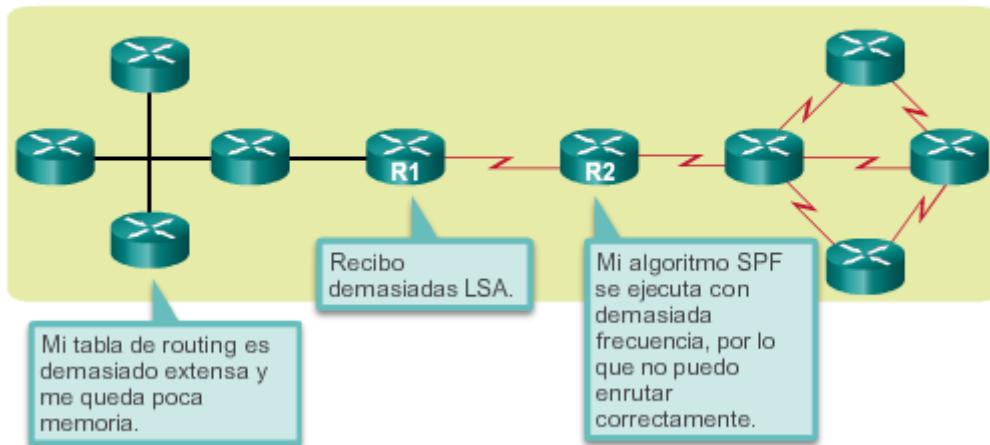
PF de área única es útil en redes más pequeñas, donde la red de enlaces entre routers es simple y las rutas a los destinos individuales se deducen con facilidad.

No obstante, si un área crece demasiado, se deben resolver los siguientes problemas de inmediato (consulte la ilustración para obtener un ejemplo):

- **Tablas de routing extensas:** OSPF no realiza la sumarización de rutas de manera predeterminada. Si las rutas no se resumen, la tabla de routing se vuelve muy extensa, según el tamaño de la red.
- **Bases de datos de estado de enlace (LSDB) muy grandes:** debido a que la LSDB abarca la topología de toda la red, cada router debe mantener una entrada para cada red en el área, incluso aunque no se seleccionen todas las rutas para la tabla de routing.
- **Cálculos frecuentes del algoritmo SPF:** en las redes grandes, las modificaciones son inevitables, por lo que los routers pasan muchos ciclos de CPU volviendo a calcular el algoritmo SPF y actualizando la tabla de routing.

Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área de OSPF es un grupo de routers que comparten la misma información de estado de enlace en las bases de datos de estado de enlace.

### Problemas en un área OSPF única muy grande



#### Capítulo 6: OSPF multiárea 6.1.1.2 OSPF multiárea

Cuando se divide un área OSPF grande en áreas más pequeñas, esto se denomina “OSPF multiárea”. OSPF multiárea es útil en implementaciones de red más grandes, ya que reduce la sobrecarga de procesamiento y de memoria.

Por ejemplo, cada vez que un router recibe información nueva acerca de la topología, como la adición, la eliminación o la modificación de un enlace, el router debe volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar la tabla de routing. El algoritmo SPF representa una gran exigencia para el CPU y el tiempo que le toma realizar los cálculos depende del tamaño del área. Si hubiera demasiados routers en un área, la LSDB sería más grande y se incrementaría la carga en la CPU. Por lo tanto, la disposición de los routers en distintas áreas divide de manera eficaz una base de datos potencialmente grande en bases de datos más pequeñas y más fáciles de administrar.

OSPF multiárea requiere un diseño de red jerárquico. El área principal se denomina “de red troncal” (área 0) y el resto de las áreas deben estar conectadas a esta. Con el routing jerárquico, se sigue produciendo el routing entre áreas (routing interárea), y muchas de las tediosas operaciones de routing, como volver a calcular la base de datos, se guardan en un área.

Como se ilustra en la figura 1, las posibilidades de topología jerárquica de OSPF multiárea presentan las siguientes ventajas:

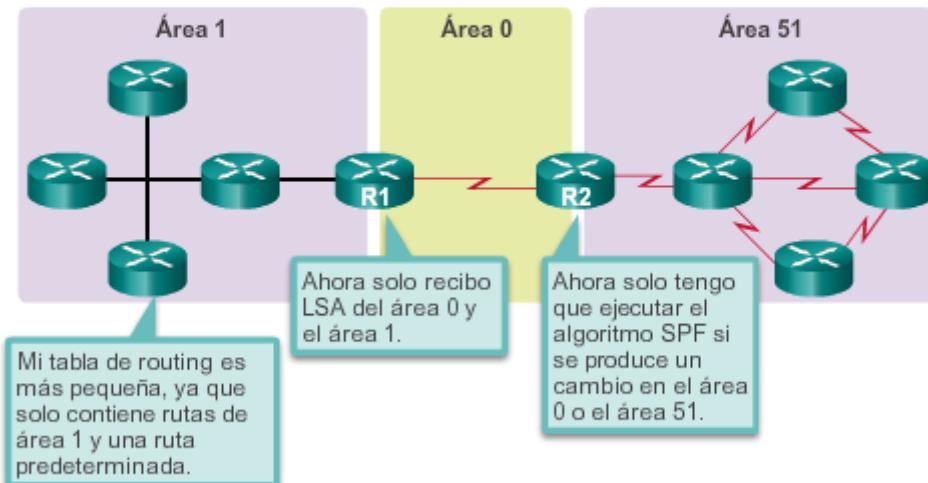
- **Tablas de routing más pequeñas:** hay menos entradas de la tabla de routing, ya que las direcciones de red pueden resumirse entre áreas. Por ejemplo, el R1 resume las rutas

del área 1 al área 0 y el R2 resume las rutas del área 51 al área 0. Además, el R1 y el R2 propagan una ruta estática predeterminada a las áreas 1 y 51.

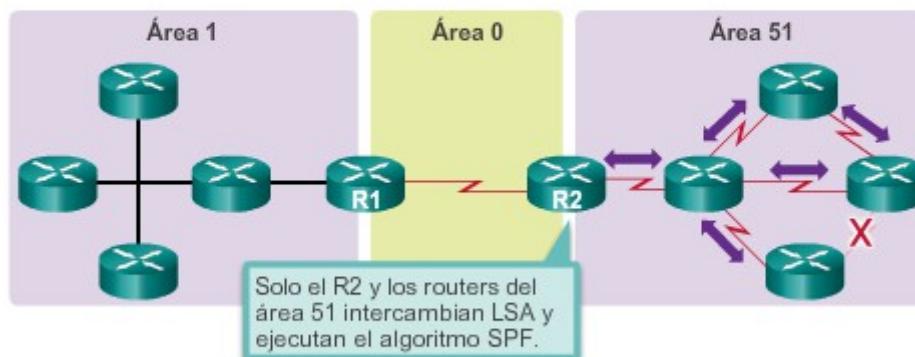
- **Menor sobrecarga de actualización de estado de enlace:** minimiza los requisitos de procesamiento y memoria, ya que hay menos routers que intercambian LSA.
- **Menor frecuencia de cálculos de SPF:** localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de una actualización de routing, porque la inundación de LSA se detiene en la frontera del área.

En la figura 2, suponga que un enlace entre dos routers internos en el área 51 falla. Solo los routers en el área 51 intercambian LSA y vuelven a ejecutar el algoritmo SPF para este evento. El R1 no recibe los LSA del área 51 y no vuelve a calcular el algoritmo SPF.

#### Ventajas de OSPF multiárea



#### Ventajas de OSPF multiárea



## Capítulo 6: OSPF multiárea 6.1.1.3 Jerarquía de área de OSPF de dos capas

El OSPF de diversas áreas se implementa con una jerarquía de área de dos capas:

- **Área de red troncal (de tránsito):** un área OSPF cuya función principal es la transmisión rápida y eficaz de los paquetes IP. Las áreas de red troncal se interconectan con otros tipos de área de OSPF. En general, los usuarios finales no se encuentran en un área de red troncal. El área de red troncal también se denomina “área OSPF 0”. En las redes jerárquicas, se define al área 0 como el núcleo al que se conectan directamente todas las demás áreas (figura 1).
- **Área común (no de red troncal):** conecta usuarios y recursos. Las áreas regulares se configuran generalmente en grupos funcionales o geográficos. De manera predeterminada, un área regular no permite que el tráfico de otra área utilice sus enlaces para alcanzar otras áreas. Todo el tráfico de otras áreas debe atravesar un área de tránsito (figura 2).

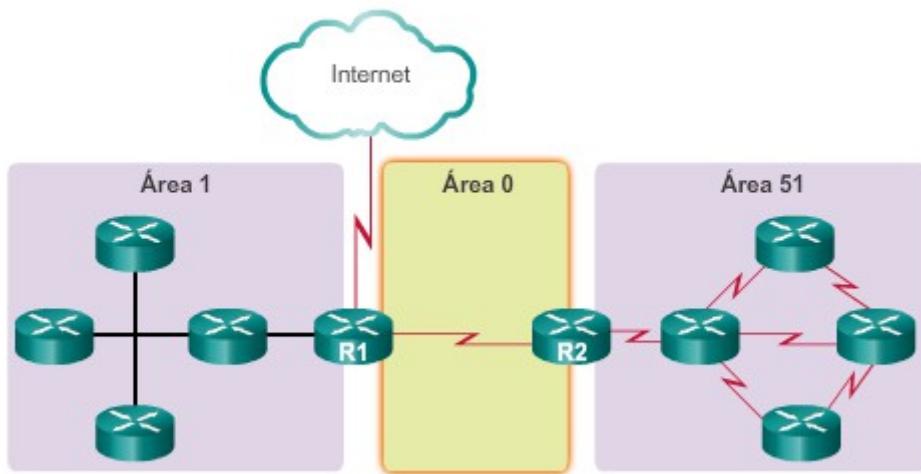
**Nota:** las áreas comunes pueden tener una variedad de subtipos, incluidas un área estándar, un área de rutas internas, un área exclusiva de rutas internas y un área no exclusiva de rutas internas (NSSA). Las áreas de rutas internas, las áreas exclusivas de rutas internas y las áreas NSSA exceden el ámbito de este capítulo.

OSPF aplica esta rígida jerarquía de área de dos capas. La conectividad física subyacente de la red se debe asignar a la estructura del área de dos capas, con solo áreas que no son de red troncal conectadas directamente al área 0. Todo el tráfico que se transfiere de un área a la otra debe atravesar el área de red troncal. Este tráfico se denomina “tráfico interárea”.

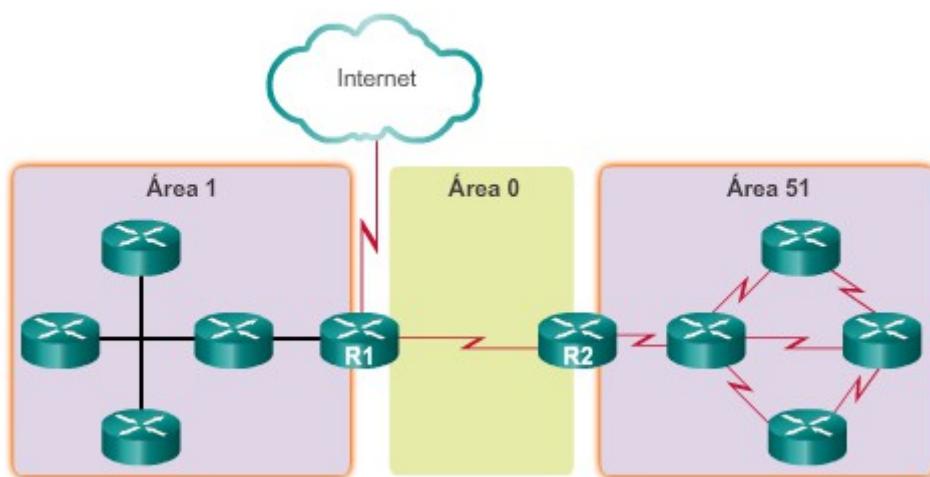
La cantidad óptima de routers por área depende de factores como la estabilidad de la red, pero Cisco recomienda tener en cuenta las siguientes pautas:

- Un área no debe tener más de 50 routers.
- Un router no debe estar en más de tres áreas.
- Ningún router debe tener más de 60 vecinos.

### Área backbone (de tránsito)



### Área común (no backbone)



#### Capítulo 6: OSPF multiárea 6.1.1.4 Tipos de routers de OSPF

Distintos tipos de routers OSPF controlan el tráfico que entra a las áreas y sale de estas. Los routers OSPF se categorizan según la función que cumplen en el dominio de routing.

Existen cuatro tipos diferentes de routers de OSPF:

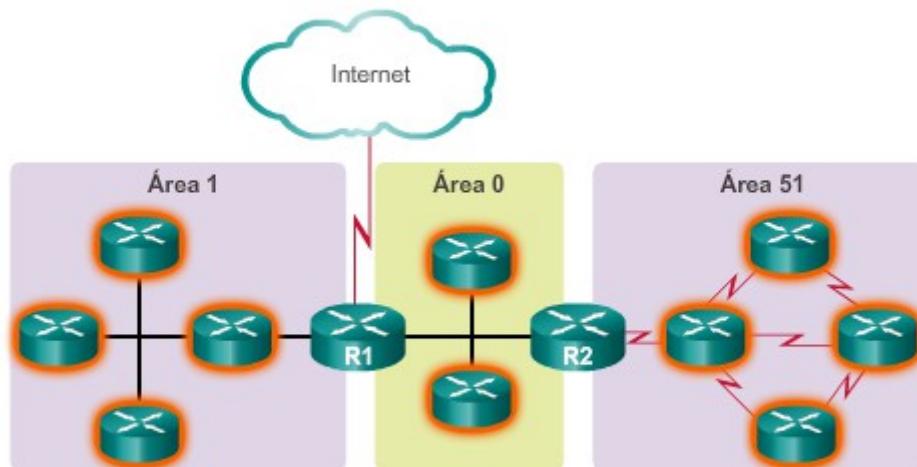
- **Router interno:** es un router cuyas interfaces están todas en la misma área. Todos los routers internos de un área tienen LSDB idénticas. (figura 1).

- **Router de respaldo:** es un router que se encuentra en el área de red troncal. Por lo general, el área de red troncal se configura como área 0. (figura 2).
- **Router de área perimetral. (ABR):** es un router cuyas interfaces se conectan a varias áreas. Debe mantener una LSDB para cada área a la que está conectado; puede hacer routing entre áreas. Los ABR son puntos de salida para cada área. Esto significa que la información de routing que se destina hacia otra área puede llegar únicamente mediante el ABR del área local. Es posible configurar los ABR para resumir la información de routing que proviene de las LSDB de las áreas conectadas. Los ABR distribuyen la información de routing en la red troncal. Luego, los routers de red troncal reenvían la información a otros ABR. En una red de diversas áreas, un área puede tener uno o más ABR. (figura 3).
- **Router límite del sistema autónomo (ASBR):** es un router que tiene al menos una interfaz conectada a una internetwork externa (otro sistema autónomo), por ejemplo, una red que no es OSPF. Un ASBR puede importar información de una red no OSPF hacia una red OSPF, y viceversa, mediante un proceso que se llama "redistribución de rutas". (figura 4).

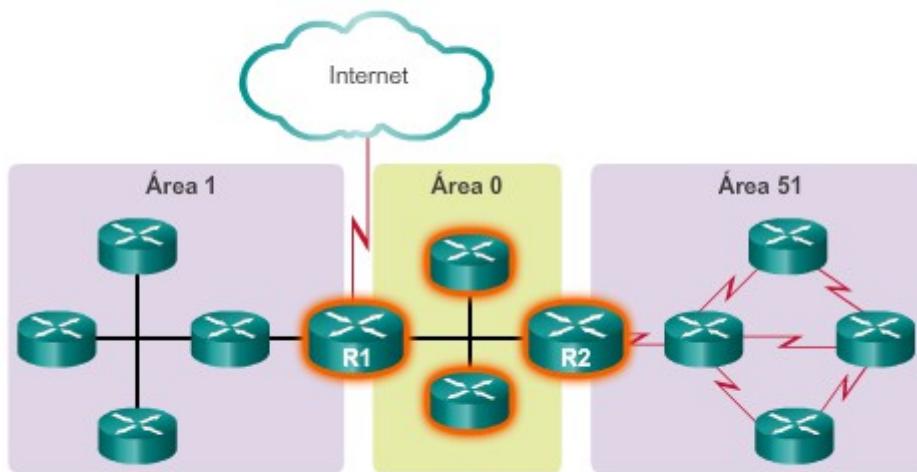
La redistribución en OSPF de diversas áreas ocurre cuando un ASBR conecta diferentes dominios de routing (por ejemplo, EIGRP y OSPF) y los configura para intercambiar y anunciar información de routing entre dichos dominios de routing.

Un router se puede clasificar como uno o más tipos de router. Por ejemplo, si un router se conecta a las áreas 0 y 1, y además mantiene información de routing de otra red que no es OSPF, se ubica en tres categorías diferentes: router de respaldo, ABR y ASBR.

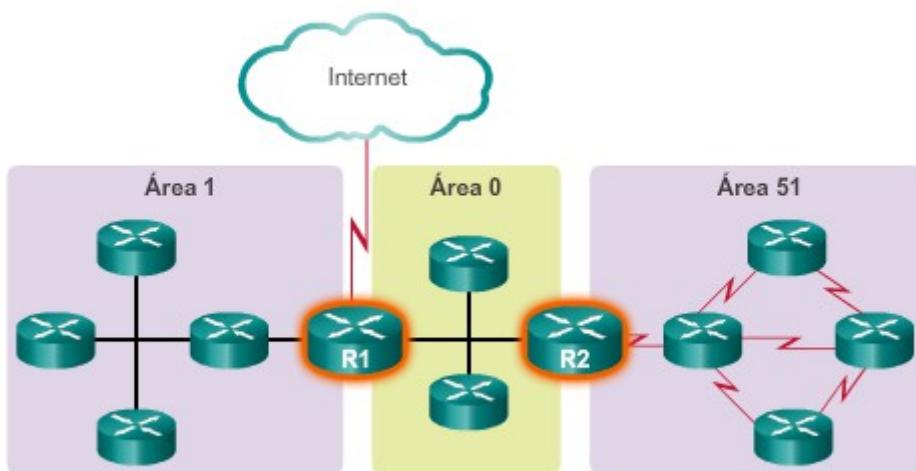
#### Routers internos



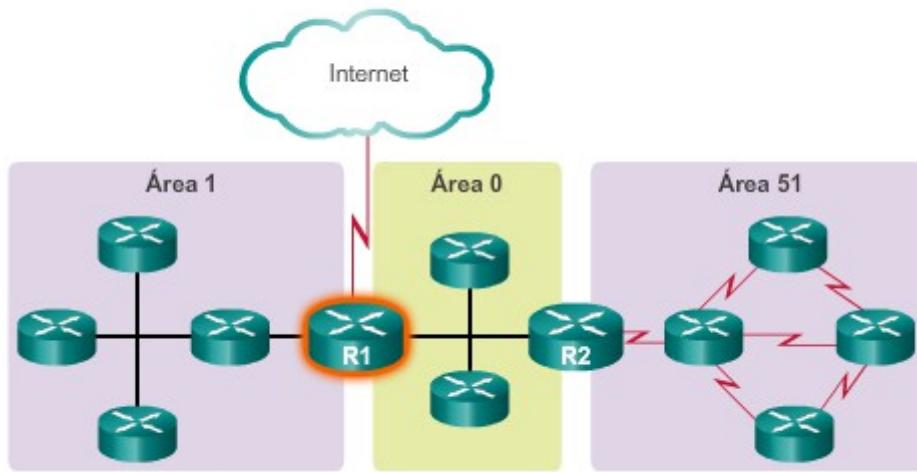
Routers de red troncal



Routers de área perimetral (ABR)



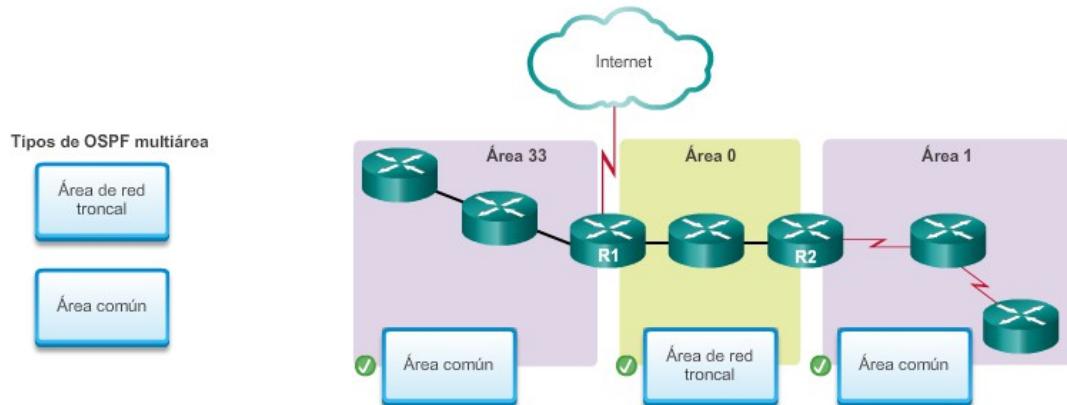
## Router de frontera de sistema autónomo (ASBR)



### Capítulo 6: OSPF multiárea 6.1.1.5 Actividad: Identificar la terminología de OSPF multiárea

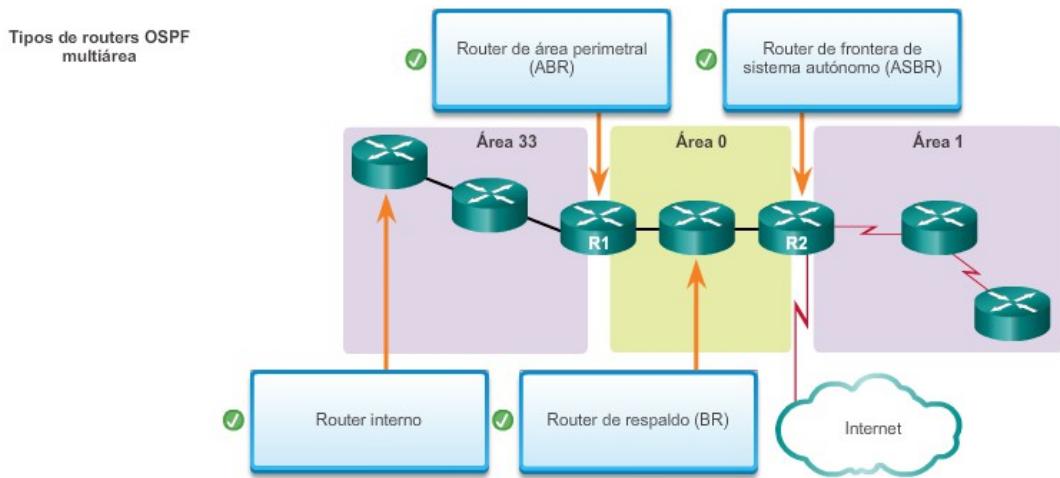
#### Actividad: Identificar la terminología de OSPF multiárea (parte 1)

Identifique las áreas OSPF multiárea y arrastre el nombre de los tipos de áreas a los campos proporcionados en la topología. Haga clic en la parte 2 para continuar la actividad.



**Actividad: Identificar la terminología de OSPF multiárea (parte 2)**

Identifique los tipos de routers OSPF multiárea y arrastre el nombre de los tipos de routers a los campos proporcionados en la topología.

**Capítulo 6: OSPF multiárea 6.1.2.1 Tipos de LSA de OSPF**

Las LSA son los bloques funcionales de la LSDB de OSPF. De manera individual, funcionan como registros de la base de datos y proporcionan detalles específicos de las redes OSPF. En conjunto, describen toda la topología de un área o una red OSPF.

Actualmente, las RFC para OSPF especifican hasta 11 tipos de LSA diferentes (figura 1). Sin embargo, cualquier implementación de OSPF multiárea debe admitir las primeras cinco LSA: de la LSA 1 a la LSA 5 (figura 2). Este tema se centra en estas cinco primeras LSA.

Todo enlace de router se define como un tipo de LSA. El LSA comprende un campo de Id. de enlace que identifica, por número y máscara de red, el objeto al cual se conecta el enlace. Según el tipo, el Id. de enlace tiene diferentes significados. Los LSA varían según cómo se generaron y propagaron dentro del dominio de routing.

**Nota:** OSPFv3 incluye tipos de LSA adicionales.

**Tipos de LSA de OSPF**

Tipo de LSA	Descripción
1	LSA del router
2	LSA de la red
3 y 4	LSA de resumen
5	LSA externo de AS
6	LSA de multidifusión OSPF
7	Definido para las NSSA
8	LSA de atributos externos para el protocolo de gateway fronterizo (BGP)
9, 10 u 11	LSA opacos

## Tipos de LSA de OSPF más comunes

Tipo de LSA	Descripción
1	LSA del router
2	LSA de la red
3 y 4	LSA de resumen
5	LSA externo de AS
6	LSA de multidifusión OSPF
7	Definido para las NSSA
8	LSA de atributos externos para el protocolo de gateway fronterizo (BGP)
9, 10 u 11	LSA opacos

### Capítulo 6: OSPF multiárea 6.1.2.2 LSA de OSPF de tipo 1

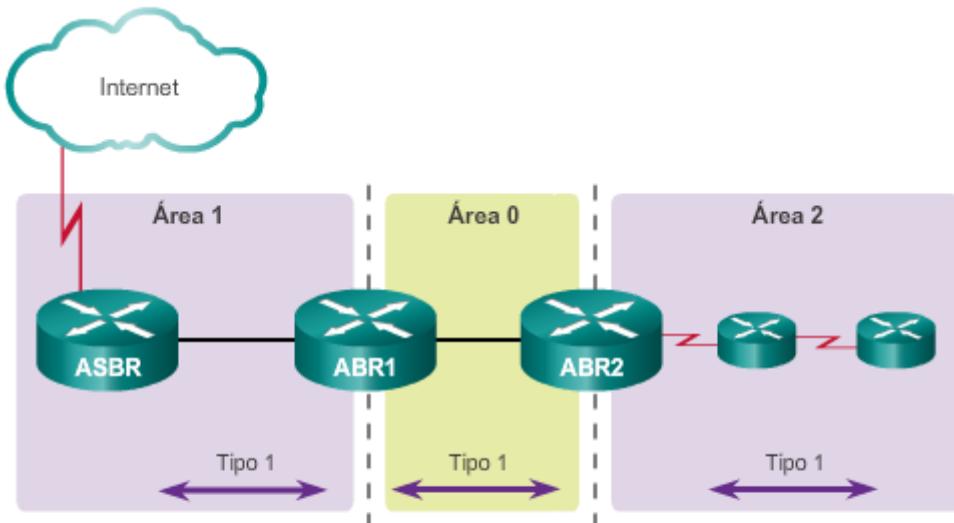
Como se muestra en la figura, todo router anuncia sus enlaces de OSPF con conexión directa mediante un LSA de tipo 1 y reenvía la información de su red a los vecinos OSPF. El LSA contiene una lista de interfaces con conexión directa, tipos de enlace y estados de enlace.

A los LSA de tipo 1 también se los denomina "entradas de enlace de router".

Los LSA de tipo 1 solo inundan el área que los origina. Los ABR, a la vez, anuncian a otras áreas las redes descubiertas a partir de las LSA de tipo 1 como LSA de tipo 3.

El Id. de router que origina el área identifica el Id. de enlace de un LSA de tipo 1.

### Propagación de mensaje de LSA de tipo 1



- Las LSA de tipo 1 incluyen una lista de prefijos de redes conectadas directamente y de los tipos de enlaces.
- Todo router genera LSA de tipo 1.
- El área se satura con LSA de tipo 1, y estas no se propagan más allá del ABR.
- La ID del router de origen identifica la ID de estado de enlace de una LSA de tipo 1.

### Capítulo 6: OSPF multiárea 6.1.2.3 LSA de OSPF de tipo 2

Un LSA de tipo 2 solo existe para redes de diversos accesos y redes sin diversos accesos ni difusión (NBMA) en donde se selecciona un DR y al menos dos routers en el segmento de diversos accesos. La LSA de tipo 2 contiene la ID del router y la dirección IP del DR, además de la ID del router de todos los demás routers en el segmento de accesos múltiples. Se crea una LSA de tipo 2 para cada red de accesos múltiples en el área.

El propósito de una LSA de tipo 2 es proporcionar a otros routers información sobre las redes de accesos múltiples dentro de la misma área.

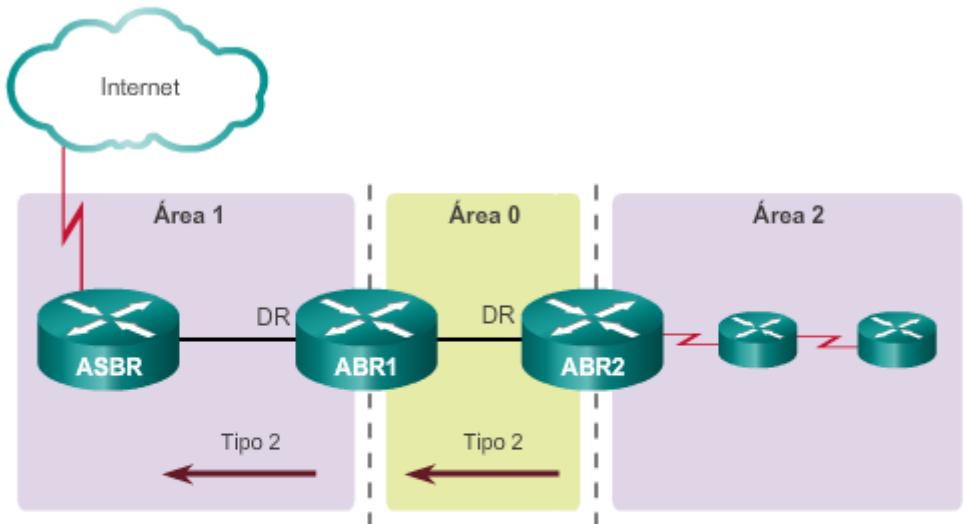
El DR inunda los LSA de tipo 2 solo en el área en que se originan. Los LSA de tipo 2 no se reenvían fuera del área.

A las LSA de tipo 2 también se las denomina “entradas de enlace de red”.

Como se muestra en la figura, ABR1 es el DR de la red de Ethernet del área 1. Genera LSA de tipo 2 y los reenvía al área 1. ABR2 es el DR de la red de diversos accesos del área 0. No existen redes de diversos accesos en el área 2; por lo tanto, nunca se propagarán LSA de tipo 2 en dicha área.

La ID de estado de enlace para una LSA de red es la dirección IP de la interfaz del DR que la anuncia.

### Propagación de mensaje de LSA de tipo 2



- Las LSA de tipo 2 identifican los routers y las direcciones de red de los enlaces de accesos múltiples.
- Solo el DR genera LSA de tipo 2.
- La red de accesos múltiples se satura con LSA de tipo 2, y estas no van más allá del ABR.
- La ID del router DR identifica la ID de estado de enlace de una LSA de tipo 2.

### Capítulo 6: OSPF multiárea 6.1.2.4 LSA de OSPF de tipo 3

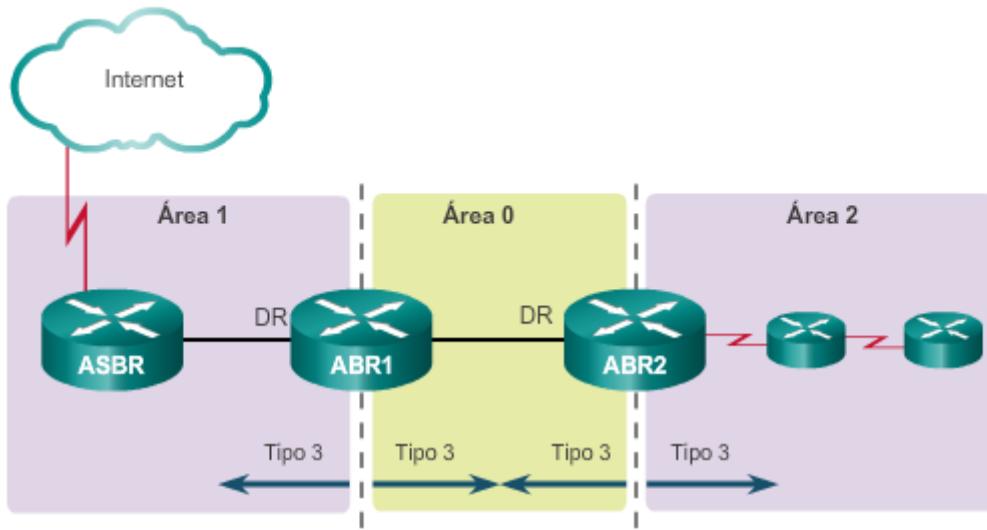
Los ABR utilizan los LSA de tipo 3 para anunciar redes de otras áreas. Los ABR recopilan LSA de tipo 1 en la LSDB. Después de que converge un área de OSPF, el ABR crea un LSA de tipo 3 para cada red de OSPF reconocida. Por lo tanto, un ABR con varias rutas OSPF debe crear un LSA de tipo 3 para cada red.

Como se muestra en la figura, ABR1 y ABR2 propagan LSA de tipo 3 de un área a otras. Los ABR propagan LSA de tipo 3 hacia otras áreas. Durante una implementación importante de OSPF con muchas redes, la propagación de LSA de tipo 3 puede causar problemas de inundación significativos. Por esta razón, se recomienda con énfasis que se configure manualmente el resumen de ruta en el ABR.

La ID de estado de enlace se establece en el número de red, y también se anuncia la máscara.

La recepción de LSA de tipo 3 en su área no incita al router a ejecutar el algoritmo de SPF. Los routers que se anuncian en las LSA de tipo 3 se agregan a la tabla de routing del router o se eliminan de esta según corresponda, pero no se necesita el cálculo completo de SPF.

### Propagación de mensajes de LSA de tipo 3



- Las LSA de tipo 3 describen direcciones de red descubiertas por las LSA de tipo 1.
- Se requieren LSA de tipo 3 para todas las subredes.
- Los ABR saturan otras áreas con LSA de tipo 3, y otros ABR las vuelven a generar.
- La dirección de red identifica la ID de estado de enlace de una LSA de tipo 3.
- De manera predeterminada, las rutas no se resumen.

#### Capítulo 6: OSPF multiárea 6.1.2.5 LSA de OSPF de tipo 4

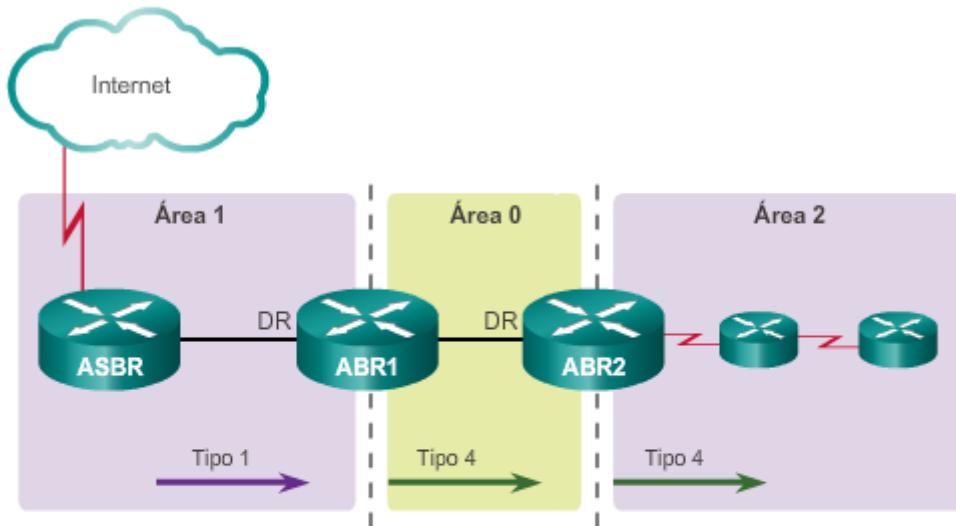
Los LSA de tipo 4 y tipo 5 se utilizan en conjunto para identificar un ASBR y anunciar redes externas que llegan a un dominio de routing de OSPF.

El ABR genera un LSA de resumen de tipo 4 solo cuando existe un ASBR en el área. Un LSA de tipo 4 identifica el ASBR y le asigna una ruta. Todo tráfico destinado a un sistema autónomo externo requiere conocimiento de la tabla de routing del ASBR que originó las rutas externas.

Como se muestra en la ilustración, el ASBR envía una LSA de tipo 1 para identificarse como ASBR. El LSA incluye un bit especial llamado "bit externo" (e bit) que se utiliza para identificar el router como un ASBR. Cuando el ABR1 recibe el LSA de tipo 1, reconoce el e bit, genera un LSA de tipo 4 y lo propaga a la red troncal (área 0). Los ABR posteriores propagan el LSA de tipo 4 hacia otras áreas.

La ID de estado de enlace se establece en la ID del router ASBR.

### Propagación de mensajes de LSA de tipo 4



- Las LSA de tipo 4 se utilizan para anunciar un ASBR a otras áreas y proporcionar una ruta al ASBR.
- Los ABR generan LSA de tipo 4.
- El ABR de origen genera la LSA de tipo 4, y otros ABR la vuelven a generar.
- La ID del router ASBR identifica la ID de estado de enlace de una LSA de tipo 4.

### Capítulo 6: OSPF multiárea 6.1.2.6 LSA de OSPF de tipo 5

Los LSA externos de tipo 5 anuncian rutas a redes que se encuentran afuera del sistema autónomo de OSPF. Los LSA de tipo 5 se originan en el ASBR y se propagan hacia todo el sistema autónomo.

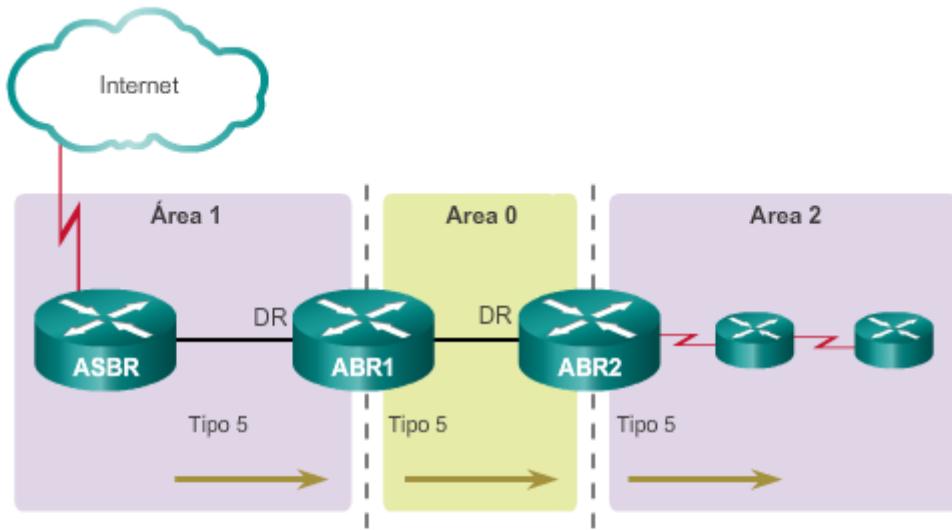
Los LSA de tipo 5 también se conocen como entradas de LSA externas del sistema autónomo.

En la figura, el ASBR genera LSA de tipo 5 para cada ruta externa y los propaga hacia el área. Los ABR posteriores también propagan el LSA de tipo 5 hacia otras áreas. Los routers de otras áreas utilizan la información del LSA de tipo 4 para llegar a las rutas externas.

Durante una implementación grande de OSPF con muchas redes, la propagación de LSA de tipo 5 puede causar problemas de inundación significativos. Por esta razón, se recomienda con énfasis que se configure manualmente el resumen de ruta en el ASBR.

La ID de estado de enlace es el número de red externa.

### Propagación de mensajes de LSA de tipo 5

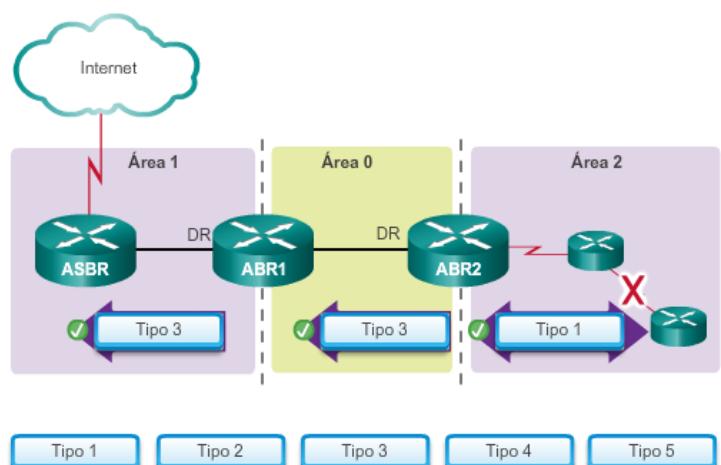


- Las LSA de tipo 5 se utilizan para anunciar direcciones de red externas (es decir, que no son OSPF).
- Un ASBR genera LSA de tipo 5.
- Toda el área se satura con LSA de tipo 5, y otros ABR las vuelven a generar.
- La ID de estado de enlace de una LSA de tipo 5 es la dirección de red externa.
- De manera predeterminada, las rutas no se resumen.

### Capítulo 6: OSPF multiárea 6.1.2.7 Actividad: Identificar el tipo de LSA de OSPF

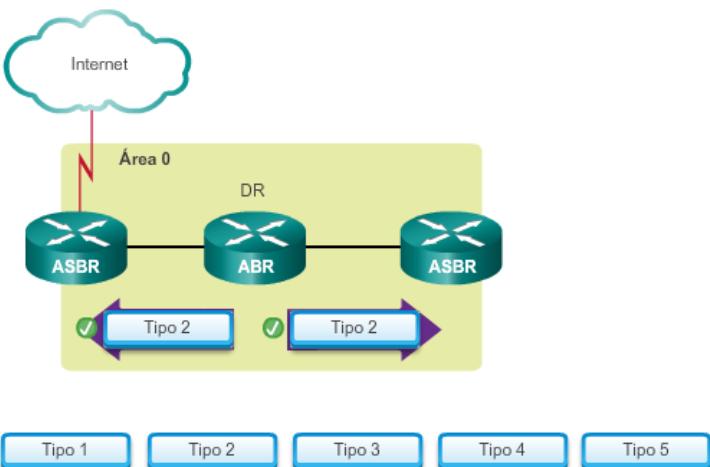
#### Actividad: Identificar el tipo de LSA de OSPF, situación 1

Un router en el área 2 tuvo un cambio de estado de enlace e inició una actualización OSPF dirigida por el evento. Cada router ABR envía una actualización de LSA. Arrastre las etiquetas para los tipos de LSA hasta las flechas proporcionadas en la topología de la red. Haga clic en el botón 2 para continuar la actividad.



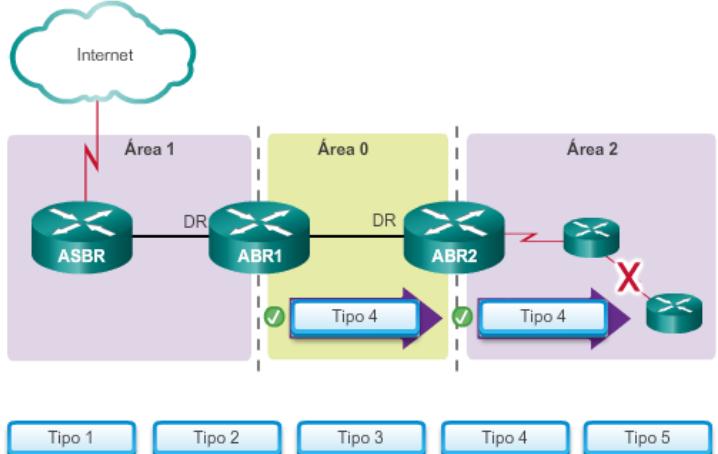
**Actividad: Identificar el tipo de LSA de OSPF, situación 2**

El router DR en el área 0 envía una LSA con una lista de todos los routers OSPF en esta área. Arrastre las etiquetas para los tipos de LSA hasta las flechas proporcionadas en la topología de la red. Haga clic en el botón 3 para continuar la actividad.



**Actividad: Identificar el tipo de LSA de OSPF, situación 3**

Cada router ABR envía una actualización de LSA después de descubrir que existe un router ASBR en el área 1. Arrastre las etiquetas correctas para los tipos de LSA hasta las flechas proporcionadas en la topología de la red.



### Capítulo 6: OSPF multiárea 6.1.3.1 Entradas de la tabla de routing de OSPF

En la figura 1, se proporciona una tabla de routing de ejemplo para una topología OSPF multiárea con un enlace a una red externa que no es OSPF. Las rutas OSPF en una tabla de routing IPv4 se identifican mediante los siguientes descriptores:

- **O:** las LSA de router (tipo 1) y de red (tipo 2) describen los detalles dentro de un área. La tabla de routing refleja esta información de estado de enlace con la designación **O**, lo que significa que la ruta es intraárea.
- **IA O:** cuando un ABR recibe LSA de resumen, las agrega a su LSDB y vuelve a generarlas en el área local. Cuando un ABR recibe un LSA externo, lo agrega a su LSDB y lo propaga en el área. Luego, los routers internos asimilan la información en su base de datos. Los LSA de resumen aparecen en la tabla de routing como IA (rutas interárea).
- **O E1 u O E2:** en la tabla de routing, las LSA externas aparecen marcadas como rutas externas tipo 1 (E1) o externas tipo 2 (E2).

En la figura 2, se muestra una tabla de routing IPv6 con entradas de tabla de routing interárea, externas y de router OSPF.

## Entradas de la tabla de routing de red y router

```
R1# show ip route
Codes:L - local, 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, H-NHRP, l-LISP
      + - replicated route, % - next hop override

Gateway of last resort is 192.168.10.2 to network 0.0.0.0

O*E2 0.0.0.0/0 [110/1] via 192.168.10.2, 00:00:19, Serial0/0/0
  10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
C    10.1.1.0/24 is directly connected, GigabitEthernet0/0
L    10.1.1.1/32 is directly connected, GigabitEthernet0/0
C    10.1.2.0/24 is directly connected, GigabitEthernet0/1
L    10.1.2.1/32 is directly connected, GigabitEthernet0/1
O    10.2.1.0/24 [110/648] via 192.168.10.2, 00:04:34, Serial0/0/0
O  IA 192.168.1.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
O  IA 192.168.2.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
  192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C    192.168.10.0/30 is directly connected, Serial0/0/0
L    192.168.10.1/32 is directly connected, Serial0/0/0
O    192.168.10.4/30 [110/1294] via 192.168.10.2, 00:01:55,Serial0/0/0
R1#
```

## Entradas de tabla de routing OSPFv3

```
R1# show ipv6 route
IPv6 Routing Table - default - 9 entries
Codes:C - Connected, L - Local, S - Static, U-Per-user Static route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
      EX - EIGRP external, ND-ND Default,NDp-ND Prefix,DCE-Destination
      NDr - Redirect, O-OSPF Intra, OI-OSPF Inter, OE1-OSPF ext 1
      OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

OE2 ::/0 [110/1], tag 10
  via FE80::2, Serial0/0/0
C  2001:DB8:CAFE:1::/64 [0/0]
  via GigabitEthernet0/0, directly connected
L  2001:DB8:CAFE:1::1/128 [0/0]
  via GigabitEthernet0/0, receive
O  2001:DB8:CAFE:2::/64 [110/648]
  via FE80::2, Serial0/0/0
OI 2001:DB8:CAFE:3::/64 [110/1295]
  via FE80::2, Serial0/0/0
C  2001:DB8:CAFE:A001::/64 [0/0]
  via Serial0/0/0, directly connected
L  2001:DB8:CAFE:A001::1/128 [0/0]
  via Serial0/0/0, receive
O  2001:DB8:CAFE:A002::/64 [110/1294]
  via FE80::2, Serial0/0/0
L  FF00::/8 [0/0]
  via Null0, receive
R1#
```

## Capítulo 6: OSPF multiárea 6.1.3.2 Cálculo de router de OSPF

Cada router utiliza el algoritmo SPF en virtud de la LSDB para crear un árbol SPF. El árbol de SPF se utiliza para determinar las mejores rutas.

Como se muestra en la figura, el orden en el que se calculan las mejores rutas es el siguiente:

1. Todo router calcula las mejores rutas a destinos de su área (intraárea) y agrega estas entradas a la tabla de routing. Se trata de LSA de tipo 1 y tipo 2, que se indican en la tabla de routing con el designador "O". (1)
2. Todo router calcula las mejores rutas hacia otras áreas en la internetwork. Las mejores rutas son las entradas de rutas interárea, o LSA de tipo 3 y tipo 4, y se indican con el designador de routing "O IA". (2)
3. Todo router (excepto los que se ubican en una forma de rutas internas) calcula las mejores rutas hacia destinos del sistema autónomo externo (tipo 5). Estas se indican con el designador de ruta O E1 u O E2, según la configuración. (3)

Cuando converge, un router se comunica con cualquier red dentro o fuera del sistema autónomo OSPF.

### Pasos para la convergencia de OSPF

```
R1# show ip route | begin Gateway
Gateway of last resort is 192.168.10.2 to network 0.0.0.0
O*E2 0.0.0.0/0 [110/1] via 192.168.10.2, 00:00:19, Serial0/0/0
    10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
    C      10.1.1.0/24 is directly connected, GigabitEthernet0/0
    L      10.1.1.1/32 is directly connected, GigabitEthernet0/0
    C      10.1.2.0/24 is directly connected, GigabitEthernet0/1
    L      10.1.2.1/32 is directly connected, GigabitEthernet0/1
    O      10.2.1.0/24 [110/648] via 192.168.10.2, 00:04:34,Serial0/0/0
    O  IA  192.168.1.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
    O  IA  192.168.2.0/24 [110/1295] via 192.168.10.2, 00:01:48,Serial0/0/0
        192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
        C      192.168.10.0/30 is directly connected, Serial0/0/0
        L      192.168.10.1/32 is directly connected, Serial0/0/0
    O      192.168.10.4/30 [110/1294] via 192.168.10.2, 00:01:55,Serial0/0/0
R1#
```

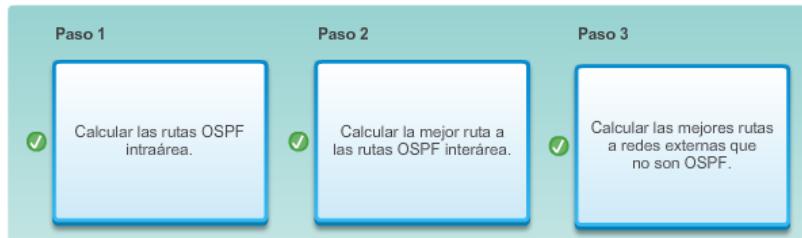
- 3
  - 1
  - 2
  - 1
- Calcular las rutas OSPF intraárea.
  - Calcular la mejor ruta a las rutas OSPF interárea.
  - Calcular las mejores rutas a redes externas que no son OSPF.

## Capítulo 6: OSPF multiárea 6.1.3.3 Actividad: Ordenar los pasos para calcular la mejor ruta en OSPF

### OSPF

#### **Actividad: Calcular las mejores rutas en OSPF**

Los routers OSPF utilizan los criterios que se indican a continuación para seleccionar la mejor ruta para instalar en la tabla de routing. Ordene dichos criterios y arrastre cada instrucción al campo numerado correspondiente.



## Capítulo 6: OSPF multiárea 6.2.1.1 Implementación de OSPF multiárea

La implementación de OSPF puede ser de área única o multiárea. El tipo de implementación de OSPF que se elige depende de los requisitos específicos y de la topología existente.

Para implementar OSPF multiárea, se deben seguir cuatro pasos, los cuales se muestran en la ilustración.

Los pasos 1 y 2 forman parte del proceso de planificación.

**Paso 1. Recopile los parámetros y los requisitos de la red:** esto incluye determinar la cantidad de dispositivos host y de red, el esquema de direccionamiento IP (si ya se implementó), el tamaño del dominio y de las tablas de routing, el riesgo de los cambios en la topología y otras características de la red.

**Paso 2. Defina los parámetros de OSPF:** sobre la base de la información que recopiló en el paso 1, el administrador de red debe determinar si la implementación preferida es OSPF de área única o multiárea. Si se selecciona OSPF multiárea, el administrador de red debe tener en cuenta varias consideraciones al determinar los parámetros de OSPF, incluido lo siguiente:

- **Plan de direccionamiento IP:** este rige la manera en que se puede implementar OSPF y qué tan bien se podría escalar la implementación de OSPF. Se debe crear un plan de direccionamiento IP detallado, así como la información de división en subredes IP. Un buen plan de direccionamiento IP debe habilitar el uso de la sumarización y del diseño de OSPF multiárea. Este plan escala la red con mayor facilidad y optimiza el comportamiento de OSPF y la propagación de LSA.
- **Áreas OSPF:** la división de una red OSPF en áreas disminuye el tamaño de la LSDB y limita la propagación de las actualizaciones de estado de enlace cuando se modifica la topología. Se deben identificar los routers que van a cumplir la función de ABR y ASBR, así como los que van a realizar la sumarización o la redistribución.
- **Topología de la red:** esta consta de enlaces que conectan los equipos de red y que pertenecen a áreas OSPF diferentes en un diseño de OSPF multiárea. La topología de la red es importante para determinar los enlaces principales y de respaldo. Los enlaces principales y de respaldo se definen mediante la modificación del costo de OSPF en las

interfaces. También se debe usar un plan detallado de la topología de la red para determinar las distintas áreas OSPF, el ABR y el ASBR, además de los puntos de summarización y redistribución, si se utiliza OSPF multiárea.

**Paso 3.** Configure la implementación de OSPF multiárea según los parámetros.

**Paso 4.** Verifique la implementación de OSPF multiárea según los parámetros.

#### Pasos del plan de implementación

1. Recopilar los requisitos y los parámetros de la red.
2. Definir los parámetros de OSPF.
3. Configurar OSPF.
4. Verifique el protocolo OSPF.

#### Capítulo 6: OSPF multiárea 6.2.1.2 Configuración de OSPF de diversas áreas

En la figura 1, se muestra la topología OSPF multiárea de referencia. En este ejemplo:

- El R1 es un ABR porque tiene interfaces en el área 1 y una interfaz en el área 0.
- R2 es un router de respaldo interno porque todas sus interfaces están en el área 0.
- R3 es un ABR porque tiene interfaces en el área 2 y una interfaz en el área 0.

No se requieren comandos especiales para implementar esta red de OSPF de diversas áreas. Un router simplemente se convierte en ABR cuando tiene dos instrucciones **network** en diferentes áreas.

Como se muestra en la figura 2, se asignó la ID de router 1.1.1.1 al R1. Este ejemplo activa OSPF en las dos interfaces LAN del área 1. La interfaz serial se configura como parte de OSPF de área 0. Dado que el R2 tiene interfaces conectadas a dos áreas diferentes, es un ABR.

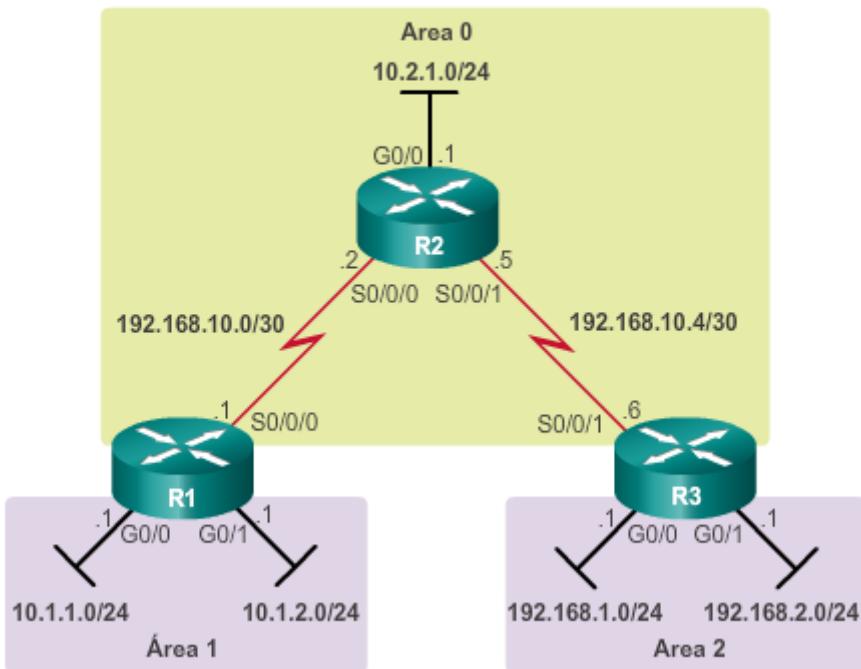
Utilice el verificador de sintaxis de la figura 3 para configurar OSPF multiárea en el R2 y el R3. En este verificador de sintaxis, en el R2, use la máscara wildcard de la dirección de red de la interfaz. En el R3, use la máscara wildcard 0.0.0.0 para todas las redes.

Al finalizar la configuración del R2 y el R3, observe los mensajes informativos acerca de las adyacencias con el R1 (1.1.1.1).

Al finalizar la configuración del R3, observe los mensajes informativos acerca de una adyacencia con el R1 (1.1.1.1) y el R2 (2.2.2.2). Asimismo, observe cómo el esquema de direccionamiento IP utilizado para la ID del router facilita la identificación del vecino.

**Nota:** las máscaras wildcard inversas utilizadas para configurar el R2 y el R3 difieren a propósito, con el fin de mostrar las dos alternativas para introducir las instrucciones **network**. El método utilizado para el R3 es más simple, ya que la máscara wildcard siempre es **0.0.0.0** y no es necesario calcularla.

## Topología OSPFv2 multiárea



### Configuración de OSPF multiárea en el R1

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.1.1 0.0.0.0 area 1
R1(config-router)# network 10.1.2.1 0.0.0.0 area 1
R1(config-router)# network 192.168.10.1 0.0.0.0 area 0
R1(config-router)# end
R1#
```

## Configuración de OSPF multiárea en el R2 y el R3

Ingrese al modo de configuración del router OSPF en el R2 con la ID de proceso 10 y configure lo siguiente en orden:

- Configure la ID de router 2.2.2.2.
- Anuncie la red 192.168.10.0/30 para el área 0.
- Anuncie la red 192.168.10.4/30 para el área 0.
- Anuncie la red 10.2.1.0/24 para el área 0.
- Vuelva al modo EXEC privilegiado.

```
R2(config)# router ospf 10
R2(config-router)# router-id 2.2.2.2
R2(config-router)# network 192.168.10.0 0.0.0.3 area 0
R2(config-router)# network 192.168.10.4 0.0.0.3 area 0
R2(config-router)# network 10.2.1.0 0.0.0.255 area 0
R2(config-router)# end
R2#
*Apr 19 18:11:04.029: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on
Serial0/0/0 from LOADING to FULL, Loading Done
R2#
*Apr 19 18:11:06.781: %SYS-5-CONFIG_I: Configured from console by
Consola
R2#
```

Ahora configure el R3. Ingrese al modo de configuración del router OSPF en el R3 con la ID de proceso 10 y configure lo siguiente en orden:

- Configure la ID de router 3.3.3.3.
- Anuncie la interfaz 192.168.10.6 para el área 0.
- Anuncie la interfaz 192.168.1.1 para el área 2.
- Anuncie la interfaz 192.168.2.1 para el área 2.
- Vuelva al modo EXEC privilegiado.

```
R3(config)# router ospf 10
R3(config-router)# router-id 3.3.3.3
R3(config-router)# network 192.168.10.6 0.0.0.0 area 0
R3(config-router)# network 192.168.1.1 0.0.0.0 area 2
R3(config-router)# network 192.168.2.1 0.0.0.0 area 2
R3(config-router)# end
*Apr 19 18:12:55.881: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3#
```

Configuró correctamente OSPF multiárea en los routers R2 y R3.

### Capítulo 6: OSPF multiárea 6.2.1.3 Configuración de OSPFv3 de diversas áreas

Al igual que en OSPFv2, la implementación de la topología OSPFv3 multiárea de la figura 1 es sencilla. No se requieren comandos especiales. Un router se convierte en ABR cuando tiene dos interfaces en dos áreas diferentes.

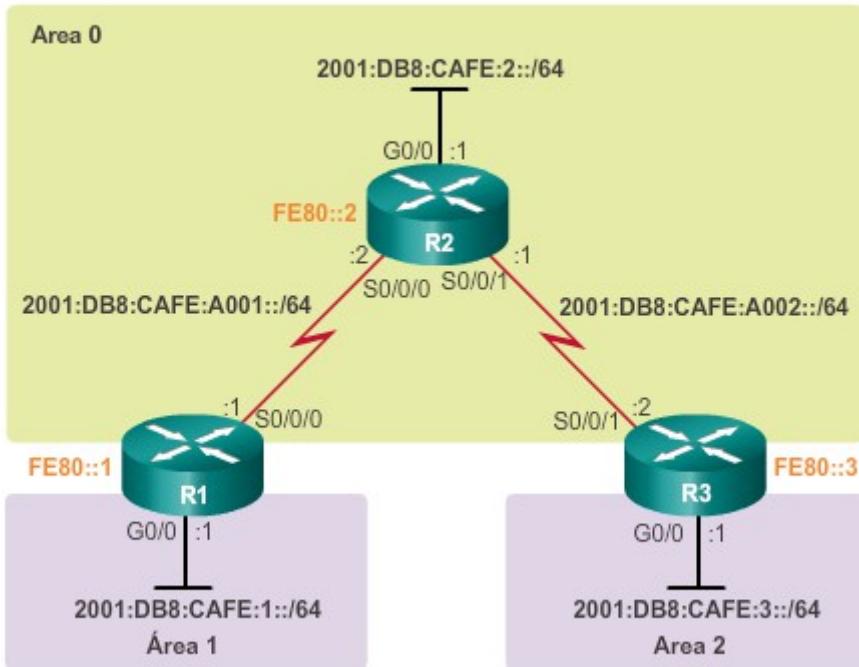
Por ejemplo, en la figura 2, se asignó la ID de router 1.1.1.1 al R1. El ejemplo también habilita OSPF en las dos interfaces LAN en el área 1 y en la interfaz serial en el área 0. Dado que R1 tiene interfaces conectadas a dos áreas diferentes, es un ABR.

Utilice el verificador de sintaxis de la figura 3 para configurar OSPFv3 multiárea en el R2 y en el R3.

Al finalizar la configuración del R2, observe el mensaje que indica que hay una adyacencia con el R1 (1.1.1.1).

Al finalizar la configuración del R3, observe el mensaje que indica que hay una adyacencia con el R2 (2.2.2.2).

### Topología OSPFv3 multiárea



### Configuración de OSPFv3 multiárea en el R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# exit
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 1
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

## Configuración de OSPFv3 multiárea en el R2 y el R3

Ingrese al modo de configuración del router OSPFv3 en el R2 con la ID de proceso 10.

- Configure la ID de router 2.2.2.2.
- Vuelva al modo de configuración global.

```
R2(config)# ipv6 router ospf 10
*Apr 24 14:18:10.463: %OSPFV3-4-NORTRID: Process OSPFv3-10-IPv6
could not pick a router-id, please configure manually
R2(config-rtr)# router-id 2.2.2.2
R2(config-rtr)# exit
```

Configure OSPFv3 para la ID de proceso 10 en cada una de las interfaces en el siguiente orden:

- Interfaz g0/0 para el área 0
- Interfaz s0/0/0 para el área 0
- Interfaz S0/0/1 para el área 0
- Vuelva al modo EXEC privilegiado.

```
R2(config)# interfaz g0/0
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)# interfaz s0/0/0
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)# interfaz s0/0/1
R2(config-if)# ipv6 ospf 10 area 0
R2(config-if)# end
*Apr 24 14:18:35.135: %OSPFV3-5-ADJCHG: Process 10, Nbr 1.1.1.1
on
Serial0/0/0 from LOADING to FULL, Loading Done
R2#
```

Ahora configure el R3. Ingrese al modo de configuración del router OSPFv3 en el R3 con la ID de proceso 10.

- Configure la ID de router 3.3.3.3.
- Vuelva al modo de configuración global.

```
R3(config)# ipv6 router ospf 10
*Apr 24 14:20:42.463: %OSPFV3-4-NORTRID: Process OSPFv3-10-IPv6
could not pick a router-id, please configure manually
R3(config-rtr)# router-id 3.3.3.3
R3(config-rtr)# exit
```

Configure OSPFv3 para la ID de proceso 10 en cada una de las interfaces en el siguiente orden:

- Interfaz g0/0 para el área 2
- Interfaz S0/0/1 para el área 0
- Vuelva al modo EXEC privilegiado.

```
R3(config)# interfaz g0/0
R3(config-if)# ipv6 ospf 10 area 2
R3(config-if)# interfaz s0/0/1
R3(config-if)# ipv6 ospf 10 area 0
R3(config-if)# end
*Apr 24 14:21:01.439: %OSPFV3-5-ADJCHG: Process 10, Nbr 2.2.2.2
on
Serial0/0/1 from LOADING to FULL, Loading Done
R3#
```

Configuró correctamente OSPFv3 multiárea en los routers R2 y R3.

El resumen colabora para que las tablas de routing sean más breves. Implica consolidar varias rutas en un único anuncio, que luego se propaga hacia el área de red troncal.

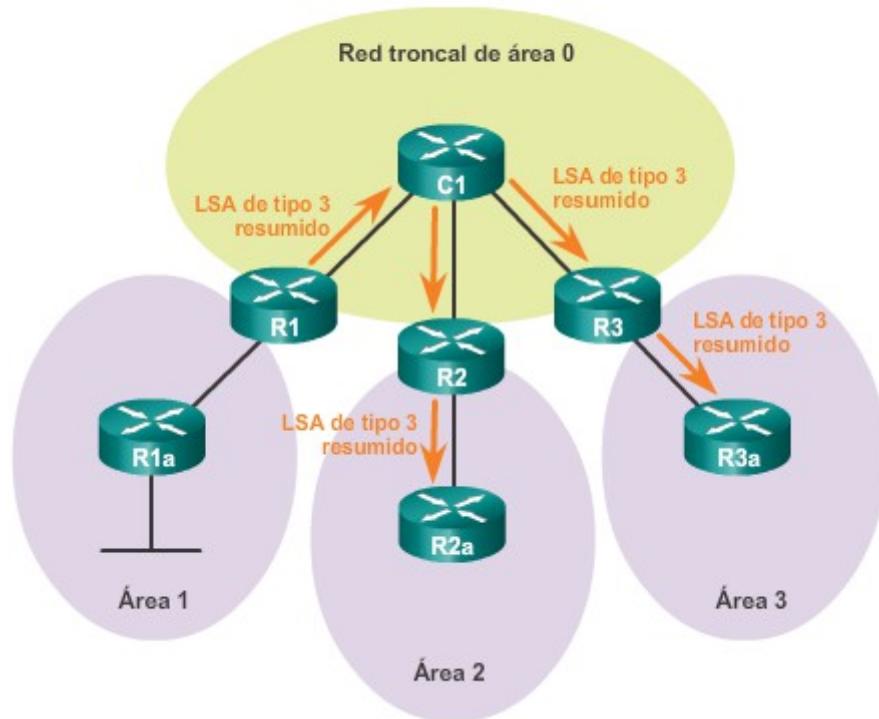
Por lo general, los LSA de tipo 1 y tipo 2 se generan dentro de cada área, se traducen a LSA de tipo 3 y se envían a otras áreas. Si el área 1 tuviera treinta redes para anunciar, se reenviarían treinta LSA de tipo 3 hacia la red troncal. Con la sumarización de ruta, el ABR consolida las 30 redes en uno de dos anuncios.

En la figura 1, el R1 consolida todos los anuncios de red en una LSA de resumen. En lugar de reenviar LSA de manera individual para cada ruta del área 1, R1 reenvía un LSA de resumen al core router C1. C1, a su vez, reenvía el LSA de resumen hacia R2 y R3. R2 y R3 luego lo reenvían a sus respectivos routers internos.

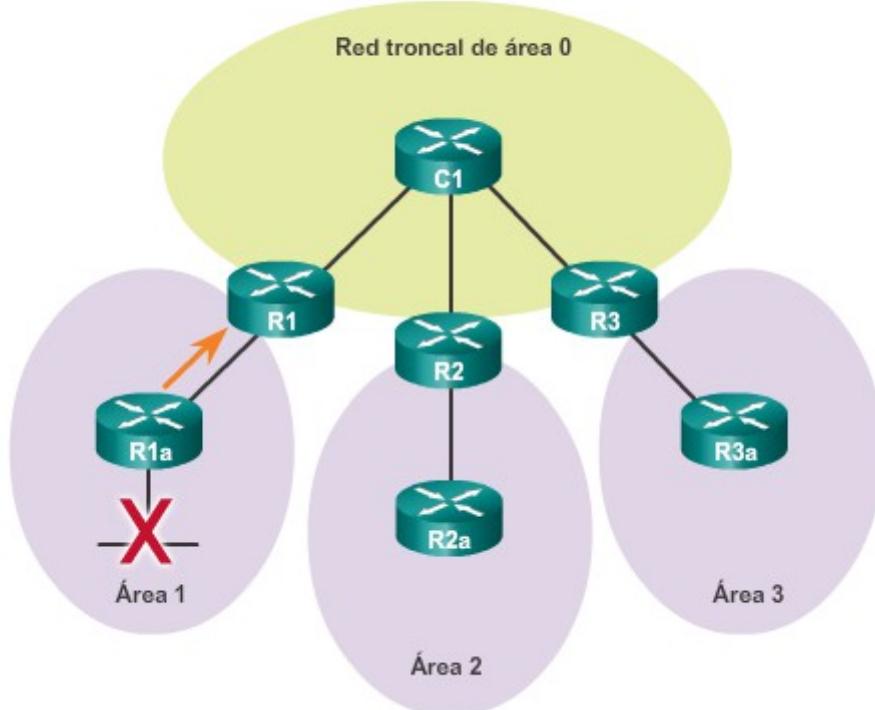
El resumen también contribuye a aumentar la estabilidad de la red, porque reduce la inundación innecesaria de LSA. Esta situación afecta directamente la cantidad de recursos de memoria, CPU y ancho de banda utilizados por el proceso de routing de OSPF. Sin un resumen de rutas, todo LSA de enlace específico se propaga en la red troncal OSPF y más allá, lo que genera tráfico de red y recarga del router innecesarios.

En la figura 2, un enlace de red en el R1 falla. El R1a envía una LSA al R1. Sin embargo, el R1 no propaga la actualización, ya que tiene configurada una ruta resumida. No se produce la saturación de enlaces específicos fuera del área con LSA.

#### Propagación de rutas resumidas



## Supresión de actualizaciones con la sumarización



### Capítulo 6: OSPF multiárea 6.2.2.2 Sumarización de rutas externas e interárea

En OSPF, la sumarización se puede configurar solo en los ABR o los ASBR. En lugar de anunciar muchas redes específicas, los routers ABR y ASBR anuncian una ruta resumida. Los routers ABR resumen LSA de tipo 3 y los routers ASBR resumen LSA de tipo 5.

De manera predeterminada, las LSA de resumen (LSA de tipo 3) y las LSA externas (tipo 5) no contienen rutas resumidas (agregadas); es decir que, de manera predeterminada, las LSA de resumen no se resumen.

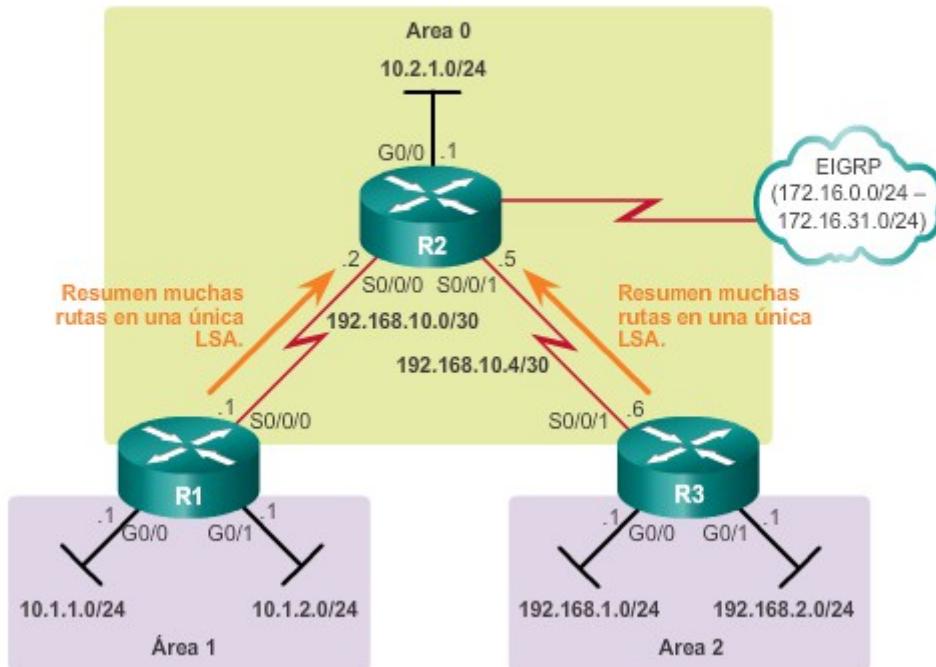
Como se muestra en las figuras 1 y 2, la sumarización de ruta se puede configurar de la siguiente manera:

- **Sumarización de rutas interárea:** la sumarización de rutas interárea se produce en los ABR y se aplica a las rutas dentro de cada área. No se aplica a las rutas externas introducidas en OSPF mediante la redistribución. Para realizar una sumarización de rutas interárea eficaz, las direcciones de red se deben asignar de manera contigua, para que dichas direcciones se puedan resumir en una cantidad mínima de direcciones de resumen.
- **Sumarización de rutas externas:** la sumarización de rutas externas es específica de las rutas externas que se introducen en OSPF mediante la redistribución de rutas. Una vez más, es importante asegurar la contigüidad de los rangos de direcciones externas que se resumen. Por lo general, solo los ASBR resumen rutas externas. Como se muestra en

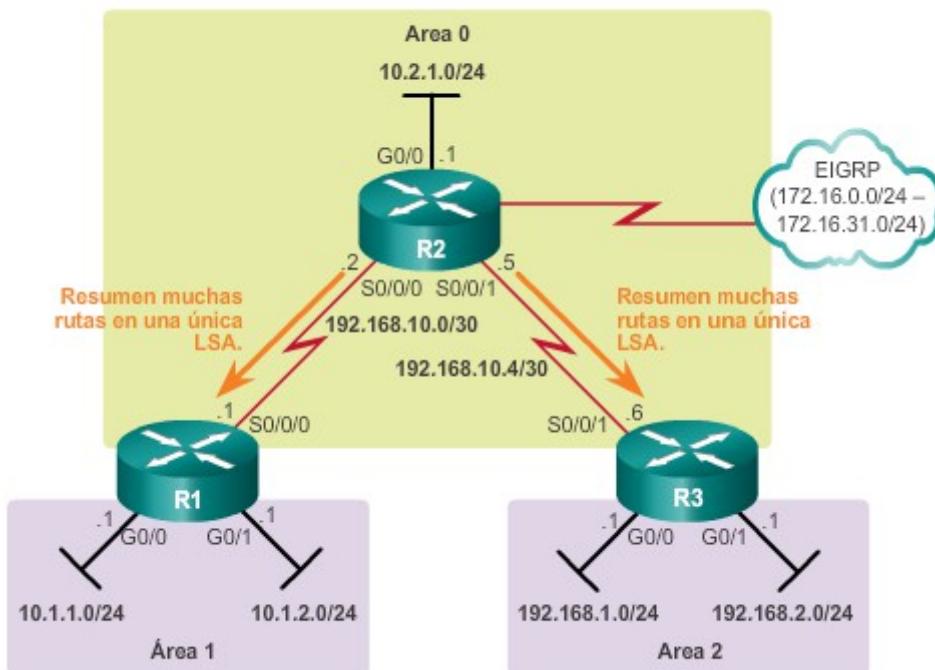
En la figura 2, el ASBR R2 resume las rutas externas EIGRP en una única LSA y las envía al R1 y al R3.

**Nota:** en los ASBR, la sumarización de rutas externas se configura mediante el comando **summary-address address mask** del modo de configuración del router.

### Sumarización de rutas interárea en los ABR



### Sumarización de rutas externas en un ASBR



## Capítulo 6: OSPF multiárea 6.2.2.3 Sumarización de rutas interárea

OSPF no realiza la sumarización automática. La sumarización interárea se debe configurar manualmente en los ABR.

Solo los ABR pueden realizar la sumarización de rutas internas. Cuando se habilita la sumarización en un ABR, se introduce en el backbone una única LSA de tipo 3 que describe la ruta resumida. Esta única LSA resume varias rutas dentro del área.

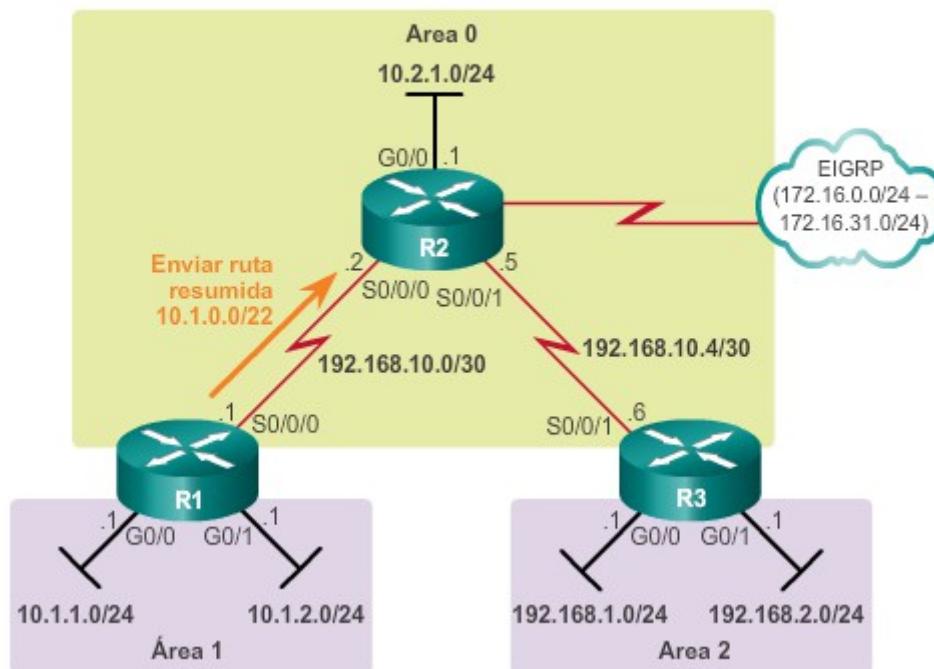
Una ruta resumida se genera si por lo menos una subred dentro del área se encuentra dentro del rango de direcciones de resumen. La métrica de ruta resumida equivale al costo más bajo de todas las subredes dentro del rango de direcciones de resumen.

**Nota:** los ABR solo pueden resumir rutas que se encuentran dentro de las áreas conectadas a ellos.

En la figura 1, se muestra una topología OSPF multiárea. Las tablas de routing del R1 y el R3 se analizan para ver el efecto de la sumarización.

En la figura 2, se muestra la tabla de routing del R1 antes de que se configure la sumarización, mientras que en la figura 3, se muestra la tabla de routing del R3. Observe que, actualmente, el R3 tiene dos entradas de rutas interárea a las redes del área 1 del R1.

### Sumarización de rutas interárea en los ABR



### Verificación de la tabla de routing del R1 antes de la summarización

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
O       10.2.1.0/24 [110/648] via 192.168.10.2, 00:00:49,
          Serial0/0/0
O IA   192.168.1.0/24 [110/1295] via 192.168.10.2, 00:00:49,
          Serial0/0/0
O IA   192.168.2.0/24 [110/1295] via 192.168.10.2, 00:00:49,
          Serial0/0/0
          192.168.10.0/24 is variably subnetted, 3 subnets, 2
          masks
O       192.168.10.4/30 [110/1294] via 192.168.10.2,
          00:00:49, Serial0/0/0
R1#
```

### Verificación de la tabla de routing del R3 antes de la summarización

```
R3# show ip route ospf | begin Gateway
Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 3 subnets
O IA   10.1.1.0 [110/1295] via 192.168.10.5, 00:27:14, Serial0/0/1
O IA   10.1.2.0 [110/1295] via 192.168.10.5, 00:27:14, Serial0/0/1
O       10.2.1.0 [110/648] via 192.168.10.5, 00:27:57, Serial0/0/1
          192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O       192.168.10.0/30 [110/1294] via 192.168.10.5, 00:27:57,
          Serial0/0/1
R3#
```

### Capítulo 6: OSPF multiárea 6.2.2.4 Cálculo de la ruta sumarizada

La figura muestra que el resumen de redes en una única dirección y máscara se puede realizar en tres pasos:

**Paso 1.** Enumerar las redes en formato binario. En el ejemplo, las dos redes del área 1 (10.1.1.0/24 y 10.1.2.0/24) se indican en formato binario.

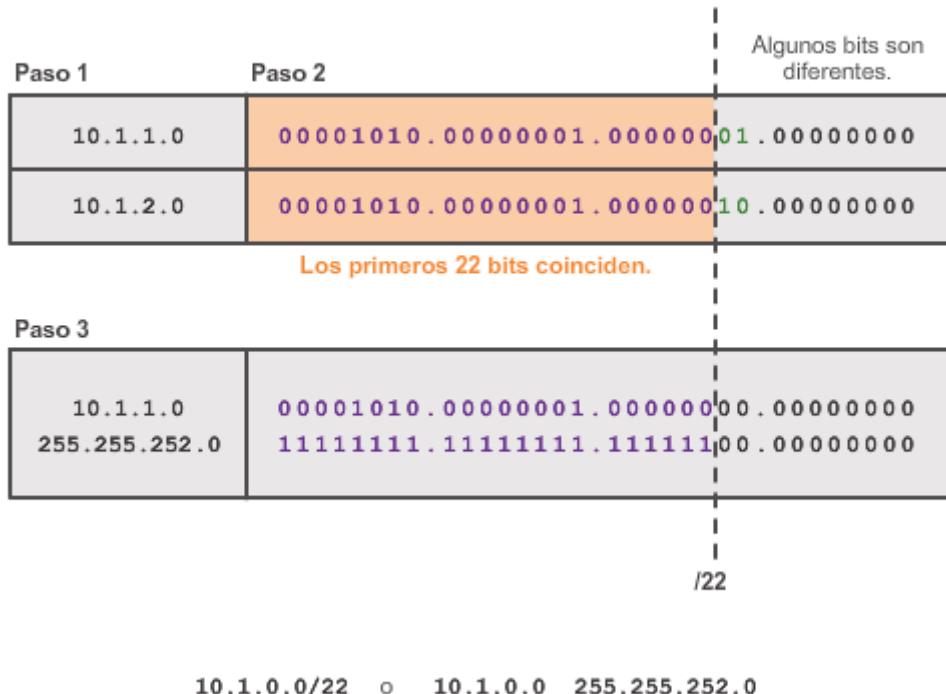
**Paso 2.** Contar el número de bits que coinciden en el extremo izquierdo para determinar la máscara de ruta sumarizada. Según lo resaltado, los primeros 22 dígitos del extremo izquierdo coinciden. Esto produce el prefijo /22 o la máscara de subred **255.255.252.0**.

**Paso 3.** Copie los bits coincidentes y luego agregue los cero bits para determinar la dirección de red resumida. En este ejemplo, los bits coincidentes con ceros al final nos muestran como

resultado la dirección de red 10.1.0.0/22. Esta dirección de resumen reúne cuatro redes: 10.1.0.0/24, 10.1.1.0/24, 10.1.2.0/24 y 10.1.3.0/24.

En el ejemplo, la dirección de resumen coincide con cuatro redes aunque solo existen dos redes.

### Cálculo de la ruta sumarizada



#### Capítulo 6: OSPF multiárea 6.2.2.5 Configuración de resumen de rutas interárea

En la figura 1, para demostrar el efecto de la sumarización de ruta, el R1 está configurado para resumir las rutas internas del área 1.

Para configurar manualmente la sumarización de rutas interárea en un ABR, utilice el comando **area *id*-área *range* dirección *máscara*** del modo de configuración de router. Esto le ordena al ABR que resuma las rutas para un área específica antes de introducirlas en otra área en forma de LSA de tipo 3 de resumen a través del backbone.

**Nota:** en OSPFv3, el comando es idéntico, excepto por la dirección de red IPv6. La sintaxis del comando para OSPFv3 es **area *id*-área *range* prefijo/*longitud-prefijo***.

En la figura 2, se resumen las dos rutas internas del área 1 en una ruta resumida interárea OSPF en el R1. La ruta resumida 10.1.0.0/22 resume cuatro direcciones de red: de la 10.1.0.0/24 a la 10.1.3.0/24.

En la figura 3, se muestra la tabla de routing IPv4 del R1. Observe que apareció una nueva entrada con una interfaz de salida Null0. Cuando se configura la sumarización manual para evitar los bucles de routing, el IOS de Cisco crea de manera automática una ruta resumida falsa a la interfaz Null0. Todo paquete enviado a una interfaz nula se descarta.

Por ejemplo, supongan que R1 recibió un paquete destinado a 10.1.0.10. Aunque coincidiría con la ruta sumarizada de R1, R1 no posee una ruta válida en el área 1. Por lo tanto, el R1 consultaría la tabla de routing para buscar la siguiente coincidencia más extensa, que sería la entrada de Null0. El paquete se reenviaría a la interfaz Null0 y se descartaría. Este proceso evita que el router reenvíe el paquete a una ruta predeterminada y posiblemente cree un bucle.

En la figura 4, se muestra la tabla de routing actualizada del R3. Noten cómo ahora solo existe una entrada de interárea que se dirige a la ruta sumarizada 10.1.0.0/22. Si bien este ejemplo solo redujo la tabla de routing en una entrada, la sumarización se puede implementar para resumir muchas redes. Esto reduciría el tamaño de las tablas de routing.

Utilice el verificador de sintaxis de la figura 5 para resumir las rutas del área 2 en el R3.

### Cálculo de la ruta sumarizada

Paso 1	Paso 2				
10.1.1.0	00001010.00000001.000000001.00000000	Algunos bits son diferentes.			
10.1.2.0	00001010.00000001.0000000010.00000000				
Los primeros 22 bits coinciden.					
<b>Paso 3</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="padding: 5px; vertical-align: top;">           10.1.1.0            255.255.252.0         </td><td style="padding: 5px; vertical-align: top;">           00001010.00000001.0000000000.00000000            11111111.11111111.11111100.00000000         </td><td style="padding: 5px; vertical-align: top; text-align: right;">/22</td></tr> </table>			10.1.1.0 255.255.252.0	00001010.00000001.0000000000.00000000 11111111.11111111.11111100.00000000	/22
10.1.1.0 255.255.252.0	00001010.00000001.0000000000.00000000 11111111.11111111.11111100.00000000	/22			

10.1.0.0/22    o    10.1.0.0 255.255.252.0

### Sumarización de rutas del área 1 en el R1

```
R1(config)# router ospf 10
R1(config-router)# area 1 range 10.1.0.0 255.255.252.0
R1(config-router)#

```

### Verificación de la tabla de routing del R1 después de la summarización

```
R1# show ip route ospf | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
O 10.1.0.0/22 is a summary, 00:00:09, Null0
O 10.2.1.0/24 [110/648] via 192.168.10.2, 00:00:09, Serial0/0/0
O IA 192.168.1.0/24 [110/1295] via 192.168.10.2, 00:00:09, Serial0/0/0
O IA 192.168.2.0/24 [110/1295] via 192.168.10.2, 00:00:09, Serial0/0/0
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O      192.168.10.4/30 [110/1294] via 192.168.10.2, 00:00:09, Serial0/0/0
R1#
```

### Verificación de la tabla de routing del R1 después de la summarización

```
R3# show ip route ospf | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
O IA 10.1.0.0/22 [110/1295] via 192.168.10.5, 00:00:06, serial0/0/1
O      10.2.1.0/24 [110/648] via 192.168.10.5, 00:29:23, Serial0/0/1
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O      192.168.10.0/30 [110/1294] via 192.168.10.5, 00:29:23,
Serial0/0/1
R3#
```

## Sumarización de rutas del área 2

Ingrese al modo de configuración del router OSPF en el R3 con la ID de proceso 10.

- Configure la ruta resumida del área 2 para la red 192.168.0.0/22.
- Vuelva al modo EXEC privilegiado.

```
R3(config)# router ospf 10
R3(config-router)# area 2 range 192.168.0.0 255.255.252.0
R3(config-router)# end
R3#
*Apr 19 18:11:06.781: %SYS-5-CONFIG_I: Configured from console by
console
R3#
```

Verifique la ruta resumida seleccionando las rutas OSPF en la tabla de routing.

```
R3# show ip route ospf
Codes: L - local, C - connected, S - static, R - RIPv1, M - mobile, E - 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, H - NHRP, l - LISP
      + - replicated route, # - next hop override

Gateway of last resort is not set

  10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
  O IA 10.1.0.0/22 [110/1295] via 192.168.10.5, 00:01:07, Serial0/0/1
  O 10.2.1.0/24 [110/648] via 192.168.10.5, 00:01:07, Serial0/0/1
  O 192.168.0.0/22 is a summary, 00:01:07, Null0
    192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
    O 192.168.10.0/30 [110/1294] via 192.168.10.5, 00:01:07, Serial0/0/1
R3#
```

Resumió correctamente las rutas del área 2 en el R3.

### Capítulo 6: OSPF multiárea 6.2.3.1 Verificación de OSPF de diversas áreas

Para verificar la topología OSPF multiárea de la ilustración, se pueden usar los mismos comandos de verificación que se utilizan para verificar OSPF de área única:

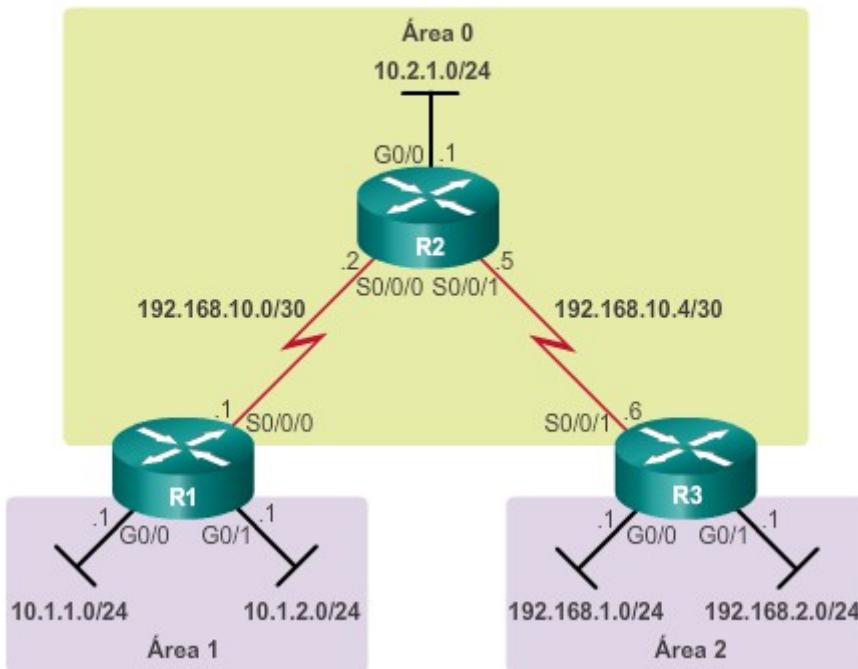
- **show ip ospf neighbor**
- **show ip ospf**
- **show ip ospf interface**

Los comandos que verifican información específica de OSPF multiárea son los siguientes:

- **show ip protocols**
- **show ip ospf interface brief**
- **show ip route ospf**
- **show ip ospf database**

**Nota:** para obtener el comando equivalente de OSPFv3, simplemente reemplace **ip** por **ipv6**.

## Topología OSPF multiárea



### Capítulo 6: OSPF multiárea 6.2.3.2 Verificación de la configuración general de OSPF multiárea

Utilice el comando **show ip protocols** para verificar el estado de OSPF. El resultado del comando revela qué protocolos de routing están configurados en un router. También incluye las especificaciones de protocolo de routing, como Id. de router, cantidad de áreas del router y redes incluidas en la configuración del protocolo de routing.

En la figura 1, se muestra la configuración OSPF del R1. Observen que el comando muestra que existen dos áreas. La sección **Routing for Networks** identifica las redes y sus respectivas áreas.

Utilice el comando **show ip ospf interface brief** para mostrar información concisa relacionada con OSPF acerca de las interfaces con OSPF habilitado. Este comando revela información útil, como Id. del proceso OSPF al que la interfaz está asignada, el área en la que se encuentra la interfaz y el costo de la interfaz.

En la figura 2, se verifican las interfaces con OSPF habilitado y las áreas a las que pertenecen.

Utilice el verificador de sintaxis de la figura 3 para verificar la configuración general del R2 y el R3.

### Verificación del estado de OSPF multiárea en el R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.1 0.0.0.0 area 1
    10.1.2.1 0.0.0.0 area 1
    192.168.10.1 0.0.0.0 area 0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          02:20:36
    2.2.2.2           110          02:20:39
  Distance: (default is 110)

R1#
```

### Verificación de las interfaces con OSPF habilitado en el R1

```
R1# show ip ospf interface brief
Interface  PID  Area  IP Address/Mask  Cost  State Nbrs F/C
Se0/0/0    10   0     192.168.10.1/30  64    P2P   1/1
Gi0/1      10   1     10.1.2.1/24    1      DR     0/0
Gi0/0      10   1     10.1.1.1/24    1      DR     0/0
R1#
```

## Verificación de OSPF multiárea

Muestre la información del protocolo IP.

```
R2# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 2.2.2.2
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.2.1.0 0.0.0.255 area 0
    192.168.10.0 0.0.0.7 area 0
  Routing Information Sources:
    Gateway          Distance      Last Update
    3.3.3.3           110          00:05:34
    1.1.1.1           110          00:05:34
  Distance: (default is 110)
```

R2#

Muestre la lista resumida de las interfaces que participan en OSPF en el R2.

```
R2# show ip ospf interface brief
Interface   PID   Areas          IP Address/Mask   Cost  State  Nbrs
P/C
Se0/0/1     10    0              192.168.10.5/30   647   P2P   1/1
Se0/0/0     10    0              192.168.10.2/30   647   P2P   1/1
Gi0/0       10    0              10.2.1.1/24      1     DR    0/0
R2#
```

Ahora, inició sesión en el R3. Muestre la información del protocolo IP.

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.1.1 0.0.0.0 area 2
    192.168.2.1 0.0.0.0 area 2
    192.168.10.4 0.0.0.3 area 0
  Routing Information Sources:
    Gateway          Distance      Last Update
    1.1.1.1           110          00:06:25
    2.2.2.2           110          00:06:25
  Distance: (default is 110)
R3#
```

Muestre la lista resumida de las interfaces que participan en OSPF en el R3.

```
R3# show ip ospf interface brief
Interface   PID   Areas          IP Address/Mask   Cost  State  Nbrs
P/C
Se0/0/1     10    0              192.168.10.6/30   647   P2P   1/1
Gi0/1       10    2              192.168.2.1/24    1     DR    0/0
Gi0/0       10    2              192.168.1.1/24    1     DR    0/0
R3#
```

Verificó correctamente el estado de OSPF multiárea.

## Capítulo 6: OSPF multiárea 6.2.3.3 Verificación de rutas OSPF

El comando que más se utiliza para verificar una configuración OSPF multiárea es el comando **show ip route**. Agregue el parámetro **ospf** para mostrar solo la información relacionada con OSPF.

En la figura 1, se muestra la tabla de routing del R1. Observe que las entradas **IA O** en la tabla de routing identifican redes descubiertas a partir de otras áreas. Específicamente, la **O** representa las rutas OSPF, e **IA** significa “interárea”, lo que quiere decir que la ruta se originó en otra área. Recuerde que el R1 está en el área 0 y que las subredes 192.168.1.0 y 192.168.2.0 se conectan al R3 en el área 2. La entrada [110/1295] de la tabla de routing representa la distancia administrativa que se asigna a OSPF (110) y el costo total de las rutas (costo de 1295).

Utilice el verificador de sintaxis de la figura 2 para verificar la tabla de routing del R2 y el R3 mediante el comando **show ip route ospf**.

#### Verificación de rutas OSPF multiárea en el R1

## Verificación de rutas OSPF multiárea en el R2 y el R3

### Muestre las rutas OSPF en la tabla de routing en el R2.

```
R2# show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISPs,
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O IA 10.1.1.0/24 [110/648] via 192.168.10.1, 00:07:52, Serial0/0/0
O IA 10.1.2.0/24 [110/648] via 192.168.10.1, 00:07:52, Serial0/0/0
O IA 192.168.1.0/24 [110/648] via 192.168.10.6, 00:07:52, Serial0/0/1
O IA 192.168.2.0/24 [110/648] via 192.168.10.6, 00:07:52, Serial0/0/1
R2#
```

### Ahora, inició sesión en el R3. Muestre las rutas OSPF en la tabla de routing en el R3.

```
R3# show ip route ospf
Codes: L - local, 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, H - NHRP, l - LISPs,
       + - replicated route, % - next hop override

Gateway of last resort is not set

      10.0.0.0/24 is subnetted, 3 subnets
O IA 10.1.1.0 [110/1295] via 192.168.10.5, 00:12:36, Serial0/0/1
O IA 10.1.2.0 [110/1295] via 192.168.10.5, 00:12:36, Serial0/0/1
O   10.2.1.0 [110/648] via 192.168.10.5, 00:12:36, Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
O   192.168.10.0/30 [110/1294] via 192.168.10.5, 00:12:36, Serial0/0/1
R3#
```

Verificó correctamente las rutas OSPF multiárea.

## Capítulo 6: OSPF multiárea 6.2.3.4 Verificación de LSDB de OSPF de diversas áreas

Utilice el comando **show ip ospf database** para verificar el contenido de la LSDB.

Existen muchas opciones disponibles con el comando **show ip ospf database**.

Por ejemplo, en la figura 1, se muestra el contenido de la LSDB del R1. Observe que el R1 tiene entradas para las áreas 1 y 0, dado que los ABR deben mantener una LSDB distinta para cada área a la que pertenecen. En el resultado, Router Link States en el área 0 identifica tres routers. La sección Summary Net Link States identifica las redes descubiertas a partir de otras áreas y el vecino que anunció la red.

Utilice el verificador de sintaxis de la figura 2 para verificar la LSDB del R2 y el R3 con el comando **show ip ospf database**. El R2 solo tiene interfaces en el área 0; por lo tanto, solo se requiere una LSDB. Al igual que el R1, el R3 contiene dos LSDB.

#### Verificación de LSDB de OSPF de R1

```
R1# show ip ospf database
OSPF Router with ID (1.1.1.1) (Process ID 10)

      Router Link States (Area 0)
Link ID      ADV Router  Age  Seq#      Checksum Link count
1.1.1.1        1.1.1.1    725  0x80000005  0x00F9B0 2
2.2.2.2        2.2.2.2    695  0x80000007  0x003DB1 5
3.3.3.3        3.3.3.3    681  0x80000005  0x00FF91 2
      Summary Net Link States (Area 0)
Link ID      ADV Router  Age  Seq#      Checksum
10.1.1.0       1.1.1.1    725  0x80000006  0x00D155
10.1.2.0       1.1.1.1    725  0x80000005  0x00C85E
192.168.1.0     3.3.3.3    681  0x80000006  0x00724E
192.168.2.0     3.3.3.3    681  0x80000005  0x006957

      Router Link States (Area 1)
Link ID      ADV Router  Age  Seq#      Checksum Link count
1.1.1.1        1.1.1.1    725  0x80000006  0x007D7C 2
      Summary Net Link States (Area 1)
Link ID      ADV Router  Age  Seq#      Checksum
10.2.1.0       1.1.1.1    725  0x80000005  0x004A9C
192.168.1.0     1.1.1.1    725  0x80000005  0x00B593
192.168.2.0     1.1.1.1    725  0x80000005  0x00AA9D
192.168.10.0    1.1.1.1    725  0x80000005  0x00B3D0
192.168.10.4    1.1.1.1    725  0x80000005  0x000E32
R1#
```

## Verificación de la LSDB de OSPF en el R2 y el R3

Muestre la base de datos de estado de enlace de OSPF en el R2.

```
R2# show ip ospf database

OSPF Router with ID (2.2.2.2) (Process ID 10)

Router Link States (Area 0)

Link ID      ADV Router  Age   Seq#      Checksum Link count
1.1.1.1      1.1.1.1    843    0x80000002 0x00B961 2
2.2.2.2      2.2.2.2    839    0x80000004 0x007458 5
3.3.3.3      3.3.3.3    834    0x80000002 0x00BF42 2

Summary Net Link States (Area 0)

Link ID      ADV Router  Age   Seq#      Checksum
10.1.1.0     1.1.1.1    117    0x80000002 0x00D951
10.1.2.0     1.1.1.1    117    0x80000002 0x00CE5B
192.168.1.0  3.3.3.3    103    0x80000003 0x00784B
192.168.2.0  3.3.3.3    103    0x80000002 0x006F54
R2#
```

Ahora, inició sesión en el R3. Muestre la base de datos de estado de enlace de OSPF en el R3.

```
R3# show ip ospf database

OSPF Router with ID (3.3.3.3) (Process ID 10)

Router Link States (Area 0)

Link ID      ADV Router  Age   Seq#      Checksum Link count
1.1.1.1      1.1.1.1    904    0x80000002 0x00B961 2
2.2.2.2      2.2.2.2    900    0x80000004 0x007458 5
3.3.3.3      3.3.3.3    893    0x80000002 0x00BF42 2

Summary Net Link States (Area 0)

Link ID      ADV Router  Age   Seq#      Checksum
10.1.1.0     1.1.1.1    178    0x80000002 0x00D951
10.1.2.0     1.1.1.1    178    0x80000002 0x00CE5B
192.168.1.0  3.3.3.3    162    0x80000003 0x00784B
192.168.2.0  3.3.3.3    162    0x80000002 0x006F54

Router Link States (Area 2)

Link ID      ADV Router  Age   Seq#      Checksum Link count
3.3.3.3      3.3.3.3    162    0x80000003 0x00CF60 2

Summary Net Link States (Area 2)

Link ID      ADV Router  Age   Seq#      Checksum
10.1.1.0     3.3.3.3    892    0x80000003 0x0055B9
10.1.2.0     3.3.3.3    892    0x80000003 0x004AC3
10.2.1.0     3.3.3.3    892    0x80000002 0x00EEA9
192.168.10.0 3.3.3.3   892    0x80000003 0x00B2F8
192.168.10.4 3.3.3.3   892    0x80000002 0x003002
R3#
```

Verificó correctamente la base de datos de estado de enlace de OSPF.

Al igual que OSPFv2, OSPFv3 proporciona comandos de verificación de OSPFv3 similares. Consulte la topología OSPFv3 de referencia en la figura 1.

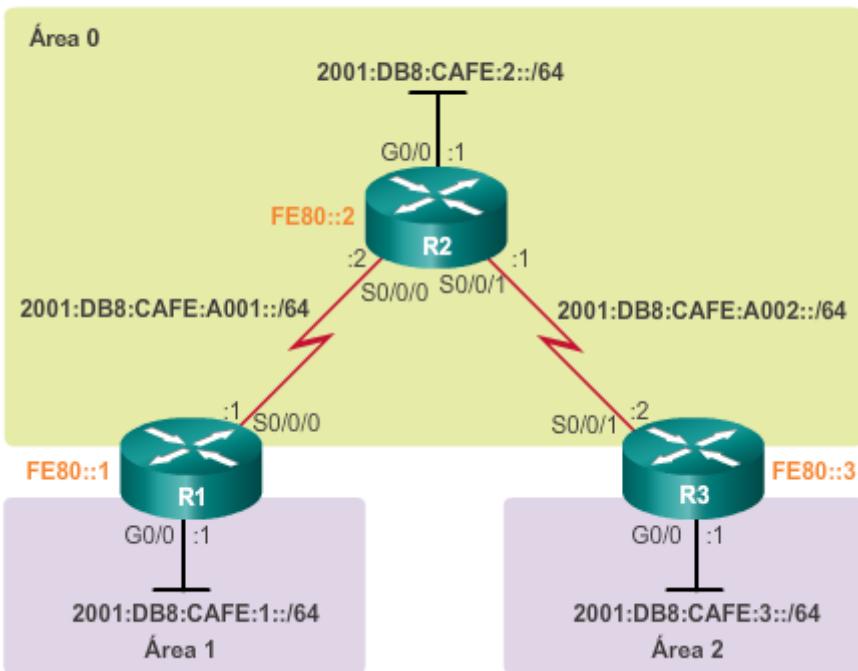
En la figura 2, se muestra la configuración OSPFv3 del R1. Observe que el comando confirma que ahora existen dos áreas. También identifica cada interfaz habilitada para las respectivas áreas.

En la figura 3, se verifican las interfaces con OSPFv3 habilitado y el área a la que pertenecen.

En la figura 4, se muestra la tabla de routing del R1. Observe que la tabla de routing IPv6 muestra entradas **OI** en la tabla de routing para identificar las redes descubiertas a partir de otras áreas. Específicamente, la **O** representa las rutas OSPF, y la **I** significa “interárea”, lo que quiere decir que la ruta se originó en otra área. Recuerde que el R1 está en el área 0 y que la subred 2001:DB8:CAFE3::/64 se conecta al R3 en el área 2. La entrada [110/1295] de la tabla de routing representa la distancia administrativa que se asigna a OSPF (110) y el costo total de las rutas (costo de 1295).

En la figura 5, se muestra el contenido de la LSDB del R1. El comando muestra información similar a la de su equivalente de OSPFv2. No obstante, la LSDB de OSPFv3 contiene tipos de LSA adicionales que no están disponibles en OSPFv2.

## Topología OSPFv3



### Verificación del estado de OSPFv3 multiárea en el R1

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Area border router
  Number of areas: 2 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/0
  Interfaces (Area 1):
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

### Verificación de las interfaces con OSPFv3 habilitado en el R1

Interface	PID	Area	Intf ID	Cost	State	Nbrs	F/C
Se0/0/0	10	0	6	647	P2P	1/1	
Gi0/0	10	1	3	1	DR	0/0	

## Verificación de rutas multiárea en el R1

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D -
      EIGRP
      EX - EIGRP external, ND - ND Default, NDP - ND Prefix, DCE -
Destination
      NDR - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF
      ext 1
      OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
O  2001:DB8:CAFE:2::/64 [110/648]
  via FE80::2, Serial0/0/0
OI  2001:DB8:CAFE:3::/64 [110/1295]
  via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:A002::/64 [110/1294]
  via FE80::2, Serial0/0/0
R1#
```

## Verificación de LSDB de OSPF de R1

```
R1# show ipv6 ospf database

OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

        Router Link States (Area 0)

ADV Router    Age      Seq#      Fragment ID  Link count Bits
1.1.1.1      1617     0x80000002 0          1           B
2.2.2.2      1484     0x80000002 0          2           None
3.3.3.3      14       0x80000001 0          1           B

        Inter Area Prefix Link States (Area 0)

ADV Router    Age      Seq#      Prefix
1.1.1.1      1833     0x80000001 2001:DB8:CAFE:1::/64
3.3.3.3      1476     0x80000001 2001:DB8:CAFE:3::/64

        Link (Type-8) Link States (Area 0)

ADV Router    Age      Seq#      Link ID      Interface
1.1.1.1      1843     0x80000001 6          Se0/0/0
2.2.2.2      1619     0x80000001 6          Se0/0/0

        Intra Area Prefix Link States (Area 0)

ADV Router    Age      Seq#      Link ID      Ref-lstype  Ref-LSID
1.1.1.1      1843     0x80000001 0          0x2001      0
2.2.2.2      1614     0x80000002 0          0x2001      0
3.3.3.3      1486     0x80000001           0x2001      0

        Router Link States (Area 1)

ADV Router    Age      Seq#      Fragment ID Link count Bits
1.1.1.1      1843     0x80000001 0          0           B

        Inter Area Prefix Link States (Area 1)

ADV Router    Age      Seq#      Prefix
1.1.1.1      1833     0x80000001 2001:DB8:CAFE:A001::/64
1.1.1.1      1613     0x80000001 2001:DB8:CAFE:A002::64
1.1.1.1      1613     0x80000001 2001:DB8:CAFE:2::/64
1.1.1.1      1474     0x80000001 2001:DB8:CAFE:3::/64

        Link (Type-8) Link States (Area 1)

ADV Router    Age      Seq#      Link ID      Interface
1.1.1.1      1844     0x80000001 3          Gi0/0

        Intra Area Prefix Link States (Area 1)

ADV Route    Age      Seq#      Link ID Ref-lstype Ref-LSID
1.1.1.1      1844     0x80000001 0          0x2001      0
R1#
```

### **Información básica/situación**

En esta actividad, configurará OSPFv2 multiárea. La red ya está conectada, y las interfaces están configuradas con el direccionamiento IPv4. Su trabajo es habilitar OSPFv2 multiárea, verificar la conectividad y examinar el funcionamiento de OSPFv2 multiárea.

[Packet Tracer: Configuración de OSPFv2 multiárea \(instrucciones\)](#)

[Packet Tracer: Configuración de OSPFv2 multiárea \(PKA\)](#)

Capítulo 6: OSPF multiárea 6.2.3.7 Packet Tracer: Configuración de OSPFv3 multiárea

### **Información básica/situación**

En esta actividad, configurará OSPFv3 multiárea. La red ya está conectada, y las interfaces están configuradas con el direccionamiento IPv6. Su trabajo es habilitar OSPFv3 multiárea, verificar la conectividad y examinar el funcionamiento de OSPFv3 multiárea.

[Packet Tracer: Configuración de OSPFv3 multiárea \(instrucciones\)](#)

[Packet Tracer: Configuración de OSPFv3 multiárea \(PKA\)](#)

Capítulo 6: OSPF multiárea 6.2.3.8 Práctica de laboratorio: Configuración de OSPFv2 multiárea

### **En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar una red OSPFv2 multiárea
- Parte 3: Configurar las rutas resumidas interárea

[Práctica de laboratorio: Configuración de OSPFv2 multiárea](#)

Capítulo 6: OSPF multiárea 6.2.3.9 Práctica de laboratorio: Configuración de OSPFv3 multiárea

### **En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: Configurar el routing OSPFv3 multiárea
- Parte 3: Configurar la sumarización de rutas interárea

[Práctica de laboratorio: Configuración de OSPFv3 multiárea](#)

## Capítulo 6: OSPF multiárea 6.2.3.10 Práctica de laboratorio: Resolución de problemas de

### OSPFv2 y OSPFv3 multiárea

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de conectividad de capa 3
- Parte 3: Resolver problemas de OSPFv2
- Parte 4: Resolver problemas de OSPFv3

## [Práctica de laboratorio: Resolución de problemas de OSPFv2 y OSPFv3 multiárea](#)

### Capítulo 6: OSPF multiárea 6.3.1.1 Actividad de clase: Tranvías digitales

#### **Tranvías digitales**

Su ciudad cuenta con un sistema de tranvías digitales antiguo basado en un diseño de área única. Todas las comunicaciones dentro de esta área tardan más en procesarse a medida que se agregan tranvías a las rutas que brindan servicios a la población de esta ciudad en crecimiento. Las salidas y llegadas de los tranvías también tardan un poco más, porque cada tranvía debe revisar grandes tablas de routing para determinar dónde suben y bajan los residentes en las calles de origen y destino.

A un ciudadano preocupado se le ocurrió la idea de dividir la ciudad en distintas áreas para tener una manera más eficaz de determinar la información de routing de los tranvías. Se cree que si los mapas de tranvías son más pequeños, el sistema se puede mejorar, ya que habría actualizaciones más rápidas y más pequeñas de las tablas de routing.

La comisión de la ciudad aprueba e implementa el nuevo sistema de tranvías digitales basado en áreas. Sin embargo, para asegurar que las nuevas rutas de área sean más eficaces, la comisión necesita información para demostrar los resultados en la próxima reunión pública de la comisión.

Complete las instrucciones que se encuentran en el PDF de esta actividad. Comparta sus respuestas con la clase.

## [Actividad de clase: Tranvías digitales](#)

### Capítulo 6: OSPF multiárea 6.3.1.2 Resumen

OSPF de área única es útil en redes más pequeñas, pero en redes más grandes, OSPF multiárea es una mejor opción. OSPF multiárea resuelve los problemas de las tablas de routing extensas, las bases de datos de estado de enlace muy grandes y los cálculos frecuentes del algoritmo SPF, como se muestra en las figuras 1 y 2.

El área principal se denomina “de red troncal” (área 0) y el resto de las áreas deben estar conectadas a esta. Se sigue produciendo el routing entre áreas, y muchas de las operaciones de routing, como volver a calcular la base de datos, se guardan en un área.

Existen cuatro tipos de routers OSPF diferentes: el router interno, el router de respaldo, el router de área perimetral (ABR) y el router limítrofe del sistema autónomo (ASBR). Un router se puede clasificar como uno o más tipos de router.

Las notificaciones de estado de enlace (LSA) son los bloques funcionales de OSPF. Este capítulo se centró en las LSA de tipo 1 a 5. Las LSA de tipo 1 se denominan “entradas de enlace de router”. Las LSA de tipo 2 se denominan “entradas de enlace de red”, y los DR saturan las áreas con ellas. Las LSA de tipo 3 se denominan “entradas de enlace de resumen”, y los ABR saturan las áreas con ellas. El ABR genera un LSA de resumen de tipo 4 solo cuando existe un ASBR en el área. Los LSA externos de tipo 5 anuncian rutas a redes que se encuentran afuera del sistema autónomo de OSPF. Los LSA de tipo 5 se originan en el ASBR y se propagan hacia todo el sistema autónomo.

En las tablas de routing IPv4, las rutas OSPF se identifican con los siguientes descriptores: O, IA O, O E1 u O E2. Cada router utiliza el algoritmo SPF en virtud de la LSDB para crear un árbol SPF. El árbol de SPF se utiliza para determinar las mejores rutas.

No se requieren comandos especiales para implementar una red OSPF multiárea. Un router simplemente se convierte en ABR cuando tiene dos instrucciones **network** en diferentes áreas.

Este es un ejemplo de una configuración OSPF:

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.1.1 0.0.0.0 area 1
R1(config-router)# network 10.1.2.1 0.0.0.0 area 1
R1(config-router)# network 192.168.10.1 0.0.0.0 area 0
```

OSPF no realiza la summarización automática. En OSPF, la summarización se puede configurar solo en los ABR o los ASBR. La summarización de rutas interárea se debe configurar manualmente, se produce en los ABR y se aplica a las rutas dentro de cada área. Para configurar manualmente la summarización de rutas interárea en un ABR, utilice el comando **area id-área range dirección máscara** del modo de configuración de router.

La summarización de rutas externas es específica de las rutas externas que se introducen en OSPF mediante la redistribución de rutas. Por lo general, solo los ASBR resumen rutas externas. En los ASBR, la summarización de rutas externas se configura mediante el comando **summary-address dirección máscara** del modo de configuración del router.

Los comandos que se utilizan para verificar la configuración de OSPF son los siguientes:

- **show ip ospf neighbor**
- **show ip ospf**

- **show ip ospf interface**
- **show ip protocols**
- **show ip ospf interface brief**
- **show ip route ospf**
- **show ip ospf database**

#### Capítulo 7: EIGRP 7.0.1.1 Introducción

El protocolo de routing de gateway interior mejorado (EIGRP) es un protocolo de routing vector distancia avanzado desarrollado por Cisco Systems. Como lo sugiere el nombre, EIGRP es una mejora de otro protocolo de routing de Cisco: el protocolo de routing de gateway interior (IGRP). IGRP es un protocolo de routing vector distancia con clase anterior, que quedó obsoleto a partir del IOS 12.3.

EIGRP es un protocolo de routing vector distancia que incluye características propias de los protocolos de routing de estado de enlace. EIGRP es apto para numerosas topologías y medios diferentes. En una red bien diseñada, EIGRP puede escalar para incluir varias topologías y puede proporcionar tiempos de convergencia extremadamente rápidos con un mínimo tráfico de red.

En este capítulo, se presenta el protocolo EIGRP y se proporcionan comandos básicos de configuración para habilitarlo en un router con IOS de Cisco. También se explora la operación del protocolo de routing y se proporcionan más detalles acerca de la manera en que EIGRP determina la mejor ruta.

**Al finalizar este capítulo, podrá hacer lo siguiente:**

- Describir las características básicas de EIGRP.
- Describir los tipos de paquetes que se utilizan para establecer y mantener una adyacencia de vecino EIGRP.
- Describir la encapsulación de los mensajes EIGRP.
- Configurar EIGRP para IPv4 en una red enrutada pequeña.
- Verificar la implementación de EIGRP para IPv4 en una red enrutada pequeña.
- Explicar cómo se forman las adyacencias de vecinos utilizando EIGRP.
- Explicar el propósito de las métricas utilizadas por EIGRP.
- Explicar la operación de DUAL y el uso de la tabla de topología.
- Describir los eventos que desencadenan actualizaciones de EIGRP.
- Comparar las características y la operación de EIGRP para IPv4 y EIGRP para IPv6.
- Configurar EIGRP para IPv6 en una red enrutada pequeña.
- Verificar la implementación de EIGRP para IPv6 en una red de tamaño pequeño a mediano.

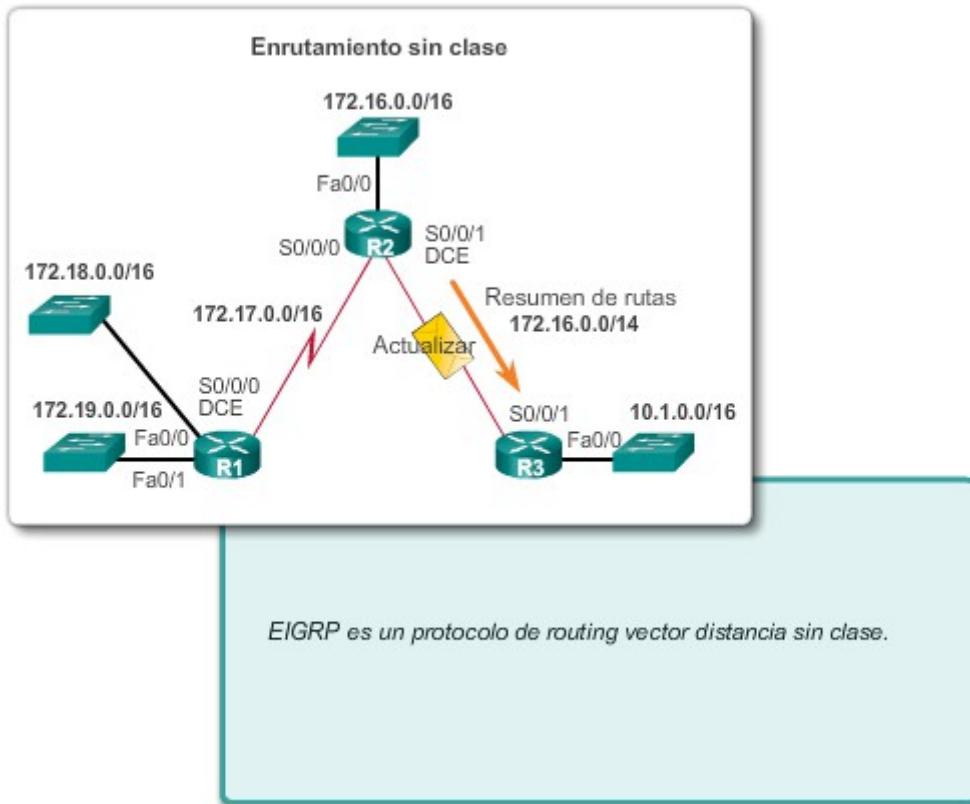
#### Capítulo 7: EIGRP 7.0.1.2 Actividad de clase: EIGRP sin clase

##### **EIGRP sin clase**

EIGRP se presentó como protocolo de routing vector distancia en 1992. En los inicios, se diseñó para funcionar como protocolo exclusivo en los dispositivos de Cisco únicamente. En 2013, EIGRP se convirtió en un protocolo de routing de varios proveedores, lo que significa que lo pueden utilizar los proveedores de otros dispositivos además de los dispositivos de Cisco.

Complete las preguntas de reflexión que se proporcionan con el archivo PDF de esta actividad. Guarde su trabajo y esté preparado para compartir las respuestas con la clase.

#### [Actividad de clase: EIGRP sin clase](#)



#### Capítulo 7: EIGRP 7.1.1.1 Características de EIGRP

EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF, como una RFC informativa. Esto significa que otros proveedores de redes ahora pueden implementar EIGRP en sus equipos para que interoperen con routers que ejecuten EIGRP, ya sean de Cisco o de otros fabricantes. Sin embargo, las características avanzadas de EIGRP, como las rutas internas de EIGRP necesarias para la implementación de la red privada virtual dinámica multipunto (DMVPN), no se cederán al IETF. Como RFC informativa, Cisco mantendrá el control de EIGRP.

EIGRP incluye características de protocolos de routing de estado de enlace y vector distancia. Sin embargo, aún se basa en el principio clave del protocolo de routing vector distancia, según el cual la información acerca del resto de la red se obtiene a partir de vecinos conectados directamente.

EIGRP es un protocolo de routing vector distancia avanzado que incluye características que no se encuentran en otros protocolos de routing vector distancia, como RIP e IGRP.

### **Algoritmo de actualización difusa**

El algoritmo de actualización por difusión (DUAL), que es el motor de cómputo detrás del EIGRP, constituye el centro del protocolo de routing. DUAL garantiza rutas de respaldo y sin bucles en todo el dominio de routing. Al usar DUAL, EIGRP almacena todas las rutas de respaldo disponibles a los destinos, de manera que se puede adaptar rápidamente a rutas alternativas si es necesario.

### **Establecimiento de adyacencias de vecinos**

EIGRP establece relaciones con routers conectados directamente que también están habilitados para EIGRP. Las adyacencias de vecinos se usan para rastrear el estado de esos vecinos.

### **Protocolo de transporte confiable**

El protocolo de transporte confiable (RTP) es exclusivo de EIGRP y se encarga de la entrega de los paquetes EIGRP a los vecinos. RTP y el rastreo de las adyacencias de vecinos establecen el marco para DUAL.

### **Actualizaciones parciales y limitadas**

En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos “parcial” y “limitada”. A diferencia de RIP, EIGRP no envía actualizaciones periódicas, y las entradas de ruta no vencen. El término “parcial” significa que la actualización solo incluye información acerca de cambios de ruta, como un nuevo enlace o un enlace que deja de estar disponible. El término “limitada” se refiere a la propagación de las actualizaciones parciales que se envían solo a aquellos routers que se ven afectados por el cambio. Esto minimiza el ancho de banda que se requiere para enviar actualizaciones de EIGRP.

### **Balanceo de carga de mismo costo o con distinto costo**

EIGRP admite balanceo de carga de mismo costo y balanceo de carga con distinto costo, lo que permite a los administradores distribuir mejor el flujo de tráfico en sus redes.

**Nota:** en algunos documentos antiguos, se utiliza el término “protocolo de routing híbrido” para definir a EIGRP. Sin embargo, este término es engañoso, porque EIGRP no es un híbrido entre protocolos de routing vector distancia y protocolos de estado de enlace. EIGRP es únicamente un protocolo de routing vector distancia; por lo que Cisco ya no usa ese término para referirse a él.

## Tipos de protocolos de routing

	Protocolos de gateway interior				Protocolos de gateway exterior
	Protocolos de routing vector distancia		Protocolos de routing de estado de enlace		Vector ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-4 para IPv6

**Nota:** IGRP es un IGP vector distancia que no se incluye en este gráfico.

### Capítulo 7: EIGRP 7.1.1.2 Módulos dependientes de protocolo

EIGRP tiene la capacidad para enrutar varios protocolos diferentes, incluidos IPv4 e IPv6, mediante el uso de módulos dependientes de protocolo (PDM). Si bien ahora son obsoletos, EIGRP también usaba PDM para enrutar los protocolos de capa de red IPX de Novell y AppleTalk de Apple Computer.

Los PDM son responsables de tareas específicas de los protocolos de capa de red. Un ejemplo de esto es el módulo de EIGRP, que es responsable de enviar y recibir paquetes EIGRP encapsulados en IPv4. Este módulo también es responsable de analizar los paquetes EIGRP y de informar a DUAL la nueva información recibida. EIGRP pide a DUAL que tome decisiones de routing, pero los resultados se almacenan en la tabla de routing IPv4.

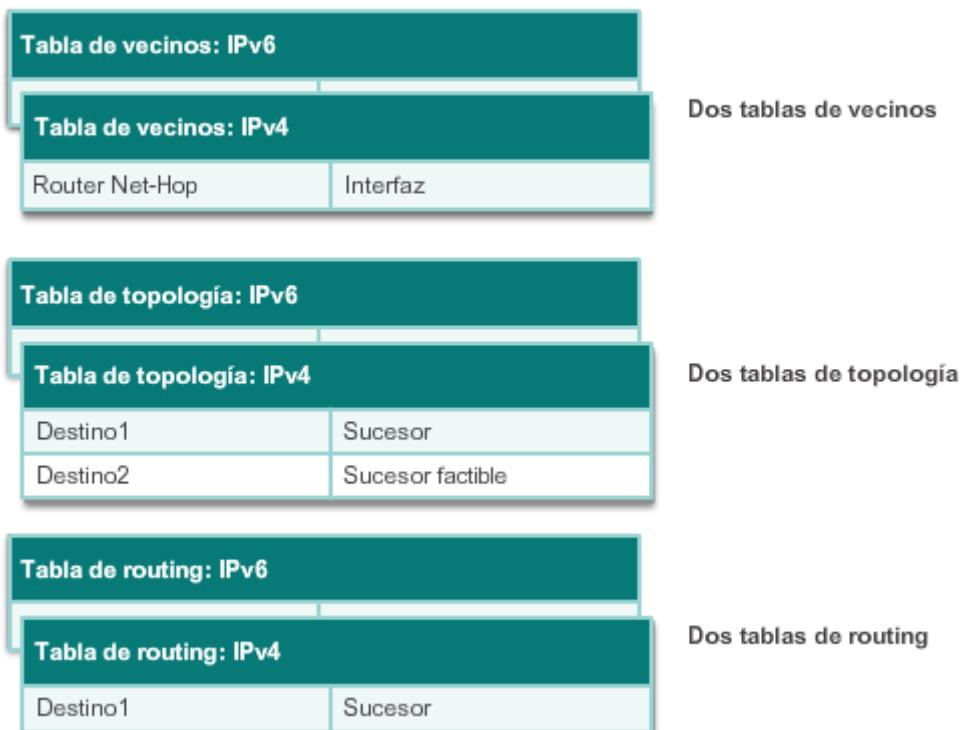
Los PDM son responsables de las tareas específicas de routing de cada protocolo de capa de red, incluido lo siguiente:

- Mantener las tablas de vecinos y de topología de los routers EIGRP que pertenecen a esa suite de protocolos.
- Construir y traducir paquetes específicos del protocolo para DUAL.
- Conectar a DUAL con la tabla de routing específica del protocolo.
- Calcular la métrica y pasar esa información a DUAL.
- Implementar listas de filtrado y de acceso.
- Realizar funciones de redistribución hacia otros protocolos de routing y desde ellos.

- Redistribuir rutas descubiertas por otros protocolos de routing.

Cuando un router descubre a un nuevo vecino, registra su dirección y su interfaz como una entrada en la tabla de vecinos. Existe una tabla de vecinos para cada módulo dependiente de protocolo, como IPv4. EIGRP también mantiene una tabla de topología. La tabla de topología contiene todos los destinos que anuncian los routers vecinos. También existe una tabla de topología separada para cada PDM.

### EIGRP con módulos dependientes de protocolo (PDM)



### Capítulo 7: EIGRP 7.1.1.3 Protocolo de transporte confiable

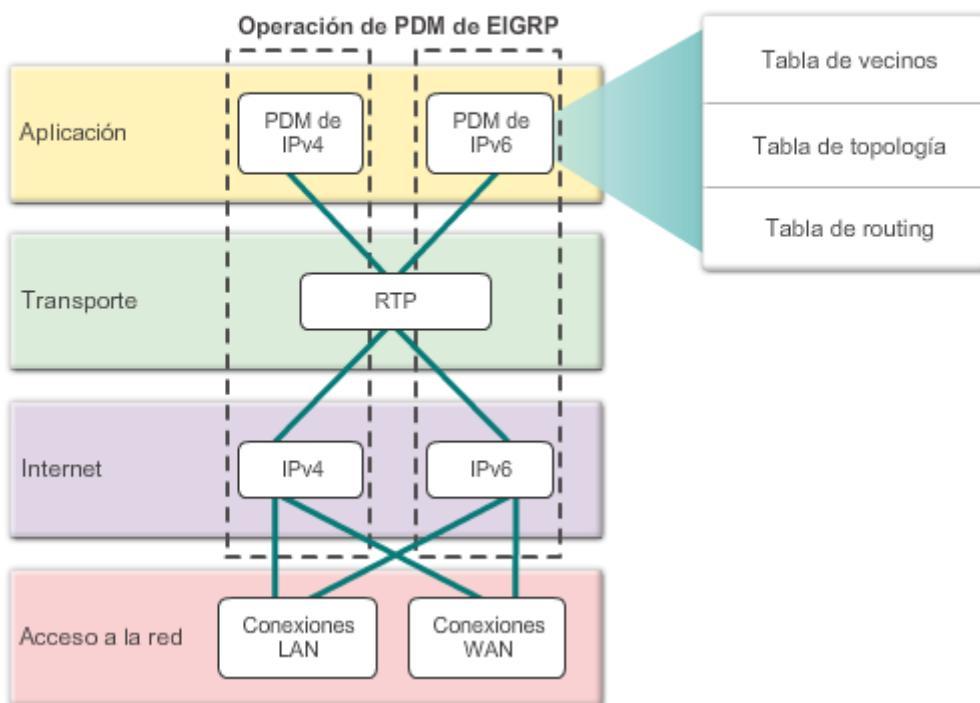
EIGRP utiliza el protocolo de transporte confiable (RTP) para la entrega y recepción de paquetes EIGRP. EIGRP se diseñó como un protocolo de routing independiente de capa de red y; debido a este diseño, no puede usar los servicios de UDP o TCP. Esto permite que EIGRP se utilice para protocolos distintos de aquellos de la suite de protocolos TCP/IP, como IPX y Apple Talk. En la ilustración se muestra conceptualmente cómo opera RTP.

Si bien el término “confiable” forma parte de su nombre, RTP incluye entrega confiable y entrega poco confiable de los paquetes EIGRP, de manera similar a TCP y UDP respectivamente. RTP confiable requiere que el receptor envíe un acuse de recibo al emisor. Los paquetes RTP poco confiables no requieren acuse de recibo. Por ejemplo, un paquete de actualización EIGRP se envía de manera confiable por RTP y requiere un acuse de recibo. Un paquete de saludo EIGRP también se envía por RTP, pero de manera poco confiable. Esto significa que los paquetes de saludo EIGRP no requieren un acuse de recibo.

RTP puede enviar paquetes EIGRP como unidifusión o multidifusión.

- Los paquetes de multidifusión EIGRP para IPv4 utilizan la dirección IPv4 de multidifusión reservada 224.0.0.10.
- Los paquetes de multidifusión EIGRP para IPv6 se envían a la dirección IPv6 de multidifusión reservada FF02::A.

### EIGRP reemplaza a TCP con RTP



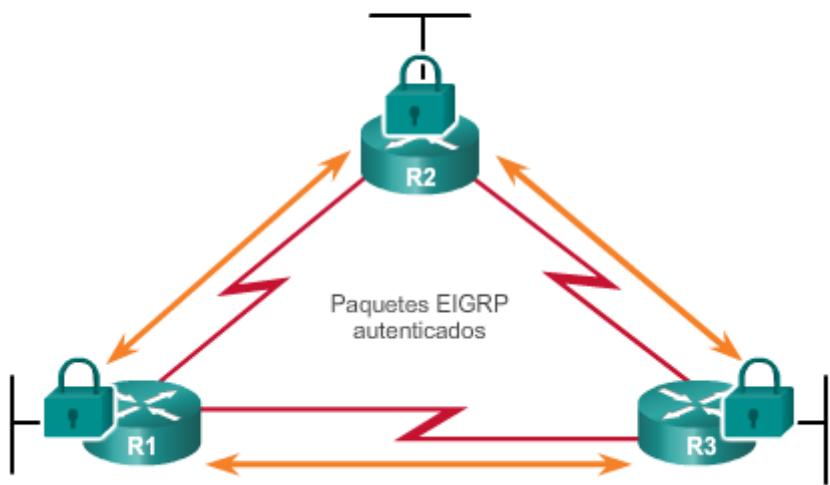
#### Capítulo 7: EIGRP 7.1.1.4 Autenticación

Al igual que otros protocolos de routing, EIGRP puede configurarse para autenticación. RIPv2, EIGRP, OSPF, IS-IS y BGP pueden configurarse para autenticar la información de routing.

Es aconsejable autenticar la información de routing que se transmite. Al hacerlo, se asegura de que los routers solo acepten información de routing de otros routers que se configuraron con la misma contraseña o información de autenticación.

**Nota:** la autenticación no cifra las actualizaciones de routing EIGRP.

## Autenticación



### Capítulo 7: EIGRP 7.1.2.1 Tipos de paquetes EIGRP

EIGRP utiliza cinco tipos de paquetes distintos, algunos en pares. Los paquetes EIGRP se envían mediante entrega RTP confiable o poco confiable y se pueden enviar como unidifusión o multidifusión —o, a veces, de ambas maneras. Los tipos de paquetes EIGRP también reciben el nombre de “formatos de paquetes EIGRP” o “mensajes EIGRP”.

Como se muestra en la figura 1, los cinco tipos de paquetes EIGRP incluyen:

**Paquetes de saludo:** se utilizan para descubrir a los vecinos y para mantener las adyacencias de vecinos.

- Enviados con entrega poco confiable
- Multidifusión (en la mayoría de los tipos de redes)

**Paquetes de actualización:** propagan información de routing a vecinos EIGRP.

- Enviados con entrega confiable
- Unidifusión o multidifusión

**Paquetes de acuse de recibo:** se utilizan para acusar recibo de un mensaje EIGRP que se envió con entrega confiable.

- Enviados con entrega poco confiable
- Unidifusión

**Paquetes de consulta:** se utilizan para consultar rutas de vecinos.

- Enviados con entrega confiable
- Unidifusión o multidifusión

**Paquetes de respuesta:** se envían en respuesta a consultas EIGRP.

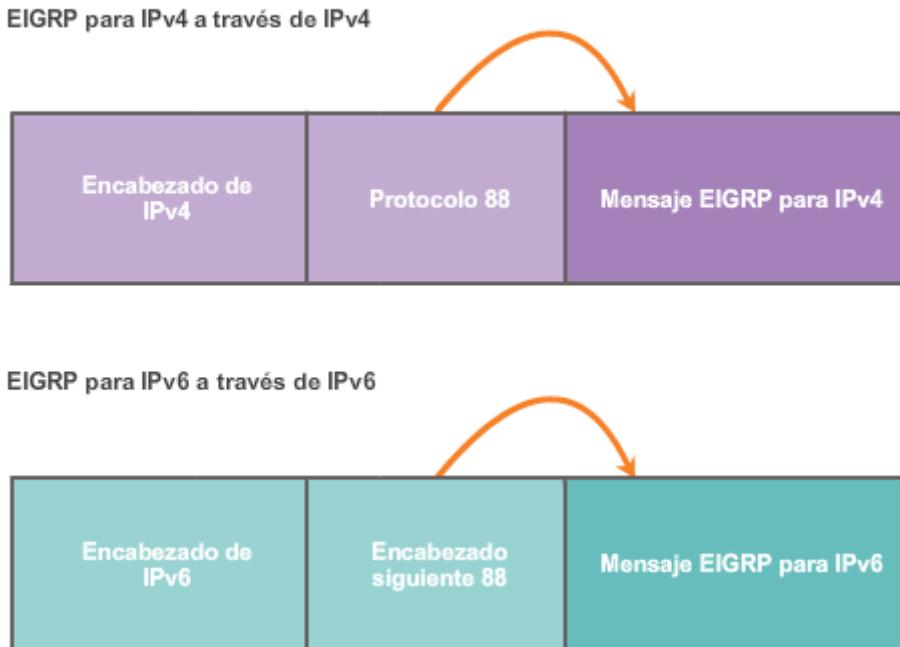
- Enviados con entrega poco confiable
- Unidifusión

En la figura 2, se muestra que los mensajes EIGRP normalmente se encapsulan en paquetes IPv4 o IPv6. Los mensajes EIGRP para IPv4 usan IPv4 como el protocolo de capa de red. El campo de protocolo IPv4 usa 88 para indicar que la porción de datos del paquete es un mensaje EIGRP para IPv4. Los mensajes EIGRP para IPv6 se encapsulan en paquetes IPv6 que utilizan el campo de encabezado siguiente 88. Al igual que el campo de protocolo para IPv4, el campo de encabezado siguiente de IPv6 indica el tipo de datos transportados en el paquete IPv6.

#### Tipos de paquetes EIGRP

Tipo de paquete	Descripción
Saludo	Utilizado para descubrir otros routers EIGRP en la red.
Acuse de recibo	Utilizado para acusar recibo de cualquier paquete EIGRP.
Actualizar	Transmite información de routing a destinos conocidos.
Consulta	Utilizado para solicitar información específica de un router vecino.
Respuesta	Utilizado para responder a una consulta.

### **Los mensajes EIGRP se envían a través de IP**



#### Capítulo 7: EIGRP 7.1.2.2 Paquetes de saludo EIGRP

EIGRP utiliza pequeños paquetes de saludo para descubrir otros routers con EIGRP habilitado en enlaces conectados directamente. Los routers utilizan los paquetes de saludo para formar adyacencias de vecinos EIGRP, también conocidas como “relaciones de vecinos”.

Los paquetes de saludo EIGRP se envían como transmisiones IPv4 o IPv6 de multidifusión y utilizan entrega RTP poco confiable. Esto significa que el receptor no responde con un paquete de acuse de recibo.

- La dirección de multidifusión EIGRP reservada para IPv4 es 224.0.0.10.
- La dirección de multidifusión EIGRP reservada para IPv6 es FF02::A.

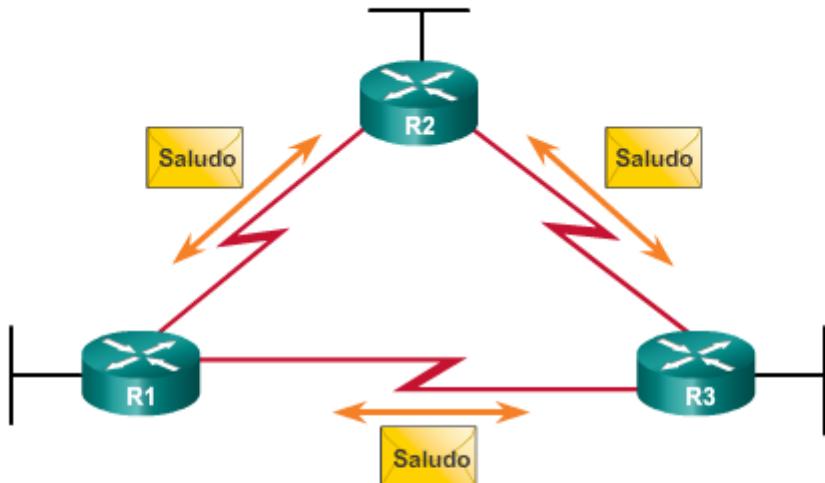
Los routers EIGRP descubren vecinos y establecen adyacencias con los routers vecinos mediante el paquete de saludo. En la mayoría de las redes, los paquetes de saludo EIGRP se envían como paquetes de multidifusión cada cinco segundos. Sin embargo, en redes multipunto multiacceso sin difusión (NBMA), como X.25, Frame Relay, e interfaces de modo de transferencia asíncrona (ATM) con enlaces de acceso de T1 (1,544 Mb/s) o más lentos, los paquetes de saludo se envían como paquetes de unidifusión cada 60 segundos.

EIGRP también usa paquetes de saludo para mantener adyacencias establecidas. Un router EIGRP supone que, mientras reciba paquetes de saludo de un vecino, el vecino y sus rutas siguen siendo viables.

EIGRP utiliza un temporizador de espera para determinar el tiempo máximo que el router debe esperar para recibir el siguiente saludo antes de declarar que el vecino es inalcanzable. De

manera predeterminada, el tiempo de espera es tres veces el intervalo de saludo, es decir, 15 segundos en la mayoría de las redes y 180 segundos en redes NBMA de baja velocidad. Si el tiempo de espera expira, EIGRP declara la ruta como inactiva y DUAL busca una nueva ruta mediante el envío de consultas.

#### Intervalos de saludo y tiempos de espera predeterminados para EIGRP



Ancho de banda	Enlace de ejemplo	Intervalo de saludo predeterminado	Tiempo de espera predeterminado
1.544 Mbps	Frame relay multipunto	60segundos	180segundos
Superior a 1544 Mb/s	T1, Ethernet	5segundos	15segundos

#### Capítulo 7: EIGRP 7.1.2.3 Paquetes de actualización y acuse de recibo EIGRP

##### Paquetes de actualización EIGRP

EIGRP envía paquetes de actualización para propagar información de routing. 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.

A diferencia de RIP, EIGRP (otro protocolo de routing vector distancia) no envía actualizaciones periódicas, y las entradas de ruta no vencen. En cambio, EIGRP envía actualizaciones incrementales solo cuando se modifica el estado de un destino. Esto puede incluir cuando una nueva red está disponible, cuando una red existente deja de estar disponible, o cuando ocurre un cambio en la métrica de routing de una red existente.

En lo que respecta a sus actualizaciones, en EIGRP se utilizan los términos *parcial* y *limitada*. El término *parcial* significa que la actualización sólo envía información acerca de los cambios de ruta. El término “*limitada*” se refiere a la propagación de las actualizaciones parciales que se envían solo a aquellos routers que se ven afectados por el cambio.

Al enviar solo la información de routing necesaria únicamente a los routers que la necesitan, EIGRP minimiza el ancho de banda que se requiere para enviar actualizaciones EIGRP.

Los paquetes de actualización EIGRP usan entrega confiable, lo que significa que el router emisor requiere un acuse de recibo. 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.

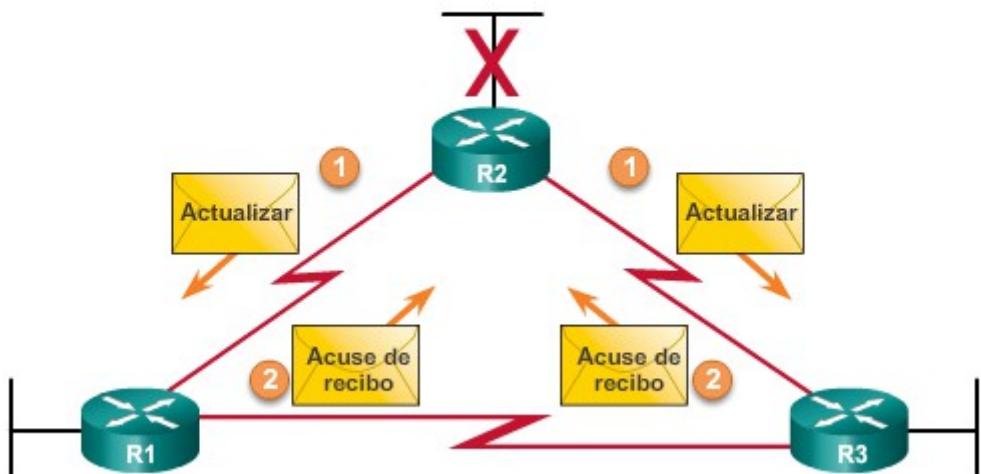
### **Paquetes de acuse de recibo EIGRP**

EIGRP envía paquetes de acuse de recibo (ACK) cuando se usa el método de entrega confiable. Un acuse de recibo EIGRP es un paquete de saludo EIGRP sin ningún dato. RTP utiliza una entrega confiable para los paquetes EIGRP de actualización, consulta y respuesta. Los paquetes de acuse de recibo EIGRP se envían siempre como transmisiones de unidifusión poco confiables. El sentido de la entrega poco confiable es que, de otra manera, habría un bucle interminable de acuses de recibo.

En la ilustración, el R2 perdió la conectividad a la LAN conectada a su interfaz Gigabit Ethernet. El R2 envía inmediatamente una actualización al R1 y al R3, donde se señala la ruta fuera de servicio. El R1 y el R3 responden con un acuse de recibo para que el R2 sepa que recibieron la actualización.

**Nota:** en algunos documentos, se hace referencia al saludo y al acuse de recibo como un único tipo de paquete EIGRP.

### **Mensajes EIGRP de actualización y de acuse de recibo**



### **Capítulo 7: EIGRP 7.1.2.4 Paquetes de consulta y de respuesta EIGRP**

### **Paquetes de consulta EIGRP**

DUAL utiliza paquetes de consulta y de respuesta cuando busca redes y cuando realiza otras tareas. Los paquetes de consulta y respuesta utilizan una entrega confiable. Las consultas utilizan multicast o unicast, mientras que las respuestas se envían siempre como unicast.

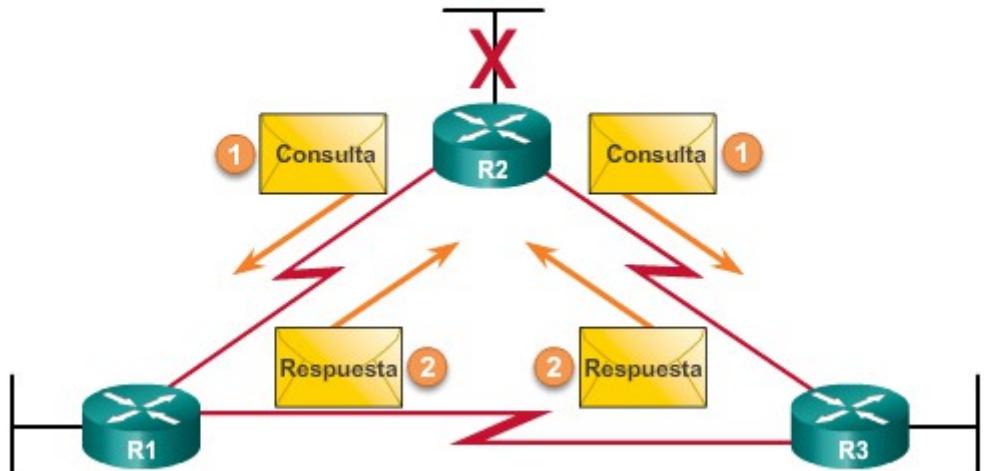
En la figura, R2 ha perdido la conectividad con LAN y envía consultas a todos los vecinos EIGRP y busca cualquier ruta posible hacia la LAN. Debido a que las consultas utilizan entrega confiable, el router receptor debe devolver un paquete de acuse de recibo EIGRP. El acuse de recibo informa al emisor de la consulta que se recibió el mensaje de consulta. Para que el ejemplo sea más simple, se omitieron los acuses de recibo en el gráfico.

### Paquetes de respuesta EIGRP

Todos los vecinos deben enviar una respuesta, independientemente de si tienen o no una ruta a la red fuera de servicio. Debido a que las respuestas también usan entrega confiable, los routers como el R2 deben enviar un acuse de recibo.

Quizá no sea obvio por qué el R2 debería enviar una consulta para una red que sabe que está inactiva. En realidad, solo la interfaz del R2 que está conectada a la red está inactiva. Otro router podría estar conectado a la misma LAN y tener una ruta alternativa a la misma red. Por lo tanto, el R2 consulta por un router tal antes de eliminar completamente la red de su tabla de topología.

Mensajes EIGRP de consulta y de respuesta



Capítulo 7: EIGRP 7.1.2.5 Actividad: Identificar el tipo de paquete EIGRP

**Actividad: Tipos de paquetes EIGRP**

Arrastre el tipo de paquete EIGRP a la definición correspondiente.

Definición de paquete EIGRP	Tipo de paquete
Utilizado para crear adyacencias con los vecinos.	<input checked="" type="checkbox"/> Paquete de saludo
Indica la recepción de un paquete cuando se utiliza el protocolo de transporte en tiempo real (RTP).	<input checked="" type="checkbox"/> Acuse de recibo Paquete
Enviado a vecinos cuando el DUAL coloca una ruta en estado activo.	<input checked="" type="checkbox"/> Paquete de consulta
Utilizado para darle información a DUAL acerca del destino.	<input checked="" type="checkbox"/> Paquete de respuesta
Envia en unicast información sobre la red a un nuevo vecino.	<input checked="" type="checkbox"/> Paquete de actualización

#### Capítulo 7: EIGRP 7.1.3.1 Encapsulación de mensajes EIGRP

La porción de datos de un mensaje EIGRP se encapsula en un paquete. Este campo de datos se llama “tipo, longitud, valor” (TLV). Los tipos de TLV pertinentes a este curso son los parámetros de EIGRP, las rutas IP internas y las rutas IP externas.

El encabezado del paquete EIGRP se incluye con cada paquete EIGRP, independientemente de su tipo. Luego, el encabezado del paquete EIGRP y el TLV se encapsulan en un paquete IPv4. En el encabezado del paquete IPv4, el campo de protocolo se establece en 88 para indicar EIGRP, y la dirección IPv4 de destino se establece en multidifusión 224.0.0.10. Si el paquete EIGRP se encapsula en una trama de Ethernet, la dirección MAC de destino también es una dirección de multidifusión, 01-00-5E-00-00-0A.

En las figuras 1 a 4, se muestra la trama de Ethernet de enlace de datos. EIGRP para IPv4 se encapsula en un paquete IPv4. EIGRP para IPv6 usa un tipo de encapsulación similar. EIGRP para IPv6 se encapsula con un encabezado de IPv6. La dirección IPv6 de destino es la dirección de multidifusión FF02::A, y el campo de encabezado siguiente se establece en 88.

### Tipo/longitud/tipos de valores

Encabezado de trama de enlace de datos	Encabezado de paquete IP	Encabezado de paquete EIGRP	Tipos de TLV
--	--------------------------	-----------------------------	--------------

#### Trama de enlace de datos

Dirección MAC de origen = dirección de la interfaz emisora

Dirección MAC de destino = multidifusión: 01-00-5E-00-00-0A

#### Paquete IP

Dirección IPv4 de origen = dirección de la interfaz emisora

Dirección IPv4 de destino = multidifusión: 224.0.0.10

Campo de protocolo = 88 para EIGRP

#### Encabezado de paquete EIGRP

Código de operación del tipo de paquete EIGRP Número de sistema autónomo

**Tipos de TLV**  
Algunos tipos incluyen:  
0x0001: Parámetros EIGRP  
0x0102: Rutas IP internas  
0x0103: Rutas IP externas

### Capítulo 7: EIGRP 7.1.3.2 TLV y encabezado de paquetes EIGRP

Todos los paquetes EIGRP incluyen el encabezado, como se muestra en la figura 1. Los campos importantes incluyen el campo de código de operación y el campo de número de sistema autónomo. El código de operación especifica el tipo de paquete EIGRP de la siguiente manera:

- Actualizar
- Consulta
- Respuesta
- Saludo

El número de sistema autónomo especifica el proceso de routing EIGRP. A diferencia de RIP, se pueden ejecutar varias instancias de EIGRP en una red, y el número de sistema autónomo se usa para realizar el seguimiento de cada proceso EIGRP en ejecución.

En la figura 2, se muestra el TLV de parámetros de EIGRP. El mensaje de parámetros de EIGRP incluye las ponderaciones que EIGRP usa para su métrica compuesta. Solo el ancho de banda y el retardo se ponderan de manera predeterminada. Ambos se ponderan de igual manera, por ello, tanto el campo K1 para el ancho de banda como el campo K3 para el retraso se establecen en uno (1). Los demás valores K se establecen en cero (0).

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.

En la figura 3, se muestra el TLV de rutas IP internas. El mensaje de IP internas se usa para anunciar las rutas EIGRP dentro de un sistema autónomo. Los campos importantes incluyen los campos de métrica (retraso y ancho de banda), el campo de máscara de subred (longitud de prefijo) y el campo de destino.

El retardo se calcula como la suma de retardos 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.

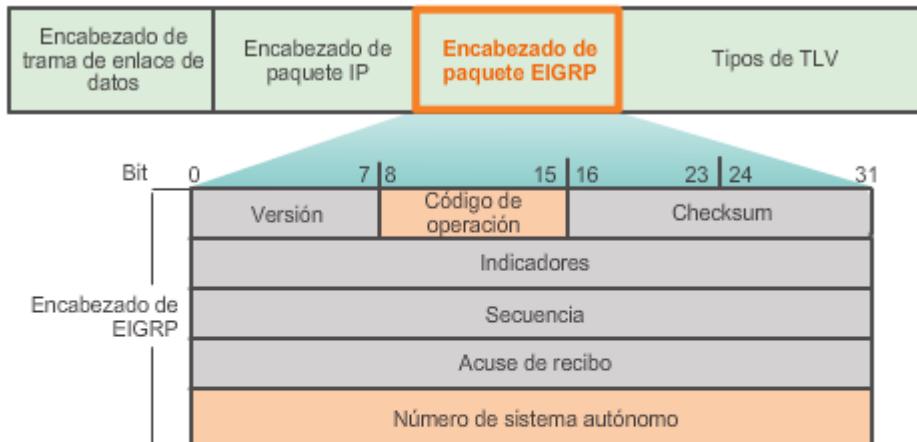
La máscara de subred se especifica como la duración de prefijo o el número de bits de la red en la máscara de subred. Por ejemplo, la longitud de prefijo para la máscara de subred 255.255.255.0 es 24, porque 24 es el número de bits de red.

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 de 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.

En la figura 4, se muestra el TLV de rutas IP externas. El mensaje de IP externas se usa cuando las rutas externas se importan al proceso de routing EIGRP. En este capítulo, importaremos o redistribuiremos una ruta estática predeterminada en EIGRP. Observe que la mitad inferior del TLV de rutas IP externas incluye todos los campos utilizados por el TLV de IP internas.

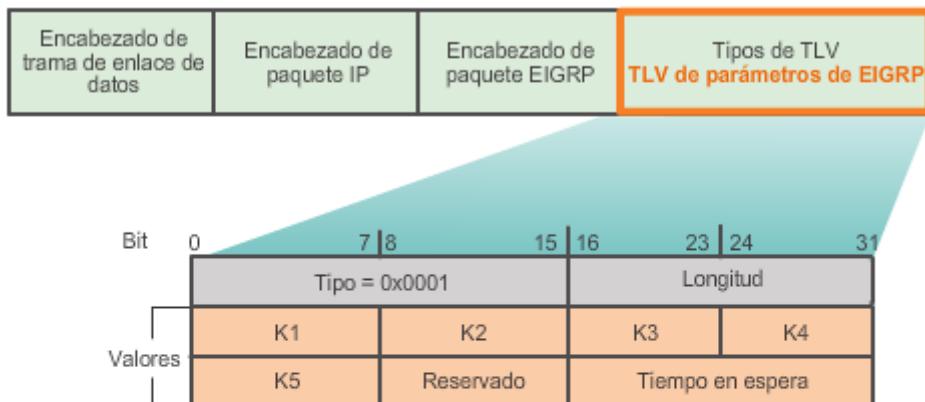
**Nota:** La unidad máxima de transmisión (MTU) no es una métrica utilizada por EIGRP. La MTU se incluye en las actualizaciones de routing, pero no se usa para determinar la métrica de routing.

### Encabezado de paquete EIGRP



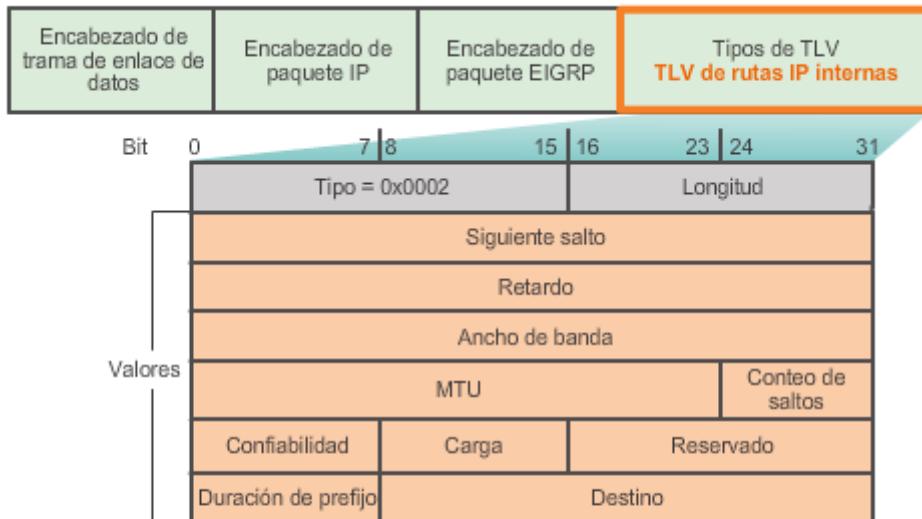
- Código de operación:** tipo de paquete EIGRP: actualización (1), consulta (3) respuesta (4), saludo (5).
- Número de sistema autónomo:** ID para este proceso de routing EIGRP.

### Parámetros EIGRP



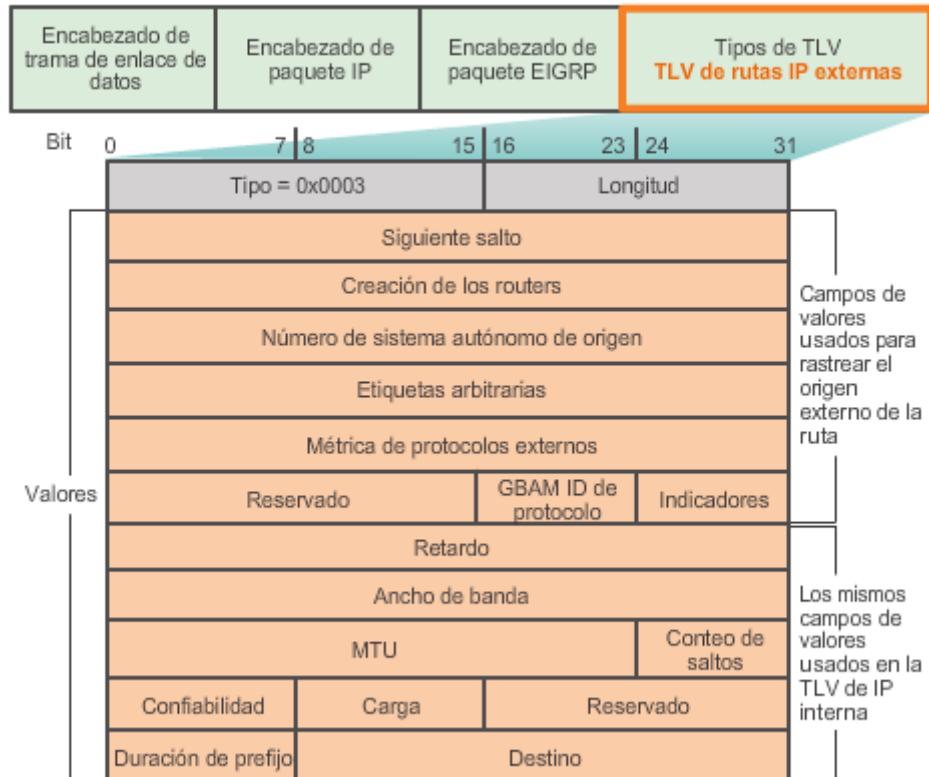
- K1 y K3:** evalúa el ancho de banda y el retraso; se establece en 1.
- Tiempo de espera:** tiempo máximo que debe esperar el router al siguiente saludo.

### TLV de EIGRP: interna



- Retraso:** suma de todos los retrasos de origen a destino en unidades de 10 microsegundos; 0xFFFFFFFF indica una ruta inalcanzable.
- Ancho de banda:** el ancho de banda más bajo configurado en cualquier interfaz en toda la ruta.
- Longitud de prefijo:** especifica el número de bits de red en la máscara de subred.
- Destino:** la dirección de la red de destino; este campo es variable.

### TLV de EIGRP: externa



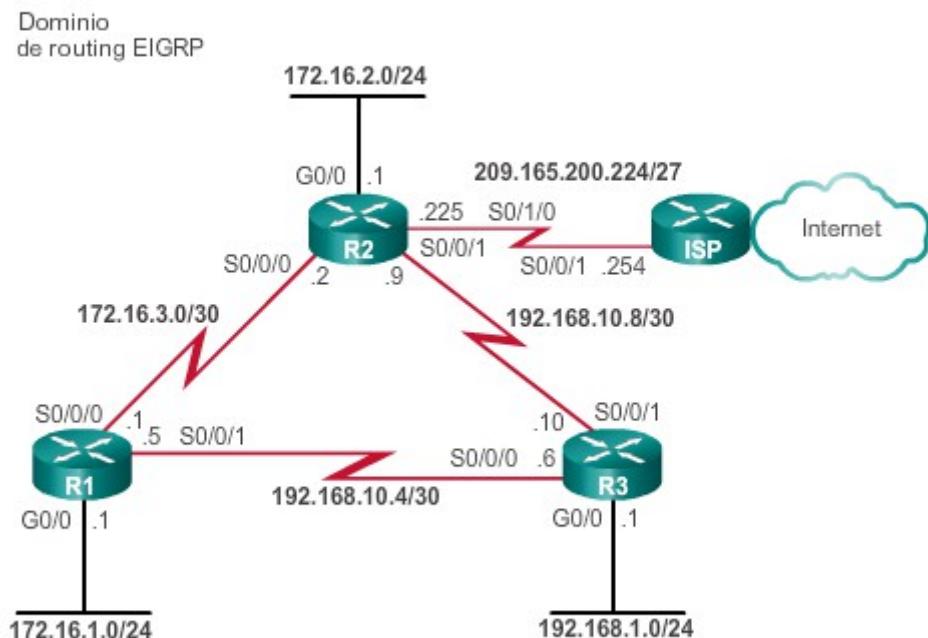
## Capítulo 7: EIGRP 7.2.1.1 Topología de la red EIGRP

En la figura 1, se muestra la topología que se usa en este curso para configurar EIGRP para IPv4. Es posible que los tipos de interfaces seriales y sus anchos de banda asociados no reflejen necesariamente los tipos de conexiones más frecuentes que se encuentran en las redes en la actualidad. Los anchos de banda de los enlaces seriales que se usan en esta topología se eligieron para ayudar a explicar el cálculo de las métricas de los protocolos de routing y el proceso de selección de la mejor ruta.

Los routers en la topología tienen una configuración inicial, que incluye las direcciones de las interfaces. En este momento, ninguno de los routers tiene configurado routing estático o routing dinámico.

En las figuras 2, 3 y 4, se muestran las configuraciones de las interfaces para los tres routers EIGRP en la topología. Solo los routers R1, R2, y R3 forman parte del dominio de routing EIGRP. El router ISP se usa como gateway del dominio de routing a Internet.

**Topología EIGRP para IPv4**



### Configuración de la interfaz para el R1

```
R1# show running-config
<resultado omitido>
!
interface GigabitEthernet0/0
  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
  ip address 192.168.10.5 255.255.255.252
```

### Configuración de la interfaz para el R2

```
R2# show running-config
<resultado omitido>
!
interface GigabitEthernet0/0
  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
  clock rate 64000
!
interface Serial0/1/0
  ip address 209.165.200.225 255.255.255.224
```

## Configuración de la interfaz para el R3

```
R3# show running-config
<resultado omitido>
!
interface GigabitEthernet0/0
 ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
 ip address 192.168.10.6 255.255.255.252
 clock rate 64000
!
interface Serial0/0/1
 ip address 192.168.10.10 255.255.255.252
```

### Capítulo 7: EIGRP 7.2.1.2 Números de sistema autónomo

EIGRP utiliza el comando **router eigrpsistema-autónomo** para habilitar el proceso EIGRP. El número de sistema autónomo que se menciona en la configuración EIGRP no se relaciona con los números de sistema autónomo asignados globalmente por la Autoridad de números asignados de Internet (IANA), que usan los protocolos de routing externos.

Entonces ¿cuál es la diferencia entre el número de sistema autónomo asignado globalmente por IANA y el número de sistema autónomo de EIGRP?

El sistema autónomo asignado globalmente por IANA es un conjunto de redes bajo el control administrativo de una única entidad que presenta una política de routing común a Internet. En la figura, las empresas A, B, C y D se encuentran todas bajo el control administrativo de ISP1. Cuando anuncia rutas a ISP2, ISP1 presenta una política de routing común para todas estas empresas.

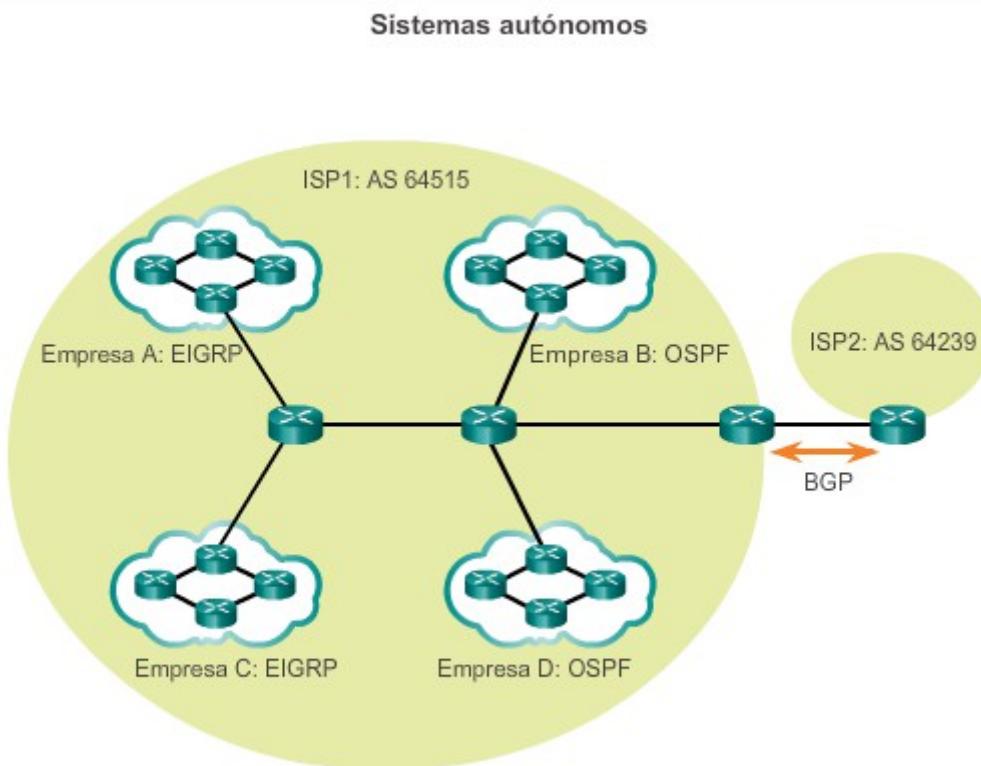
Las pautas para la creación, la selección y el registro de un sistema autónomo se describen en RFC 1930. IANA asigna los números de sistema autónomo globales y es la misma autoridad que asigna el espacio de direcciones IP. El registro regional de Internet (RIR) local tiene la responsabilidad de asignarles a las entidades un número de sistema autónomo de su bloque de números de sistema autónomo asignado. Antes de 2007, los números de sistema autónomo eran números de 16 bits que iban de 0 a 65 535. En la actualidad, se asignan números de sistema autónomo de 32 bits, lo que aumenta la cantidad de números de sistema autónomo disponibles a más de 4000 millones.

Por lo general, los proveedores de servicios de Internet (ISP), los proveedores de servicios de Internet troncales y las grandes instituciones conectadas a otras entidades requieren un número de sistema autónomo. Estos ISP y grandes instituciones utilizan el protocolo de routing de gateway exterior, el protocolo de gateway fronterizo (BGP), para propagar la información de routing. BGP es el único protocolo de routing 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 sistema autónomo, porque se encuentran bajo el control de una entidad más grande, como un

ISP. Estas empresas usan protocolos de gateway interior, como RIP, EIGRP, OSPF e IS-IS para enrutar paquetes dentro de sus propias redes. Son una de muchas redes independientes dentro del sistema autónomo de ISP. ISP es responsable del enruteamiento de paquetes dentro del sistema autónomo y entre otros sistemas autónomos.

El número de sistema autónomo que se usa para la configuración EIGRP solo es importante para el dominio de routing EIGRP. Funciona como una ID de proceso para ayudar a los routers a realizar un seguimiento de varias instancias de EIGRP en ejecución. Esto es necesario porque es posible tener más de una instancia de EIGRP en ejecución en una red. Cada instancia de EIGRP se puede configurar para admitir e intercambiar actualizaciones de routing de diferentes redes.



#### Capítulo 7: EIGRP 7.2.1.3 El comando router de EIGRP

El IOS de Cisco incluye procesos para habilitar y configurar varios tipos de protocolos de routing dinámico diferentes. El comando del modo de configuración global **router** se usa para iniciar la configuración de cualquier protocolo de routing dinámico. La topología que se muestra en la figura 1 se utiliza para ilustrar este comando.

Como se muestra en la figura 2, cuando está seguido de un signo de pregunta (?), el comando **router** del modo de configuración global enumera todos los protocolos de routing disponibles que admite la versión específica del IOS que se ejecuta en el router.

El siguiente comando del modo de configuración global se usa para ingresar al modo de configuración del router para EIGRP y comenzar a configurar el proceso EIGRP:

```
Router(config)# router eigrp sistema-autónomo
```

El argumento *sistema-autónomo* se puede asignar a cualquier valor de 16 bits entre los números 1 y 65 535. Todos los routers dentro del dominio de routing EIGRP deben usar el mismo número de sistema autónomo.

En la figura 3, se muestra la configuración del proceso EIGRP en los routers R1, R2 y R3. Observe que la petición de entrada cambia de la petición del modo de configuración global a la del modo de configuración del router.

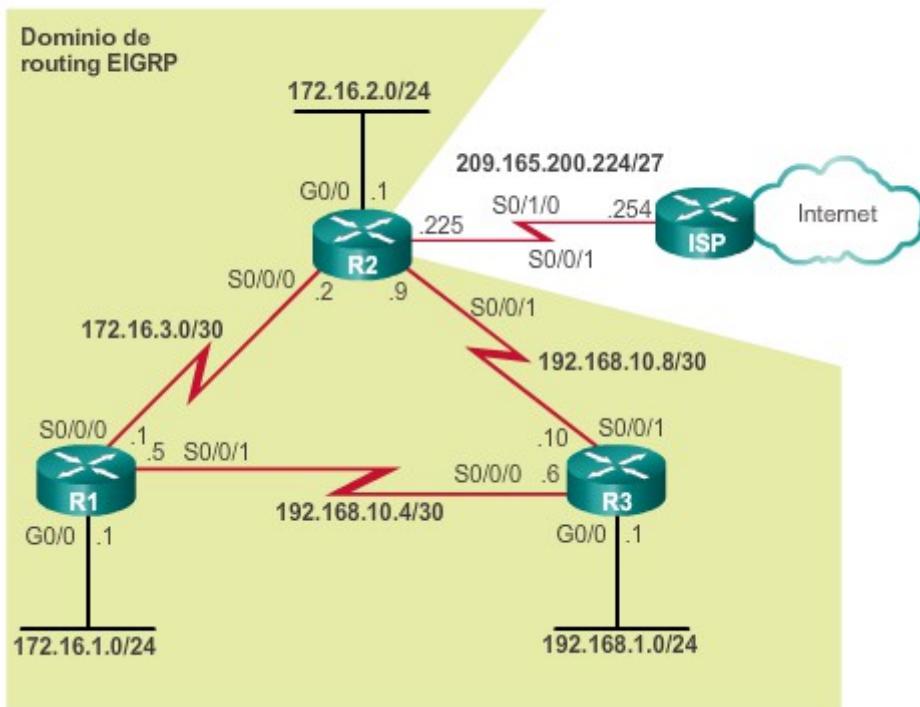
En este ejemplo, **1** identifica este proceso EIGRP en particular, que está en ejecución en el router. Para establecer adyacencias de vecinos, EIGRP requiere que todos los routers en el mismo dominio de routing estén configurados con el mismo número de sistema autónomo. En la figura 3, se habilita el mismo EIGRP en los tres routers mediante el uso del mismo número de sistema autónomo **1**.

**Nota:** EIGRP y OSPF pueden admitir varias instancias de cada protocolo de routing, si bien este tipo de implementación de varios protocolos de routing generalmente no es necesario o recomendado.

El comando **router eigrp sistema-autónomo** no inicia el proceso EIGRP propiamente dicho; el router no comienza a enviar actualizaciones. En cambio, este comando solo proporciona acceso para configurar los parámetros EIGRP.

Para eliminar completamente el proceso de routing EIGRP de un dispositivo, utilice el comando **no router eigrp sistema-autónomo** del modo de configuración global, que detiene el proceso EIGRP y elimina todas las configuraciones de router EIGRP.

## Topología EIGRP para IPv4



Comando de configuración router

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router ?
  bgp      Border Gateway Protocol (BGP)
  eigrp    Enhanced Interior Gateway Routing Protocol (EIGRP)
  isis     ISO IS-IS
  iso-igrp IGRP for OSI networks
  mobile   Mobile routes
  odr      On Demand stub Routes
  ospf    Open Shortest Path First (OSPF)
  ospfv3  OSPFv3
  rip     Routing Information Protocol (RIP)

R1(config)# router
```

### Comando de configuración router en el R1, el R2 y el R3

```
R1(config)# router eigrp 1  
R1(config-router)#{
```

```
R2(config)# router eigrp 1  
R2(config-router)#{
```

```
R3(config)# router eigrp 1  
R3(config-router)#{
```

### Capítulo 7: EIGRP 7.2.1.4 Id. de router EIGRP

#### Determinación del ID del router

La ID de router EIGRP se utiliza para identificar de forma única a cada router en el dominio de routing EIGRP. La ID del router se utiliza en los protocolos de routing EIGRP y OSPF, si bien la función de esta ID del router es más importante en OSPF.

En las implementaciones de IPv4 EIGRP, el uso de la ID del router no es tan evidente. EIGRP para IPv4 utiliza la ID de router de 32 bits para identificar el router de origen para la redistribución de rutas externas. La necesidad de una ID de router es más evidente en el análisis de EIGRP para IPv6. Mientras que la ID del router es necesaria para la redistribución, los detalles de la redistribución de EIGRP exceden el ámbito de este currículo. Para la finalidad de este currículo, solo es necesario comprender qué es la ID del router y como se deriva.

Los routers Cisco derivan la ID del router sobre la base de tres criterios, en el siguiente orden de prioridad:

1. Se utiliza la dirección IPv4 configurada con el comando **eigrp router-id** del modo de configuración del router.
2. Si la ID del router no está configurada, el router elige la dirección IPv4 más alta de cualquiera de sus interfaces loopback.
3. Si no se configuró ninguna interfaz loopback, el router elige la dirección IPv4 activa más alta de cualquiera de sus interfaces físicas.

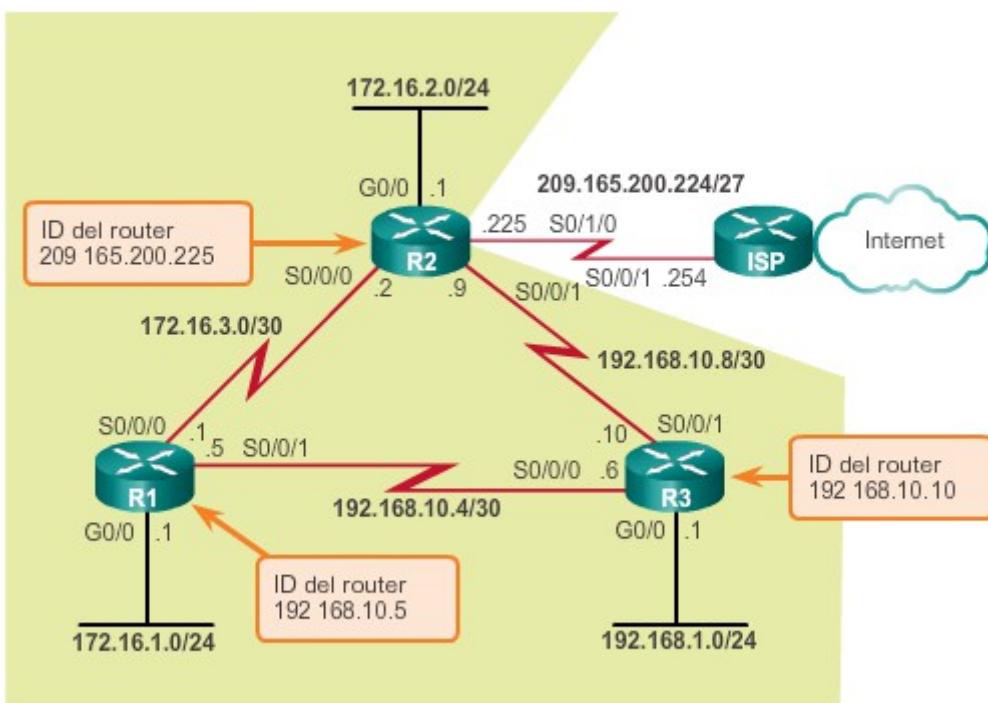
Si el administrador de red no configura explícitamente una ID de router mediante el uso del comando **eigrp router id**, EIGRP genera su propia ID de router a partir de una dirección loopback o una dirección IPv4 física. Una dirección de loopback es una interfaz virtual y se encuentra en estado up de manera automática cuando está configurada. No es necesario que la interfaz esté habilitada para EIGRP, lo que significa que no se necesita que esté incluida en

uno de los comandos `network` de EIGRP. Sin embargo, la interfaz debe estar en el estado `up/up`.

Según el criterio descrito anteriormente, en la ilustración se muestran las ID de router EIGRP predeterminadas, que se determinan sobre la base de la dirección IPv4 activa más alta de los routers.

**Nota:** el comando `eigrp router-id` se utiliza para configurar la ID del router para EIGRP. Algunas versiones del IOS aceptan el comando `router-id`, sin tener que especificar `eigrp` primero. Sin embargo, la configuración en ejecución muestra `eigrp router-id`, independientemente de cuál sea el comando que se utiliza.

### Topología con ID de router EIGRP predeterminadas



### Capítulo 7: EIGRP 7.2.1.5 Configuración de la ID del router EIGRP

#### `eigrp router-id` (comando)

El comando `eigrp router-id` se usa para configurar la ID del router EIGRP y tiene prioridad sobre cualquier dirección de loopback o dirección IPv4 de interfaz física. La sintaxis del comando es:

```
Router(config)# router eigrpsistema-autónomo
```

```
Router(config-router)# eigrp router-id dirección-ipv4
```

**Nota:** la dirección IPv4 utilizada para indicar la ID del router es en realidad cualquier número de 32 bits que se muestre en notación decimal con puntos.

La ID del router se puede configurar con cualquier dirección IPv4, con dos excepciones: 0.0.0.0 y 255.255.255.255. La ID del router debe ser un número único de 32 bits en el dominio de routing EIGRP; de lo contrario, pueden ocurrir incongruencias de routing.

En la figura 1, se muestra la configuración de la ID de router EIGRP para los routers R1 y R2 mediante el uso del comando **router eigrp sistema-autónomo**.

#### Uso de la dirección de loopback como ID del router

Otra opción para especificar la ID del router EIGRP es usar una dirección de loopback IPv4. La ventaja de usar una interfaz loopback en lugar de la dirección IPv4 de una interfaz física es que, a diferencia de las interfaces físicas, 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, usar una dirección de loopback como ID del router puede proporcionar una ID de router más coherente que usar una dirección de interfaz.

Si no se utiliza el comando **eigrp router-id** y hay interfaces loopback configuradas, EIGRP elige la dirección IPv4 más alta de cualquiera de las interfaces loopback. Los siguientes comandos se utilizan para habilitar y configurar una interfaz loopback:

```
Router(config)# interface loopback número
```

```
Router(config-if)# ip address dirección-ipv4 máscara-subred
```

**Nota:** la ID de router EIGRP no cambia, salvo que se elimine el proceso EIGRP con el comando **no router eigrp** o que la ID del router se configure manualmente con el comando **eigrp router-id**.

#### Verificación del proceso EIGRP

En la figura 2, se muestra el resultado **deshow ip protocols** para el R1, incluida la ID del router. El comando **show ip protocols** muestra los parámetros y el estado actual de cualquier proceso de protocolo de routing activo, incluidos EIGRP y OSPF. El comando **show ip protocols** muestra distintos tipos de resultados específicos de cada protocolo de routing.

Utilice el verificador de sintaxis de la figura 3 para configurar y verificar la ID del router para el R3.

#### Configuración de la ID de router en el R1 y el R2

```
R1(config)# router eigrp 1
R1(config-router)# eigrp router-id 1.1.1.1
R1(config-router)#

```

```
R2(config)# router eigrp 1
R2(config-router)# eigrp router-id 2.2.2.2
R2(config-router)#

```

## Verificación de la ID del router en el R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

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-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
      Topology : 0 (base)
        Active Timer: 3 min
        Distance: internal 90 external 170
        Maximum path: 4
        Maximum hopcount 100
        Maximum metric variance 1

    Automatic Summarization: disabled
    Maximum path: 4
    Routing for Networks:
    Routing Information Sources:
      Gateway          Distance      Last Update
      Distance: internal 90 external 170

R1#
```

## Configuración de la ID del router EIGRP

Ingrese al modo de configuración del router EIGRP usando 1 como el número de AS.

```
R3 (config)# router eigrp 1
Configure la ID 3.3.3.3 del router EIGRP y regrese al modo EXEC privilegiado.
R3 (config-router)# eigrp router-id 3.3.3.3
R3 (config-router)# end
Utilice el comando show adecuado para mostrar los parámetros de EIGRP,
incluida la ID del router.
R3# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 1"
<resultado omitido>
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 3.3.3.3
      Topology : 0 (base)
        Active Timer: 3 min
        Distance: internal 90 external 170
<resultado omitido>
Configuró correctamente la ID del router EIGRP.
```

El modo de configuración del router EIGRP permite la configuración del protocolo de routing EIGRP. En la figura 1, se muestra que el R1, el R2, y el R3 tienen redes que deberían estar incluidas dentro de un único dominio de routing EIGRP. Para habilitar un routing EIGRP en una interfaz, utilice el comando **network** del modo de configuración del router e introduzca la dirección de red con clase para cada red conectada directamente.

El comando **network** tiene la misma función que en todos los protocolos de routing IGP. Con el comando **network** en EIGRP:

- Se habilita cualquier interfaz en el router que coincida con la dirección de red en el comando **network** del modo de configuración del router para enviar y recibir actualizaciones de EIGRP.
- Se incluye la red de las interfaces en las actualizaciones de routing EIGRP.

```
Router(config-router)# network dirección de red ipv4
```

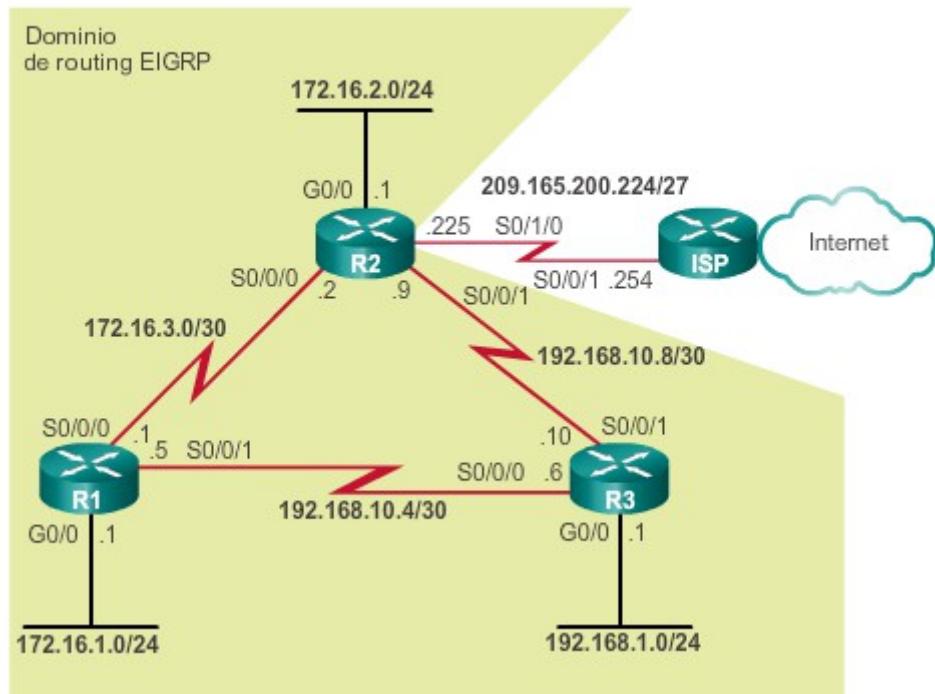
El argumento *dirección de red ipv4* es la dirección de red IPv4 con clase para esta interfaz. En la figura 2, se muestran los comandos network configurados para el R1. En la ilustración, se utiliza una única instrucción **network** con clase (**network 172.16.0.0**) en el R1 para incluir ambas interfaces en las subredes 172.16.1.0/24 y 172.16.3.0/30. Observe que solo se utiliza la dirección de red con clase.

En la figura 3, se muestra el uso del comando **network** para habilitar EIGRP en las interfaces del R2 para las subredes 172.16.1.0/24 y 172.16.2.0/24. Cuando se configura EIGRP en la interfaz S0/0/0 del R2, DUAL envía un mensaje de notificación a la consola que indica que se estableció una adyacencia de vecino con otro router EIGRP en esa interfaz. Esta nueva adyacencia se produce automáticamente, porque el R1 y el R2 usan el mismo número de sistema autónomo **eigrp 1** y ambos routers envían ahora actualizaciones en sus interfaces en la red 172.16.0.0.

El comando **eigrp log-neighbor-changes** del modo de configuración del router está habilitado de manera predeterminada. Este comando se utiliza para lo siguiente:

- Mostrar cualquier cambio en las adyacencias de vecinos EIGRP.
- Ayudar a verificar adyacencias de vecinos durante la configuración de EIGRP.
- Avisar al administrador de red cuando se elimine cualquier adyacencia EIGRP.

## Topología EIGRP para IPv4



### Comandos network de EIGRP para el R1

Habilita EIGRP para las interfaces en las subredes en 172.16.1.0/24 y 172.16.3.0/30.

```
R1(config)# router eigrp 1
R1(config-router)# network 172.16.0.0
R1(config-router)# network 192.168.10.0
R1(config-router)#

```

Habilita EIGRP para las interfaces en la subred 192.168.10.4/30.

### Comando network de EIGRP para el R2

```
R2(config)# router eigrp 1
R2(config-router)# network 172.16.0.0
R2(config-router)#
*Feb 28 17:51:42.543: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1:
Neighbor 172.16.3.1 (Serial0/0/0) is up: new adjacency
R2(config-router)#

```

#### Capítulo 7: EIGRP 7.2.1.7 El comando network y la máscara wildcard

De manera predeterminada, cuando se usan el comando **network** y una dirección de red IPv4, como 172.16.0.0, todas las interfaces en el router que pertenecen a esa dirección de red con clase se habilitan 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. Por ejemplo, en la figura 1, suponga que un administrador desea habilitar EIGRP en el R2, pero solo para la subred 192.168.10.8 255.255.255.252, en la interfaz S0/0/1.

Para configurar EIGRP para que anuncie únicamente subredes específicas, utilice la opción *máscara-wildcard* con el comando **network**:

```
Router(config-router)# networkdirección de red [máscara-wildcard]
```

Piense en la máscara wildcard como 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 el valor inverso de la máscara de subred, reste la máscara de subred de 255.255.255.255 de la siguiente manera:

255.255.255.255

- 255.255.255.252

-----

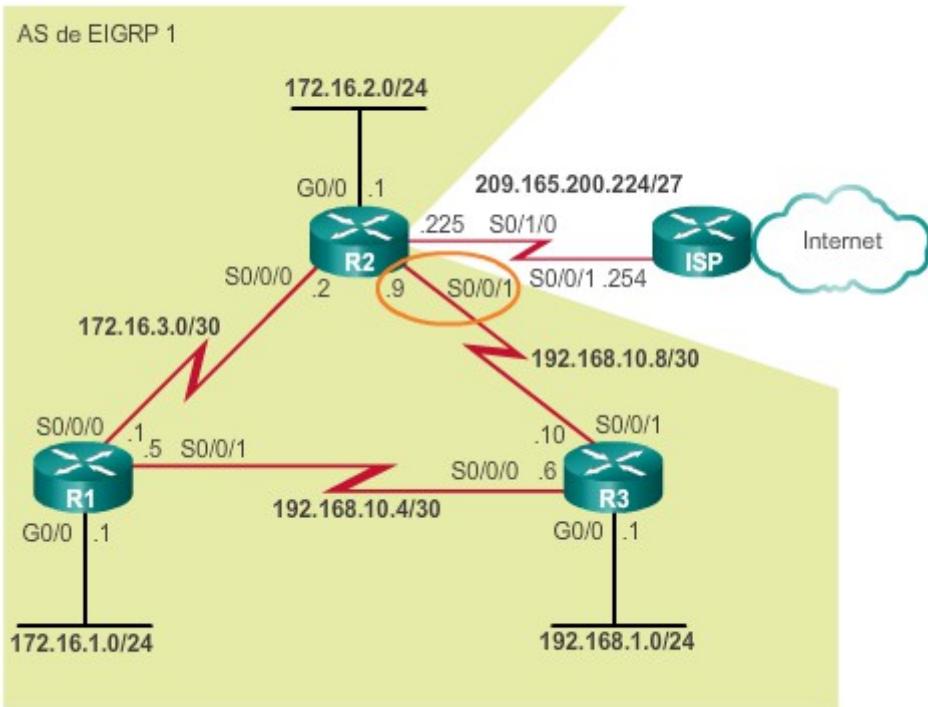
0. 0. 0. 3máscara wildcard

En la figura 2, continúa la configuración de red EIGRP del R2. El comando **network 192.168.10.8 0.0.0.3** habilita específicamente EIGRP en la interfaz S0/0/1, un miembro de la subred 192.168.10.8 255.255.255.252.

Algunas versiones de IOS también le permiten introducir la máscara de subred en lugar de una máscara wildcard. En la figura 3, se muestra un ejemplo de configuración de la misma interfaz S0/0/1 en el R2, solo que en este caso se utiliza una máscara de subred en el comando **network**. Sin embargo, si se utiliza la máscara de subred, el IOS convierte el comando al formato *máscara-wildcard*dentro de la configuración. Esto se verifica en el resultado de **show running-config** en la figura 3.

Utilice el verificador de sintaxis de la figura 4 para configurar los comandos**network** de EIGRP para el router R3.

## Topología EIGRP para IPv4



### Comando network con máscara wildcard

Habilita EIGRP para una interfaz específica, usando la subred 192.168.10.8/30.

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.10.8 0.0.0.3
R2(config-router)
```

## Configuración alternativa del comando network con una máscara de subred

```
R2(config)# router eigrp 1
R2(config-router)# network 192.168.10.8 255.255.255.252
R2(config-router)# end
R2# show running-config | section eigrp 1
router eigrp 1
  network 172.16.0.0
  network 192.168.10.8 0.0.0.3
    eigrp router-id 2.2.2.2
R2#
```

## Configuración del comando network y la máscara wildcard

Configure R3 para que permita EIGRP en todas las interfaces en el siguiente orden:

- Ingrese el modo de configuración del router mediante AS 1
- Habilite EIGRP para la red 192.168.1.0/24 de R3 sin usar una máscara wildcard
- Habilite EIGRP para la red 192.168.10.4.30/24 de R3 mediante una máscara wildcard
- Habilite EIGRP para la red 192.168.10.8.30/24 de R3 mediante una máscara wildcard

```
R3(config)# router eigrp 1
R3(config-router)# network 192.168.1.0
R3(config-router)# network 192.168.10.4 0.0.0.3
*Feb 28 20:47:22.695: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.5 (Serial0/0/0) is up: new adjacency
R3(config-router)# network 192.168.10.8 0.0.0.3
*Feb 28 20:47:06.555: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.9 (Serial0/0/1) is up: new
R3(config-router)#
Ha configurado satisfactoriamente el comando network y la máscara wildcard.
```

## Capítulo 7: EIGRP 7.2.1.8 Interfaz pasiva

Tan pronto como se habilita una nueva interfaz dentro de la red EIGRP, EIGRP intenta formar una adyacencia de vecino con cualquier router vecino para enviar y recibir actualizaciones de EIGRP.

Cada tanto puede ser necesario, o ventajoso, incluir una red conectada directamente en la actualización de routing EIGRP, pero no permitir que se forme ninguna adyacencia de vecino fuera de esa interfaz. El comando **passive-interface** se puede utilizar para evitar que se formen adyacencias de vecino. Existen dos razones principales para habilitar el comando **passive-interface**:

- Para suprimir tráfico de actualización innecesario, por ejemplo, cuando una interfaz es una interfaz LAN, sin otros routers conectados
- Para aumentar los controles de seguridad, por ejemplo, para evitar que dispositivos desconocidos de routing no autorizados reciban actualizaciones de EIGRP

En la figura 1, se muestra que el R1, el R2 y el R3 no tienen vecinos en sus interfaces GigabitEthernet 0/0.

El comando **passive-interface** del modo de configuración del router inhabilita la transmisión y recepción de paquetes de saludo EIGRP en estas interfaces.

```
Router(config)# router eigrp número-as
```

```
Router(config-router)# passive-interface tipo-interfaz número-interfaz
```

En la figura 2, se muestra el comando **passive-interface** configurado para suprimir los paquetes de saludo en las LAN para el R1 y el R3. El R2 se configura mediante el verificador de sintaxis.

Sin una adyacencia de vecino, EIGRP no puede intercambiar rutas con un vecino. Por lo tanto, el comando **passive-interface** evita el intercambio de rutas en la interfaz. Si bien EIGRP no envía ni recibe actualizaciones de routing mediante una interfaz configurada con el comando **passive-interface**, sí incluye la dirección de la interfaz en las actualizaciones de routing enviadas por otras interfaces no pasivas.

**Nota:** para configurar todas las interfaces como pasivas, utilice el comando **passive-interface default**. Para deshabilitar una interfaz como pasiva, utilice el comando **no passive-interface tipo-interfaz número-interfaz**.

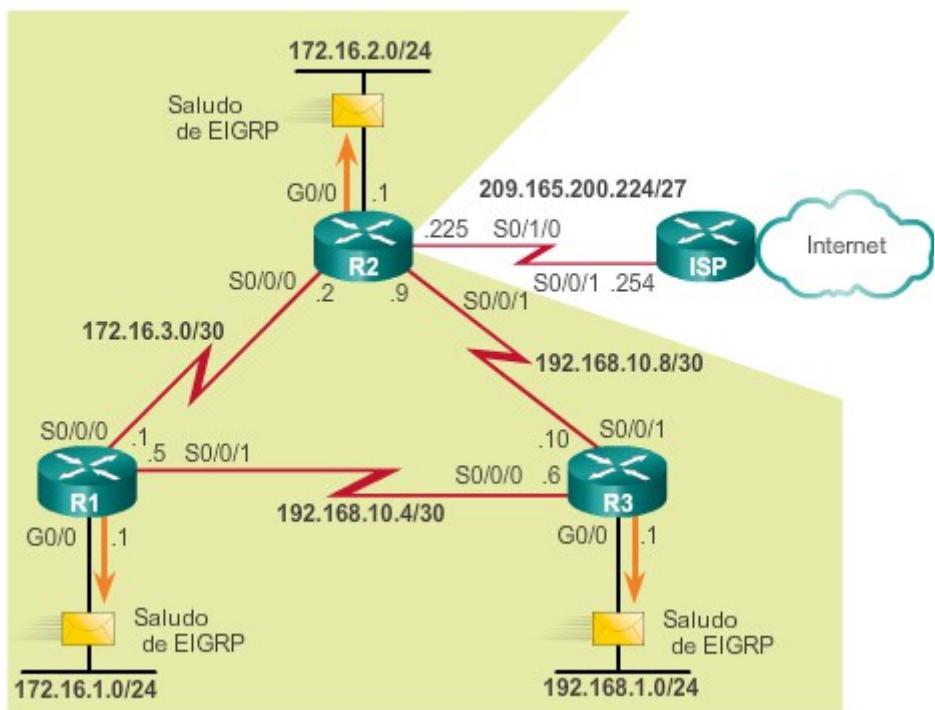
Un ejemplo del uso de la interfaz pasiva para aumentar los controles de seguridad es cuando una red se debe conectar a una organización externa, sobre la cual el administrador local no tiene ningún control, como cuando se conecta a una red ISP. En este caso, el administrador de red local necesitará anunciar el enlace de la interfaz a través de su propia red, pero no querrá que la organización externa reciba actualizaciones de routing del dispositivo local de routing, ni las envíe a dicho dispositivo, ya que esto es un riesgo de seguridad.

### Verificación de la interfaz pasiva

Para verificar si cualquier interfaz en un router está configurada como pasiva, utilice el comando **show ip protocols** del modo EXEC privilegiado, como se muestra en la figura 3. Observe que, si bien la interfaz GigabitEthernet 0/0 del R3 es una interfaz pasiva, EIGRP aún incluye la dirección de red de la interfaz de la red 192.168.1.0 en sus actualizaciones de routing.

Utilice el verificador de sintaxis de la figura 4 para configurar el R2 a fin de que suprima los paquetes de saludo EIGRP en su interfaz GigabitEthernet 0/0.

### Topología EIGRP para IPv4



## Configuración de interfaces pasivas con EIGRP para IPv4

```
R1(config)# router eigrp 1
R1(config-router)# passive-interface gigabitethernet 0/0
```

```
R3(config)# router eigrp 1
R3(config-router)# passive-interface gigabitethernet 0/0
```

## Verificación de la interfaz pasiva con EIGRP para IPv4

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
<resultado omitido>
Routing for Networks:
  192.168.1.0
  192.168.10.4/30
  192.168.10.8/30
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway          Distance      Last Update
    192.168.10.5      90          01:37:57
    192.168.10.9      90          01:37:57
  Distance: internal 90 external 170
R3#
```

## Interfaz EIGRP pasiva

Configure el R2 para que suprima los paquetes de saludo EIGRP en su interfaz GigabitEthernet 0/0 mientras sigue anunciando esa red en las actualizaciones de EIGRP.

Realice las tareas en el siguiente orden:

- Ingrese al modo de configuración del router usando 1 como AS.
- Configure la interfaz pasiva.
- Regrese al modo EXEC privilegiado.
- Verifique la interfaz pasiva mediante el análisis de la información del protocolo.

```
R2(config)# router eigrp 1
R2(config-router)# passive-interface gigabitethernet 0/0
R2(config-router)# end
R2# show ip protocols
*** IP Routing is NSF aware ***

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
  Redistributing: static
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 2.2.2.2
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.8/30
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    192.168.10.10      90          02:14:28
    172.16.3.1         90          02:14:28
  Distance: internal 90 external 170

R2#
```

Configuró correctamente la interfaz EIGRP pasiva.

### Capítulo 7: EIGRP 7.2.2.1 Verificación de EIGRP: análisis de vecinos

Antes de que EIGRP pueda enviar o recibir 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. Para cada router, debe poder ver la

dirección IPv4 del router adyacente y la interfaz que ese router utiliza para llegar a ese vecino EIGRP. Con esta topología, cada router tiene dos vecinos incluidos en la tabla de vecinos.

El resultado del comando **show ip eigrp neighbors** incluye lo siguiente:

- **Columna H:** enumera los vecinos en el orden en que fueron descubiertos.
- **Address:** dirección IPv4 del vecino.
- **Interface:** la interfaz local en la cual se recibió este paquete de saludo.
- **Hold:** el tiempo de espera actual. Cuando se recibe un paquete de saludo, este valor se restablece al tiempo de espera máximo para esa interfaz y, luego, se realiza una cuenta regresiva hasta cero. Si se llega a cero, el vecino se considera inactivo.
- **Uptime:** la cantidad de tiempo desde que se agregó este vecino a la tabla de vecinos.
- **SRTT y RTO (tiempo de ida y vuelta promedio y tiempo de espera de retransmisión):** utilizados por RTP para administrar paquetes EIGRP confiables.
- **Q Cnt (conteo de cola):** siempre debe ser cero. Si es más que cero, hay paquetes EIGRP que esperan ser enviados.
- **Seq Num (número de secuencia):** se utiliza para rastrear paquetes de actualización, de consulta y de respuesta.

El comando **show ip eigrp neighbors** es muy útil para verificar y resolver problemas de EIGRP. Si un vecino no está incluido después de establecer adyacencias con los vecinos de un router, revise la interfaz local para asegurarse de que esté activa con el comando **show ip interface brief**. Si la interfaz está activa, intente hacer ping a la dirección IPv4 del vecino. Si el ping falla, significa que la interfaz del vecino está inactiva y debe activarse. Si el ping es exitoso y EIGRP aún no ve al router como vecino, examine las siguientes configuraciones:

- ¿Ambos routers están configurados con el mismo número de sistema autónomo de EIGRP?
- ¿La red conectada directamente está incluida en las instrucciones **network** de EIGRP?

### Comando show ip eigrp neighbors

R1# show ip eigrp neighbors								
EIGRP-IPv4 Neighbors for AS(1)		Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Seq
H							Cnt	Num
1		192.168.10.6	Se0/0/1	11	04:57:14	27	162	0 8
0		172.16.3.2	Se0/0/0	13	07:53:46	20	120	0 10

R1#

Dirección IPv4 del vecino

Interfaz local que recibe paquetes de saludo EIGRP

Segundos restantes antes de declarar que el vecino está inactivo  
El tiempo de espera actual se restablece al tiempo de espera máximo cada vez que se recibe un paquete de saludo.

Cantidad de tiempo desde que el vecino se agregó a la tabla de vecinos

### Capítulo 7: EIGRP 7.2.2.2 Verificación de EIGRP: comando show ip protocols

El comando **show ip protocols** muestra los parámetros y otra información acerca del estado actual de cualquier proceso activo de protocolo de routing IPv4 configurado en el router. El comando **show ip protocols** muestra distintos tipos de resultados específicos de cada protocolo de routing.

El resultado en la figura 1 indica varios parámetros EIGRP, incluido lo siguiente:

1. EIGRP es un protocolo de routing dinámico activo en el R1, configurado con el número de sistema autónomo 1.
2. La ID de router EIGRP del R1 es 1.1.1.1.
3. Las distancias administrativas de EIGRP en el R1 son AD interna de 90 y externa de 170 (valores predeterminados).
4. De manera predeterminada, EIGRP no resume redes automáticamente. Las subredes se incluyen en las actualizaciones de routing.
5. Las adyacencias de vecinos EIGRP que el R1 tiene con otros routers utilizados para recibir actualizaciones de routing EIGRP.

**Nota:** con anterioridad al IOS 15, la sumarización automática de EIGRP estaba habilitada de manera predeterminada.

El resultado del comando **show ip protocols** es útil para depurar operaciones de routing. La información en el campo Routing Information Sources (Orígenes de información de routing) puede ayudar a identificar a un router sospechoso de entregar información de routing defectuosa. El campo Routing Information Sources enumera todos los orígenes de routing

EIGRP que el software IOS de Cisco utiliza para armar su tabla de routing IPv4. Para cada origen, observe lo siguiente:

- Dirección IPv4
- Distancia administrativa
- Momento en que se recibió la última actualización de este origen

Como se muestra en la figura 2, EIGRP tiene una AD predeterminada de 90 para las rutas internas y de 170 para las rutas importadas de un origen externo, como las rutas predeterminadas. En comparación con otros IGP, EIGRP es el preferido por el IOS de Cisco, porque tiene la distancia administrativa más baja. EIGRP tiene un tercer valor de AD de 5, para las rutas resumidas.

#### Comando show ip protocols

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1" 1 Protocolo de routing e Id. de proceso (número de AS)
    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-IPv4 Protocol for AS(1)
        Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
        NSF-aware route hold timer is 240
        Router-ID: 1.1.1.1 2 Id. de router EIGRP
        Topology : 0 (base)
            Active Timer: 3 min
            Distance: internal 90 external 170 3 Distancias administrativas de EIGRP
            Maximum path: 4
            Maximum hopcount 100
            Maximum metric variance 1

    Automatic summarization: disabled 4 La sumarización automática de EIGRP está deshabilitada.
    Maximum path: 4
    Routing for Networks:
        172.16.0.0
        192.168.10.0
    Routing Information Sources: 5 El campo Routing information Sources de EIGRP enumera todos los orígenes de routing EIGRP que el IOS utiliza para armar su tabla de routing IPv4.
        Gateway          Distance      Last Update
        192.168.10.6      90          00:40:20
        172.16.3.2        90          00:40:20
    Distance: internal 90 external 170

R1#
```

## Distancias administrativas predeterminadas

Origen de la ruta	Distancia administrativa
Conectada	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

### Capítulo 7: EIGRP 7.2.2.3 Verificación de EIGRP: análisis de la tabla de routing IPv4

Otra manera de verificar que EIGRP y otras funciones del router estén configuradas correctamente es examinar las tablas de routing IPv4 con el comando **show ip route**. Al igual que con cualquier protocolo de routing dinámico, el administrador de red debe verificar la información en la tabla de routing para asegurarse de que esté completada como se espera, con base en las configuraciones introducidas. Por esta razón, es importante tener un buen nivel de conocimiento de los comandos de configuración del protocolo de routing, así como de las operaciones del protocolo de routing y los procesos usados por dicho protocolo para armar la tabla de routing IP.

Observe que los resultados que se utilizan en todo este curso corresponden al IOS 15 de Cisco. Con anterioridad al IOS 15, la sumarización automática de EIGRP estaba habilitada de manera predeterminada. El estado de la sumarización automática puede hacer una diferencia en la información que se muestra en la tabla de routing IPv4. Si se usa una versión anterior del IOS, se puede deshabilitar la sumarización automática mediante el comando **no auto-summary** del modo de configuración del router:

```
Router(config-router)# no auto-summary
```

En la figura 1, se muestra la topología del R1, el R2 y el R3.

En la figura 2, la tabla de routing IPv4 se examina mediante el comando **show ip route**. Las rutas EIGRP se indican en la tabla de routing con una **D**. Se usó la letra “D” para representar a EIGRP porque el protocolo se basa en algoritmo DUAL.

El comando **show ip route** verifica que las rutas recibidas por los vecinos EIGRP estén instaladas en la tabla de routing IPv4. El comando **show ip route** muestra la tabla de routing completa, incluidas las redes remotas descubiertas de manera dinámica, las rutas conectadas directamente y las rutas estáticas. Por esta razón, generalmente es el primer comando que se utiliza para verificar la convergencia. Una vez que el routing se configura correctamente en

todos los routers, el comando **show ip route** muestra que cada router tiene una tabla de routing completa, con una ruta a cada red en la topología.

Observe que en el R1 se instalaron rutas a tres redes IPv4 remotas en su tabla de routing IPv4:

- La red 172.16.2.0/24, recibida del router R2 en la interfaz Serial0/0/0
- La red 192.168.1.0/24, recibida del router R2 en la interfaz Serial0/0/1
- La red 192.168.10.8/30, recibida del R2 en la interfaz Serial0/0/0 y del R3 en la interfaz Serial0/0/1

El R1 tiene dos rutas hacia la red 192.168.10.8/30, porque su costo o métrica para llegar a esa red es la misma al utilizar ambos routers. Estas se conocen como “rutas del mismo costo”. El R1 utiliza ambas rutas para llegar a esta red, lo que se conoce como “balanceo de carga”. La métrica de EIGRP se analiza más adelante en este capítulo.

En la figura 3, se muestra la tabla de routing del R2. Observe que se muestran resultados similares, incluida una ruta del mismo costo para la red 192.168.10.4/30.

En la figura 4, se muestra la tabla de routing del R3. De manera similar a los resultados para el R1 y el R2, las redes remotas se descubren mediante EIGRP, incluida una ruta del mismo costo para la red 172.16.3.0/30.

### Topología EIGRP para IPv4

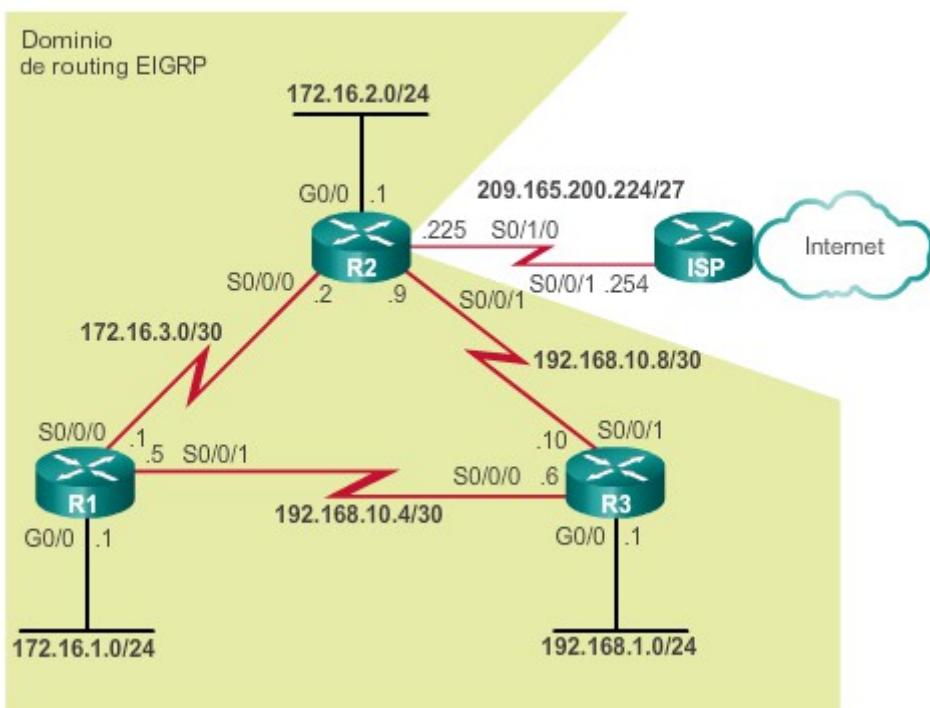


Tabla de routing IPv4 del R1

```

R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
<resultado omitido>
Gateway of last resort is not set

  172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
C    172.16.1.0/24 is directly connected, GigabitEthernet0/0
L    172.16.1.1/32 is directly connected, GigabitEthernet0/0
D    172.16.2.0/24 [90/2170112] via 172.16.3.2, 00:14:35, Serial0/0/0
C    172.16.3.0/30 is directly connected, serial0/0/0
L    172.16.3.1/32 is directly connected, serial0/0/0
D 192.168.1.0/24 [90/2170112] via 192.168.10.6, 00:13:57, Serial0/0/1
  192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
C    192.168.10.4/30 is directly connected, Serial0/0/1
L    192.168.10.5/32 is directly connected, Serial0/0/1
D  192.168.10.8/30 [90/2681856] via 192.168.10.6, 00:50:42, Serial0/0/1
     [90/2681856] via 172.16.3.2, 00:50:42, Serial0/0/0
R1#
    
```

### Tabla de routing IPv4 del R2

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
<resultado omitido>
Gateway of last resort is not set

  172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D  172.16.1.0/24 [90/2170112] via 172.16.3.1, 00:11:05, Serial0/0/0
C  172.16.2.0/24 is directly connected, GigabitEthernet0/0
L  172.16.2.1/32 is directly connected, GigabitEthernet0/0
C  172.16.3.0/30 is directly connected, Serial0/0/0
L  172.16.3.2/32 is directly connected, Serial0/0/0
D  192.168.1.0/24 [90/2170112] via 192.168.10.10, 00:15:16, Serial0/0/1
  192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D  192.168.10.4/30 [90/2681856] via 192.168.10.10, 00:52:00, Serial0/0/1
    [90/2681856] via 172.16.3.1, 00:52:00, Serial0/0/0
C  192.168.10.8/30 is directly connected, Serial0/0/1
L  192.168.10.9/32 is directly connected, Serial0/0/1
  209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C  209.165.200.224/27 is directly connected, Loopback209
L  209.165.200.225/32 is directly connected, Loopback209
R2#
```

### Tabla de routing IPv4 del R3

```
R3# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
<resultado omitido>
Gateway of last resort is not set

  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D  172.16.1.0/24 [90/2170112] via 192.168.10.5, 00:12:00, Serial0/0/0
D  172.16.2.0/24 [90/2170112] via 192.168.10.9, 00:16:49, Serial0/0/1
D  172.16.3.0/30 [90/2681856] via 192.168.10.9, 00:52:55, Serial0/0/1
    [90/2681856] via 192.168.10.5, 00:52:55, Serial0/0/0
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C  192.168.1.0/24 is directly connected, GigabitEthernet0/0
L  192.168.1.1/32 is directly connected, GigabitEthernet0/0
  192.168.10.0/24 is variably subnetted, 4 subnets, 2 masks
C  192.168.10.4/30 is directly connected, Serial0/0/0
L  192.168.10.6/32 is directly connected, Serial0/0/0
C  192.168.10.8/30 is directly connected, Serial0/0/1
L  192.168.10.10/32 is directly connected, Serial0/0/1
R3#
```

En esta actividad, implementará la configuración de EIGRP básico, incluidos los comandos **network**, las interfaces pasivas y la deshabilitación de la sumarización automática. A continuación, verificará la configuración EIGRP mediante una variedad de comandos **show** y la prueba de conectividad de extremo a extremo.

[Packet Tracer: Configuración de EIGRP básico con IPv4 \(instrucciones\)](#)

[Packet Tracer: Configuración de EIGRP básico con IPv4 \(PKA\)](#)

#### Capítulo 7: EIGRP 7.2.2.5 Práctica de laboratorio: Configuración de EIGRP básico con IPv4

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y verificar la conectividad
- Parte 2: configurar el routing EIGRP
- Parte 3: Verificar el routing EIGRP
- Parte 4: Configurar el ancho de banda y las interfaces pasivas

[Práctica de laboratorio: Configuración de EIGRP básico para IPv4](#)

#### Capítulo 7: EIGRP 7.3.1.1 Adyacencia de vecinos EIGRP

El objetivo de cualquier protocolo de routing dinámico es descubrir redes remotas de otros routers y lograr la convergencia en el dominio de routing. Antes de que se pueda intercambiar cualquier paquete de actualización EIGRP entre routers, EIGRP debe descubrir a sus vecinos. Los EIGRP vecinos son otros routers que ejecutan EIGRP en redes conectadas directamente.

EIGRP utiliza paquetes de saludo para establecer y mantener las adyacencias de vecinos. Para que dos routers EIGRP se conviertan en vecinos, deben coincidir varios parámetros entre ambos. Por ejemplo, dos routers EIGRP deben usar los mismos parámetros de métrica de EIGRP y ambos deben estar configurados con el mismo número de sistema autónomo.

Cada router EIGRP mantiene una tabla de vecinos, que contiene una lista de los routers en los enlaces compartidos que tienen una adyacencia EIGRP con ese router. La tabla de vecinos se usa para rastrear el estado de estos vecinos EIGRP.

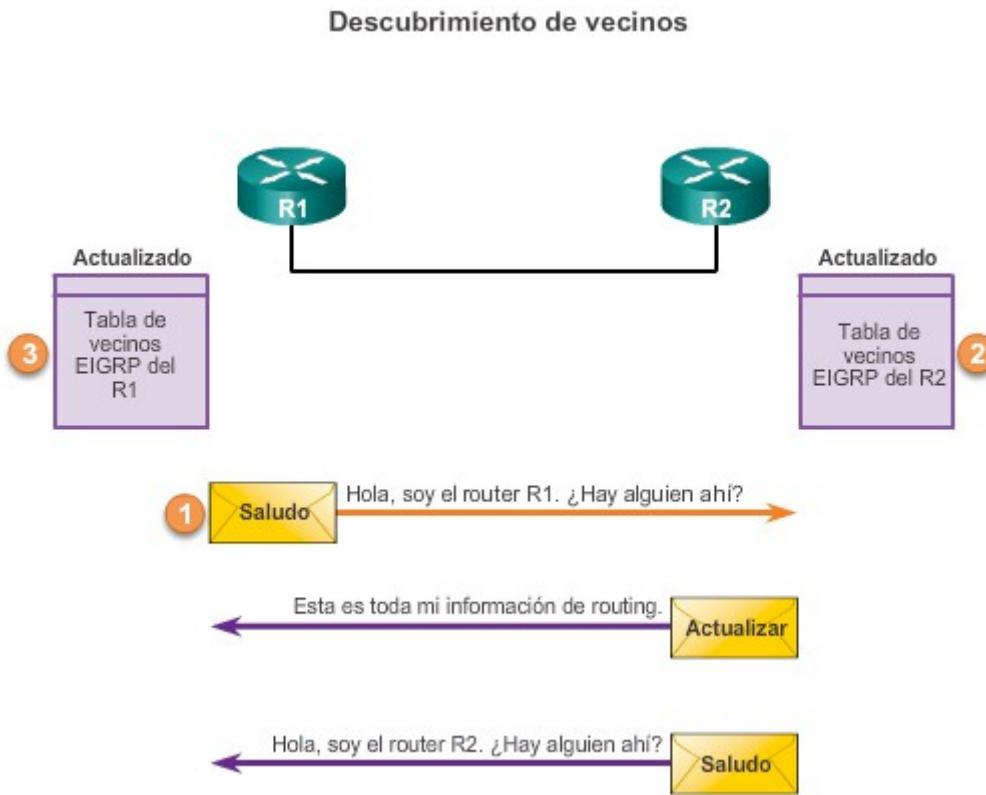
En la ilustración se muestran dos routers EIGRP que intercambian paquetes de saludo EIGRP iniciales. Cuando un router con EIGRP habilitado recibe un paquete de saludo en una interfaz, agrega a ese router a su tabla de vecinos.

1. Un nuevo router (R1) aparece en el enlace y envía un paquete de saludo EIGRP a través de todas sus interfaces EIGRP configuradas.

2. El router R2 recibe el paquete de saludo en una interfaz con EIGRP habilitado. El R2 responde con un paquete de actualización EIGRP que contiene todas las rutas incluidas en su tabla de routing, excepto aquellas descubiertas por medio de esa interfaz (horizonte dividido).

Sin embargo, la adyacencia de vecino no se establece hasta que el R2 también envía un paquete de saludo EIGRP al R1.

3. Una vez que ambos routers intercambian saludos, se establece la adyacencia de vecino. El R1 y el R2 actualizan sus tablas de vecinos EIGRP y agregan el router adyacente como vecino.



#### Capítulo 7: EIGRP 7.3.1.2 Tabla de topología de EIGRP

Las actualizaciones de EIGRP contienen redes a las que se puede llegar desde el router que envía la actualización. A medida que se intercambian actualizaciones EIGRP entre vecinos, el router receptor agrega esas entradas a su tabla de topología de EIGRP.

Cada router EIGRP mantiene una tabla de topología para cada protocolo de routing configurado, como IPv4 e IPv6. La tabla de topología incluye las entradas de ruta para cada destino que el router descubre de sus vecinos EIGRP conectados directamente.

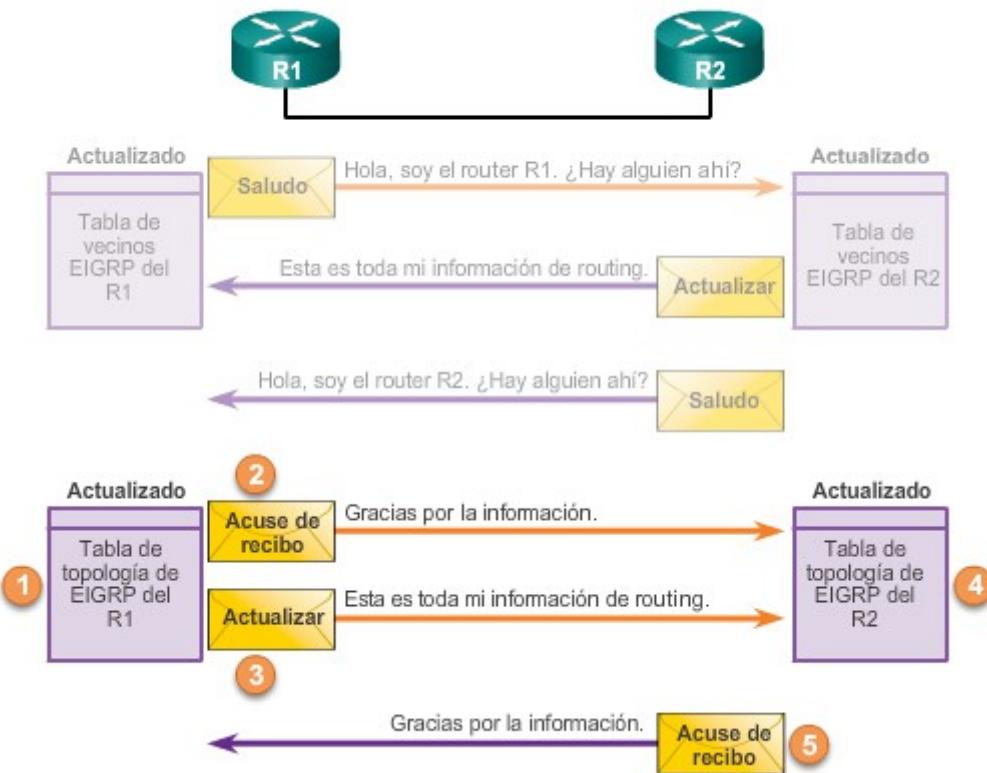
En la ilustración, se muestra la continuación del proceso inicial de descubrimiento de rutas de la página anterior. Ahora, se muestra la actualización de la tabla de topología.

Cuando un router recibe una actualización de routing EIGRP, agrega la información de routing a su tabla de topología de EIGRP y responde con un acuse de recibo EIGRP.

1. El R1 recibe la actualización de EIGRP del vecino R2 e incluye información acerca de las rutas que anuncia el vecino, incluida la métrica a cada destino. El R1 agrega todas las entradas de actualización a su tabla de topología. La tabla de topología incluye todos los destinos anunciados por los routers vecinos (adyacentes) y el costo (métrica) para llegar a cada red.

2. Los paquetes de actualización EIGRP utilizan entrega confiable; por lo tanto, el R1 responde con un paquete de acuse de recibo EIGRP que informa al R2 que recibió la actualización.
3. El R1 envía una actualización de EIGRP al R2 en la que anuncia las redes que conoce, excepto aquellas descubiertas del R2 (horizonte dividido).
4. El R2 recibe la actualización de EIGRP del vecino R1 y agrega esta información a su propia tabla de topología.
5. El R2 responde al paquete de actualización EIGRP del R1 con un acuse de recibo EIGRP.

### Intercambio de actualizaciones de routing

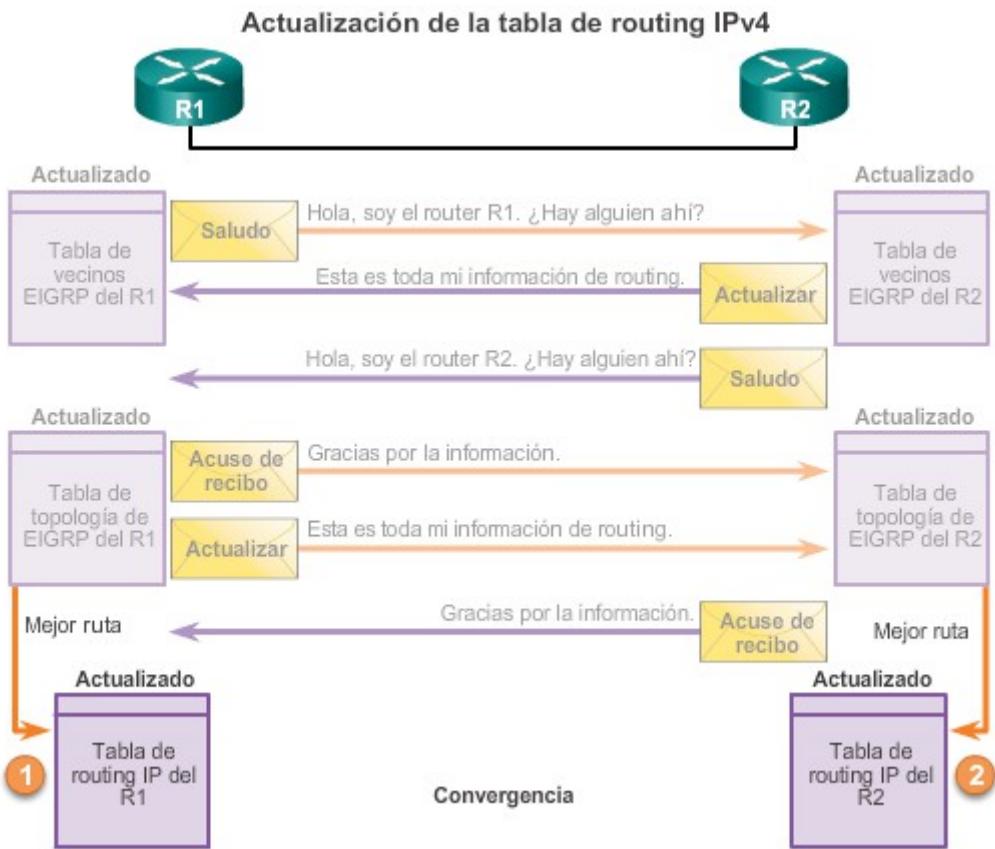


### Capítulo 7: EIGRP 7.3.1.3 Convergencia de EIGRP

En la ilustración, se muestran los últimos pasos del proceso inicial de descubrimiento de rutas.

1. Después de recibir los paquetes de actualización EIGRP del R2, el R1 utiliza la información en la tabla de topología para actualizar su tabla de routing IP con la mejor ruta a cada destino, incluidos la métrica y el router del siguiente salto.
2. De la misma manera que el R1, el R2 actualiza su tabla de routing IP con las mejores rutas a cada red.

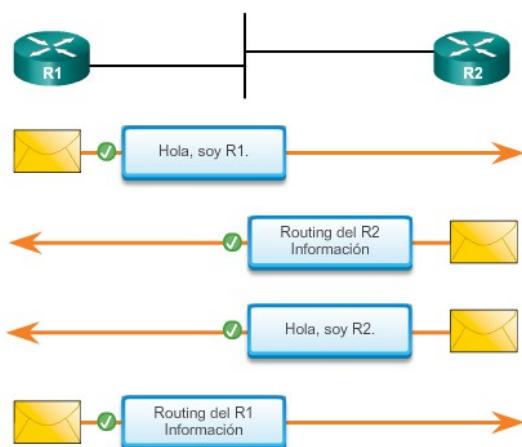
Llegado a este punto, se considera que EIGRP está en estado convergente en ambos routers.



#### Capítulo 7: EIGRP 7.3.1.4 Actividad: Identificar los pasos para establecer adyacencias de vecinos EIGRP

Actividad: Identificar los pasos para establecer adyacencias de vecinos EIGRP

El router 1 (R1) y el router 2 (R2) establecen adyacencias de vecinos. Ordene los mensajes EIGRP arrastrándolos a los campos correctos proporcionados.



#### Capítulo 7: EIGRP 7.3.2.1 Métrica compuesta de EIGRP

De manera predeterminada, EIGRP utiliza los siguientes valores en su métrica compuesta para calcular la ruta preferida a una red:

- **Ancho de banda:** el ancho de banda más lento entre todas las interfaces de salida, a lo largo de la ruta de origen a destino.
- **Retraso:** la acumulación (suma) de todos los retrasos de las interfaces a lo largo de la ruta (en decenas de microsegundos).

Se pueden utilizar los valores siguientes, pero no se recomienda, porque generalmente dan como resultado recálculos frecuentes de la tabla de topología:

- **Confiabilidad:** representa la peor confiabilidad entre origen y destino, que se basa en keepalives.
- **Carga:** representa la peor carga en un enlace entre origen y destino, que se calcula sobre la base de la velocidad de paquetes y el ancho de banda configurado de la interfaz.

**Nota:** si bien la MTU se incluye en las actualizaciones de la tabla de routing, no es una métrica de routing utilizada por EIGRP.

### La métrica compuesta

En la figura 1, se muestra la fórmula de métrica compuesta que utiliza EIGRP. La fórmula consiste en los valores K1 a K5, conocidos como “ponderaciones de la métrica de EIGRP”. K1 y K3 representan el ancho de banda y el retraso, respectivamente. K2 representa carga, y K4 y K5 representan la confiabilidad. De manera predeterminada, K1 y K3 están establecidos en 1, y K2, K4 y K5 están establecidos en 0. Como resultado, solamente se usan los valores de ancho de banda y de retraso en el cálculo de la métrica compuesta predeterminada. En EIGRP para IPv4 y EIGRP para IPv6 se utiliza la misma fórmula para la métrica compuesta.

El método para calcular la métrica (valores  $k$ ) y el número de sistema autónomo de EIGRP deben coincidir entre vecinos EIGRP. Si no coinciden, los routers no forman una adyacencia.

Los valores  $k$  predeterminados se pueden cambiar con el comando **metric weights** del modo de configuración del router:

```
Router(config-router)# metric weights tos k1 k2 k3 k4 k5
```

**Nota:** la modificación del valor de **metric weights** generalmente no es recomendable y excede el ámbito de este curso. No obstante, su importancia es pertinente al establecimiento de adyacencias de vecinos. Si un router modificó las ponderaciones de la métrica y otro router no lo hizo, no se forma una adyacencia.

### Verificación de los valores $k$

El comando **show ip protocols** se utiliza para verificar los valores  $k$ . En la figura 2, se muestra el resultado del comando para el R1. Observe que los valores  $k$  en el R1 están establecidos en la configuración predeterminada.

## Métrica compuesta de EIGRP

Fórmula compuesta predeterminada:  
métrica =  $(K1 \cdot \text{ancho de banda} + K3 \cdot \text{retraso})$

Fórmula compuesta completa:  
métrica =  $(K1 \cdot \text{ancho de banda} + [K2 \cdot \text{ancho de banda}] / [256 - \text{carga}] + K3 \cdot \text{retraso}) +$   
 $(K5 / [\text{confiabilidad} + K4])$

(No se usa si los valores "K" son 0)

**Nota:** Esta es una fórmula condicional. Si  $K5 = 0$ , el último término se reemplaza por 1 y la fórmula se convierte en: métrica =  $(K1 \cdot \text{ancho de banda} + [K2 \cdot \text{ancho de banda}] / [256 - \text{carga}] + K3 \cdot \text{retraso})$

### Valores

#### predeterminados:

K1 (ancho de banda) = 1  
K2 (carga) = 0  
K3 (retraso) = 1  
K4 (confiabilidad) = 0  
K5 (confiabilidad) = 0

Los valores "K" se pueden cambiar con el comando

**metric weights**.

```
Router(config-router)# metric weights tos k1 k2 k3 k4 k5
```

## Verificación de los valores de métrica K

```
R1# show ip protocols
*** IP Routing is NSF aware **

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-IPv4 Protocol for AS(1)
    Metric weight k1-1, k2-0, k3-1, k4-0, k5-0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
<resultado omitido>
R1#
```

## Capítulo 7: EIGRP 7.3.2.2 Análisis de los valores de interfaz

### Examen de los valores de la métrica

El comando **show interfaces** muestra información de las interfaces, incluidos los parámetros utilizados para el cálculo de la métrica de EIGRP. En la ilustración, se muestra el comando **show interfaces** para la interfaz Serial 0/0/0 en el R1.

- **BW:** ancho de banda de la interfaz (en kilobits por segundo).
- **DLY:** retraso de la interfaz (en microsegundos).
- **Reliability:** confiabilidad de la interfaz expresada como una fracción de 255 (255/255 es una confiabilidad del 100%), calculada como un promedio exponencial durante cinco minutos. De manera predeterminada, EIGRP no incluye su valor al calcular la métrica.
- **Txload, Rxload:** carga transmitida y recibida a través de la interfaz expresada como una fracción de 255 (255/255 es completamente saturada), calculada como un promedio exponencial durante cinco minutos. De manera predeterminada, EIGRP no incluye su valor al calcular la métrica.

**Nota:** a lo largo de este curso, el ancho de banda se indica como kb/s. No obstante, el resultado del router muestra el ancho de banda mediante la abreviatura "Kbit/sec". En el resultado del router, el retraso se muestra como "usec", mientras que, en este curso, el retraso se indica como microsegundos.

#### Comando show interfaces

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
<resultado omitido>
R1#

R1# show interfaces gigabitethernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0 (bia
fc99.4775.c3e0)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
<resultado omitido>
R1#
```

#### Capítulo 7: EIGRP 7.3.2.3 Métrica de ancho de banda

La métrica de ancho de banda es un valor estático que usan algunos protocolos de routing, como EIGRP y OSPF, para calcular la métrica de routing. El ancho de banda se muestra en kilobits por segundo (kb/s). La mayoría de las interfaces seriales usan el valor de ancho de banda predeterminado de 1544 kb/s o 1 544 000 b/s (1,544 Mb/s). Éste es el ancho de banda de una conexión T1. Sin embargo, algunas interfaces seriales utilizan otro valor de ancho de

banda predeterminado. En la figura 1, se muestra la topología que se utiliza en esta sección. Es posible que los tipos de interfaces seriales y sus anchos de banda asociados no reflejen necesariamente los tipos de conexiones más frecuentes que se encuentran en las redes en la actualidad.

Verifique siempre el ancho de banda con el comando **show interfaces**.

El valor predeterminado del ancho de banda puede reflejar o no el ancho de banda físico real de la interfaz. Si el ancho de banda real del enlace difiere del valor de ancho de banda predeterminado, se debe modificar el valor de ancho de banda.

### Configuración del parámetro de ancho de banda

En la mayoría de los enlaces seriales, la métrica de ancho de banda predeterminada es 1544 kb/s. 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.

Utilice el siguiente comando del modo de configuración de interfaz para modificar la métrica de ancho de banda:

```
Router(config-if)# bandwidth valor-kilobits-ancho-de-banda
```

Utilice el comando **no bandwidth** para restaurar el valor predeterminado.

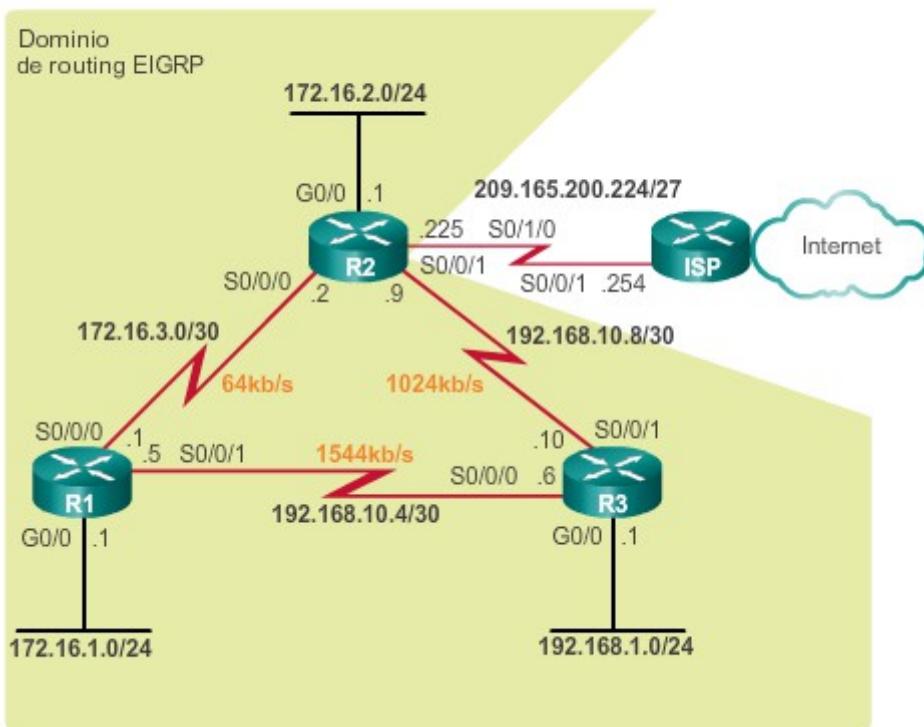
En la figura 2, el enlace entre el R1 y el R2 tiene un ancho de banda de 64 kb/s, y el enlace entre el R2 y el R3 tiene un ancho de banda de 1024 kb/s. La figura muestra la configuración utilizada en los tres routers para modificar el ancho de banda en las interfaces seriales adecuadas.

### Verificación del parámetro de ancho de banda

Utilice el comando **show interfaces** para verificar los nuevos parámetros de ancho de banda, como se muestra en la figura 3. Es importante modificar la métrica del ancho de banda en ambos lados del enlace para garantizar el enrutamiento adecuado en ambas direcciones.

La modificación del valor del ancho de banda no cambia el ancho de banda real del enlace. El comando **bandwidth** solo modifica la métrica de ancho de banda que utilizan los protocolos de routing, como EIGRP y OSPF.

## Topología EIGRP para IPv4



Configuración del valor de ancho de banda en el R1, el R2 y el R3

```
R1(config)# interface s 0/0/0
R1(config-if)# bandwidth 64
```

```
R2(config)# interface s 0/0/0
R2(config-if)# bandwidth 64
R2(config-if)# exit
R2(config)# interface s 0/0/1
R2(config-if)# bandwidth 1024
```

```
R3(config)# interface s 0/0/1
R3(config-if)# bandwidth 1024
```

## Verificación del valor de ancho de banda

```
R1# show interface s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
    MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R1#

R2# show interface s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.2/30
    MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R2#
```

Es importante que los parámetros de ancho de banda sean los mismos en ambos lados del enlace para asegurar el enrutamiento adecuado en ambos sentidos.

### Capítulo 7: EIGRP 7.3.2.4 Métrica de retraso

El retraso es la medida del tiempo que tarda un paquete en atravesar la 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 de manera dinámica. En otras palabras, el router no hace un seguimiento realmente del tiempo que les toma 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.

Cuando se utiliza para determinar la métrica de EIGRP, el retraso es la acumulación (suma) de todos los retrasos de las interfaces a lo largo de la ruta (medida en decenas de microsegundos).

En la tabla de la figura 1, se muestran los valores de retraso predeterminados para diversas interfaces. Observe que el valor predeterminado es de 20 000 microsegundos para las interfaces serials y de 10 microsegundos para las interfaces GigabitEthernet.

Utilice el comando **show interfaces** para verificar el valor de retraso en una interfaz, como se muestra en la figura 2. Si bien una interfaz con varios anchos de banda puede tener el mismo valor de retraso predeterminado, Cisco recomienda no modificar el parámetro de retraso, salvo que el administrador de red tenga una razón específica para hacerlo.

### Valores de retraso de interfaz

Medios	Retardo
Ethernet	1.000
Fast Ethernet	100
Gigabit Ethernet	10
Token Ring 16 M	630
FDDI	100
T1 (serial predeterminada)	20 000
DS0 (64kb/s)	20 000
1024 kb/s	20 000
56 kb/s	20 000

### Verificación del valor de retraso

```
R1# show interfaces s 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R1#

R1# show interfaces g 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e0
(bia fc99.4775.c3e0)
  Internet address is 172.16.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R1#
```

### Capítulo 7: EIGRP 7.3.2.5 Como calcular la métrica de EIGRP

Si bien EIGRP calcula automáticamente la métrica de la tabla de routing utilizada para elegir la mejor ruta, es importante que el administrador de red comprenda cómo se determinaron estas métricas.

La figura muestra la métrica compuesta utilizada por EIGRP. Mediante el uso de los valores predeterminados para K1 y K3, el cálculo puede simplificarse al ancho de banda más lento (o ancho de banda mínimo), más la suma de todos los retrasos.

En otras palabras, al analizar los valores de ancho de banda y de retraso para todas las interfaces de salida de la ruta, podemos determinar la métrica de EIGRP de la siguiente manera:

**Paso 1.** Determine el enlace con el ancho de banda más lento. Utilice ese valor para calcular el ancho de banda ( $10\ 000\ 000/\text{ancho de banda}$ ).

**Paso 2.** Determine el valor de retraso para cada interfaz de salida en el camino al destino. Sume los valores de retraso y divida por 10 (suma de los retrasos/10).

**Paso 3.** Sume los valores de ancho de banda y de retraso calculados y multiplique la suma por 256 para obtener la métrica de EIGRP.

El resultado de la tabla de routing para el R2 muestra que la ruta a 192.168.1.0/24 tiene una métrica de EIGRP de 3 012 096.

### Métrica de EIGRP predeterminada

$$(K1 \cdot \text{ancho de banda} + K3 \cdot \text{retraso}) * 256 = \text{Métrica}$$

Debido a que K1 y K3 ambos son iguales a 1, la fórmula se convierte en:

$$(\text{ancho de banda} + \text{retraso}) * 256 = \text{Métrica}$$

El ancho de banda se calcula usando la velocidad del enlace más lento en la ruta hacia el destino.

El retraso se calcula con la suma de todos los retrasos en la ruta hacia el destino.

$$([10\ 000\ 000/\text{ancho de banda}] + [\text{suma de retrasos}/10]) * 256 = \\ \text{Métrica}$$

```
R2# show ip route
D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:12:32, Serial0/0/1
```

### Capítulo 7: EIGRP 7.3.2.6 Cálculo de la métrica de EIGRP

En la figura 1, se muestra la topología de los tres routers. Este ejemplo ilustra la manera en que EIGRP determina la métrica que se muestra en la tabla de routing del R2 para la red 192.168.1.0/24.

#### Ancho de banda

EIGRP usa el ancho de banda más lento en el cálculo de su métrica. El ancho de banda más lento se puede determinar por medio de analizar cada interfaz entre el R2 y la red de destino 192.168.1.0. La interfaz Serial 0/0/1 en el R2 tiene un ancho de banda de 1024 kb/s. La interfaz GigabitEthernet 0/0 en el R3 tiene un ancho de banda de 1 000 000 kb/s. Por lo tanto, el ancho de banda más lento es de 1024 kb/s y se usa en el cálculo de la métrica.

EIGRP divide un valor de ancho de banda de referencia de 10 000 000 por el valor en kb/s del ancho de banda de la interfaz. Como resultado, los valores más altos de ancho de banda reciben una métrica más baja, y los valores más bajos de ancho de banda reciben una métrica más alta. 10 000 000 se divide por 1024. Si el resultado no es un número entero, el valor se redondea hacia abajo. En este caso, 10 000 000 dividido por 1024 es igual a 9765,625. Los decimales (625) se descartan, y el resultado es 9765 para la porción de ancho de banda de la métrica compuesta, como se muestra en la figura 2.

### Retardo

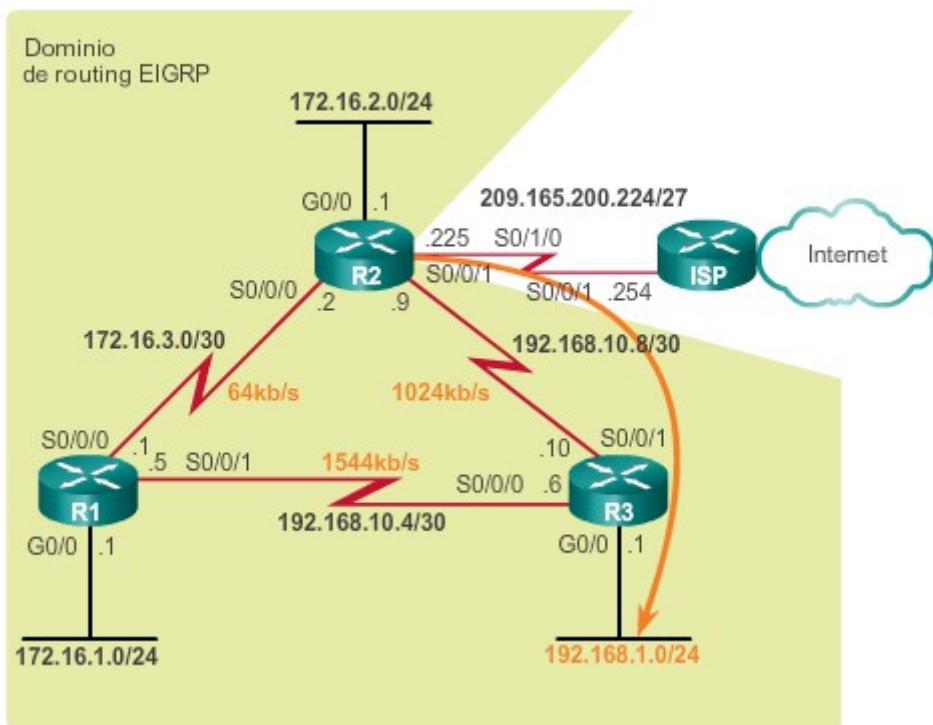
Como se muestra en la figura 3, se utilizan las mismas interfaces de salida para determinar el valor de retraso.

EIGRP usa la suma de todos los retrasos hasta el destino. La interfaz Serial 0/0/1 en el R2 tiene un retraso de 20 000 microsegundos. La interfaz Gigabit 0/0 en el R3 tiene un retraso de 10 microsegundos. La suma de estos retrasos se divide por 10. En el ejemplo,  $(20\ 000 + 10)/10$ , da como resultado un valor de 2001 para la porción de retraso de la métrica compuesta.

### Cálculo de la métrica

Utilice los valores calculados para el ancho de banda y el retraso en la fórmula de la métrica. El resultado es una métrica de 3 012 096, como se muestra en la figura 4. Este valor coincide con el valor que se muestra en la tabla de routing para el R2.

**Topología EIGRP para IPv4**



### Cálculo del ancho de banda

```
R2# show interface s 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.10.9/30
    MTU 1500 bytes, BW 1024 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R2#
```

```
R3# show interface g 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4771.7a20
(bia fc99.4771.7a20)
  Internet address is 192.168.1.1/24
    MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R3#
```

Calcule el ancho de banda usando el ancho de banda más lento al destino: **1024**

$$(10\,000\,000 \div 1024) = 9765$$

Nota: 9765,625 se redondea hacia abajo, a 9765.

### Análisis de los valores de retraso

```
R2# show interface s 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Internet address is 192.168.10.9/30
    MTU 1500 bytes, BW 1024 Kbit/sec, DLY 20000 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R2#
```

```
R3# show interface g 0/0
GigabitEthernet0/0 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4771.7a20
(bia fc99.4771.7a20)
  Internet address is 192.168.1.1/24
    MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
      reliability 255/255, txload 1/255, rxload 1/255
<resultado omitido>
R3#
```

Calcule el retraso usando la suma de todos los retrasos al destino: **20 000 + 10**

$$(20\,000 + 10) \div 10 = 2001$$

## Verificación de la métrica de EIGRP

```
R2# show ip route
<resultado omitido>
D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:12:32,
  Serial0/0/1
```

Utilice los resultados en la fórmula predeterminada de la métrica:

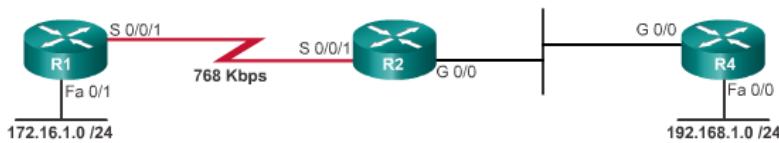
$$(\text{Ancho de banda} + \text{Retraso}) * 256 = \text{Métrica}$$

$$(9765 + 2001) * 256 = 3\,012\,096$$

### Capítulo 7: EIGRP 7.3.2.7 Actividad: Calcular la métrica de EIGRP

#### Actividad (parte 1): Calcular la métrica de EIGRP desde el R1 hasta la red de destino 192.168.1.0

El router 1 (R1) calcula la métrica de EIGRP para llegar a la red de destino 192.168.1.0. Arrastre los valores de ancho de banda y de retraso correctos hacia la fórmula en los campos correspondientes. Haga clic en el botón 2 para continuar.

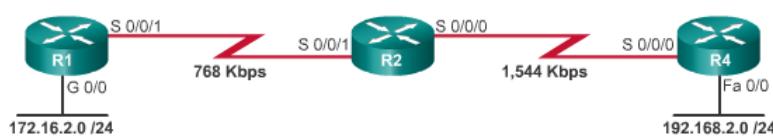


Medios	Retardo
Ethernet	1,000
Fast Ethernet	100
Gig Ethernet	10
Serie WAN	20,000

Métrica	Ancho de banda (Kb/s)	Retardo
$3848149 = 256 * (( 10^7 / \checkmark ) + ( \checkmark / 10 ))$	768	20,110

#### Actividad (parte 2): Calcular la métrica de EIGRP desde el R1 hasta la red de destino 192.168.2.0

El router 1 (R1) calcula la métrica de EIGRP para llegar a la red de destino 192.168.2.0. Arrastre los valores de ancho de banda y de retraso correctos hacia la fórmula en los campos correspondientes. Haga clic en el botón 3 para continuar.

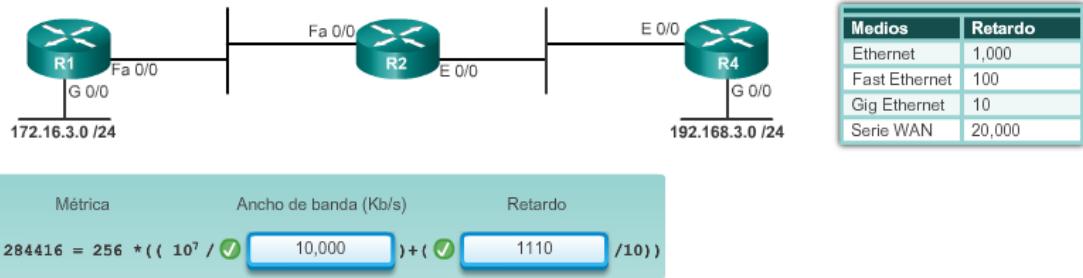


Medios	Retardo
Ethernet	1,000
Fast Ethernet	100
Gig Ethernet	10
Serie WAN	20,000

Métrica	Ancho de banda (Kb/s)	Retardo
$4359893 = 256 * (( 10^7 / \checkmark ) + ( \checkmark / 10 ))$	768	40,100

**Actividad (parte 3): Calcular la métrica de EIGRP desde el R1 hasta la red de destino 192.168.3.0**

El router 1 (R1) calcula la métrica de EIGRP para llegar a la red de destino 192.168.3.0. Arrastre los valores de ancho de banda y de retraso correctos hacia la fórmula en los campos correspondientes.



### Capítulo 7: EIGRP 7.3.3.1 Conceptos acerca de DUAL

EIGRP utiliza el algoritmo de actualización por difusión (DUAL) para proporcionar la mejor ruta sin bucles y las mejores rutas de respaldo sin bucles.

En el contexto de DUAL se utilizan varios términos, que se analizan más detalladamente en esta sección:

- Sucesor
- Distancia factible (FD)
- Sucesor factible (FS)
- Distancia publicada (AD, Advertised Distance) o Distancia notificada (RD, Reported Distance):
- Condición factible o Condición de factibilidad (FC)

Estos términos y conceptos son esenciales en el mecanismo de prevención de bucles de DUAL.

### **Conceptos acerca de DUAL**

#### DUAL proporciona:

- Rutas sin bucles
- Rutas de respaldo sin bucles que se pueden utilizar inmediatamente
- Convergencia rápida
- Mínimo uso de ancho de banda con actualizaciones limitadas

### Capítulo 7: EIGRP 7.3.3.2 Introducción a DUAL

EIGRP utiliza el algoritmo de convergencia DUAL. La convergencia es fundamental para las redes para evitar bucles de routing.

Los bucles de routing, incluso los temporarios, pueden ser perjudiciales para el rendimiento de la red. Los protocolos de routing vector distancia, como RIP, evitan los bucles de routing con temporizadores de espera y horizonte dividido. A pesar de que EIGRP utiliza ambas técnicas, las usa de manera un tanto diferentes; la manera principal en la que EIGRP evita los loops de enrutamiento es con el algoritmo DUAL.

Haga clic en Reproducir en la ilustración para ver la operación básica de DUAL.

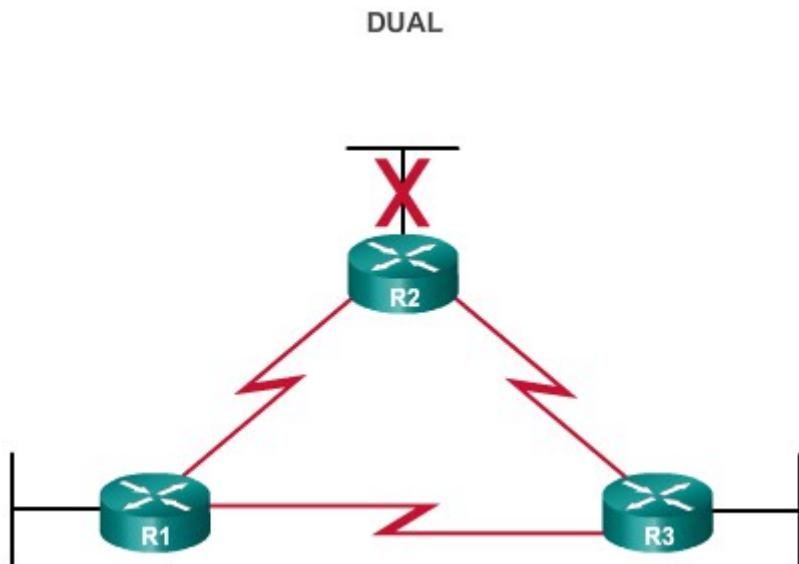
El algoritmo DUAL se utiliza para asegurar que no haya bucles en cada instancia a través del cómputo de una ruta. Esto permite que todos los routers involucrados en un cambio de topología se sincronicen al mismo tiempo. Los routers que no se ven afectados por los cambios en la topología no se encuentran involucrados en el recálculo. Este método proporciona a EIGRP mayor tiempo de convergencia que a otros protocolos de enrutamiento vector distancia.

La máquina de estados finitos (FSM) DUAL realiza el proceso de decisión para todos los cálculos de ruta. Una FSM es un modelo de flujo de trabajo, similar a un diagrama de flujo, que está compuesto por lo siguiente:

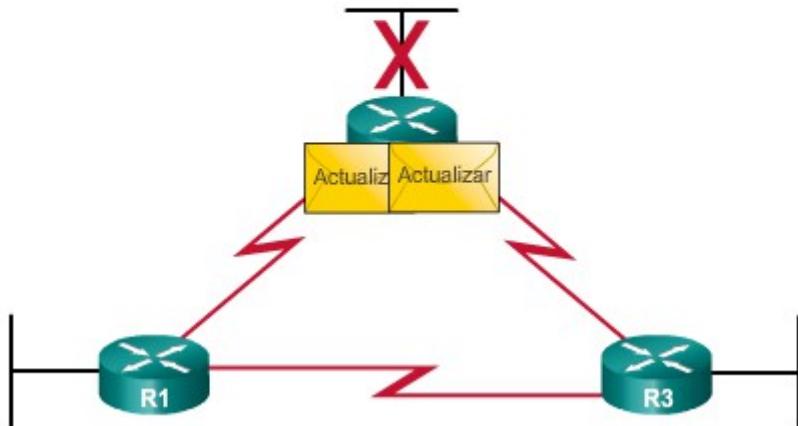
- Un número finito de etapas (estados)
- Transiciones entre estas etapas
- Operaciones

La FSM DUAL rastrea todas las rutas, utiliza las métricas de EIGRP para elegir rutas eficaces sin bucles e identifica las rutas con el menor costo para insertarlas en la tabla de routing.

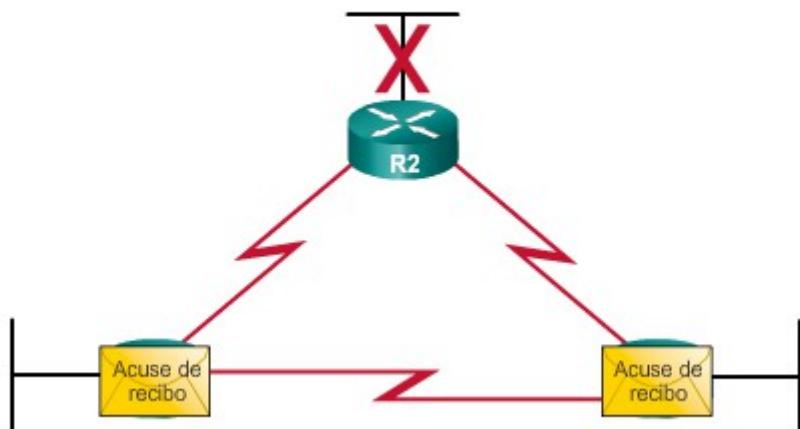
El recálculo del algoritmo DUAL puede ser muy exigente para el procesador. EIGRP mantiene una lista de rutas de respaldo que DUAL ya determinó que no tienen bucles para evitar los recálculos siempre que sea posible. Si la ruta principal en la tabla de enrutamiento falla, el mejor camino de respaldo se agrega de inmediato a la tabla de enrutamiento.



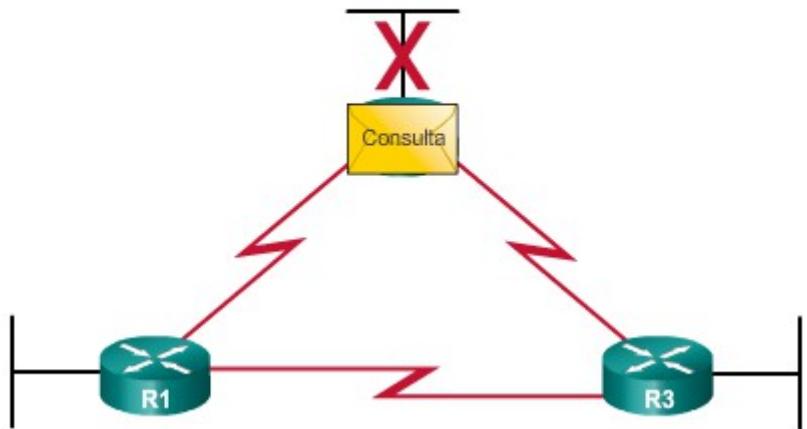
DUAL



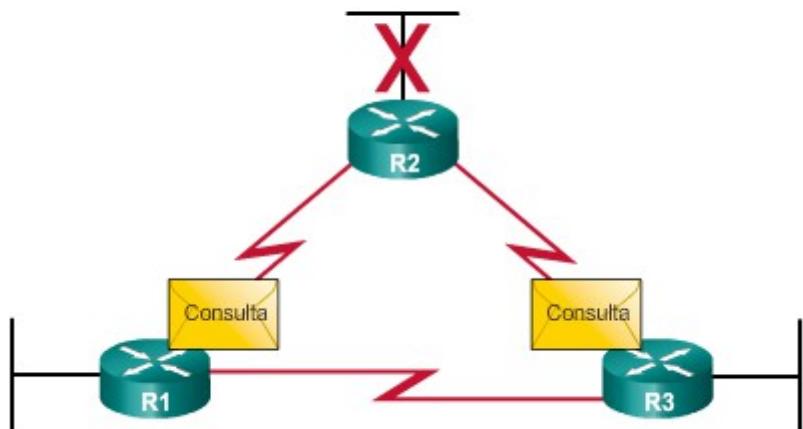
DUAL



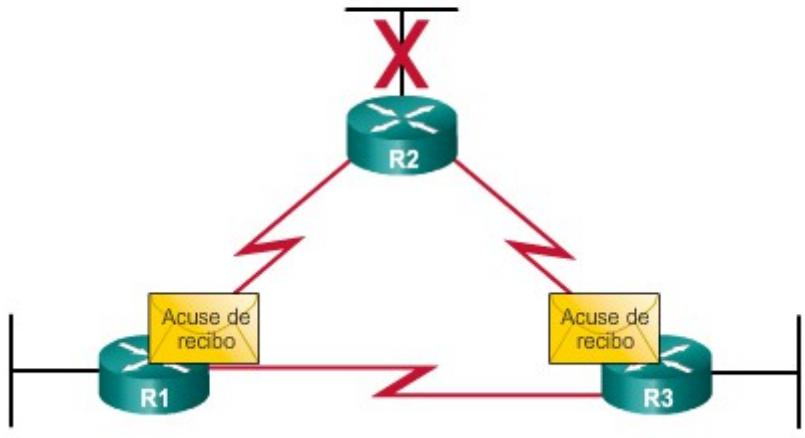
DUAL



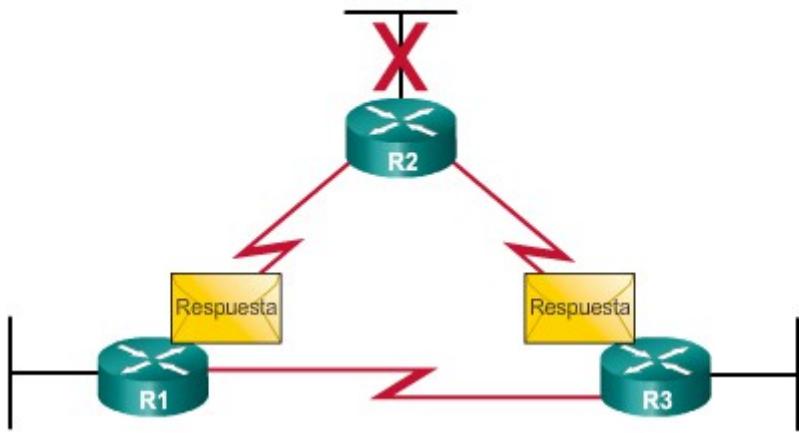
DUAL



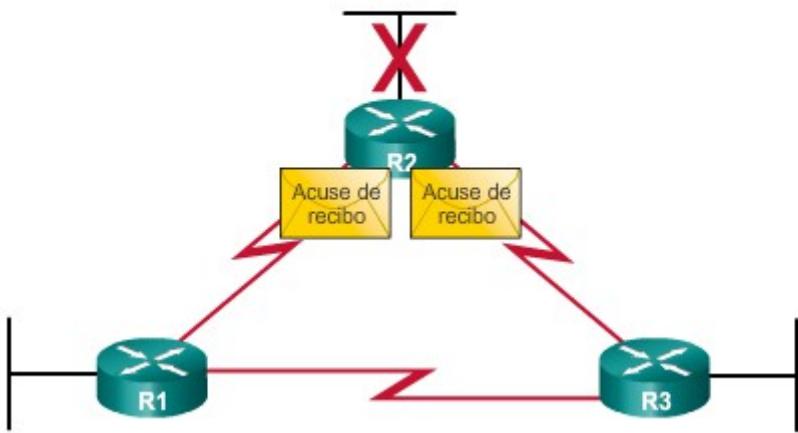
DUAL



DUAL



DUAL



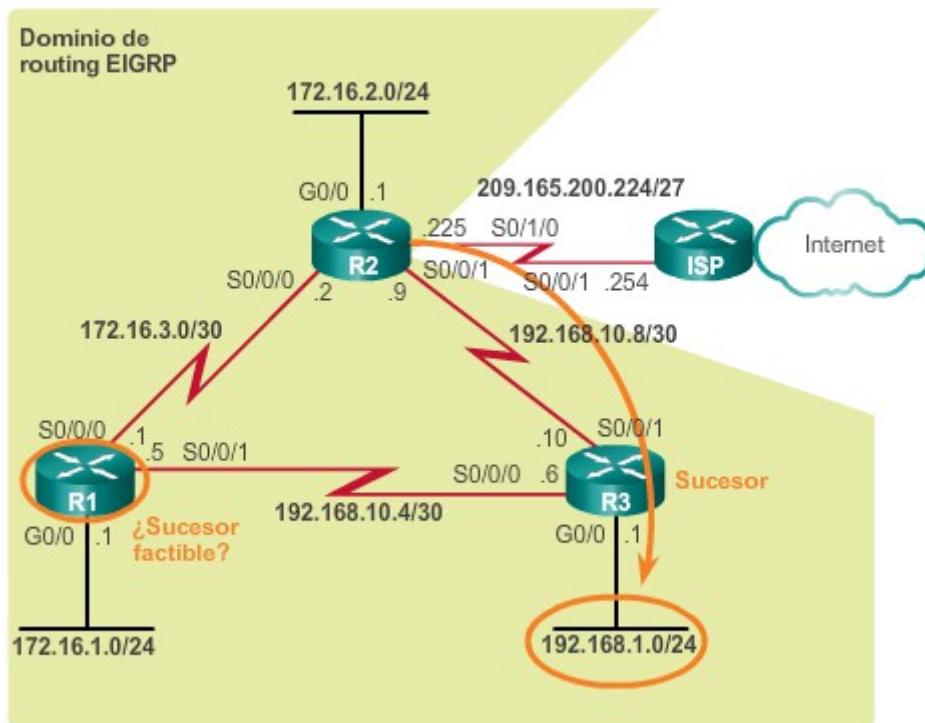
### Capítulo 7: EIGRP 7.3.3.3 Sucesor y distancia factible

En la figura 1, se muestra la topología para este tema. 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.

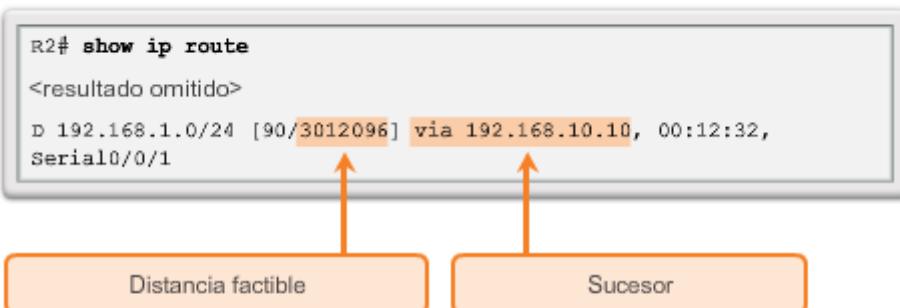
FD es la métrica más baja calculada para llegar a la red de destino. FD es la métrica enumerada en la entrada de la tabla de enrutamiento como el segundo número dentro de los corchetes. Al igual que en otros protocolos de routing, esto también se conoce como la “métrica para la ruta”.

Analice la tabla de routing para el R2 en la figura 2 y observe que la mejor ruta EIGRP para la red 192.168.1.0/24 es a través del router R3 y que la distancia factible es 3 012 096. Esta es la métrica que se calculó en el tema anterior.

Topología EIGRP para IPv4



## Distancia factible y sucesor



- El R3 en 192.168.10.10 es la red sucesora a 192.168.1.0/24.
- Esta ruta tiene una distancia factible de 3 012 096.

### Capítulo 7: EIGRP 7.3.3.4 Sucesores factibles, condición de factibilidad y distancia notificada

DUAL puede converger rápidamente después de un cambio en la topología, debido a que puede usar rutas de respaldo a otras redes sin recalcular DUAL. Estas rutas de respaldo se conocen como “sucesores factibles” (FS).

Un FS es un vecino que tiene una ruta de respaldo sin bucles a la misma red que el sucesor y satisface la condición de factibilidad (FC). El sucesor de R2 para la red 192.168.1.0/24 es el R3, que proporciona la mejor ruta o la métrica más baja a la red de destino. Observe en la figura 1 que el R1 proporciona una ruta alternativa, pero ¿es un FS? Antes de que el R1 pueda ser un FS para el R2, debe cumplir la FC.

La FC se cumple cuando la distancia notificada (RD) desde un vecino hasta una red es menor que la distancia factible desde el router local hasta la misma red de destino. Si la distancia notificada es menor, representa una ruta sin bucles. La distancia notificada es simplemente una distancia factible desde el vecino EIGRP hasta 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.

En la figura 2, la distancia factible del R1 a 192.168.1.0/24 es 2 170 112.

- El R1 informa al R2 que su FD a 192.168.1.0/24 es 2 170 112.
- Desde la perspectiva del R2, 2 170 112 es la RD del R1.

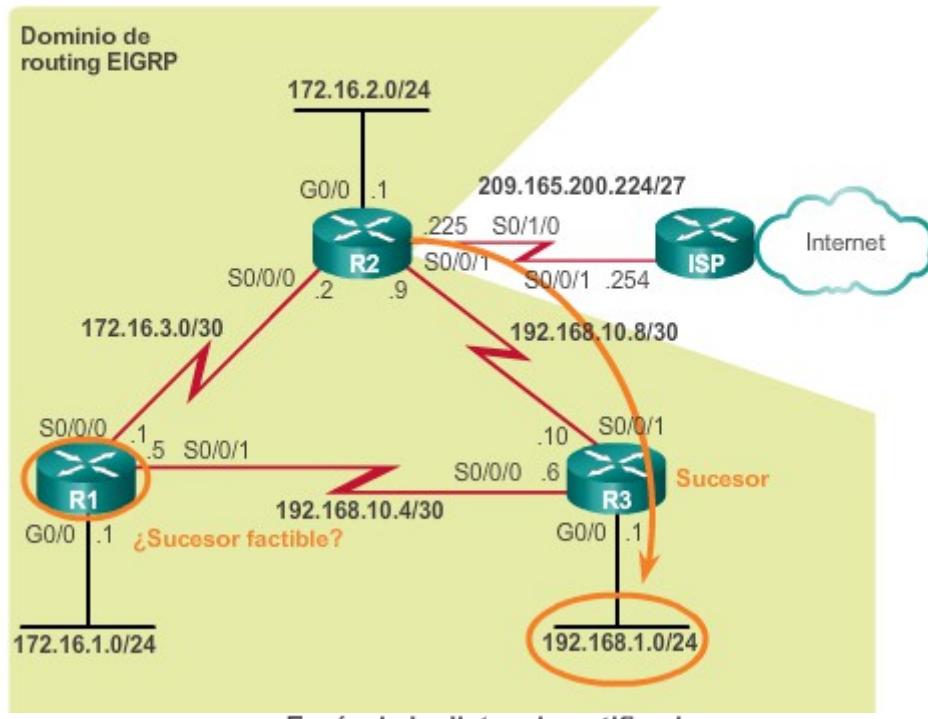
El R2 utiliza esta información para determinar si el R1 cumple la FC y, por lo tanto, puede ser un FS.

Como se muestra en la figura 3, debido a que la RD del R1 (2 170 112) es menor que la propia FD del R2 (3 012 096), el R1 cumple con la FC.

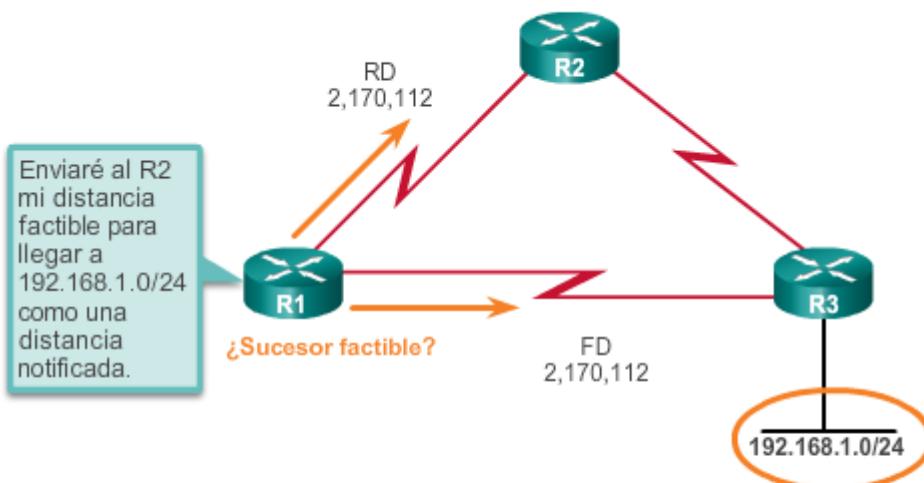
El R1 es ahora un FS para el R2 a la red 192.168.1.0/24.

Si hay un error en la ruta del R2 a 192.168.1.0/24 a través del R3 (sucesor), el R2 instala inmediatamente la ruta a través del R1 (FS) en su tabla de routing. El R1 se convierte en el nuevo sucesor para la ruta del R2 a esta red, como se muestra en la figura 4.

## Topología EIGRP para IPv4



Envío de la distancia notificada



```
R1# show ip route
<resultado omitido>
D    192.168.1.0/24 [90/2170112] via 192.168.10.6, 02:44:50,
Serial0/0/1
```

## ¿Cumple con la condición de factibilidad?

- La distancia factible del R2 a 192.168.1.0 es 3 012 096.
- La distancia notificada del R1 a 192.168.1.0 es 2 170 112.
- El R1 cumple con la condición de factibilidad.

```
R2# show ip route
```

<resultado omitido>

```
D 192.168.1.0/24 [90/3012096] via 192.168.10.10,  
00:12:32, Serial0/0/1
```

Distancia factible

Sucesor (R3)

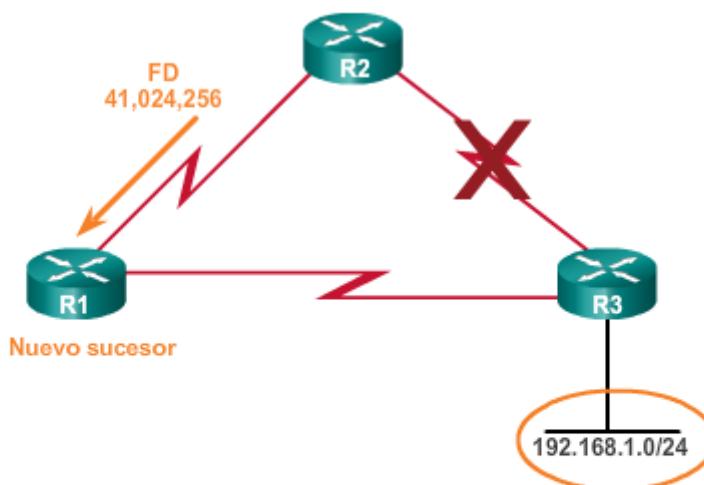
```
R1# show ip route
```

<resultado omitido>

```
D 192.168.1.0/24 [90/2170112] via 192.168.10.6, 02:44:50,  
Serial0/0/1
```

Distancia factible  
Enviado al R2 como la distancia notificada del R1.

### Uso del sucesor factible



```
R2# show ip route
```

<resultado omitido>

```
D 192.168.1.0/24 [90/41024256] via 172.16.3.1, 00:00:13,  
Serial0/0/0
```

Distancia factible

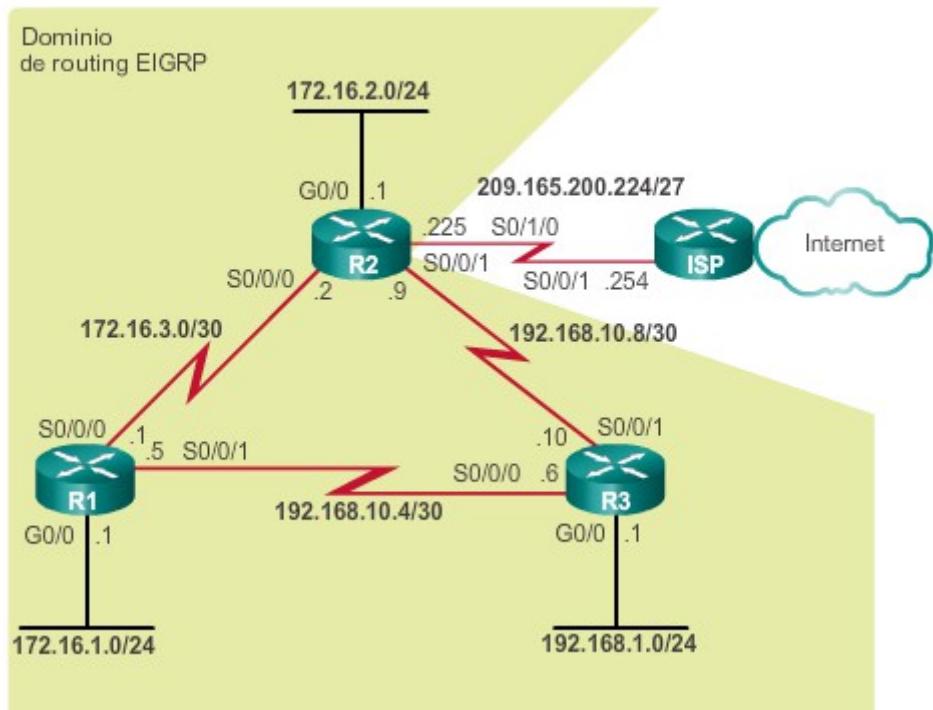
Sucesor (R1)

En la figura 1, se muestra la topología.

La tabla de topología de EIGRP contiene todas las rutas conocidas a cada vecino EIGRP. A medida que un router EIGRP descubre rutas de sus vecinos, dichas rutas se instalan en su tabla de topología de EIGRP.

Como se muestra en la figura 2, utilice el comando **show ip eigrp topology** para ver la tabla de topología. La tabla de topología incluye todos los sucesores y FS a las redes de destino calculados por DUAL. Solo el sucesor se instala en la tabla de routing IP.

Topología EIGRP para IPv4



## Tabla de topología del R2

```
R2# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 172.16.2.0/24, 1 successors, FD is 2816
      via Connected, GigabitEthernet0/0
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 3012096
      via 192.168.10.10 (3012096/2816), Serial0/0/1
      via 172.16.3.1 (41024256/2170112), Serial0/0/0
P 172.16.3.0/30, 1 successors, FD is 40512000
      via Connected, Serial0/0/0
P 172.16.1.0/24, 1 successors, FD is 3524096
      via 192.168.10.10 (3524096/2170112), Serial0/0/1
      via 172.16.3.1 (40512256/2816), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
      via Connected, Serial0/0/1

R2#
```

### Capítulo 7: EIGRP 7.3.3.6 Tabla de topología: comando show ip eigrp topology (cont.)

Como se muestra en la figura 1, la primera línea en la tabla de topología muestra lo siguiente:

- **P:** ruta en estado pasivo. Cuando DUAL no realiza sus cálculos por difusión para determinar la ruta para una red, la ruta se encuentra en modo estable, conocido como “estado pasivo”. Si DUAL recalcula o busca una nueva ruta, la ruta está en estado activo, y se muestra una “A”. Todas las rutas en la tabla de topología deberían estar en el estado pasivo para un dominio de enrutamiento estable.
- **192.168.1.0/24:** red de destino, que también se encuentra en la tabla de routing.
- **1 successors:** muestra el número de sucesores para esta red. Si hay varias rutas del mismo costo a esta red, hay varios sucesores.
- **FD is 3012096:** FD es la métrica de EIGRP para llegar a la red de destino. Esta es la métrica que se muestra en la tabla de routing IP.

Como se muestra en la figura 2, la primera subentrada en el resultado muestra el sucesor:

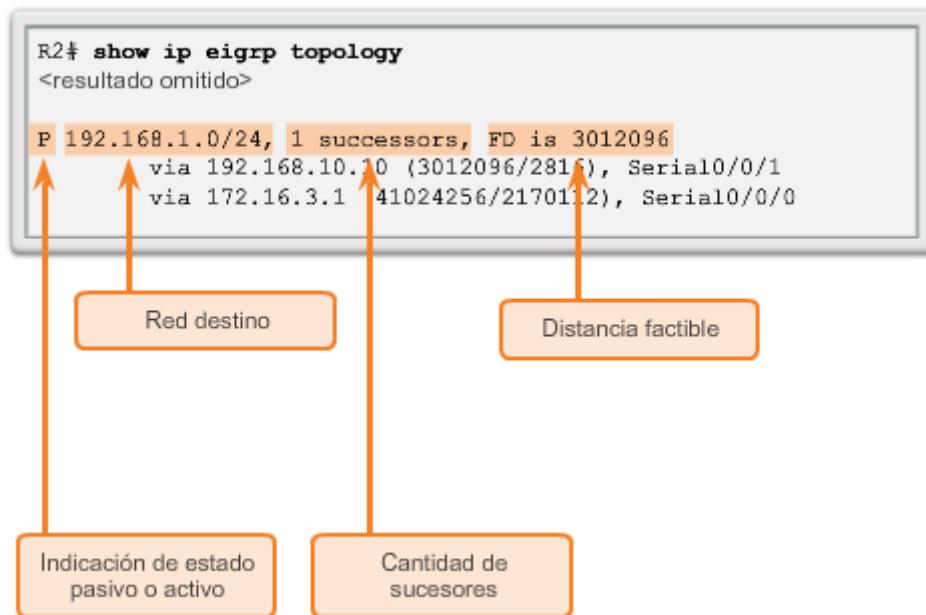
- **via 192.168.10.10:** dirección del siguiente salto del sucesor, el R3. Esta dirección se muestra en la tabla de enrutamiento.
- **3012096:** FD a 192.168.1.0/24. Es la métrica que se muestra en la tabla de routing IP.
- **2816:** RD del sucesor; es el costo del R3 para llegar a esta red.

- **Serial 0/0/1:** interfaz de salida usada para llegar a esta red, que también se muestra en la tabla de routing.

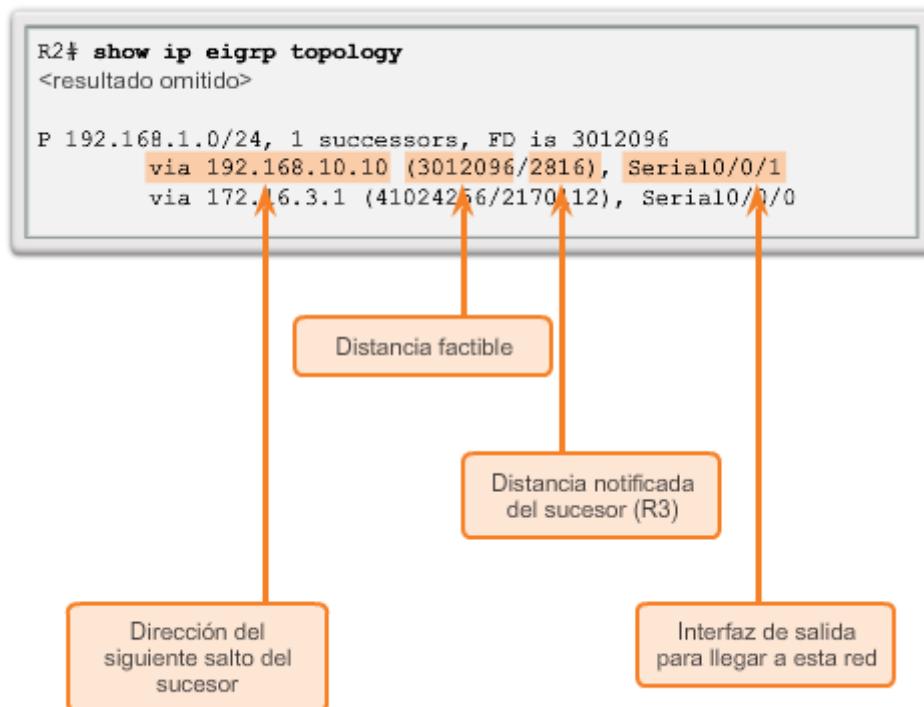
Como se ve en la figura 3, en la segunda subentrada se muestra el FS, el R1 (si no hay una segunda entrada, entonces no hay FS):

- **vía 172.16.3.1:** dirección del siguiente salto del FS, el R1.
- **41024256:** la nueva FD del R2 a 192.168.1.0/24, en caso de que el R1 se convierta en el nuevo sucesor y sea la nueva métrica mostrada en la tabla de routing IP.
- **2170112:** RD del FS, o la métrica del R1 para llegar a esta red. Para cumplir la FC, la RD debe ser inferior a la FD actual de 3 012 096.
- **Serial 0/0/0:** la interfaz de salida que se usa para llegar al FS, si este router se convierte en el sucesor.

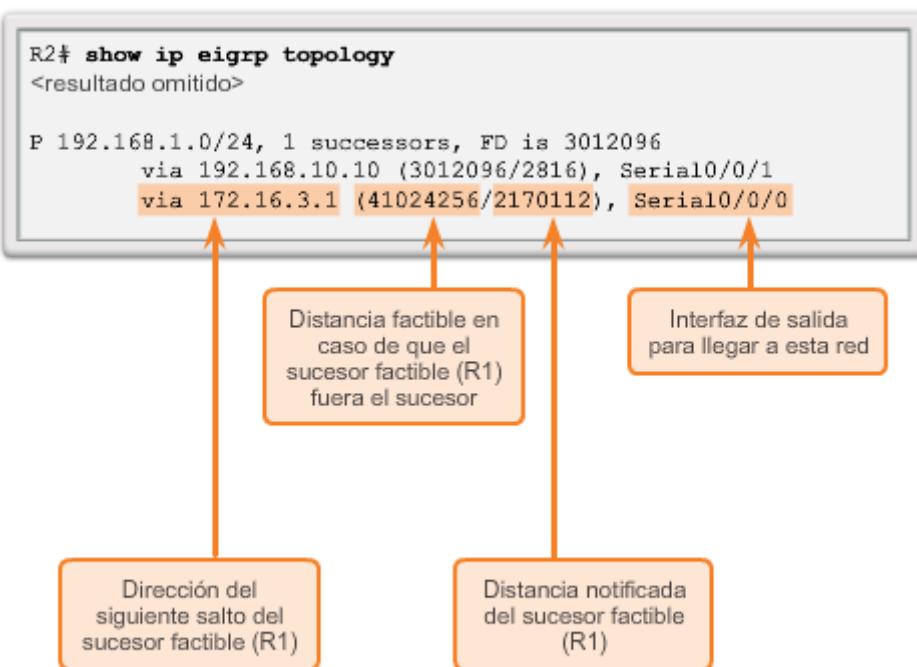
#### Análisis de una entrada de la tabla de topología



### Análisis de una entrada de la tabla de topología



### Análisis de una entrada de la tabla de topología



Para ver la manera en que DUAL usa los sucesores y los FS, examine la tabla de routing del R1 partiendo de la suposición de que la red es convergente, como se muestra en la figura 1.

En la figura 2, se muestra un resultado parcial del comando **show ip route** en el R1. La ruta a 192.168.1.0/24 muestra que el sucesor es el R3 a través de 192.168.10.6, con una FD de 2 170 112.

En la tabla de routing IP solo incluye la mejor ruta, es decir, el sucesor. Para ver si hay algún FS, debemos analizar la tabla de topología de EIGRP. En la tabla de topología en la figura 3 solo se muestra el sucesor 192.168.10.6, que es el R3. No hay ningún FS. 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. El R2 no es un FS, debido a que no cumple la FC. No obstante, al observar la topología, es obvio que el R2 es una ruta de respaldo, dado que EIGRP no tiene un mapa de la topología de la red. EIGRP es un protocolo de enrutamiento vector distancia y sólo conoce la información de la red remota a través de sus vecinos.

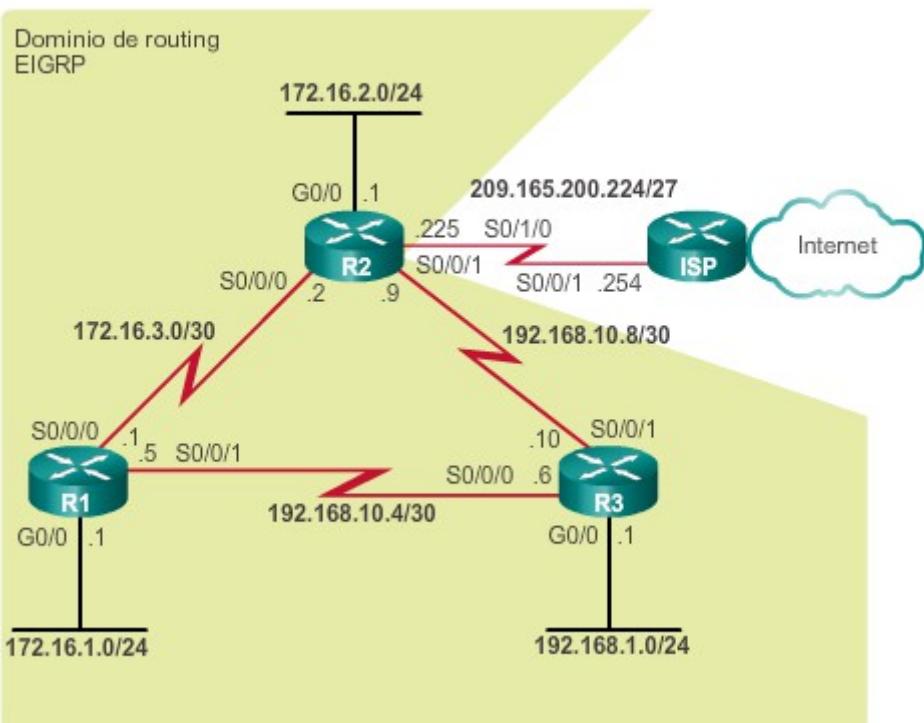
DUAL no almacena la ruta a través del R2 en la tabla de topología. Todos los enlaces se pueden mostrar mediante el comando **show ip eigrp topology all-links**. Este comando muestra los enlaces, independientemente de que cumplan la FC o no.

Como se muestra en la figura 4, el comando **show ip eigrp topology all-links** muestra todas las rutas posibles a una red, incluidos los sucesores, los FS y hasta las rutas que no son FS. La FD del R1 a 192.168.1.0/24 es 2 170 112, a través del sucesor R3. Para que el R2 se considere un FS, debe cumplir la FC. La RD del R2 al R1 para llegar a 192.168.1.0/24 debe ser inferior a la FD actual del R1. Según la ilustración, la RD del R2 es 3 012 096, lo cual es más alto que la FD actual del R1, de 2 170 112.

Aunque el R2 parece una ruta de respaldo posible para 192.168.1.0/24, el R1 no sabe que la ruta no es un loop back potencial a través de sí mismo. EIGRP es un protocolo de enrutamiento vector 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 tiene una ruta sin bucles es que la métrica del vecino cumpla con la FC. Al asegurarse de que la RD del vecino es inferior a su propia FD, el router puede suponer que ese router vecino no es parte de su propia ruta anunciada y, por lo tanto, evitar siempre un bucle potencial.

El R2 se puede usar como sucesor si el R3 falla, sin embargo, hay un retraso mayor antes de agregarlo a la tabla de routing. Antes de que el R2 se pueda usar como sucesor, DUAL debe llevar a cabo más procesos.

## Topología EIGRP para IPv4



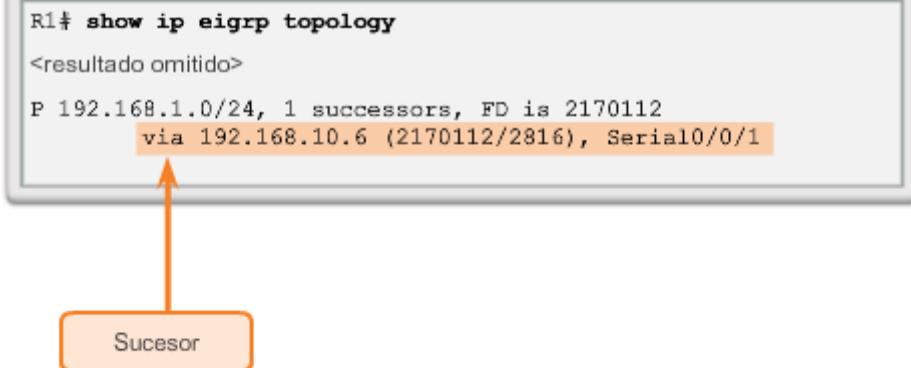
Entrada de la tabla de routing del R1 para 192.168.1.0/24

```
R1# show ip route
<resultado omitido>
D 192.168.1.0/24 [90/2170112] via 192.168.10.6,
01:23:13, Serial0/0/1
```

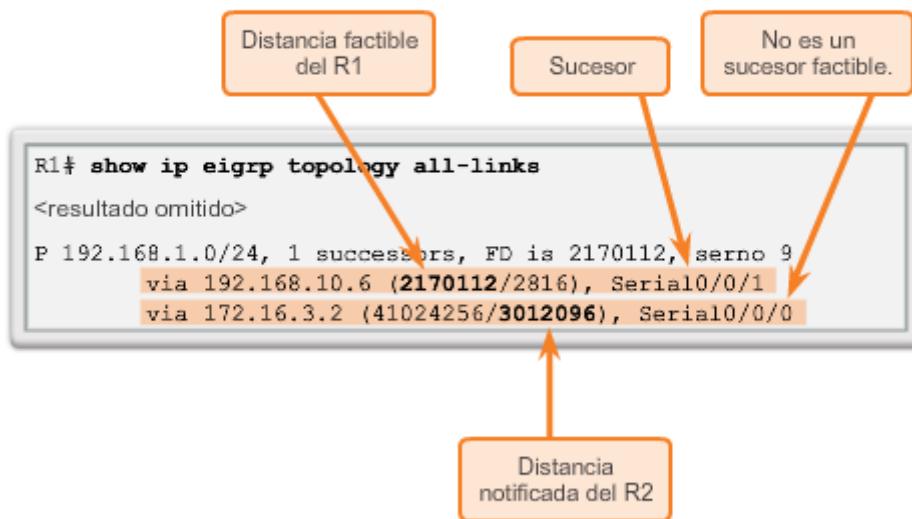
Distancia factible

El router de siguiente salto (R3) es el sucesor.

#### Entrada de la tabla de topología del R1 para 192.168.1.0/24

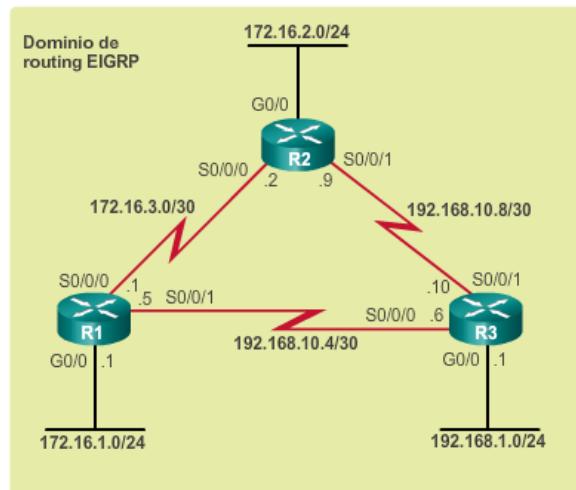


#### Entrada de la tabla de topología de todos los enlaces del R1 para 192.168.1.0/24



**Actividad: Determinar la topología de red de sucesor y de sucesor factible**

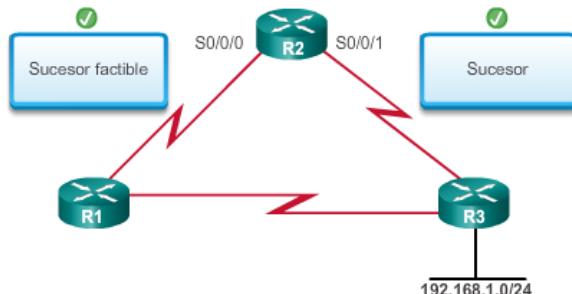
Utilice la topología de la red como referencia para determinar el sucesor y el sucesor factible EIGRP en cada situación. Haga clic en el botón 2 para comenzar.



**Actividad (situación 1): Determinar el sucesor factible**

Determine las rutas del sucesor y del sucesor factible para el R2 y arrastre las etiquetas del sucesor y del sucesor factible a los campos correctos en la topología. Haga clic en el botón 1 para revisar. Haga clic en el botón 3 para continuar la actividad.

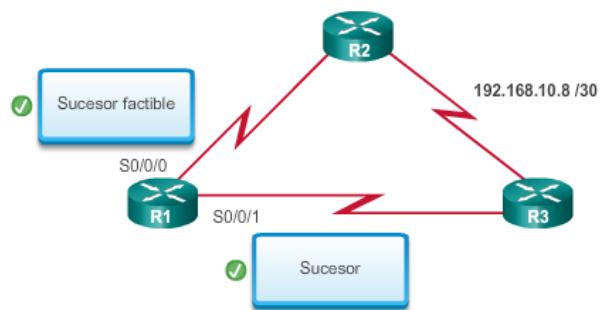
```
R2# show ip eigrp topology
<resultado omitido>
P 192.168.1.0/24, 1 successors, FD is 3014400
via 192.168.10.10 (3014400/5120), Serial0/0/1
via 172.16.3.1 (41026560/2172416), Serial0/0/0
```



**Actividad (situación 2): Determinar el sucesor y el sucesor factible**

Determine las rutas del sucesor y del sucesor factible para el R1 y arrastre las etiquetas del sucesor y del sucesor factible a los campos correctos en la topología. Haga clic en el botón 1 para revisar la topología.

```
R1# show ip eigrp topology
<resultado omitido>
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
```



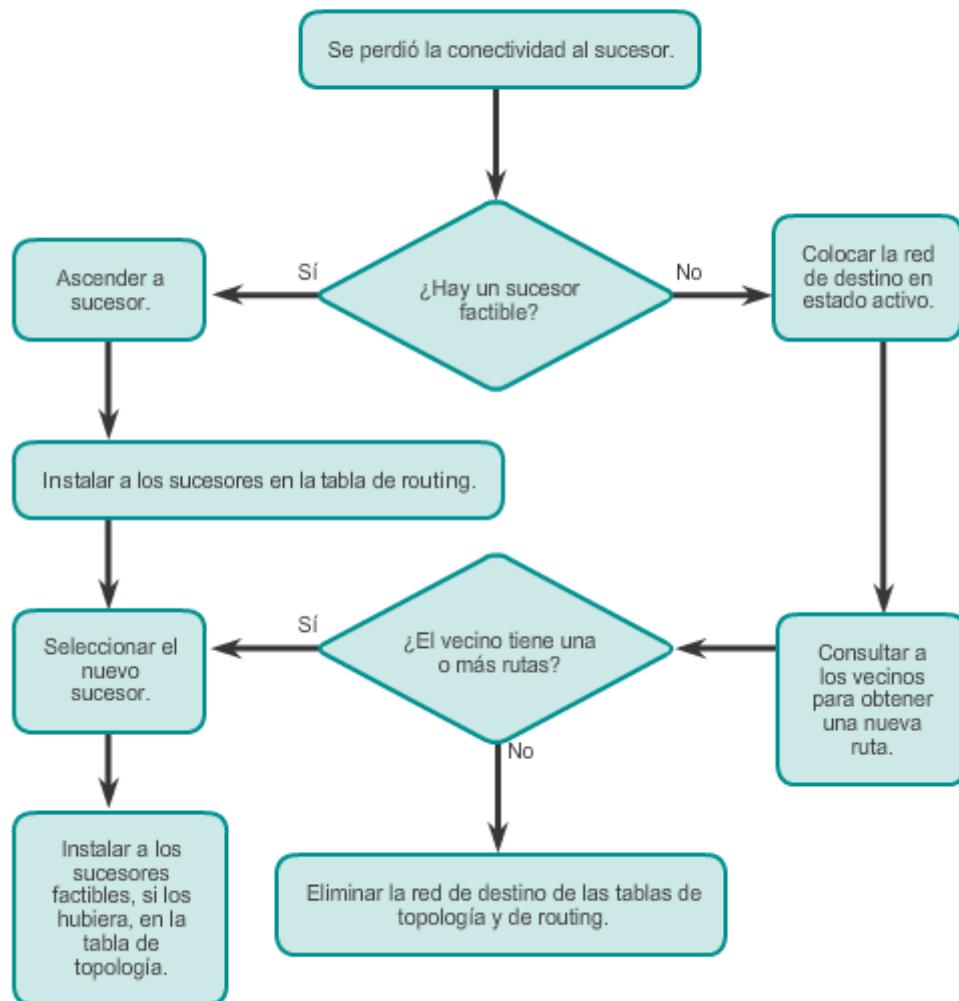
El núcleo de EIGRP son DUAL y su motor de cálculos de ruta EIGRP. El nombre real de esta tecnología es Máquina de Estados Finito (FSM) DUAL. Esta FSM contiene toda la lógica que se utiliza para calcular y comparar rutas en una red EIGRP. La figura muestra una versión simplificada de FSM DUAL.

Una FSM es una máquina abstracta, no un dispositivo mecánico con partes móviles. 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 la manera en que un dispositivo, un programa informático o un algoritmo de routing reaccionan ante un conjunto de eventos de entrada.

Las FSM exceden el ámbito de este curso. Sin embargo, el concepto se utiliza para examinar algunos de los resultados de las FSM de EIGRP mediante el uso del comando **debug eigrp fsm**. Utilice este comando para analizar qué hace DUAL cuando se elimina una ruta de la tabla de routing.

## Comando show ip protocols

### Máquina de estados finitos DUAL



### Capítulo 7: EIGRP 7.3.4.2 DUAL: sucesor factible

Actualmente, el R2 usa al R3 como el sucesor a 192.168.1.0/24. Además, el R2 actualmente incluye al R1 como un FS, como se muestra en la figura 1.

El resultado de **show ip eigrp topology** para el R2 en la figura 2 verifica que el R3 es el sucesor y el R1 es el FS para la red 192.168.1.0/24. Para comprender la manera en que DUAL puede usar un FS cuando la ruta que usa el sucesor no está disponible, se simula una falla de enlace entre el R2 y el R3.

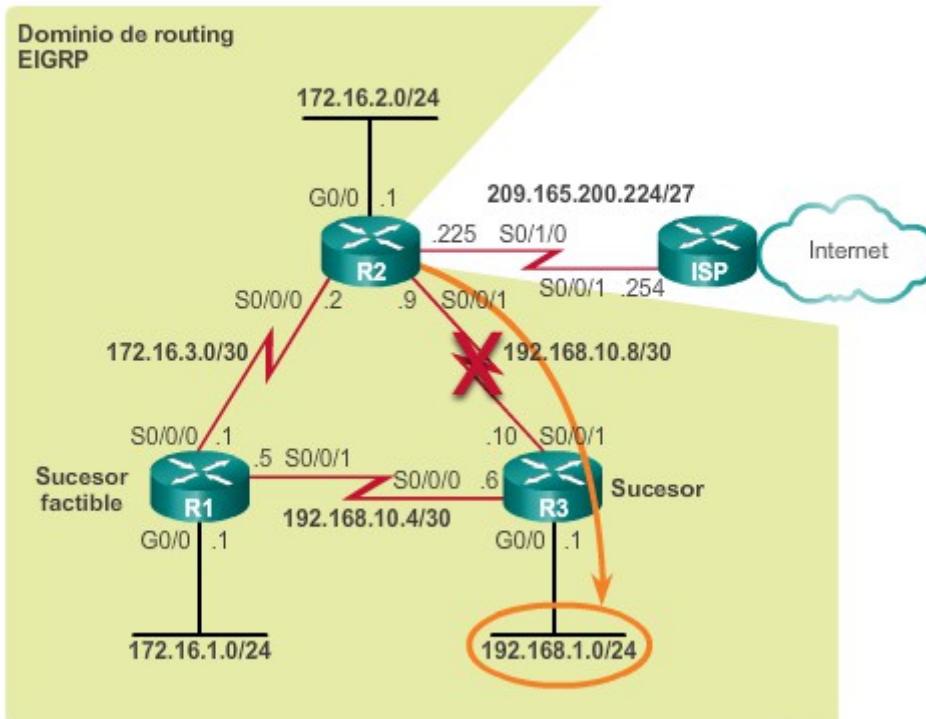
Antes de simular la falla, debe habilitarse la depuración de DUAL mediante el comando **debug eigrp fsm** en el R2, como se muestra en la figura 3. La falla de enlace se simula mediante el comando **shutdown** en la interfaz Serial 0/0/1 del R2.

El resultado de **debug** muestra la actividad que genera DUAL cuando un enlace queda fuera de servicio. El R2 debe informar a todos los vecinos EIGRP del enlace perdido y también actualizar sus propias tablas de routing y de topología. En este ejemplo, solo se muestran resultados de **debug** seleccionados. Observe en particular que la FSM DUAL busca y encuentra un FS para la ruta en la tabla de topología de EIGRP.

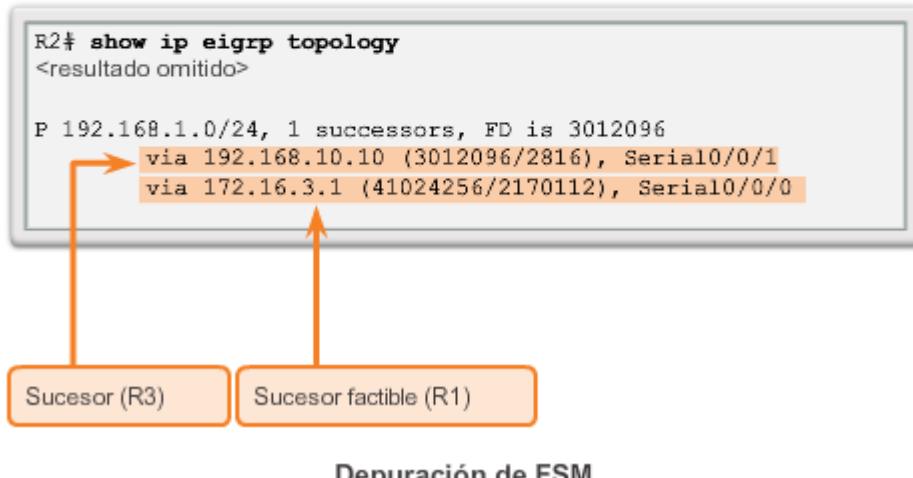
El FS R1 ahora se convierte en el sucesor y se instala en la tabla de routing como la nueva mejor ruta a 192.168.1.0/24, como se muestra en la figura 4. Con un FS, este cambio en la tabla de routing sucede casi de inmediato.

Como se muestra en la figura 5, la tabla de topología para el R2 ahora muestra al R1 como el sucesor, y no hay nuevos FS. Si el enlace entre el R2 y el R3 se activa nuevamente, el R3 vuelve a ser el sucesor y el R1 se convierte una vez más en el FS.

**Topología EIGRP para IPv4**



## Entrada de la tabla de topología del R2 para 192.168.1.0/24



```
R2# debug eigrp fsm
EIGRP Finite State Machine debugging is on
R2# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)# interface s 0/0/1
R2(config-if)# shutdown
<resultado omitido>
EIGRP-IPv4(1):Find FS for dest 192.168.1.0/24. FD is 3012096,
RD is 3012096 on tid 0
DUAL: AS(1) Removing dest 172.16.1.0/24, nexthop 192.168.10.10
DUAL: AS(1) RT installed 172.16.1.0/24 via 172.16.3.1
<resultado omitido>
R2(config-if)# end
R2# undebug all
```

### Entrada de la tabla de routing del R2 para 192.168.1.0/24

```
R2# show ip route
<resultado omitido>

D 192.168.1.0/24 [90/41024256] via 172.16.3.1, 00:15:51,
Serial0/0/0
```

Nuevo sucesor (R1)



### Entrada de la tabla de topología del R2 para 192.168.1.0/24

```
R2# show ip eigrp topology
<resultado omitido>

P 192.168.1.0/24, 1 successors, FD is 41024256
    via 172.16.3.1 (41024256/2170112), Serial0/0/0
```

Sucesor (R1)      No hay un sucesor factible.



### Capítulo 7: EIGRP 7.3.4.3 DUAL: ausencia de sucesor factible

A veces, la ruta al sucesor falla y no hay ningún FS. En este caso, DUAL no tiene una ruta de respaldo a la red sin bucles garantizada, de manera que la ruta no está en la tabla de topología como un FS. Si no hay ningún FS en la tabla de topología, DUAL pone la red en estado activo. DUAL consulta activamente a sus vecinos en busca de un nuevo sucesor.

El R1 usa actualmente al R3 como el sucesor a 192.168.1.0/24, como se muestra en la figura 1. Sin embargo, el R1 no tiene al R2 incluido como un FS, porque el R2 no cumple la FC. Para comprender la manera en que DUAL busca un nuevo sucesor cuando no hay un FS, se simula una falla de enlace entre el R1 y el R3.

Antes de simular la falla de enlace, se habilita la depuración de DUAL con el comando **debug eigrp fsm** en el R1, como se muestra en la figura 2. La falla de enlace se simula mediante el comando **shutdown** en la interfaz Serial 0/0/1 del R1.

Cuando el sucesor deja de estar disponible y no hay un sucesor factible, DUAL pone la ruta en estado activo. DUAL envía consultas EIGRP en las que les pregunta a otros routers por una ruta a la red. Los otros routers devuelven respuestas EIGRP, que le permiten al emisor de la consulta EIGRP saber si tienen o no tienen una ruta a la red solicitada. Si ninguna de estas respuestas EIGRP incluye una ruta a esa red, el emisor de la consulta no tiene una ruta a esa red.

El resultado seleccionado de debug en la figura 2 muestra a la red 192.168.1.0/24 puesta en estado activo y las consultas EIGRP enviadas a 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.

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 lleva más tiempo que si DUAL tuviese un FS en su tabla de topología y pudiese agregar la nueva ruta a la tabla de routing rápidamente. Observe que en la figura 3 el R1 tiene una nueva ruta a la red 192.168.1.0/24. El nuevo sucesor EIGRP es el router R2.

En la figura 4, se muestra que la tabla de topología para el R1 ahora tiene al R2 como el sucesor, sin nuevos FS. Si el enlace entre el R1 y el R3 se activa nuevamente, el R3 vuelve a ser el sucesor. No obstante, el R2 aún no es el FS, porque no cumple la FC.

#### Entrada de la tabla de topología del R1 para 192.168.1.0/24

```
R1# show ip eigrp topology
<resultado omitido>

P 192.168.1.0/24, 1 successors, FD is 2170112
    via 192.168.10.6 (2170112/2816), Serial0/0/1
```

The diagram illustrates the output of the `show ip eigrp topology` command on router R1. The output shows a route to network 192.168.1.0/24 with one successor, via interface Serial0/0/1 to router 192.168.10.6. An orange arrow points from the 'via' line to a box labeled "Sucesor (R3)". Another orange box labeled "No hay un sucesor factible" is shown below the command output.

## Depuración de FSM

```
R1# debug eigrp fsm
EIGRP Finite State Machine debugging is on
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface s 0/0/1
R1(config-if)# shutdown
<resultado omitido>
EIGRP-IPv4(1): Find FS for dest 192.168.1.0/24. FD is 2170112,
RD is 2170112
DUAL: AS(1) Dest 192.168.1.0/24 entering active state for tid
0.
EIGRP-IPv4(1): dest(192.168.1.0/24) active
EIGRP-IPv4(1): rcvreply: 192.168.1.0/24 via 172.16.3.2 metric
41024256/3012096 EIGRP-IPv4(1): reply count is 1
EIGRP-IPv4(1): Find FS for dest 192.168.1.0/24. FD is
72057594037927935, RD is 72057594037927935
DUAL: AS(1) Removing dest 192.168.1.0/24, nexthop 192.168.10.6
DUAL: AS(1) RT installed 192.168.1.0/24 via 172.16.3.2
<resultado omitido>
R1(config-if)# end
R1# undebug all
```

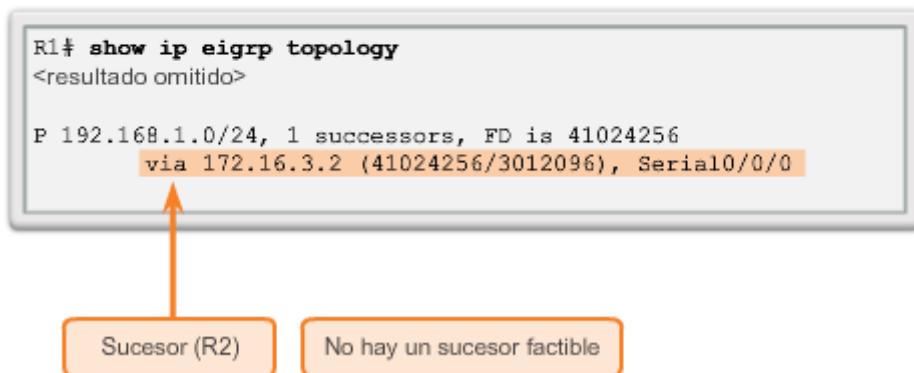
## Entrada de la tabla de routing del R1 para 192.168.1.0/24

```
R1# show ip route
<resultado omitido>

D      192.168.1.0/24 [90/41024256] via 172.16.3.2, 00:05:25,
      Serial0/0/0
```

Nuevo sucesor (R2)

## **Entrada de la tabla de topología del R1 para 192.168.1.0/24**



## [Capítulo 7: EIGRP 7.3.4.4 Packet Tracer: Investigación de la FSM DUAL](#)

### **Información básica/situación**

En esta actividad, modificará la fórmula de la métrica de EIGRP para generar un cambio en la topología. Esto le permite ver cómo reacciona EIGRP cuando un vecino queda fuera de servicio debido a circunstancias imprevistas. A continuación, utilizará el comando **debug** para ver los cambios en la topología y la manera en que la máquina de estados finitos de DUAL determina las rutas de sucesor y de sucesor factible para volver a converger la red.

[Packet Tracer: Investigación de la FSM DUAL \(instrucciones\)](#)

[Packet Tracer: Investigación de la FSM DUAL \(PKA\)](#)

## [Capítulo 7: EIGRP 7.4.1.1 EIGRP para IPv6](#)

De manera similar a su homólogo para IPv4, EIGRP para IPv6 intercambia información de routing para completar la tabla de routing IPv6 con prefijos remotos. EIGRP para IPv6 está disponible a partir del IOS de Cisco versión 12.4(6)T.

**Nota:** en IPv6, la dirección de red se denomina “prefijo” y la máscara de subred se denomina “longitud de prefijo”.

EIGRP para IPv4 se ejecuta a través de la capa de red IPv4, por lo que se comunica con otros peers IPv4 EIGRP y solo anuncia rutas IPv4. EIGRP para IPv6 tiene la misma funcionalidad

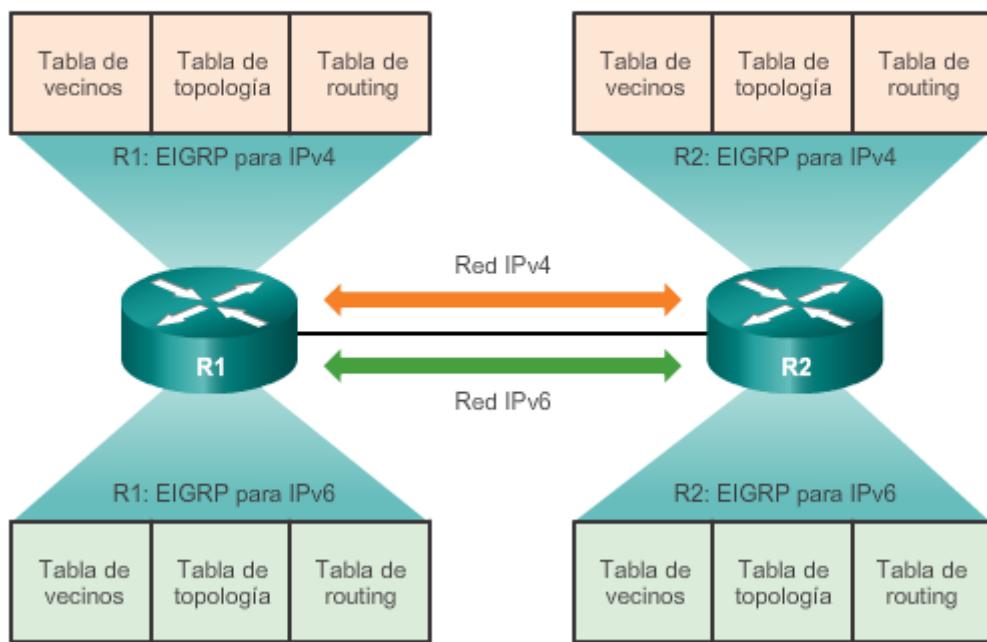
que EIGRP para IPv4, pero utiliza IPv6 como el protocolo de capa de red, se comunica con peers EIGRP para IPv6 y anuncia rutas IPv6.

EIGRP para IPv6 también usa DUAL como motor de cómputo para garantizar rutas principales y de respaldo sin bucles a través de todo el dominio de routing.

Al igual que con todos los protocolos de routing IPv6, EIGRP para IPv6 tiene procesos separados de los de su homólogo para IPv4. Los procesos y las operaciones son básicamente los mismos que en el protocolo de routing IPv4; no obstante, se ejecutan de manera independiente. EIGRP para IPv4 y EIGRP para IPv6 tienen tablas de vecinos EIGRP, tablas de topología EIGRP y tablas de IP routing separadas, como se muestra en la ilustración. EIGRP para IPv6 es un módulo dependiente de protocolo (PDM) separado.

Los comandos de configuración y verificación de EIGRP para IPv6 son muy similares a los que se utilizan en EIGRP para IPv4. Estos comandos se describen más adelante en esta sección.

### EIGRP para IPv4 y EIGRP para IPv6



#### Capítulo 7: EIGRP 7.4.1.2 Comparación entre EIGRP para IPv4 e IPv6

La siguiente es una comparación de las principales características de EIGRP para IPv4 e EIGRP para IPv6:

- **Rutas anunciadas:** EIGRP para IPv4 anuncia redes IPv4, mientras que EIGRP para IPv6 anuncia prefijos IPv6.
- **Vector distancia:** EIGRP para IPv4 y para IPv6 son protocolos de routing vector distancia avanzados. Ambos protocolos usan las mismas distancias administrativas.

- **Tecnología de convergencia:** tanto EIGRP para IPv4 como para IPv6 usan el algoritmo DUAL. Ambos protocolos usan las mismas técnicas y procesos de DUAL, incluidos sucesor, FS, FD y RD.
- **Métrica:** tanto EIGRP para IPv4 como para IPv6 usan ancho de banda, retraso, confiabilidad y carga para su métrica compuesta. Ambos protocolos de routing usan la misma métrica compuesta y, de manera predeterminada, usan solo ancho de banda y retraso.
- **Protocolo de transporte:** el protocolo de transporte confiable (RTP) es responsable de la entrega garantizada de paquetes EIGRP a todos los vecinos para ambos protocolos, EIGRP para IPv4 y para IPv6.
- **Mensajes de actualización:** tanto EIGRP para IPv4 como para IPv6 envían actualizaciones incrementales cuando el estado de un destino cambia. Los términos “parcial” y “limitada” se usan para hacer referencia a las actualizaciones de ambos protocolos.
- **Mecanismo de descubrimiento de vecinos:** tanto EIGRP para IPv4 como EIGRP para IPv6 utilizan un simple mecanismo de saludo para descubrir routers vecinos y formar adyacencias.
- **Direcciones de origen y destino:** EIGRP para IPv4 envía mensajes a la dirección de multidifusión 224.0.0.10. Estos mensajes utilizan la dirección IPv4 de origen de la interfaz de salida. EIGRP para IPv6 envía sus mensajes a la dirección de multidifusión FF02::A. Los mensajes EIGRP para IPv6 se originan en la dirección IPv6 link-local de la interfaz de salida.
- **Autenticación:** EIGRP para IPv4 puede usar autenticación de texto no cifrado o autenticación de síntesis del mensaje 5 (MD5). EIGRP para IPv6 usa MD5.
- **ID del router:** EIGRP para IPv4 y EIGRP para IPv6 usan un número de 32 bits para la ID del router EIGRP. La ID de router de 32 bits se representa con una notación decimal con puntos que comúnmente se considera una dirección IPv4. Si el router EIGRP para IPv6 no está configurado con una dirección IPv4, se debe utilizar el comando **eigrp router-id** para configurar una ID de router de 32 bits. El proceso para determinar la ID del router es el mismo para ambos protocolos EIGRP, para IPv4 y para IPv6.

## Comparación entre EIGRP para IPv4 e IPv6

	EIGRP para IPv4	EIGRP para IPv6
Rutas anunciadas	Redes IPv4	Prefijos IPv6
Vector distancia	Sí	Sí
Tecnología de convergencia	DUAL	DUAL
Métrica	El ancho de banda y el retraso de manera predeterminada, la confiabilidad y la carga son optativas.	El ancho de banda y el retraso de manera predeterminada, la confiabilidad y la carga son optativas.
Protocolo de transporte	RTP	RTP
Mensajes de actualización	Actualizaciones incrementales, parciales y limitadas	Actualizaciones incrementales, parciales y limitadas
Descubrimiento de vecinos	Paquetes de saludo	Paquetes de saludo
Direcciones de origen y destino	Dirección de origen IPv4 y dirección de destino IPv4 de multidifusión 224.0.0.10	Dirección de origen IPv6 link-local y dirección de destino IPv6 de multidifusión FF02::A
Autenticación	Texto no cifrado y MD5	MD5
Id. de router	ID del router de 32bits	ID del router de 32bits

### Capítulo 7: EIGRP 7.4.1.3 Direcciones IPv6 link-local

Los routers que ejecutan un protocolo de routing dinámico, como EIGRP, intercambian mensajes entre vecinos en la misma subred o el mismo enlace. Los routers solo necesitan enviar y recibir mensajes de protocolo de routing con sus vecinos conectados directamente. Estos mensajes siempre se envían desde la dirección IP de origen del router que realiza el reenvío.

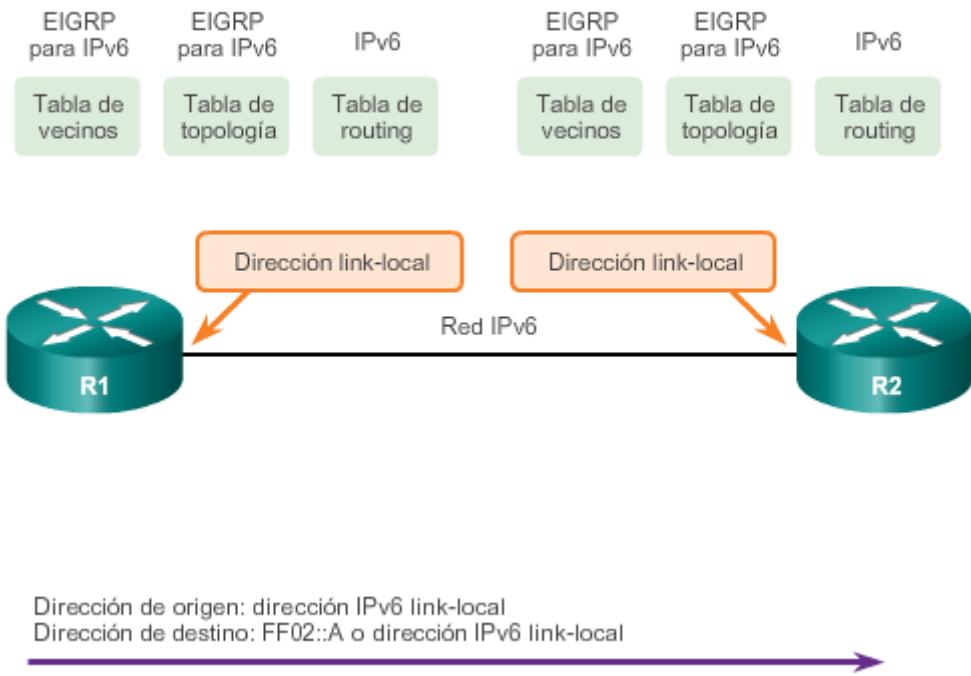
Las direcciones IPv6 link-local son ideales para este propósito. Una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en el mismo enlace y solo en ese enlace (subred). Los paquetes con una dirección link-local de origen o de destino no se pueden enrutar más allá del enlace en el cual se originó el paquete.

Los mensajes EIGRP para IPv6 se envían mediante lo siguiente:

- **Dirección IPv6 de origen:** esta es la dirección IPv6 link-local de la interfaz de salida.
- **Dirección IPv6 de destino:** cuando debe enviarse un paquete a una dirección de multidifusión, se envía a la dirección IPv6 de multidifusión FF02::A, el ámbito de todos los routers EIGRP con link-local. Si el paquete puede enviarse como una dirección de unidifusión, se envía a la dirección link-local del router vecino.

**Nota:** las direcciones IPv6 link-local están en el rango de FE80::/10. El valor /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx, lo que da como resultado un primer hexteto con el rango de 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111 (FEBF).

## EIGRP para IPv6 y direcciones link-local



### Capítulo 7: EIGRP 7.4.1.4 Actividad: comparar EIGRPv4 y EIGRPv6

Actividad: comparar EIGRPv4 y EIGRPv6	EIGRPv4	EIGRPv6	Ambos
Redes IPv4 anunciadas	✓		
Redes IPv6 anunciadas		✓	
Vector distancia			✓
Algoritmo DUAL			✓
Métrica predeterminada: ancho de banda y retraso			✓
Protocolo de transporte: RTP			✓
Actualizaciones incrementales, parciales y limitadas			✓
Descubrimiento de vecinos: paquetes de saludo			✓
Multidifusión 224.0.0.10	✓		
Multidifusión FF02::A		✓	

### Capítulo 7: EIGRP 7.4.2.1 Topología de red EIGRP para IPv6

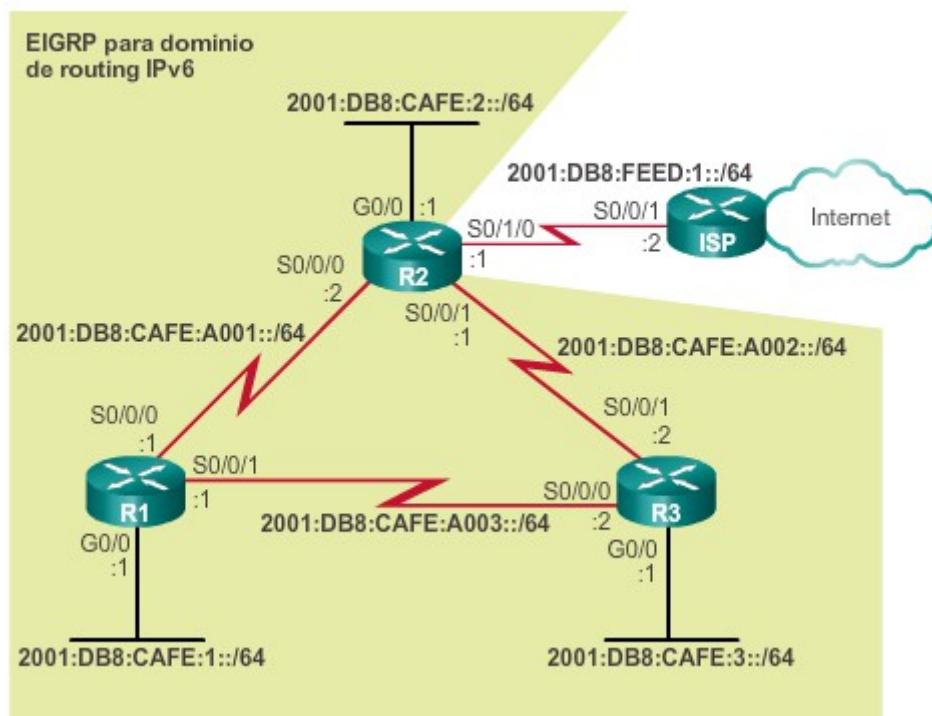
En la figura 1, se muestra la topología de la red que se utiliza para configurar EIGRP para IPv6. Si en la red se ejecuta dual-stack y se utilizan IPv4 e IPv6 en todos los dispositivos, se puede

configurar tanto EIGRP para IPv4 como para IPv6 en todos los routers. No obstante, esta sección se centra solamente en EIGRP para IPv6.

Solo las direcciones IPv6 de unidifusión global se configuraron en cada router.

En las figuras 2, 3 y 4, se muestra la configuración de inicio de interfaz en cada router. Observe los valores de ancho de banda de interfaz de la configuración EIGRP para IPv4 previa. Debido a que EIGRP utiliza las mismas métricas para IPv4 e IPv6, modificar los parámetros de ancho de banda influye en ambos protocolos de routing.

### Topología EIGRP para IPv6



### Configuración inicial de interfaces para el R1

```
R1# show running-config
<resultado omitido>
!
interface GigabitEthernet0/0
  ipv6 address 2001:DB8:CAFE:1::1/64
!
interface Serial0/0/0
  ipv6 address 2001:DB8:CAFE:A001::1/64
  clock rate 64000
!
interface Serial0/0/1
  ipv6 address 2001:DB8:CAFE:A003::1/64
```

### Configuración inicial de interfaces para el R2

```
R2# show running-config
<resultado omitido>
!
interface GigabitEthernet0/0
  ipv6 address 2001:DB8:CAFE:2::1/64
!
interface Serial0/0/0
  ipv6 address 2001:DB8:CAFE:A001::2/64
!
interface Serial0/0/1
  ipv6 address 2001:DB8:CAFE:A002::1/64
  clock rate 64000
!
interface Serial0/1/0
  ipv6 address 2001:DB8:FEED:1::1/64
```

## Configuración inicial de interfaces para el R3

```
R3# show running-config
<resultado omitido>
!
interface GigabitEthernet0/0
  ipv6 address 2001:DB8:CAFE:3::1/64
!
interface Serial0/0/0
  ipv6 address 2001:DB8:CAFE:A003::2/64
  clock rate 64000
!
interface Serial0/0/1
  ipv6 address 2001:DB8:CAFE:A002::2/64
```

### Capítulo 7: EIGRP 7.4.2.2 Configuración de direcciones IPv6 link-local

Las direcciones link-local se crean de manera automática cuando se asigna una dirección IPv6 de unidifusión global a la interfaz. No se requieren direcciones de unidifusión global en una interfaz, pero sí se requieren direcciones IPv6 link-local.

A menos que se configuren manualmente, los routers Cisco crean la dirección link-local utilizando el prefijo FE80::/10 y el proceso EUI-64, como se muestra en la figura 1. EUI-64 implica usar la dirección MAC de Ethernet de 48 bits, insertar FFFE en el medio e invertir el séptimo bit. Para las interfaces seriales, Cisco usa la dirección MAC de una interfaz Ethernet. Un router con varias interfaces seriales puede asignar la misma dirección link-local a cada interfaz IPv6, porque las direcciones link-local solo necesitan ser locales en el enlace.

Las direcciones link-local creadas con el formato EUI-64 o, en algunos casos, con ID de interfaces aleatorias, hacen que resulte difícil reconocer y recordar esas direcciones. Debido a que los protocolos de routing IPv6 utilizan direcciones IPv6 link-local para el direccionamiento de unidifusión y la información de dirección de siguiente salto en la tabla de routing, habitualmente se busca que sea una dirección fácil de reconocer. Configurar la dirección link-local manualmente permite crear una dirección reconocible y más fácil de recordar.

Las direcciones link-local se pueden configurar manualmente mediante el mismo comando del modo de configuración de interfaz que se utiliza para crear direcciones IPv6 de unidifusión global, pero con diferentes parámetros:

```
Router(config-if)# ipv6 address dirección-link-local link-local
```

Una dirección link-local tiene un prefijo dentro del rango FE80 a FEBF. Cuando una dirección comienza con este hextet (segmento de 16 bits), la palabra clave **link-local** debe escribirse después de la dirección.

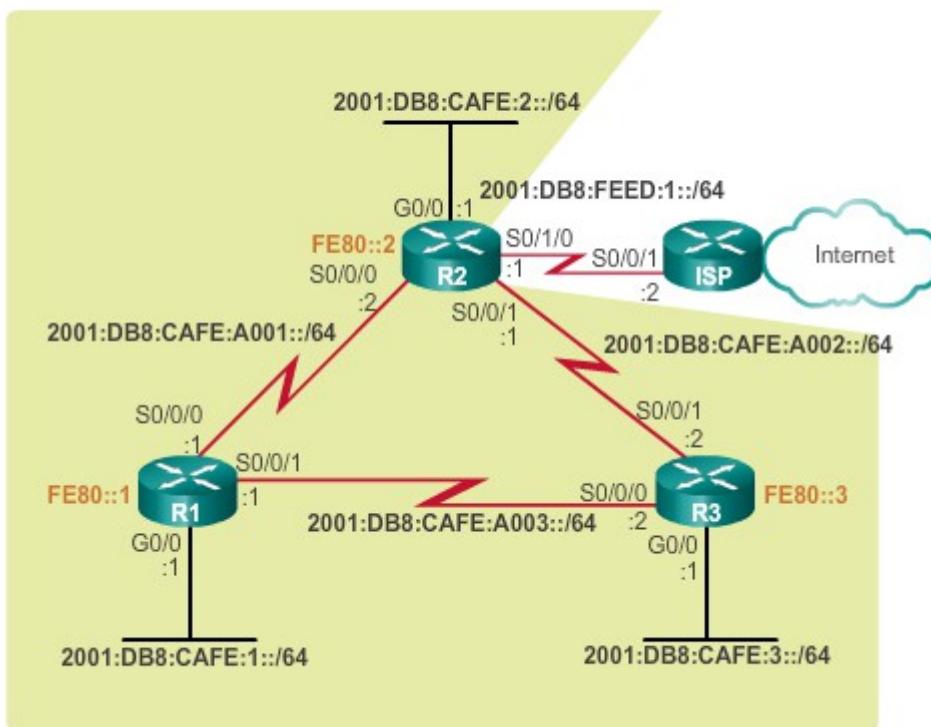
En la figura 2, se muestra la configuración de una dirección link-local mediante el comando **ipv6 address** del modo de configuración de interfaz. La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces de R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

De manera similar al R1, en la figura 3 el router R2 se configura con FE80::2 como la dirección IPv6 link-local en todas sus interfaces.

Utilice el verificador de sintaxis en la figura 4 para configurar FE80::3 como la dirección link-local en todas las interfaces del R3.

Como se muestra en la figura 5, el comando **show ipv6 interface brief** se usa para verificar las direcciones IPv6 link-local y de unidifusión global en todas las interfaces.

## Topología EIGRP para IPv6



Configuración de direcciones link-local en el R1

```
R1(config)# interface s 0/0/0
R1(config-if)# ipv6 address fe80::1 ?
      link-local  Use link-local address

R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface s 0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface g 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#

```

## Configuración de direcciones link-local en el R2

```
R2(config)# interface s 0/0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface s 0/0/1
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface s 0/1/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# exit
R2(config)# interface g 0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)#

```

Configure las interfaces del R3 con la dirección IPv6 link-local FE80::3 en el siguiente orden:

- Serial 0/0/0
- Serial 0/0/1
- GigabitEthernet 0/0
- Utilice el comando **exit** antes de configurar la siguiente interfaz.

```
R3(config)# interface serial 0/0/0
R3(config-if)# ipv6 address fe80::3 link-local
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config-if)# ipv6 address fe80::3 link-local
R3(config-if)# exit
R3(config)# interface gigabitethernet 0/0
R3(config-if)# ipv6 address fe80::3 link-local
R3(config-if)#
Configuró correctamente la dirección IPv6 link-local.
```

### Verificación de direcciones link-local en el R1

```
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::1
  2001:DB8:CAFE:1::1
Serial0/0/0              [up/up]
  FE80::1
  2001:DB8:CAFE:A001::1
Serial0/0/1              [up/up]
  FE80::1
  2001:DB8:CAFE:A003::1
R1#
```

En todas las interfaces está configurada la misma dirección IPv6 link-local.

### Capítulo 7: EIGRP 7.4.2.3 Configuración del proceso de routing EIGRP para IPv6

El comando **ipv6 unicast-routing** del modo de configuración global habilita el routing IPv6 en el router. Este comando es necesario antes de poder configurar cualquier protocolo de routing IPv6. No se requiere para configurar direcciones IPv6 en las interfaces, pero es necesario para habilitar el router como un router IPv6.

#### EIGRP para IPv6

El siguiente comando del modo de configuración global se utiliza para ingresar al modo de configuración del router para EIGRP para IPv6:

```
Router(config)# ipv6 router eigrp sistema-autónomo
```

De manera similar a lo que sucede en EIGRP para IPv4, el valor de *sistema-autónomo* debe ser el mismo en todos los routers en el dominio de routing. En la figura 1, el proceso de routing EIGRP para IPv6 no se pudo configurar hasta que el routing IPv6 se habilitó con el comando del modo de configuración global **ipv6 unicast-routing**.

#### **Id. de router**

Como se muestra en la figura 2, el comando **eigrp router-id** se utiliza para configurar la ID del router. EIGRP para IPv6 utiliza un valor de 32 bits para la ID del router. Para obtener ese valor, EIGRP para IPv6 utiliza el mismo proceso que EIGRP para IPv4. El comando **eigrp router-id** tiene prioridad sobre cualquier dirección de loopback o dirección IPv4 de interfaz física. Si un router EIGRP para IPv6 no tiene ninguna interfaz activa con una dirección IPv4, se requiere el comando **eigrp router-id**.

La ID del router debe ser un número único de 32 bits en el dominio de routing EIGRP para IP; de lo contrario, pueden ocurrir incongruencias de routing.

**Nota:** el comando **eigrp router-id** se utiliza para configurar la ID del router para EIGRP. Algunas versiones del IOS aceptan el comando **router-id**, sin tener que especificare**igrp** primero. Sin embargo, la configuración en ejecución muestra **eigrp router-id**, independientemente de cuál sea el comando que se utiliza.

De manera predeterminada, el proceso EIGRP para IPv6 se encuentra en estado desactivado. Se requiere el comando **no shutdown** para activar el proceso EIGRP para IPv6, como se muestra en la figura 3. Este comando no se requiere para EIGRP para IPv4. Aunque EIGRP para IPv6 esté habilitado, no se pueden enviar ni recibir actualizaciones de adyacencias de vecinos ni de routing hasta que EIGRP se active en las interfaces apropiadas.

Se requieren el comando **no shutdown** y una ID de router para que el router establezca adyacencias de vecinos.

En la figura 4, se muestra la configuración de EIGRP para IPv6 completa para el router R2.

Utilice el verificador de sintaxis de la figura 5 para configurar el proceso EIGRP para IPv6 en el router R3.

### Proceso de routing EIGRP para IPv6 en el R1

```
R1(config)# ipv6 router eigrp 2
% IPv6 routing not enabled
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 router eigrp 2
R1(config-rtr) #
```

### ID del router EIGRP para IPv6 en el R1

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# eigrp router-id 1.0.0.0
R1(config-rtr) #
```

### Comando no shutdown de EIGRP para IPv6 en el R1

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# eigrp router-id 1.0.0.0
R1(config-rtr)# no shutdown
R1(config-rtr) #
```

## Configuración del proceso de routing EIGRP para IPv6 en el R2

```
R2 (config)# ipv6 unicast-routing
R2 (config)# ipv6 router eigrp 2
R2 (config-rtr)# eigrp router-id 2.0.0.0
R2 (config-rtr)# no shutdown
R2 (config-rtr)#End
```

Habilitar EIGRP para IPv6 en el R3, realizando las tareas en el siguiente orden:

- Habilite el routing IPv6.
- Habilite EIGRP para IPv6 usando 2 como AS.
- Configure la ID del router 3.0.0.0.
- Active el proceso EIGRP para IPv6.

```
R3 (config)# ipv6 unicast-routing
R3 (config)# ipv6 router eigrp 2
R3 (config-rtr)# eigrp router-id 3.0.0.0
R3 (config-rtr)# no shutdown
R3 (config-if) #
```

Configuró correctamente el proceso de routing EIGRP para IPv6.

### Capítulo 7: EIGRP 7.4.2.4 Comando de interfaz ipv6 eigrp

EIGRP para IPv6 utiliza un método diferente para habilitar una interfaz para EIGRP. En lugar de usar el comando **network** del modo de configuración del router para especificar las direcciones de interfaz que coinciden, EIGRP para IPv6 se configura directamente en la interfaz.

Utilice el siguiente comando del modo de configuración de interfaz para habilitar EIGRP para IPv6 en una interfaz:

```
Router(config-if)# ipv6 eigrpsistema-autónomo
```

El valor de *sistema-autónomo* debe ser el mismo número que el utilizado para habilitar el proceso de routing EIGRP. De manera similar al comando **network** que se utiliza en EIGRP para IPv4, el comando **ipv6 eigrp interface** lleva a cabo lo siguiente:

- Habilita la interfaz para que forme adyacencias y envíe o reciba actualizaciones de EIGRP para IPv6.
- Incluye el prefijo (red) de la interfaz en las actualizaciones de routing EIGRP para IPv6.

En la figura 1, se muestra la configuración para habilitar EIGRP para IPv6 en las interfaces de los routers R1 y R2. Observe el mensaje a continuación de la interfaz serial 0/0/0 en el R2:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1 (Serial0/0/0) is up: new adjacency
```

Este mensaje indica que el R2 formó una adyacencia EIGRP-IPv6 con el vecino en la dirección link-local FE80::1. Debido a que se configuraron direcciones link-local estáticas en los tres routers, es fácil determinar que esta adyacencia es con el router R1 (FE80::1).

Utilice el verificador de sintaxis de la figura 2 para habilitar EIGRP para IPv6 en las interfaces del R3.

### Interfaz pasiva con EIGRP para IPv6

El mismo comando **passive-interface** que se utiliza para IPv4 se usa para configurar una interfaz como pasiva en EIGRP para IPv6. Como se muestra en la figura 3, se utiliza el comando **show ipv6 protocols** para verificar la configuración.

### Habilitación de EIGRP para IPv6 en una interfaz

```
R1(config)# interface g0/0
R1(config-if)# ipv6 eigrp 2
R1(config-if)# exit
R1(config)# interface s 0/0/0
R1(config-if)# ipv6 eigrp 2
R1(config-if)# exit
R1(config)# interface s 0/0/1
R1(config-if)# ipv6 eigrp 2
R1(config-if)#

```

```
R2(config)# interface g 0/0
R2(config-if)# ipv6 eigrp 2
R2(config-if)# exit
R2(config)# interface s 0/0/0
R2(config-if)# ipv6 eigrp 2
R2(config-if)# exit
%DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor FE80::1
(Serial0/0/0) is up: new adjacency
R2(config)# interface s 0/0/1
R2(config-if)# ipv6 eigrp 2
R2(config-if)#

```

### Habilitación de EIGRP para IPv6 en la interfaz

Habilite EIGRP para IPv6, con 2 como AS, en las interfaces del R3 en el siguiente orden:

- GigabitEthernet 0/0
- Serial 0/0/0
- Serial 0/0/1
- Utilice el comando **exit** antes de configurar la siguiente interfaz.

```
R3(config)# interface gigabitethernet 0/0
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface serial 0/0/0
R3(config-if)# ipv6 eigrp 2
R3(config-if)#
*Mar 4 03:02:00.696: %DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor
FE80::1 (Serial0/0/0) is up: new adjacency
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config-if)# ipv6 eigrp 2
*Mar 4 03:02:17.264: %DUAL-5-NBRCHANGE: EIGRP-IPv6 2: Neighbor
FE80::2 (Serial0/0/1) is up: new adjacency
R3(config-if)#

```

Configuró correctamente EIGRP para IPv6 en las interfaces.

## Configuración y verificación del EIGRP para IPv6 con una interfaz pasiva

```
R1(config)# ipv6 router eigrp 2
R1(config-rtr)# passive-interface gigabitethernet 0/0
R1(config-rtr)# end

R1# show ipv6 protocols

IPv6 Routing Protocol is "eigrp 2"
EIGRP-IPv6 Protocol for AS(2)
<resultado omitido>

Interfaces:
  Serial0/0/0
  Serial0/0/1
  GigabitEthernet0/0 (passive)
Redistribution:
  None
R1#
```

### Capítulo 7: EIGRP 7.4.3.1 Verificación de EIGRP para IPv6: análisis de vecinos

De manera similar a lo que sucede en EIGRP para IPv4, antes de que se puedan enviar actualizaciones de EIGRP para IPv6, los routers deben establecer adyacencias con sus vecinos, como se muestra en la figura 1.

Utilice el comando **show ipv6 eigrp neighbors** para ver la tabla de vecinos y verificar que EIGRP para IPv6 haya establecido una adyacencia con sus vecinos. El resultado que se ve en la figura 2 muestra la dirección IPv6 link-local del vecino adyacente y la interfaz que utiliza el router para llegar a ese vecino EIGRP. Al utilizar direcciones link-local detalladas, resulta más fácil reconocer a los vecinos R2 en FE80::2 y R3 en FE80::3.

El resultado del comando **show ipv6 eigrp neighbors** incluye lo siguiente:

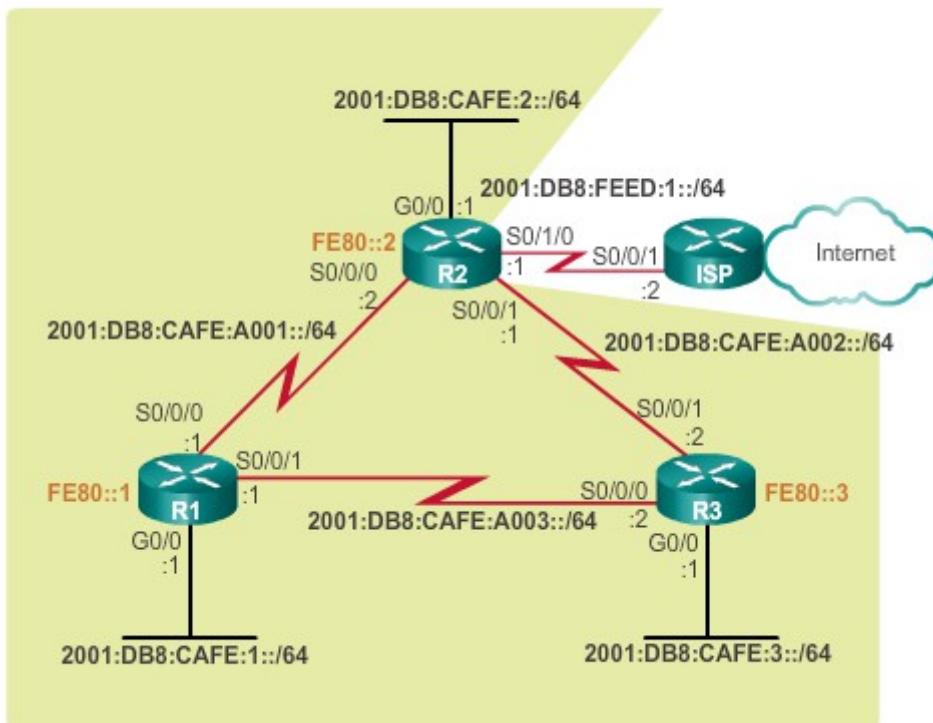
- **Columna H:** enumera los vecinos en el orden en que fueron descubiertos.
- **Address:** dirección IPv6 link-local del vecino.
- **Interface:** la interfaz local en la cual se recibió este paquete de saludo.
- **Hold:** el tiempo de espera actual. Cuando se recibe un paquete de saludo, este valor se restablece al tiempo de espera máximo para esa interfaz y, luego, se realiza una cuenta regresiva hasta cero. Si se llega a cero, el vecino se considera inactivo.
- **Uptime:** la cantidad de tiempo desde que se agregó este vecino a la tabla de vecinos.
- **SRTT y RTO:** utilizados por RTP para administrar paquetes EIGRP confiables.

- **Q Cnt (conteo de cola):** siempre debe ser cero. Si es más que cero, hay paquetes EIGRP que esperan ser enviados.
- **Seq Num (número de secuencia):** se utiliza para rastrear paquetes de actualización, de consulta y de respuesta.

El comando **show ipv6 eigrp neighbors** es útil para verificar y resolver problemas de EIGRP para IPv6. Si un vecino esperado no se encuentra en la lista, asegúrese de que ambos extremos del enlace tengan estado up/up mediante el comando **show ipv6 interface brief**. En EIGRP para IPv6, existen los mismos requisitos para establecer adyacencias de vecinos que en EIGRP para IPv4. Si ambos lados del enlace tienen interfaces activas, verifique lo siguiente:

- ¿Ambos routers están configurados con el mismo número de sistema autónomo de EIGRP?
- ¿La interfaz está habilitada para EIGRP para IPv6 con el número de sistema autónomo correcto?

## Topología EIGRP para IPv6



Comando `show ipv6 eigrp neighbors`

EIGRP-IPv6 Neighbors for AS(2)							
H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO (ms)	Q Seq Cnt Num
1	Link-local address: FE80::3	Se0/0/1	13	00:37:17	45	270	0 8
0	Link-local address: FE80::2	Se0/0/0	14	00:53:16	32	2370	0 8

Dirección IPv6 link-local del vecino.

Interfaz local que recibe paquetes de saludo EIGRP para IPv6.

Cantidad de tiempo desde que el vecino se agregó a la tabla de vecinos.

Segundos restantes antes de declarar que el vecino está inactivo.

El tiempo de espera actual, que se restablece al tiempo de espera máximo cada vez que se recibe un paquete de saludo.

### Capítulo 7: EIGRP 7.4.3.2 Verificación de EIGRP para IPv6: comando `show ip protocols`

El comando **show ipv6 protocols** muestra los parámetros y otra información acerca del estado de cualquier proceso activo de protocolo de routing IPv6 actualmente configurado en el router.

El comando **show ipv6 protocols** muestra distintos tipos de resultados específicos de cada protocolo de routing IPv6.

El resultado en la ilustración indica varios de los parámetros de EIGRP para IPv6 analizados anteriormente, incluido lo siguiente:

1. EIGRP para IPv6 es un protocolo de routing dinámico activo en el R1, configurado con el número de sistema autónomo 2.
2. Estos son los valores  $k$  utilizados para calcular la métrica compuesta de EIGRP. De manera predeterminada, K1 y K3 están establecidos en 1, y K2, K4 y K5 están establecidos en 0.
3. La ID de router EIGRP para IPv6 del R1 es 1.0.0.0.
4. Al igual que sucede con EIGRP para IPv4, las distancias administrativas de EIGRP para IPv6 son AD interna de 90 y externa de 170 (valores predeterminados).
5. Las interfaces habilitadas para EIGRP para IPv6.

El resultado del comando **show ipv6 protocols** es útil para depurar operaciones de routing. En la sección Interfaces, se muestra cuáles interfaces EIGRP para IPv6 se habilitaron. Esto es útil para verificar que EIGRP está habilitado en todas las interfaces apropiadas con el número de sistema autónomo correcto.

#### Comando show ipv6 protocols

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 2"
EIGRP-IPv6 Protocol for AS(2) 1 Protocolo de routing e Id. de proceso
(número de AS)

Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 2 Valores K utilizados
en métrica
compuesta

NSF-aware route hold timer is 240
Router-ID: 1.0.0.0 3 Id. de router EIGRP
Topology : 0 (base)
Active Timer: 3 min
Distance: internal 90 external 170 4 Distancias administrativas de
EIGRP
Maximum path: 16
Maximum hopcount 100
Maximum metric variance 1

Interfaces: 5 Interfaces habilitadas para EIGRP para IPv6
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1

Redistribution:
None
R1#
```

Capítulo 7:

[EIGRP 7.4.3.3 Verificación de EIGRP para IPv6: análisis de la tabla de routing IPv6](#)

Al igual que con cualquier protocolo de routing, el objetivo es completar la tabla de routing IP con rutas a redes remotas y las mejores rutas para llegar a aquellas redes. Como con IPv4, es importante analizar la tabla de routing IPv6 y determinar si está completada con las rutas correctas.

La tabla de routing IPv6 se examina mediante el comando **show ipv6 route**. Las rutas EIGRP para IPv6 se indican en la tabla de routing con una D, al igual que en su homólogo para IPv4.

En la figura 1, se muestra que el R1 tiene instaladas tres rutas EIGRP a redes IPv6 remotas en su tabla de routing IPv6:

- 2001:DB8:CAFE:2::/64 a través del R3 (FE80::3), mediante su interfaz Serial 0/0/1
- 2001:DB8:CAFE:3::/64 a través del R3 (FE80::3), mediante su interfaz Serial 0/0/1
- 2001:DB8:CAFE:A002::/64 a través del R3 (FE80::3), mediante su interfaz Serial 0/0/1

Las tres rutas utilizan al R3 como router de siguiente salto (sucesor). Observe que en la tabla de routing se utiliza la dirección link-local como la dirección del siguiente salto. Debido a que en cada router se configuraron todas las interfaces con una dirección link-local única y distinguible, es fácil reconocer que el router de siguiente salto a través de FE80::3 es el router R3.

En la figura 2, se muestra la tabla de routing IPv6 del R2.

En la figura 3, se muestra la tabla de routing del R3. Observe que el R3 tiene dos rutas del mismo costo a 2001:DB8:CAFE:A001::/64. Una ruta es a través del R1 en FE80::1, y la otra es a través del R2 en FE80::2.

### Análisis de la tabla de routing IPv6 del R1

```
R1# show ipv6 route
<resultado omitido>
C 2001:DB8:CAFE:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
D 2001:DB8:CAFE:2::/64 [90/3524096]
    via FE80::3, Serial0/0/1
D 2001:DB8:CAFE:3::/64 [90/2170112]
    via FE80::3, Serial0/0/1
C 2001:DB8:CAFE:A001::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:CAFE:A001::1/128 [0/0]
    via Serial0/0/0, receive
D 2001:DB8:CAFE:A002::/64 [90/3523840]
    via FE80::3, Serial0/0/1
C 2001:DB8:CAFE:A003::/64 [0/0]
    via Serial0/0/1, directly connected
L 2001:DB8:CAFE:A003::1/128 [0/0]
    via Serial0/0/1, receive
L FF00::/8 [0/0]
    via Null0, receive
R1#
```

### Análisis de la tabla de routing IPv6 del R2

```
R2# show ipv6 route
<resultado omitido>
D 2001:DB8:CAFE:1::/64 [90/3524096]
    via FE80::3, Serial0/0/1
C 2001:DB8:CAFE:2::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:2::1/128 [0/0]
    via GigabitEthernet0/0, receive
D 2001:DB8:CAFE:3::/64 [90/3012096]
    via FE80::3, Serial0/0/1
C 2001:DB8:CAFE:A001::/64 [0/0]
    via Serial0/0/0, directly connected
L 2001:DB8:CAFE:A001::2/128 [0/0]
    via Serial0/0/0, receive
C 2001:DB8:CAFE:A002::/64 [0/0]
    via Serial0/0/1, directly connected
L 2001:DB8:CAFE:A002::1/128 [0/0]
    via Serial0/0/1, receive
D 2001:DB8:CAFE:A003::/64 [90/3523840]
    via FE80::3, Serial0/0/1
C 2001:DB8:FEED:1::/64 [0/0]
    via Loopback6, directly connected
L 2001:DB8:FEED:1::1/128 [0/0]
    via Loopback6, receive
L FF00::/8 [0/0]
    via Null0, receive
R2#
```

### Análisis de la tabla de routing IPv6 del R3

```
R3# show ipv6 route
<resultado omitido>

D  2001:DB8:CAFE:1::/64 [90/2170112]
    via FE80::1, Serial0/0/0
D  2001:DB8:CAFE:2::/64 [90/3012096]
    via FE80::2, Serial0/0/1
C  2001:DB8:CAFE:3::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L  2001:DB8:CAFE:3::1/128 [0/0]
    via GigabitEthernet0/0, receive
D  2001:DB8:CAFE:A001::/64 [90/41024000]
    via FE80::1, Serial0/0/0
    via FE80::2, Serial0/0/1
C  2001:DB8:CAFE:A002::/64 [0/0]
    via Serial0/0/1, directly connected
L  2001:DB8:CAFE:A002::2/128 [0/0]
    via Serial0/0/1, receive
C  2001:DB8:CAFE:A003::/64 [0/0]
    via Serial0/0/0, directly connected
L  2001:DB8:CAFE:A003::2/128 [0/0]
    via Serial0/0/0, receive
L  FF00::/8 [0/0]
    via Null0, receive
R3#
```

### [Capítulo 7: EIGRP 7.4.3.4 Packet Tracer: Configuración de EIGRP básico con IPv6](#)

#### Información básica/situación

En esta actividad, configurará la red con el routing EIGRP para IPv6. También asignará las ID de los routers, configurará interfaces pasivas, verificará que la red haya convergido por completo y mostrará información de routing mediante los comandos **show**.

- EIGRP para IPv6 tiene el mismo funcionamiento y las mismas características generales que EIGRP para IPv4. Existen algunas diferencias importantes entre ellos:
- EIGRP para IPv6 se configura directamente en las interfaces del router.
- Con EIGRP para IPv6, se necesita una ID en cada router; de lo contrario, no se inicia el proceso de routing.
- El proceso de routing EIGRP para IPv6 utiliza una característica shutdown.

#### [Packet Tracer: Configuración de EIGRP básico con IPv6 \(instrucciones\)](#)

#### [Packet Tracer: Configuración de EIGRP básico con IPv6 \(PKA\)](#)

### [Capítulo 7: EIGRP 7.4.3.5 Práctica de laboratorio: Configuración de EIGRP básico para IPv6](#)

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y verificar la conectividad
- Parte 2: Configurar el routing EIGRP para IPv6
- Parte 3: Verificar el routing EIGRP para IPv6
- Parte 4: Configurar y verificar las interfaces pasivas

[Práctica de laboratorio: Configuración de EIGRP básico para IPv6](#)

Capítulo 7: EIGRP 7.5.1.1 Actividad de clase: Comparar RIP y EIGRP

**Comparar RIP y EIGRP**

Usted prepara un archivo para comparar los protocolos de routing RIP y EIGRP.

Piense en una red con tres routers interconectados en la que cada router proporciona una LAN para las computadoras, las impresoras y otras terminales. En el gráfico de esta página, se representa un ejemplo de una topología como esta.

En esta situación de creación de modelos, deberá crear, direccionar y configurar una topología con los comandos de verificación, así como comparar y contrastar los resultados de los protocolos de routing RIP y EIGRP.

Complete las preguntas de reflexión incluidas en el archivo PDF correspondiente a esta actividad. Guarde su trabajo y esté preparado para compartir las respuestas con la clase. También guarde una copia de su trabajo para su uso posterior en este curso o como referencia.

[Actividad de clase: Comparar RIP y EIGRP](#)

Capítulo 7: EIGRP 7.5.1.2 Resumen

EIGRP (protocolo de routing de gateway interior mejorado) es un protocolo de routing vector distancia sin clase. Es una mejora de otro protocolo de routing de Cisco: el protocolo de routing de gateway interior (IGRP) que ahora es obsoleto. EIGRP se lanzó originalmente en 1992 como un protocolo exclusivo de Cisco disponible solamente en los dispositivos de Cisco. En 2013, Cisco cedió una funcionalidad básica de EIGRP como estándar abierto al IETF.

EIGRP utiliza el código de origen "D" para DUAL en la tabla de enrutamiento. 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 predeterminadas.

EIGRP es un protocolo de routing vector distancia avanzado que incluye características que no se encuentran en otros protocolos de routing vector distancia, como RIP. Estas características incluyen: algoritmo de actualización por difusión (DUAL), establecimiento de adyacencias de vecinos, protocolo de transporte confiable (RTP), actualizaciones parciales y limitadas, y balanceo de carga de mismo costo y con distinto costo.

EIGRP utiliza módulos dependientes de protocolo (PDM), lo que le otorga la capacidad de admitir diferentes protocolos de capa 3, incluidos IPv4 e IPv6. EIGRP utiliza RTP (Reliable Transport Protocol) como protocolo de la capa de Transporte para la entrega de paquetes EIGRP. EIGRP utiliza entrega confiable para las actualizaciones, las consultas y las respuestas EIGRP, y utiliza entrega poco confiable para los saludos y acuses de recibo EIGRP. RTP confiable significa que se debe devolver un acuse de recibo EIGRP.

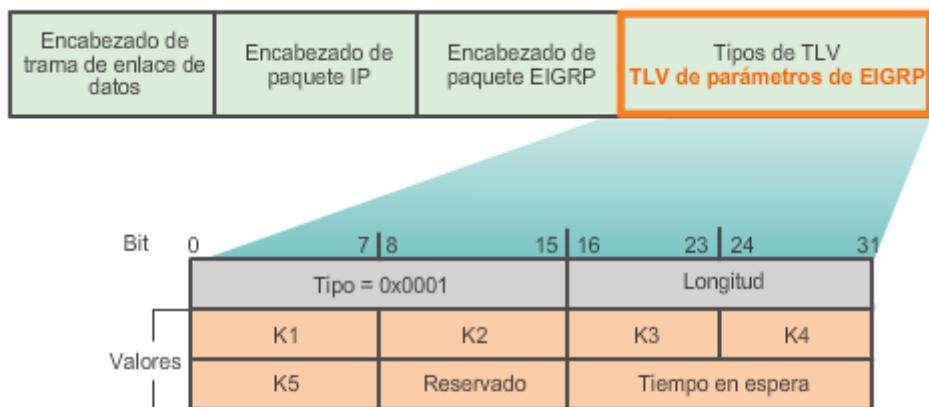
Antes de enviar cualquier actualización EIGRP, primero el router debe descubrir a sus vecinos. Esto se realiza mediante los paquetes de saludo EIGRP. No es necesario que los valores de saludo y de espera coincidan para que dos routers se conviertan en vecinos. El comando **show ip eigrp neighbors** se utiliza para ver la tabla de vecinos y para verificar que EIGRP haya establecido una adyacencia con sus vecinos.

EIGRP no envía actualizaciones periódicas, como RIP. EIGRP envía actualizaciones parciales o limitadas, que incluyen sólo los cambios de ruta y sólo los envía a los routers que se ven afectados por el cambio. La métrica compuesta de EIGRP utiliza el ancho de banda, el retraso, la confiabilidad y la carga para determinar la mejor ruta. De manera predeterminada, sólo se usan el ancho de banda y el retardo.

En el centro de EIGRP se encuentra DUAL (Algoritmo de actualización por difusión). La máquina de estados finitos DUAL se utiliza para determinar el mejor camino y las rutas de respaldo posibles hacia cada red de destino. Un sucesor es un router vecino que se utiliza para el reenvío de paquetes mediante el uso de la ruta menos costosa hacia la red de destino. Distancia factible (FD) es la métrica calculada más baja para llegar a la red de destino a través del sucesor. Un sucesor factible (FS) es un vecino que tiene una ruta de respaldo sin bucles hacia la misma red que el sucesor, y también cumple con la condición de factibilidad. 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 es simplemente una distancia factible EIGRP de vecinos a la red de destino.

EIGRP se configura con el comando **router eigrp sistema-autónomo**. El valor autonomous-system es en realidad un id de proceso y debe ser igual en todos los routers en el dominio de enrutamiento EIGRP. El comando **network** es similar al que se utiliza con RIP. La red es la dirección de red con clase de las interfaces conectadas directamente en el router. Una máscara wildcard es un parámetro opcional que puede utilizarse para incluir sólo interfaces específicas.

## Parámetros EIGRP



- **K1 y K3**: evalúa el ancho de banda y el retraso; se establece en 1.
- **Tiempo de espera**: tiempo máximo que debe esperar el router al siguiente saludo.

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.0.1.1

#### Introducción

EIGRP es un protocolo de routing versátil que se puede ajustar de muchas formas. Dos de las capacidades de ajuste más importantes son la de resumir rutas y la de implementar el balanceo de carga. Otras capacidades de ajuste son la propagación de una ruta predeterminada, el ajuste de temporizadores y la implementación de la autenticación entre vecinos EIGRP para aumentar la seguridad.

En este capítulo, se tratan estas características adicionales de ajuste y los comandos del modo de configuración para implementarlas para IPv4 e IPv6.

#### **Después de completar este capítulo, podrá hacer lo siguiente:**

- Configurar la sumarización automática de EIGRP.
- Configurar la sumarización manual de EIGRP.
- Configurar un router para propagar una ruta predeterminada en una red EIGRP.
- Modificar la configuración de las interfaces EIGRP para mejorar el rendimiento de la red.
- Configurar la autenticación de EIGRP para asegurar que las actualizaciones de routing sean seguras.
- Explicar el proceso y las herramientas que se usan para resolver problemas en una red EIGRP.
- Resolver problemas de adyacencias de vecinos en una red EIGRP.
- Resolver problemas de entradas de rutas faltantes en una tabla de routing EIGRP.

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.0.1.2 Actividad

### de clase: Volver al futuro (EIGRP)

#### **Actividad: Volver al futuro (EIGRP)**

En este capítulo, se le enseña a brindar mantenimiento a redes EIGRP y a influenciarlas para que hagan lo que usted desee que hagan. Entre los conceptos relacionados con EIGRP que aparecen en este capítulo, se incluyen los siguientes:

- Sumarización automática
- Equilibrio de carga
- Rutas predeterminadas
- Temporizadores de espera
- Autenticación

Con un compañero, escriba 10 preguntas de revisión acerca de EIGRP sobre la base del contenido del currículo del capítulo anterior. Tres de las preguntas deben abordar los elementos indicados anteriormente. Lo ideal sería que creen preguntas de selección múltiple, verdadero o falso, o para completar espacios en blanco. Mientras crean las preguntas, registren la sección del currículo y los números de página del contenido de respaldo, en caso de que necesiten consultarlos para verificar las respuestas.

Guarde el trabajo y, a continuación, reúnase con otro grupo o con la clase completa, y ponga a prueba sus conocimientos con las preguntas que formuló.

### [Actividad de clase: Volver al futuro \(EIGRP\)](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.1 Topología de la red

Antes de ajustar las características de EIGRP, empiece con una implementación básica de EIGRP.

En la figura 1, se muestra la topología de la red que se usa en este capítulo.

En las figuras 2, 3 y 4, se muestra la configuración de interfaces IPv4 y las implementaciones de EIGRP en el R1, el R2 y el R3, respectivamente.

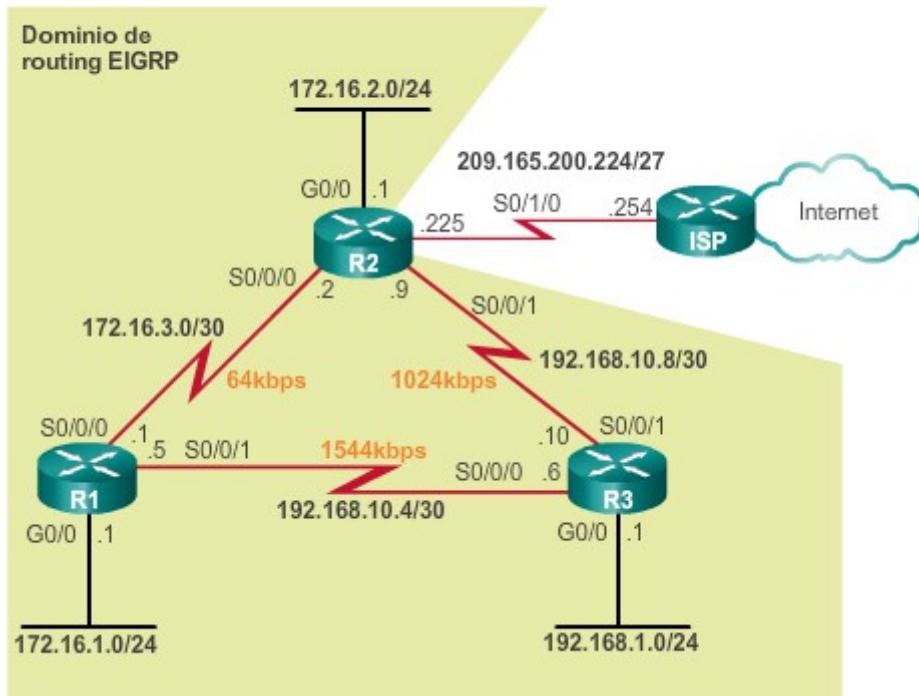
Es posible que los tipos de interfaces seriales y sus anchos de banda asociados no reflejen necesariamente los tipos de conexiones más frecuentes que se encuentran en las redes en la actualidad. Los anchos de banda de los enlaces seriales que se usan en esta topología ayudan

a explicar el cálculo de las métricas de los protocolos de routing y el proceso de selección de la mejor ruta.

Observe que se usaron los comandos **bandwidth** en las interfaces seriales para modificar el ancho de banda predeterminado de 1544 kb/s.

En este capítulo, el router ISP se usa como gateway del dominio de routing a Internet. Los tres routers ejecutan el IOS de Cisco, versión 15.2.

Topología EIGRP para IPv4



**Configuración inicial de la interfaz IPv4 y de EIGRP para IPv4 en el R1**

```
R1# show running-config
<resultado omitido>
version 15.2
!
interface GigabitEthernet0/0
  ip address 172.16.1.1 255.255.255.0
!
interface Serial0/0/0
  bandwidth 64
  ip address 172.16.3.1 255.255.255.252
  clock rate 64000
!
interface Serial0/0/1
  ip address 192.168.10.5 255.255.255.252
!
router eigrp 1
  network 172.16.0.0
  network 192.168.10.0
  eigrp router-id 1.1.1.1
```

**Configuración inicial de la interfaz IPv4 y de EIGRP para IPv4 en el R2**

```
R2# show running-config
<resultado omitido>
version 15.2
!
interface GigabitEthernet0/0
  ip address 172.16.2.1 255.255.255.0
!
interface Serial0/0/0
  bandwidth 64
  ip address 172.16.3.2 255.255.255.252
!
interface Serial0/0/1
  bandwidth 1024
  ip address 192.168.10.9 255.255.255.252
  clock rate 64000
!
interface Serial0/1/0
  ip address 209.165.200.225 255.255.255.224
!
router eigrp 1
  network 172.16.0.0
  network 192.168.10.8 0.0.0.3
  eigrp router-id 2.2.2.2
```

## Configuración inicial de la interfaz IPv4 y de EIGRP para IPv4 en el R3

```
R3# show running-config
<resultado omitido>
version 15.2
!
interface GigabitEthernet0/0
  ip address 192.168.1.1 255.255.255.0
!
interface Serial0/0/0
  ip address 192.168.10.6 255.255.255.252
  clock rate 64000
!
interface Serial0/0/1
  bandwidth 1024
  ip address 192.168.10.10 255.255.255.252
!
router eigrp 1
  network 192.168.1.0
  network 192.168.10.4 0.0.0.3
  network 192.168.10.8 0.0.0.3
  eigrp router-id 3.3.3.3
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.2

#### Sumarización automática de EIGRP

Uno de los métodos de ajuste más comunes de EIGRP es habilitar y deshabilitar la sumarización automática de rutas. La sumarización de ruta permite que un router agrupe redes y las anuncie como un gran grupo por medio de una única ruta resumida. La capacidad para resumir rutas es necesaria debido al rápido crecimiento de las redes.

Un router de frontera es un router que se ubica en el límite de una red. Este router debe poder anunciar todas las redes conocidas dentro de su tabla de rutas a un router de red o router ISP conector. Potencialmente, esta convergencia puede dar como resultado tablas de rutas muy grandes. Imagine si un solo router tuviera 10 redes diferentes y debiera anunciar las 10 entradas de rutas a un router conector. ¿Qué sucedería si ese router conector también tuviera 10 redes y debiera anunciar las 20 rutas a un router ISP? Si cada router de la empresa siguiera este patrón, la tabla de routing del router ISP sería enorme.

La sumarización disminuye la cantidad de entradas en las actualizaciones de enrutamiento y reduce la cantidad de entradas en las tablas de enrutamiento locales. Reduce, además, el uso del ancho de banda para las actualizaciones de enrutamiento y acelera las búsquedas en las tablas de enrutamiento.

Para limitar la cantidad de anuncios de routing y el tamaño de las tablas de routing, los protocolos de routing, como EIGRP, utilizan la sumarización automática en los límites con clase. Esto significa que EIGRP reconoce las subredes como una única red de clase A, B o C y crea solo una entrada en la tabla de routing para la ruta resumida. Como resultado, todo el tráfico destinado a las subredes viaja por esa ruta.

En la ilustración, se muestra un ejemplo de la manera en que funciona la summarización automática. Los routers R1 y R2 están configurados con EIGRP para IPv4, con summarización automática. El R1 tiene tres subredes en la tabla de routing: 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24. En la arquitectura de direccionamiento de redes con clase, todas estas subredes se consideran parte de una red de clase B más grande: 172.16.0.0/16. Debido a que EIGRP en el router R1 está configurado para summarización automática, cuando envía la actualización de routing al R2, resume las tres subredes /24 como una única red 172.16.0.0/16. Esto reduce la cantidad de actualizaciones de routing que se envían y la cantidad de entradas en la tabla de routing IPv4 del R2.

Todo el tráfico destinado a las tres subredes viaja a través de la única ruta. El R2 no mantiene rutas a subredes individuales y no se descubre información de subredes. En una red empresarial, es posible que la ruta elegida para alcanzar la ruta sumarizada no sea la mejor elección para el tráfico que está intentando alcanzar la subred individual. La única forma en que todos los routers pueden encontrar las mejores rutas para cada subred individual es que los vecinos envíen información sobre las subredes. En esta situación, se debe deshabilitar la summarización automática. Cuando se deshabilita la summarización automática, las actualizaciones incluyen información de subredes.

#### **Sumarización automática en el límite de una red con clase**



Redes con clase	
Clase A: de 0.0.0.0 a 127.255.255.255	Máscara predeterminada: 255.0.0.0 o /8
<b>Clase B: de 128.0.0.0 a 191.255.255.255</b>	<b>Máscara predeterminada: 255.255.0.0 o /16</b>
Clase C: de 192.0.0.0 a 223.255.255.255	Máscara predeterminada: 255.255.255.0 o /24

#### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.3

##### Configuración de la summarización automática de EIGRP

La summarización automática de EIGRP para IPv4 está deshabilitada de manera predeterminada a partir de las versiones 15.0(1)M y 12.2(33) del IOS de Cisco. Antes de esto, la summarización automática estaba habilitada de manera predeterminada. Es decir que EIGRP realizaba la

sumarización automática cada vez que la topología EIGRP cruzaba un límite entre dos redes principales con clase diferentes.

En la figura 1, el resultado del comando **show ip protocols** en el R1 indica que la sumarización automática de EIGRP está deshabilitada. Este router ejecuta IOS 15.2; por ende, la sumarización automática de EIGRP está deshabilitada de manera predeterminada. En la figura 2, se muestra la tabla de routing actual del R3. Observe que la tabla de routing IPv4 del R3 contiene todas las redes y subredes dentro del dominio de routing EIGRP.

Para habilitar la sumarización automática de EIGRP, use el comando **auto-summary** en el modo de configuración del router, como se muestra en la figura 3:

```
R1(config)# router eigrp número-as
```

```
R1(config-router)# auto-summary
```

La forma **no** de este comando se usa para deshabilitar la sumarización automática.

Utilice el verificador de sintaxis de la figura 4 para habilitar la sumarización automática en el R3.

### Verificación de si la summarización automática está deshabilitada

```
R1# show ip protocols
*** IP Routing is NSF aware ***

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-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
<resultado omitido>

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
<resultado omitido>
```

### Verificación de si las rutas no se resumen automáticamente

```
R3# show ip route eigrp
<resultado omitido>

  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D  172.16.1.0/24 [90/2170112] via 192.168.10.5, 02:21:10, Serial0/0/0
D  172.16.2.0/24 [90/3012096] via 192.168.10.9, 02:21:10, Serial0/0/1
D  172.16.3.0/30 [90/41024000] via 192.168.10.9, 02:21:10, Serial0/0/1
                           [90/41024000] via 192.168.10.5, 02:21:10, Serial0/0/0
R3#
```

## Configuración de la sumarización automática

```
R1(config)# router eigrp 1
R1(config-router)# auto-summary
R1(config-router)#
*Mar  9 19:40:19.342: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.6 (Serial0/0/1) is resync: summary configured
*Mar  9 19:40:19.342: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.6 (Serial0/0/1) is resync: summary up, remove components
*Mar  9 19:41:03.630: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor
192.168.10.6 (Serial0/0/1) is resync: peer graceful-restart
```

```
R2(config)# router eigrp 1
R2(config-router)# auto-summary
R2(config-router)#

```

## Configuración de la summarización automática de EIGRP en el R3

Muestre la tabla de routing EIGRP actual en el R3 para ver las rutas antes de la summarización.

```
R3# show ip route eigrp  
<resultado omitido>  
  
  172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks  
D  172.16.1.0/24 [90/2170112] via 192.168.10.5, 02:21:10, Serial0/0/0  
D  172.16.2.0/24 [90/3012096] via 192.168.10.9, 02:21:10, Serial0/0/1  
D  172.16.3.0/30 [90/41024000] via 192.168.10.9, 02:21:10, Serial0/0/1  
      [90/41024000] via 192.168.10.5, 02:21:10, Serial0/0/0  
R3#
```

Complete lo siguiente:

- Configure la summarización automática de EIGRP en el router R3 para un AS de EIGRP de 1.
- Vuelva al modo EXEC privilegiado.

```
R3(config)# router eigrp 1  
R3(config-router)# auto-summary  
R3(config-router)# end
```

Muestre la tabla de routing EIGRP en el R3 para ver las rutas después de la summarización automática.

```
R3# show ip route eigrp  
<resultado omitido>  
  
D  172.16.0.0/16 [90/2170112] via 192.168.10.5, 00:12:05, Serial0/0/0  
    192.168.10.0/24 is variably subnetted, 5 subnets, 3 masks  
D  192.168.10.0/24 is a summary, 00:11:43, Null0  
R3#
```

Muestre la configuración del protocolo de routing en el R1.

```
R1# show ip protocols  
*** IP Routing is NSF aware ***  
  
Routing Protocol is "eigrp 1"  
  Outgoing update filter list for all interfaces is not set  
  Outgoing update filter list for all interfaces is not set  
  Default networks flagged in outgoing updates  
  Default networks accepted from incoming updates  
  EIGRP-IPv4 Protocol for AS (1)  
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0  
<resultado omitido>
```

```
Automatic Summarization: enabled  
  192.168.10.0/24 for Gi0/0, Se0/0/0  
    Summarizing 2 components with metric 2169856  
  172.16.0.0/16 for Se0/0/1  
    Summarizing 3 components with metric 2816  
<resultado omitido>
```

Muestre la tabla de topología de EIGRP con el parámetro "all-links" en el R3.

```
R3# show ip eigrp topology all-links  
  
P 172.16.0.0/16, 1 successors, FD is 2170112, serno 9  
  via 192.168.10.5 (2170112/2816), Serial0/0/0  
  via 192.168.10.9 (3012096/2816), Serial0/0/1
```

Configuró correctamente la summarización automática de EIGRP en el R3.

Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.4

Verificación de la summarización automática: show ip protocols

En la figura 1, observe que el dominio de routing EIGRP tiene tres redes con clase:

- La red de clase B 172.16.0.0/16, que consta de las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/30.
- La red de clase C 192.168.10.0/24, que consta de las subredes 192.168.10.4/30 y 192.168.10.8/30.
- La red de clase C 192.168.1.0/24, que no está dividida en subredes.

El resultado del comando **show ip protocols** en el R1, que aparece en la figura 2, muestra que la summarización automática ahora está habilitada. El resultado también indica cuáles redes están resumidas y en qué interfaces. Observe que el R1 resume dos redes en las actualizaciones de routing EIGRP:

- 192.168.10.0/24 enviada por las interfaces GigabitEthernet 0/0 y Serial 0/0/0
- 172.16.0.0/16 enviada por la interfaz Serial 0/0/1

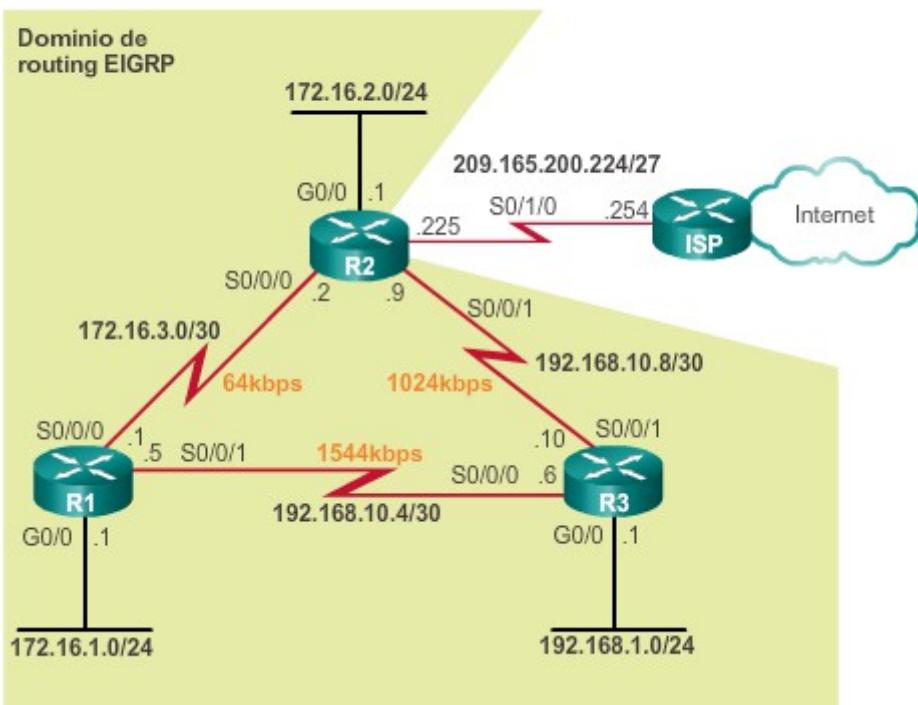
El R1 tiene las subredes 192.168.10.4/30 y 192.168.10.8/30 en la tabla de routing IPv4.

Como se indica en la figura 3, el R1 resume las subredes 192.168.10.4/30 y 192.168.10.8/30 y reenvía la dirección resumida 192.168.10.0/24 a los vecinos en las interfaces Serial 0/0/0 y GigabitEthernet 0/0. Debido a que el R1 no tiene vecinos EIGRP en la interfaz GigabitEthernet 0/0, solo el R2 recibe la actualización de routing resumida.

Como se indica en la figura 4, el R1 también tiene las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/30 en la tabla de routing IPv4. El R3 selecciona al R1 como el sucesor a 172.16.0.0/16, porque tiene una distancia factible menor. La interfaz S0/0/0 del R3 que se conecta al R1 usa un ancho de banda predeterminado de 1544 kb/s. El enlace del R3 al R2 tiene una distancia factible más alta, debido a que la interfaz S0/0/1 del R3 se configuró con un ancho de banda inferior a 1024 kb/s.

Observe que la actualización resumida de 172.16.0.0/16 no se envía por las interfaces GigabitEthernet 0/0 ni Serial 0/0/0 del R1. Esto se debe a que estas dos interfaces son miembros de la misma red de clase B 172.16.0.0/16. El R1 envía la actualización de routing no resumida de 172.16.1.0/24 al R2. Las actualizaciones resumidas solo se envían por interfaces en diferentes redes principales con clase.

## Topología EIGRP para IPv4



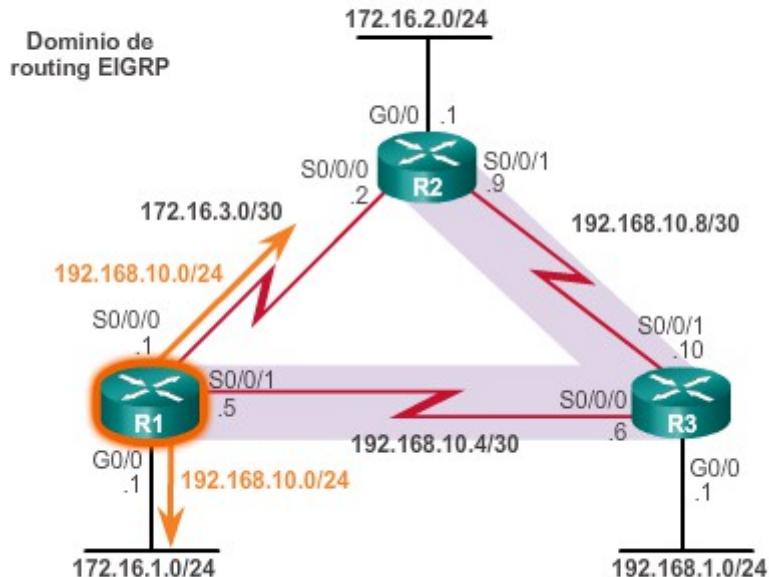
Verificación de si la summarización automática está habilitada

```
R1# show ip protocols
*** IP Routing is NSF aware ***

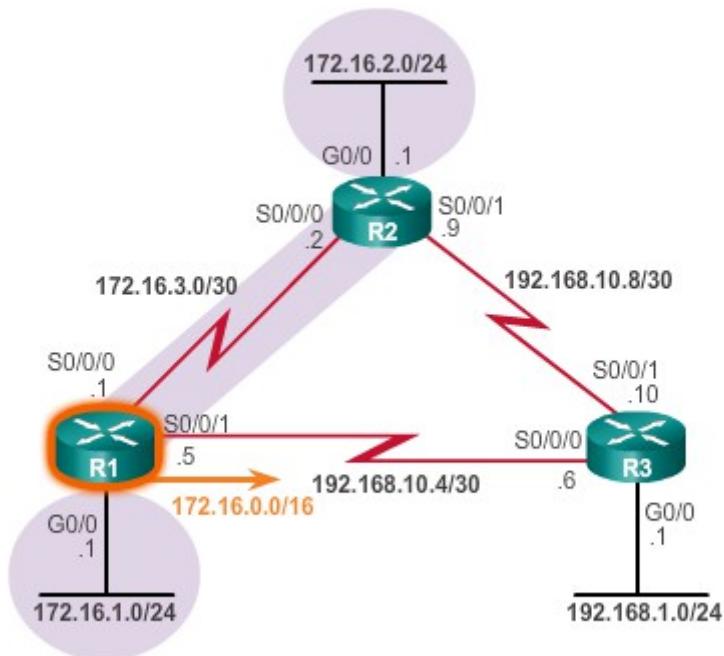
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
<resultado omitido>

Automatic Summarization: enabled
  192.168.10.0/24 for Gi0/0, Se0/0/0
    Summarizing 2 components with metric 2169856
  172.16.0.0/16 for Se0/0/1
    Summarizing 3 components with metric 2816
<resultado omitido>
```

### Resumen de 192.168.10.0/24 del R1



### Resumen de 172.16.0.0/16 del R1



Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.5

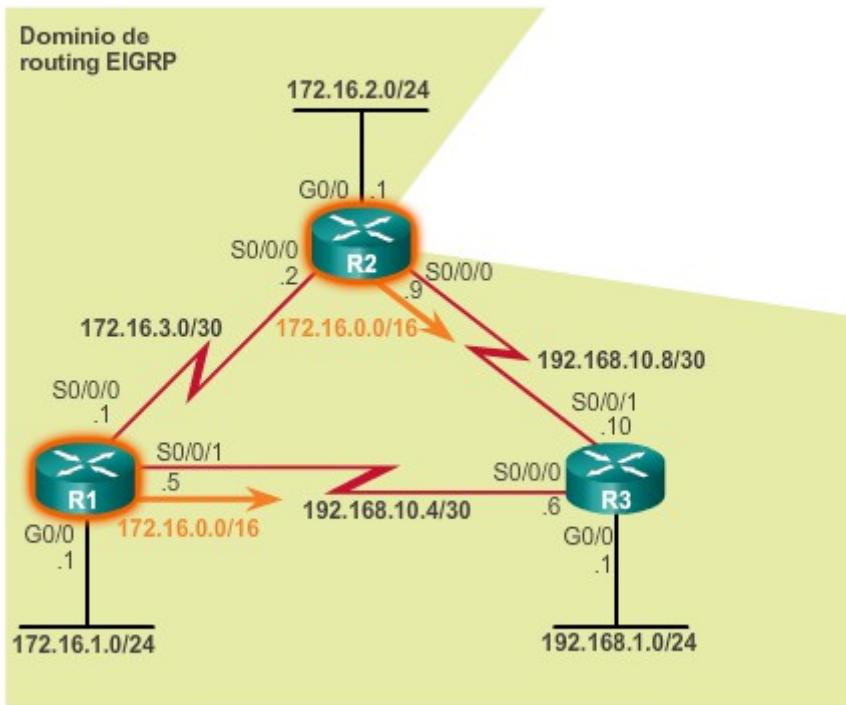
Verificación de la summarización automática: tabla de topología

En la figura 1, los routers R1 y R2 envían al R3 una actualización de routing EIGRP resumida de 172.16.0.0/16. Las tablas de routing del R1 y el R2 tienen subredes de la red 172.16.0.0/16, por lo tanto, ambos routers envían al R3 anuncios resumidos a través de una red principal diferente.

En la figura 2, se muestra el resultado del comando **show ip eigrp topology all-links** que se usó para ver la tabla completa de topología de EIGRP del R3. Esto verifica que el R3 recibió la ruta resumida 172.16.0.0/16 tanto del R1 en 192.168.10.5 como del R2 en 192.168.10.9. La primera entrada a través de 192.168.10.5 es el sucesor, y la segunda entrada a través de 192.168.10.9 es el sucesor factible. El R1 es el sucesor porque su enlace de 1544 kb/s al R3 le da a este último un mejor costo EIGRP a 172.16.0.0/16 que el del R2, que usa un enlace más lento de 1024 kb/s.

La opción **all-links** muestra todas las actualizaciones recibidas, independientemente de si la ruta califica como sucesor factible (FS) o no. En este caso, el R2 califica como FS. El R2 se considera un FS debido a que la distancia notificada (RD) de 2816 es menor que la distancia factible (FD) de 2 170 112 a través del R1.

## Topología EIGRP para IPv4



### Verificación de la ruta resumida en la tabla de topología

```
R3# show ip eigrp topology all-links
P 172.16.0.0/16, 1 successors, FD is 2170112, serno 9
    via 192.168.10.5 (2170112/2816), Serial0/0/0
    via 192.168.10.9 (3012096/2816), Serial0/0/1
<resultado omitido>
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.6

#### Verificación de la summarización automática: tabla de routing

Examine la tabla de routing para verificar que se haya recibido la ruta resumida.

En la figura 1, se muestra la tabla de routing del R3 antes de la summarización automática y, luego, con la summarización automática habilitada mediante el comando **auto-summary**. Observe que con la summarización automática habilitada, la tabla de routing del R3 ahora solo la

dirección de red de clase B 172.16.0.0/16. El sucesor o el router de siguiente salto es el R1, a través de 192.168.10.5.

**Nota:** la summarización automática solo es una opción con EIGRP para IPv4. El direccionamiento con clase no existe en IPv6, por lo tanto, la summarización automática no es necesaria con EIGRP para IPv6.

En el momento de habilitar la summarización automática, también es necesario entender la interfaz nula (Null). En la figura 2, se muestra la tabla de routing del R1. Observe que en las dos entradas destacadas se usa una interfaz de salida Null0. EIGRP automáticamente incluyó una ruta resumida a Null0 para dos redes con clase: 192.168.10.0/24 y 172.16.0.0/16.

La interfaz Null0 es una interfaz virtual del IOS que constituye una ruta hacia ninguna parte, comúnmente conocida como “el limbo electrónico”. Los paquetes que vinculan una ruta con una interfaz de salida Null0 se descartan.

EIGRP para IPv4 automáticamente incluye un resumen de rutas Null0 cuando se producen las siguientes condiciones:

- Por lo menos existe una subred que se aprendió a través de EIGRP.
- Hay dos o más comandos **network** del modo de configuración del router EIGRP.
- La summarización automática se encuentra habilitada.

El objetivo del resumen de rutas Null0 es evitar bucles de routing hacia destinos que se incluyen en el resumen, pero que no existen realmente en la tabla de routing.

## Verificación de la ruta resumida en la tabla de routing

### Sumarización automática deshabilitada

```
R3# show ip route eigrp
<resultado omitido>

 172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D   172.16.1.0/24 [90/2170112] via 192.168.10.5,
      02:21:10, Serial0/0/0
D   172.16.2.0/24 [90/3012096] via 192.168.10.9,
      02:21:10, Serial0/0/1
D   172.16.3.0/30 [90/41024000] via 192.168.10.9,
      02:21:10, Serial0/0/1
      [90/41024000] via 192.168.10.5,
      02:21:10, Serial0/0/0

R3#
```

### Sumarización automática habilitada

```
R3# show ip route eigrp
<resultado omitido>

D   172.16.0.0/16 [90/2170112] via 192.168.10.5, 00:12:05,
    Serial0/0/0
    192.168.10.0/24 is variably subnetted, 5 subnets, 3
    masks
D   192.168.10.0/24 is a summary, 00:11:43, Null0
R3#
```

## Resumen de rutas Null0 en el R1

```
R1# show ip route

 172.16.0.0/16 is variably subnetted, 6 subnets, 4 masks
D   172.16.0.0/16 is a summary, 00:03:06, Null0
C   172.16.1.0/24 is directly connected, GigabitEthernet0/0
L   172.16.1.1/32 is directly connected, GigabitEthernet0/0
D   172.16.2.0/24 [90/40512256] via 172.16.3.2, 00:02:52,
    Serial0/0/0
C   172.16.3.0/30 is directly connected, Serial0/0/0
L   172.16.3.1/32 is directly connected, Serial0/0/0
D   192.168.1.0/24 [90/2170112] via 192.168.10.6, 00:02:51,
    Serial0/0/1
    192.168.10.0/24 is variably subnetted, 4 subnets, 3 masks
D   192.168.10.0/24 is a summary, 00:02:52, Null0
C   192.168.10.4/30 is directly connected, Serial0/0/1
L   192.168.10.5/32 is directly connected, Serial0/0/1
D   192.168.10.8/30 [90/3523840] via 192.168.10.6, 00:02:59,
    Serial0/0/1
R1#
```

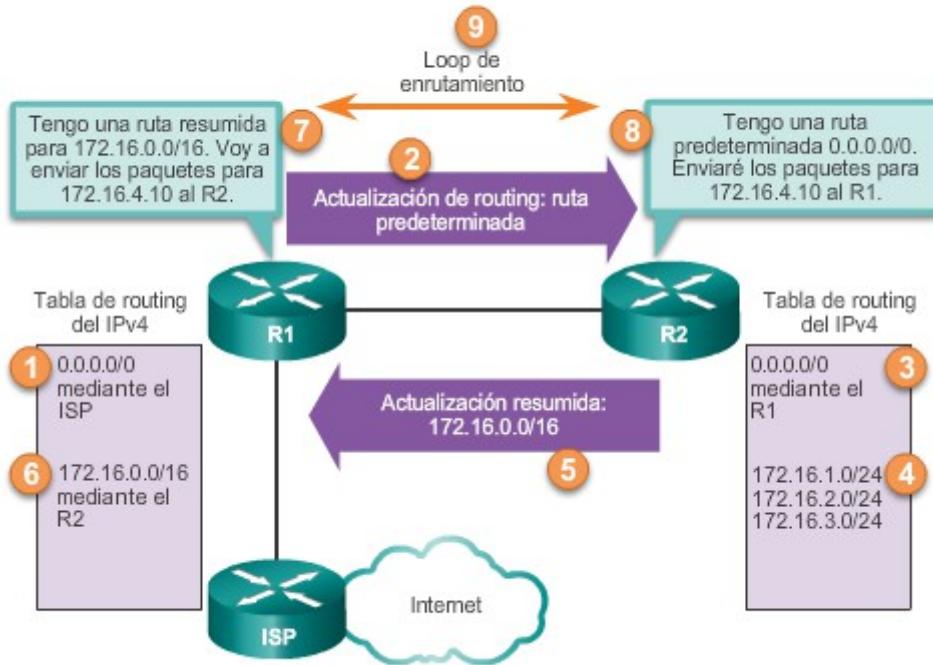
## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.7 Ruta resumida

resumida

En la ilustración, se muestra una situación en la que podría producirse un bucle de routing:

1. El R1 tiene una ruta predeterminada 0.0.0.0/0 mediante el router ISP.
2. El R1 envía una actualización de routing al R2 con la ruta predeterminada.
3. El R2 instala la ruta predeterminada del R1 en su tabla de routing IPv4.
4. La tabla de routing del R2 contiene las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24 en su tabla de routing.
5. El R2 envía una actualización resumida al R1 para la red 172.16.0.0/16.
6. El R1 instala la ruta resumida para 172.16.0.0/16 mediante el R2.
7. El R1 recibe un paquete para 172.16.4.10. Debido a que el R1 tiene una ruta para 172.16.0.0/16 mediante el R2, reenvía el paquete al R2.
8. El R2 recibe el paquete con la dirección de destino 172.16.4.10 del R1. El paquete no coincide con ninguna ruta específica, de manera que, mediante la ruta predeterminada en su tabla de routing, el R2 reenvía el paquete de regreso al R1.
9. El paquete para 172.16.4.10 va y viene en un bucle entre el R1 y el R2 hasta que el TTL expira y el paquete se descarta.

## Ejemplo de un bucle de routing



### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.8 Ruta resumida (cont.)

EIGRP usa la interfaz Null0 para evitar estos tipos de bucles de routing. En la ilustración, se muestra una situación en la que una ruta Null0 evita que se produzca un bucle de routing como el que se explicó en el ejemplo anterior:

1. El R1 tiene una ruta predeterminada 0.0.0.0/0 mediante el router ISP.
2. El R1 envía una actualización de routing al R2 con la ruta predeterminada.
3. El R2 instala la ruta predeterminada del R1 en su tabla de routing IPv4.
4. La tabla de routing del R2 contiene las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24 en su tabla de routing.
5. El R2 instala la ruta resumida 172.16.0.0/16 a Null0 en la tabla de routing.
6. El R2 envía una actualización resumida al R1 para la red 172.16.0.0/16.
7. El R1 instala la ruta resumida para 172.16.0.0/16 mediante el R2.
8. El R1 recibe un paquete para 172.16.4.10. Debido a que el R1 tiene una ruta para 172.16.0.0/16 mediante el R2, reenvía el paquete al R2.

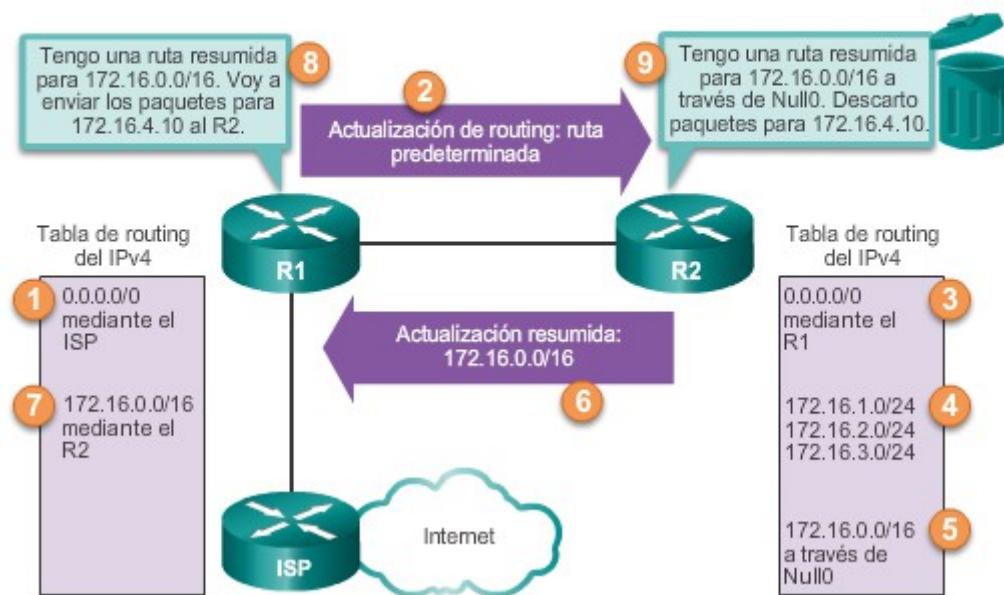
9. El R2 recibe el paquete con la dirección de destino 172.16.4.10 del R1. El paquete no coincide con ninguna subred específica de 172.16.0.0, pero coincide con la ruta resumida 172.16.0.0/16 a Null0. Mediante la ruta Null0, se descarta el paquete.

Una ruta resumida en el R2 para 172.16.0.0/16 a la interfaz Null0 descarta cualquier paquete que empiece con 172.16.x.x y que no tenga una coincidencia más larga con ninguna de las subredes: 172.16.1.0/24, 172.16.2.0/24 o 172.16.3.0/24.

Incluso si el R2 tiene una ruta predeterminada 0.0.0.0/0 en la tabla de routing, la ruta Null0 es una coincidencia más larga.

**Nota:** el resumen de rutas Null0 se elimina cuando se deshabilita la summarización automática con el comando **no auto-summary** del modo de configuración del router.

#### La ruta Null0 se usa para evitar bucles

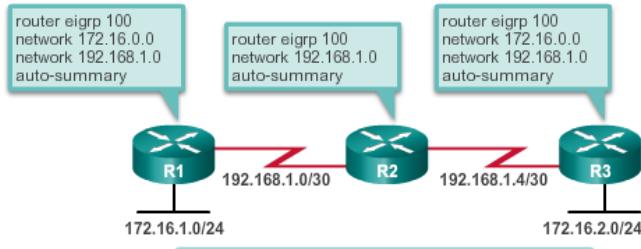


Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.9 Actividad:

Determinar la summarización con clase

**Actividad: Determinar la sumarización con clase (situación 1)**

El router 1 (R1) envía anuncios de rutas al router 2 (R2). Arrastra las redes y máscaras que anuncia el R1 hasta la tabla de topología del R2. No se utilizan todos los elementos. Haga clic en el botón 2 para continuar.

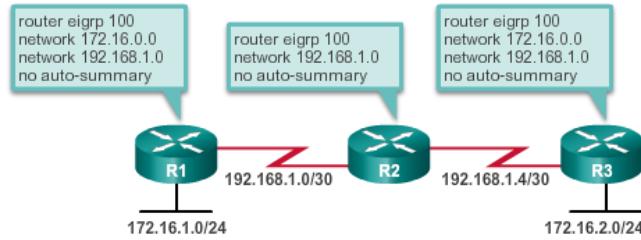


/30	192.168.1.4	/8	172.16.2.0	/26
-----	-------------	----	------------	-----

Publicación del R1	
Red	Máscara
✓ 172.16.0.0	✓ /16
✓ 192.168.1.0	✓ /24

**Actividad: Determinar la sumarización con clase (situación 2)**

El router 3 (R3) envía anuncios de rutas al router 2 (R2). Arrastra las redes y máscaras que anuncia el R3 hasta la tabla de topología del R2. No se utilizan todos los elementos. Haga clic en el botón 3 para continuar.

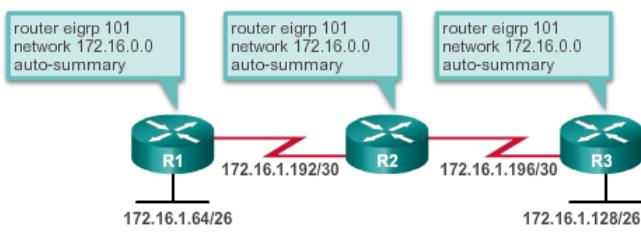


192.168.1.0	/26	172.16.0.0	/8	/16
-------------	-----	------------	----	-----

Anuncio del R3	
Red	Máscara
✓ 172.16.2.0	✓ /24
✓ 192.168.1.4	✓ /30

**Actividad: Determinar la sumarización con clase (situación 3)**

El router 1 (R1) envía anuncios de rutas al router 2 (R2). Arrastra las redes y máscaras que anuncia el R1 hasta la tabla de topología del R2. No se utilizan todos los elementos.



172.16.1.128	172.16.1.196	172.16.0.0
/30	/16	/24
/24		172.16.1.192

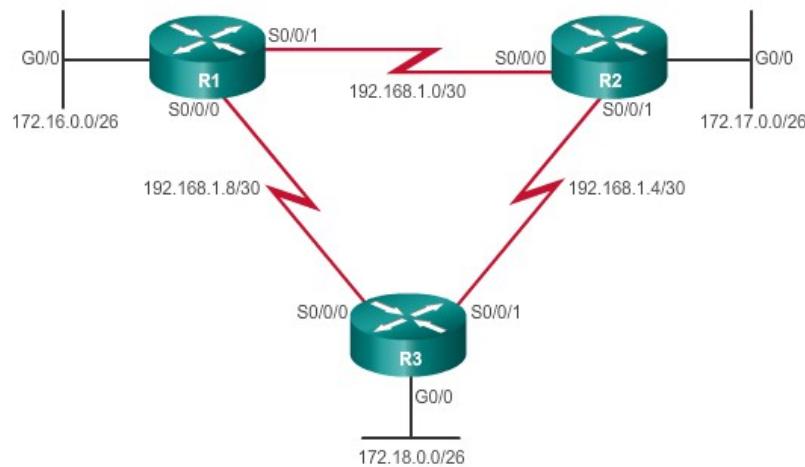
Publicación del R1	
Red	Máscara
✓ 172.16.1.64	✓ /26

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.1.10

### Actividad: Determinar la interfaz de salida para un paquete determinado

#### **Actividad de topología: Determinar la interfaz de salida de un paquete determinado**

Use este diagrama de topología como referencia para resolver cada una de las tres situaciones. Ahora, haga clic en el botón 2.



#### **Actividad: Determinar la interfaz de salida de un paquete determinado (situación 1)**

Arrastre cada dirección IP de destino hasta la interfaz de salida correcta en el router 3 (R3). Consulte la tabla de routing y el diagrama de topología. Haga clic en el botón 3 para continuar.

```
R3# show ip route
```

D	172.16.0.0/16 [90/2172416] via 192.168.1.9, 00:08:06, Serial0/0/0
D	172.17.0.0/16 [90/2172416] via 192.168.1.5, 00:08:13, Serial0/0/1
D	172.18.0.0/16 is variably subnetted, 2 subnets, 2 masks
D	172.18.0.0/16 is a summary, 00:08:21, Null0
C	172.18.0.0/26 is directly connected, GigabitEthernet0/0
D	192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
D	192.168.1.0/24 is a summary, 00:08:21, Null0
D	192.168.1.0/30 [90/2681856] via 192.168.1.9, 00:08:06, Serial0/0/0
C	192.168.1.4/30 is directly connected, Serial0/0/1
C	192.168.1.8/30 is directly connected, Serial0/0/0

INTERFACES DE SALIDA DEL ROUTER 3

S0/0/0 <input checked="" type="checkbox"/> 172.16.0.65	S0/0/1 <input checked="" type="checkbox"/> 172.17.0.17	G0/0
<input type="checkbox"/>	192.168.1.2 <input checked="" type="checkbox"/>	172.18.0.24 <input checked="" type="checkbox"/>

**Actividad: Determinar la interfaz de salida de un paquete determinado (situación 2)**

Arrastra cada dirección IP de destino hasta la interfaz de salida correcta en el router 1 (R1). Consulte la tabla de routing y el diagrama de topología. Haga clic en el botón 4 para continuar.

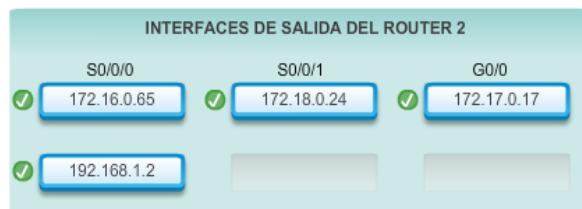
```
R1# show ip route
C      172.16.0.0 is directly connected, GigabitEthernet0/0
      172.17.0.0/26 is subnetted, 1 subnets
D      172.17.0.0 [90/2172416] via 192.168.1.2, 00:00:09, Serial0/0/1
      172.18.0.0/26 is subnetted, 1 subnets
D      172.18.0.0 [90/2172416] via 192.168.1.10, 00:00:09, Serial0/0/0
      192.168.1.0/30 is subnetted, 3 subnets
C      192.168.1.0 is directly connected, Serial0/0/1
D      192.168.1.4 [90/2681856] via 192.168.1.10, 00:00:09, Serial0/0/0
      [90/2681856] via 192.168.1.2, 00:00:09, Serial0/0/1
C      192.168.1.8 is directly connected, Serial0/0/0
```



**Actividad: Determinar la interfaz de salida de un paquete determinado (situación 3)**

Arrastra cada dirección IP de destino hasta la interfaz de salida correcta en el router 2 (R2). Consulte la tabla de routing y el diagrama de topología.

```
R2# show ip route
D      172.16.0.0/16 [90/2172416] via 192.168.1.1, 00:00:23, Serial0/0/0
      172.17.0.0/16 is variably subnetted, 2 subnets, 2 masks
D      172.17.0.0/16 is a summary, 00:00:23, Null0
C      172.17.0.0/26 is directly connected, GigabitEthernet0/0
      172.18.0.0/26 is subnetted, 1 subnets
D      172.18.0.0 [90/2172416] via 192.168.1.6, 00:00:23, Serial0/0/1
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
D      192.168.1.0/24 is a summary, 00:00:23, Null0
C      192.168.1.0/30 is directly connected, Serial0/0/0
C      192.168.1.4/30 is directly connected, Serial0/0/1
D      192.168.1.8/30 [90/2681856] via 192.168.1.6, 00:00:23, Serial0/0/1
      [90/2681856] via 192.168.1.1, 00:00:23, Serial0/0/0
```



## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.2.1

### Rutas resumidas manuales

EIGRP puede configurarse para que resuma rutas, ya sea que se encuentre habilitado la sumarización automática (**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, la sumarización manual puede incluir rutas de superredes. Recuerde, una superred es un agregado de múltiples direcciones de redes principales con clase.

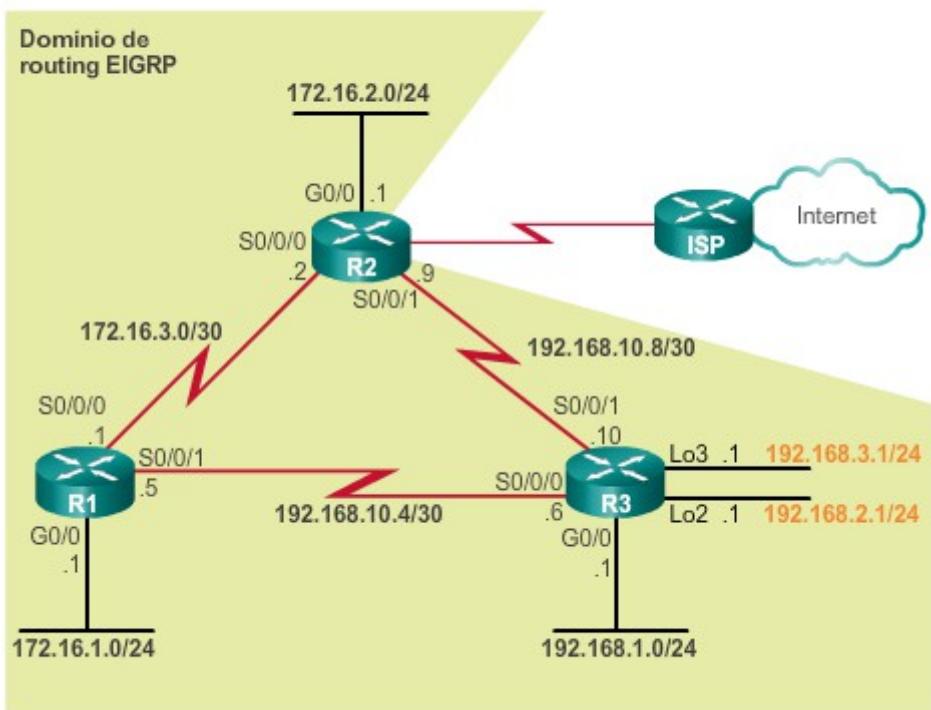
En la figura 1, se agregan dos redes más al router R3 con las interfaces loopback: 192.168.2.0/24 y 192.168.3.0/24. Aunque las interfaces loopback son interfaces virtuales, en este ejemplo se usan para representar redes físicas.

En la figura 2, se muestran los comandos para configurar las dos interfaces loopback y la configuración para habilitar ambas interfaces para EIGRP en el R3.

Para verificar que el R3 envió los paquetes de actualización EIGRP al R1 y al R2, se examinan las tablas de routing de ambos routers.

En la figura 3, solo se muestran las rutas pertinentes. En las tablas de routing del R1 y el R2 se muestran estas redes adicionales: 192.168.2.0/24 y 192.168.3.0/24. En lugar de enviar tres redes por separado, el R3 puede resumir las redes 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24 como una única ruta.

## Topología EIGRP para IPv4



### Configuración de interfaces loopback en el R3

```
R3(config)# interface loopback 2
R3(config-if)# ip add 192.168.2.1 255.255.255.0
R3(config-if)# exit
R3(config)# interface loopback 3
R3(config-if)# ip add 192.168.3.1 255.255.255.0
R3(config-if)# exit
R3(config)# router eigrp 1
R3(config-router)# network 192.168.2.0
R3(config-router)# network 192.168.3.0
R3(config-router)#

```

## Rutas adicionales verificadas en el R1 y el R2

```
R1# show ip route
<resultado omitido>

D 192.168.1.0/24 [90/2170112] via 192.168.10.6, 00:47:39,Serial0/0/1
D 192.168.2.0/24 [90/2297856] via 192.168.10.6, 00:08:09,Serial0/0/1
D 192.168.3.0/24 [90/2297856] via 192.168.10.6, 00:08:04,Serial0/0/1
R1#
```

```
R2# show ip route
<resultado omitido>

D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:47:58,Serial0/0/1
D 192.168.2.0/24 [90/3139840] via 192.168.10.10, 00:08:28,Serial0/0/1
D 192.168.3.0/24 [90/3139840] via 192.168.10.10, 00:08:23,Serial0/0/1
R2#
```

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.2.2

### Configuración de rutas resumidas manuales EIGRP

#### **Determinación de la ruta sumarizada EIGRP**

En la figura 1, se muestra las dos rutas resumidas manuales que están configuradas en el R3. Estas rutas resumidas se envían por las interfaces Serial 0/0/0 y Serial 0/0/1 a los vecinos EIGRP del R3.

Para determinar el resumen de estas tres redes, se usa el mismo método que para determinar rutas estáticas resumidas, como se muestra en la figura 2:

**Paso 1.** Escriba las redes que se resumirán en formato binario.

**Paso 2.** Para encontrar la máscara de subred para la summarización, empiece con el bit del extremo izquierdo.

**Paso 3.** De izquierda a derecha, encuentre todos los bits que coincidan en forma consecutiva.

**Paso 4.** Cuando haya una columna de bits que no coincidan, deténgase. Este es el límite de resumen.

**Paso 5.** Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo. En el ejemplo, es 22. Este número se usa para determinar la máscara de subred de la ruta resumida: /22 o 255.255.252.0.

**Paso 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 de la summarización manual de EIGRP**

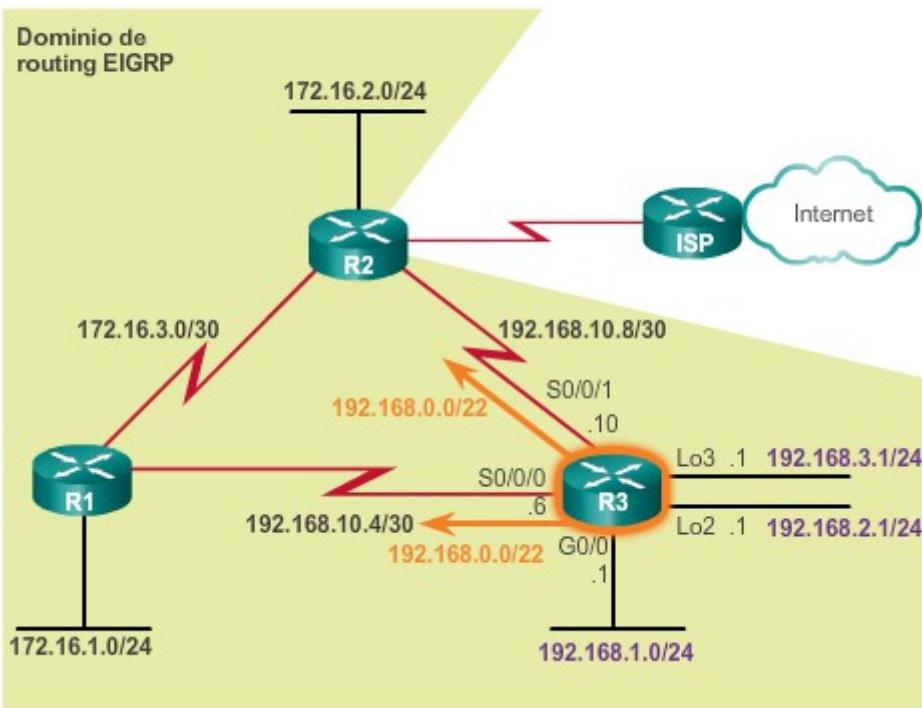
Para establecer la summarización manual EIGRP en una interfaz EIGRP específica, utilice el siguiente comando del modo de configuración de interfaz:

```
Router(config-if)# ip summary-address eigrp as-number network-address subnet-mask
```

En la figura 2, se muestra la configuración para propagar una ruta resumida manual en la interfaz Serial 0/0/0 del R3. Debido a que el R3 tiene dos vecinos EIGRP, la summarización manual de EIGRP debe configurarse tanto en Serial 0/0/0 como en Serial 0/0/1.

Utilice el verificador de sintaxis de la figura 3 para configurar la misma ruta resumida manual en la interfaz Serial 0/0/1 del R3.

## Topología EIGRP para IPv4



### Cálculo de una ruta resumida

192.168.1.0:	<b>11000000 . 10101000 . 0000000001 . 00000000</b>
192.168.2.0:	<b>11000000 . 10101000 . 0000000010 . 00000000</b>
192.168.3.0:	<b>11000000 . 10101000 . 0000000011 . 00000000</b>

←      22 bits coincidentes      →

22 bits coincidentes = una máscara de subred /22 o 255.255.252.0

```
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) #
```

Configure la ruta resumida en todas las interfaces que envían paquetes EIGRP.

## Configuración de una ruta resumida manual en el R3

**Configure una ruta resumida EIGRP para resumir las siguientes redes en la interfaz serial 0/0/1 del R3 para EIGRP AS 1**

- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

**Vuelva al modo EXEC privilegiado.**

```
R3(config)# interface serial 0/0/1  
R3(config-if)# ip summary-address eigrp 1 192.168.0.0  
255.255.252.0  
R3(config-if)# end
```

**Muestre la tabla de enrutamiento en el R1 para ver el resumen manual del R3.**

```
R1# show ip route  
<resultado omitido>
```

```
D 192.168.0.0/22 [90/2170112] via 192.168.10.6, 01:53:19,  
Serial0/0/1  
R1#
```

**Muestre la tabla de enrutamiento en el R2 para ver el resumen manual del R3.**

```
R2# show ip route  
<resultado omitido>
```

```
D 192.168.0.0/22 [90/3012096] via 192.168.10.10, 01:53:33,  
Serial0/0/1  
R2#
```

**Configuró correctamente una ruta resumida manual en el R3.**

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.2.3

### Verificación de las rutas resumidas manuales

En la ilustración se muestra que, después de configurar la ruta resumida, las tablas de routing del R1 y el R2 ya no incluyen las redes individuales 192.168.1.0/24, 192.168.2.0/24 y 192.168.3.0/24. En cambio, muestran una única ruta resumida: 192.168.0.0/22. Las rutas resumidas reducen el número total de rutas en las tablas de routing, lo que hace que el proceso de búsqueda en dichas tablas sea más eficaz. Estas rutas también requieren menor utilización de ancho de banda para las actualizaciones de routing, ya que se puede enviar una única ruta en lugar de varias rutas individuales.

## Verificación de la ruta resumida recibida en el R1 y el R2

```
R1# show ip route
<resultado omitido>
D 192.168.0.0/22 [90/2170112] via 192.168.10.6, 01:53:19, Serial0/0/1
R1#
```

```
R2# show ip route
<resultado omitido>
D 192.168.0.0/22 [90/3012096] via 192.168.10.10, 01:53:33, Serial0/0/1
R2#
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.2.4 EIGRP para IPv6: rutas resumidas manuales

Si bien la summarización automática no está disponible para redes IPv6 EIGRP, es posible habilitar la summarización manual para estas redes.

En la figura 1, se muestra la topología IPv6 EIGRP con cuatro direcciones de loopback configuradas en el R3. Estas direcciones virtuales se utilizan para representar redes físicas en la tabla de routing IPv6 del R3. En EIGRP para IPv6, estas redes pueden resumirse manualmente.

En la figura 2, se muestra la configuración de las direcciones de loopback IPv6 en el R3. Solo se muestran cuatro direcciones de loopback en la topología, que están configuradas en el R3; sin embargo, para este ejemplo, se da por sentado que se puede llegar a todas las subredes de 2001:DB8:ACAD::/48 a través del R3.

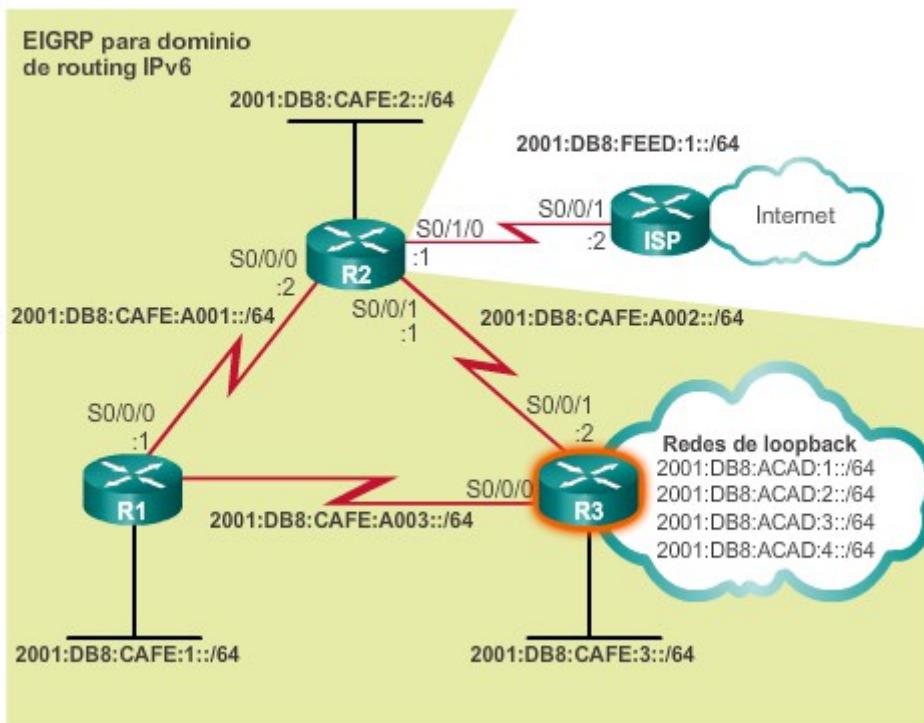
Para configurar la summarización manual de EIGRP para IPv6 en una interfaz EIGRP específica, utilice el siguiente comando del modo de configuración de interfaz:

```
Router(config-if)# ipv6 summary-address eigrp as-number prefix/prefix-length
```

En la figura 3, se muestra la configuración para propagar una ruta resumida manual EIGRP para IPv6 al R1 y al R2, para el prefijo 2001:DB8:ACAD::/48. De manera similar a lo que sucede en EIGRP para IPv4, el R3 incluye una ruta resumida a null0 para evitar la formación de bucles.

La recepción de la ruta resumida manual se puede verificar mediante la revisión de la tabla de routing de los otros routers en el dominio de routing. En la figura 4, se muestra la ruta 2001:DB8:ACAD::/48 en la tabla de routing IPv6 del R1.

## Topología EIGRP para IPv6



Configuración de loopback IPv6 en el R3

```
R3(config)# interface loopback 11
R3(config-if)# ipv6 address 2001:db8:acad:1::1/64
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface loopback 12
R3(config-if)# ipv6 address 2001:db8:acad:2::1/64
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface loopback 13
R3(config-if)# ipv6 address 2001:db8:acad:3::1/64
R3(config-if)# ipv6 eigrp 2
R3(config-if)# exit
R3(config)# interface loopback 14
R3(config-if)# ipv6 address 2001:db8:acad:4::1/64
R3(config-if)# ipv6 eigrp 2
```

### Configuración de resumen manual IPv6 en el R3

```
R3(config)# interface serial 0/0/0
R3(config-if)# ipv6 summary-address eigrp 2 2001:db8:acad::/48
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config-if)# ipv6 summary-address eigrp 2 2001:db8:acad::/48
R3(config-if)# end

R3# show ipv6 route

D 2001:DB8:ACAD::/48 [5/128256]
  via Null0, directly connected

<resultado omitido>
```

### Verificación de una ruta resumida manual EIGRP para IPv6

```
R1# show ipv6 route | include 2001:DB8:ACAD::
D 2001:DB8:ACAD::/48 [90/2297856]
R1#
```

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.2.5 Packet Tracer: Configuración de rutas resumidas manuales EIGRP para IPv4 e IPv6

### Información básica/situación

En esta actividad, calculará y configurará rutas resumidas para las redes IPv4 e IPv6. EIGRP ya está configurado; sin embargo, debe configurar las rutas resumidas IPv4 e IPv6 en las interfaces especificadas. EIGRP reemplaza las rutas actuales por una ruta resumida más específica, lo que reduce el tamaño de las tablas de routing.

[Packet Tracer: Configuración de rutas resumidas manuales EIGRP para IPv4 e IPv6 \(instrucciones\)](#)

[Packet Tracer: Configuración de rutas resumidas manuales EIGRP para IPv4 e IPv6 \(PKA\)](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.3.1 Propagación de una ruta estática predeterminada

### Propagación de una ruta estática predeterminada

## Propagación de una ruta estática predeterminada

El uso de una ruta estática a 0.0.0.0/0 como ruta predeterminada no constituye routing dependiente de protocolo. La ruta estática predeterminada "quad zero" se puede utilizar con cualquier protocolo de enrutamiento actualmente admitido. En general, la ruta estática predeterminada se configura en el router que tiene una conexión a una red fuera del dominio de routing EIGRP; por ejemplo, a un ISP.

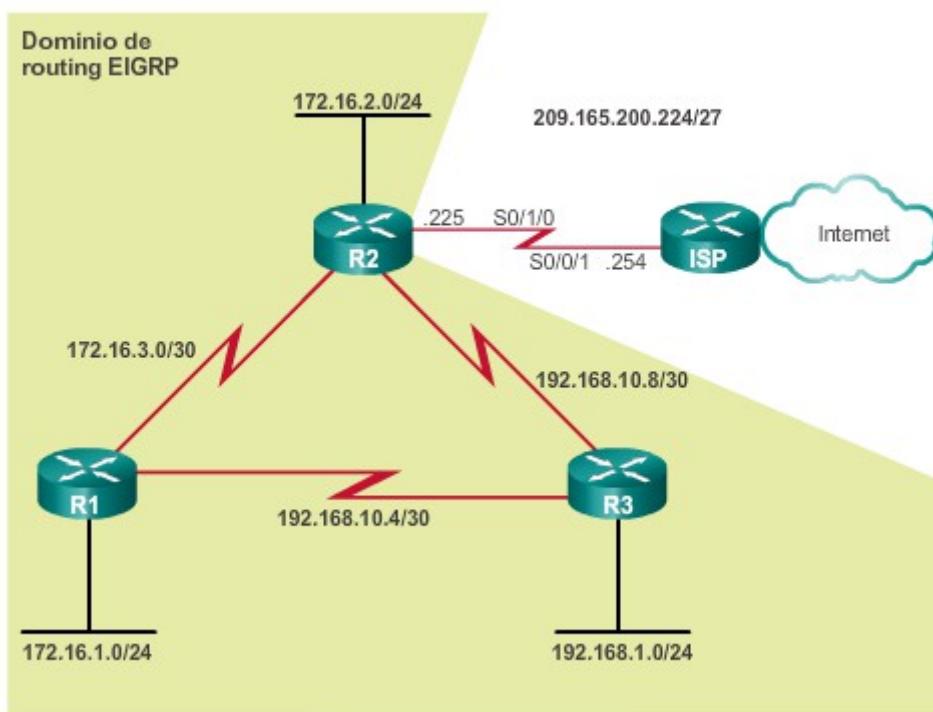
En la figura 1, el R2 es el router de gateway que conecta el dominio de routing EIGRP a Internet. Cuando se configura la ruta estática predeterminada, es necesario propagar esa ruta en todo el dominio EIGRP, como se muestra en la figura 2.

Un método para propagar una ruta estática predeterminada dentro del dominio de routing EIGRP es mediante el comando **redistribute static**. El comando **redistribute static** le indica a EIGRP que incluya rutas estáticas en sus actualizaciones de EIGRP a otros routers. En la figura 3, se muestra la configuración de la ruta estática predeterminada y el comando **redistribute static** en el router R2.

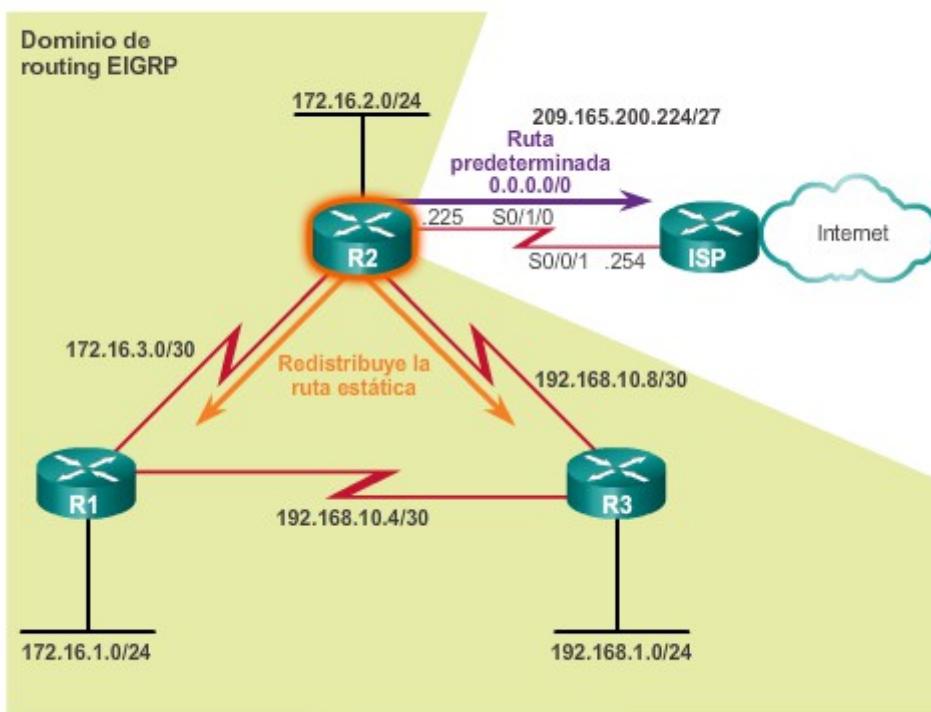
En la figura 4, se verifica que el router R2 recibió la ruta predeterminada y la instaló en su tabla de routing IPv4.

En la figura 5, el comando **show ip protocols** verifica que el R2 redistribuye las rutas estáticas dentro del dominio de routing EIGRP.

### Propagación de rutas predeterminadas



Topología EIGRP para IPv4



## Configuración y propagación de una ruta estática predeterminada en el R2

```
R2(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1/0
R2(config)# router eigrp 1
R2(config-router)# redistribute static
```

### Ruta estática predeterminada del R2

```
R2# show ip route | include 0.0.0.0
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*    0.0.0.0/0 is directly connected, Serial0/1/0
R2#
```

### Redistribución de rutas estáticas en EIGRP

```
R2# show ip protocols
*** IP Routing is NSF aware ***

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
  Redistributing: static
  EIGRP-IPv4 Protocol for AS(1)
<resultado omitido>
```

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.3.2

### Verificación de la ruta predeterminada propagada

En la ilustración, se muestra una parte de las tablas de routing IPv4 del R1 y el R3.

En las tablas de routing del R1 y el R3, observe el origen de routing y la distancia administrativa de la nueva ruta predeterminada que se descubrieron mediante EIGRP. La entrada de la ruta predeterminada que se descubrió mediante EIGRP se identifica por lo siguiente:

- **D:** esta ruta se descubrió en una actualización de routing EIGRP.
- **\***: la ruta es candidata para una ruta predeterminada.
- **EX:** la ruta es una ruta EIGRP externa, en este caso, una ruta estática fuera del dominio de routing EIGRP.
- **170:** distancia administrativa de una ruta EIGRP externa.

Observe que el R1 selecciona al R3 como el sucesor a la ruta predeterminada, porque tiene una distancia factible menor. Las rutas predeterminadas proporcionan una ruta predeterminada para salir del dominio de enrutamiento y, al igual que las rutas sumarizadas, minimizan el número de entradas en la tabla de enrutamiento.

#### **Verificación de rutas predeterminadas en el R1 y el R3**

```
R1# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.6 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/3651840] via 192.168.10.6, 00:25:23,
Serial0/0/1
R1#
```

```
R3# show ip route | include 0.0.0.0
Gateway of last resort is 192.168.10.9 to network 0.0.0.0
D*EX 0.0.0.0/0 [170/3139840] via 192.168.10.9, 00:27:17,
Serial0/0/1
R3#
```

Capítulo

o 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.3.3 EIGRP para

IPv6: ruta predeterminada.

Recuerde que EIGRP mantiene tablas independientes para IPv4 e IPv6, por lo tanto, una ruta predeterminada IPv6 debe propagarse por separado, como se muestra en la figura 1. De manera similar a lo que sucede en EIGRP para IPv4, se configura una ruta estática predeterminada en el router de gateway (R2), como se muestra en la figura 2:

```
R2(config)# ipv6 route ::/0 serial 0/1/0
```

El prefijo ::/0 y la longitud de prefijo equivalen a la dirección y máscara de subred 0.0.0.0 0.0.0.0 que se usan en IPv4. Ambas son direcciones compuestas totalmente de ceros y con una longitud de prefijo /0.

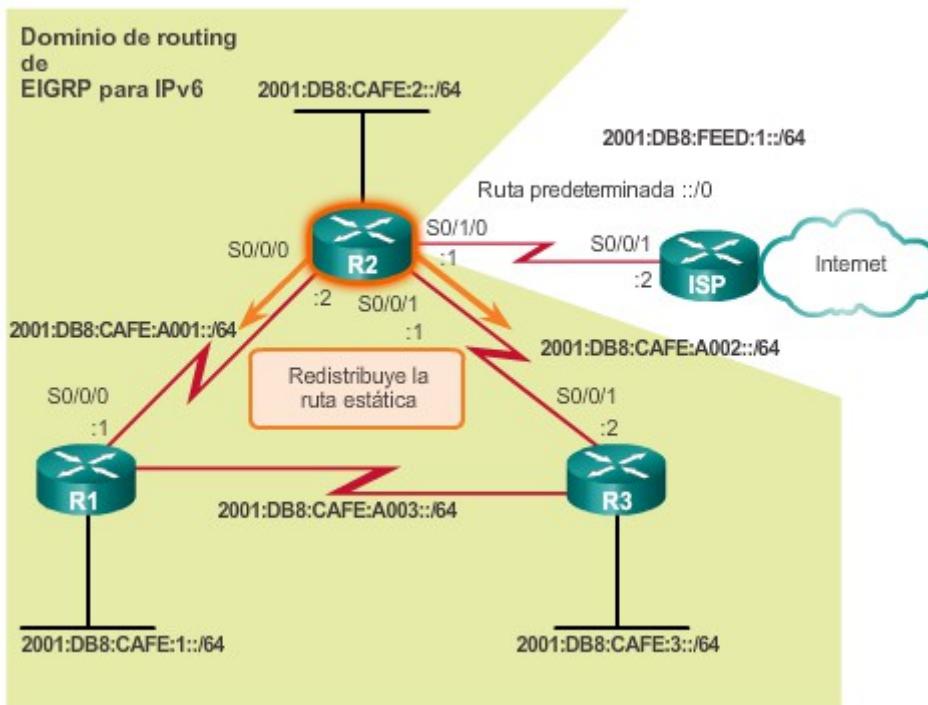
La ruta estática predeterminada IPv6 se redistribuye en el dominio EIGRP para IPv6 mediante el mismo comando **redistribute static** que se usó en EIGRP para IPv4.

**Nota:** es posible que en algunos IOS se requiera que el comando **redistribute static** incluya los parámetros de métricas de EIGRP para que se pueda redistribuir la ruta estática.

#### **Verificación de la propagación de una ruta predeterminada**

La propagación de la ruta estática predeterminada IPv6 se puede verificar mediante la revisión de la tabla de routing IPv6 del R1 con el comando **show ipv6 route**, como se muestra en la figura 3. Observe que el sucesor o la dirección del siguiente salto no es el R2, sino el R3. Esto se debe a que el R3 proporciona una mejor ruta al R2, con un costo de métrica menor que el R1.

## Topología EIGRP para IPv6



Configuración y propagación de una ruta estática predeterminada IPv6 en el R2

```
R2(config)# ipv6 route ::/0 serial 0/1/0
R2(config)# ipv6 router eigrp 2
R2(config-rtr)# redistribute static
```

Verificación de la ruta predeterminada en el R1 y el R3

```
R1# show ipv6 route
IPv6 Routing Table - default - 12 entries
Codes: C - Connected, L - Local, S - Static,
        U - Per-user Static route
        B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
        IA - ISIS interarea, IS - ISIS summary, D - EIGRP,
        EX - EIGRP external
        ND - ND Default, NDp - ND Prefix, DCE - Destination,
        NDr - Redirect
        O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1,
        OE2 - OSPF ext 2
        ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
EX ::/0 [170/3523840]
via FE80::3, Serial0/0/1
```

Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.3.4 Packet

Tracer: Propagación de una ruta predeterminada en EIGRP para IPv4 e IPv6

## Información básica/situación

En esta actividad, configurará y propagará una ruta predeterminada en EIGRP para las redes IPv4 e IPv6. El EIGRP ya está configurado. Sin embargo, debe configurar una ruta predeterminada IPv4 y una IPv6. A continuación, configurará el proceso de routing EIGRP para propagar la ruta predeterminada a los vecinos EIGRP descendentes. Por último, verificará las rutas predeterminadas haciendo ping a los hosts fuera del dominio de routing EIGRP.

[Packet Tracer: Propagación de una ruta predeterminada en EIGRP para IPv4 e IPv6 \(instrucciones\)](#)

[Packet Tracer: Propagación de una ruta predeterminada en EIGRP para IPv4 e IPv6 \(PKA\)](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.4.1 Utilización

### del ancho de banda de EIGRP

#### Ancho de banda de EIGRP para IPv4

De manera predeterminada, EIGRP usa solo hasta el 50% del ancho de banda de una interfaz para la información de 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.

Use el comando **ip bandwidth-percent eigrp** para configurar el porcentaje del ancho de banda que EIGRP puede utilizar en una interfaz.

Router(config-if)# **ip bandwidth-percent eigrp** *número-as porcentaje*

En la figura 1, el R1 y el R2 comparten un enlace muy lento de 64 kb/s. La configuración para limitar el ancho de banda que utiliza EIGRP se muestra en la figura 2. El comando **ip bandwidth-percent eigrp** usa el ancho de banda configurado (o el ancho de banda predeterminado) para calcular el porcentaje que EIGRP puede usar. En este ejemplo, EIGRP se limita a no más del 40% del ancho de banda del enlace. Por eso, EIGRP nunca usa más de 32 kb/s del ancho de banda del enlace para el tráfico de paquetes EIGRP.

Para restaurar el valor predeterminado, utilice la versión **no** de este comando.

Utilice el verificador de sintaxis de la figura 3 para limitar el ancho de banda que EIGRP usa entre el R2 y el R3 al 75% del ancho de banda del enlace.

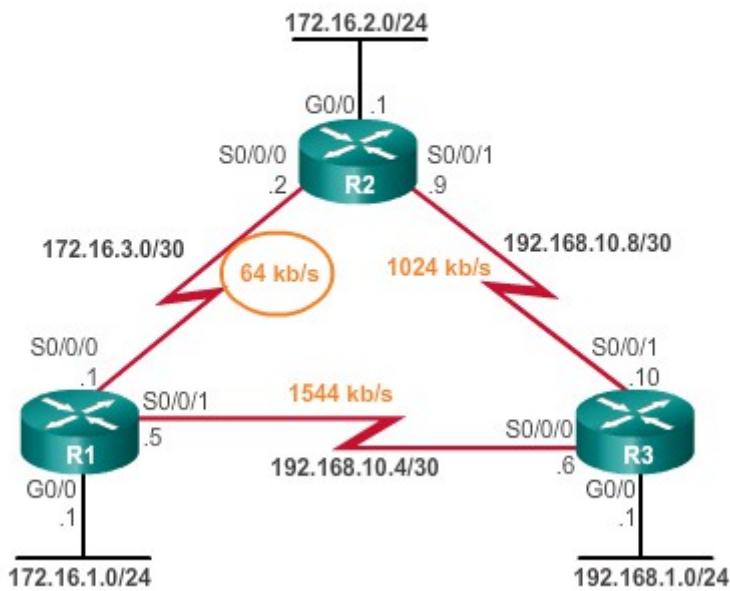
#### Ancho de banda de EIGRP para IPv6

Para configurar el porcentaje del ancho de banda que puede utilizar EIGRP para IPv6 en una interfaz, utilice el comando **ipv6 bandwidth-percent eigrp** en el modo de configuración de interfaz. Para restaurar el valor predeterminado, utilice la versión **no** de este comando.

Router(config-if)# **ipv6 bandwidth-percent eigrp** *número-as porcentaje*

En la figura 4, se muestra la configuración de las interfaces entre el R1 y el R2 para limitar el ancho de banda que utiliza EIGRP para IPv6.

## Topología EIGRP para IPv4



### Configuración del uso del ancho de banda con EIGRP para IPv4

```
R1(config)# interface serial 0/0/0
R1(config-if)# ip bandwidth-percent eigrp 1 40
R1(config-if)#
```

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip bandwidth-percent eigrp 1 40
R2(config-if)#
```

**Configure las interfaces entre el R2 y el R3 para limitar el tráfico del AS de EIGRP 1 a un máximo del 75% del ancho de banda del enlace. Realice las tareas en el siguiente orden:**

- Configure la interfaz serial 0/0/1 en el R2.
- Configure la interfaz serial 0/0/1 en el R3.

```
R2 (config)# interface serial 0/0/1  
R2 (config-if)# ip bandwidth-percent eigrp 1 75
```

**Ahora configure el R3.**

```
R3 (config)# interface serial 0/0/1  
R3 (config-if)# ip bandwidth-percent eigrp 1 75
```

**Configuró correctamente el uso del ancho de banda.**

#### **Configuración del uso del ancho de banda con EIGRP para IPv6**

```
R1 (config)# interface serial 0/0/0  
R1 (config-if)# ipv6 bandwidth-percent eigrp 2 40  
R1 (config-if) #
```

```
R2 (config)# interface serial 0/0/0  
R2 (config-if)# ipv6 bandwidth-percent eigrp 2 40  
R2 (config-if) #
```

#### **Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.4.2**

##### **Temporizadores de saludo y de espera**

##### **Intervalos de saludo y tiempos de espera en EIGRP para IPv4**

EIGRP usa un protocolo de saludo ligero para establecer y controlar el estado de conexión de los vecinos. El tiempo de espera le indica al router la cantidad máxima de tiempo que debe esperar para recibir el siguiente saludo, antes de declarar que el vecino es inalcanzable.

Los intervalos de saludo y los tiempos de espera se pueden configurar por interfaz y no tienen que coincidir con otros routers EIGRP para establecer o mantener adyacencias. El comando para configurar un intervalo de saludo diferente es el siguiente:

```
Router(config-if)# ip hello-interval eigrp número-as segundos
```

Si cambia el intervalo de saludo, asegúrese de que el valor del tiempo de espera sea igual o superior al intervalo de saludo. De lo contrario, la adyacencia de vecino se desactiva después de que expira el tiempo de espera y antes del siguiente intervalo de saludo. Para configurar un tiempo de espera diferente, use el siguiente comando:

```
Router(config-if)# ip hold-time eigrp número-as segundos
```

El valor de *segundos* para los intervalos de saludo y de tiempo de espera puede ser de 1 a 65 535.

En la figura 1, se muestra la configuración del R1 para usar un intervalo de saludo de 50 segundos y un tiempo de espera de 150 segundos. Se puede usar la forma **no** de los dos comandos para restaurar los valores predeterminados.

No es necesario que el tiempo del intervalo de saludo y el tiempo de espera coincidan para que dos routers formen una adyacencia EIGRP.

Utilice el verificador de sintaxis de la figura 2 para configurar la interfaz adyacente en el R2 con los mismos valores del R1.

#### **Intervalos de saludo y tiempos de espera en EIGRP para IPv6**

EIGRP para IPv6 utiliza los mismos tiempos de intervalo de saludo y de espera que EIGRP para IPv4. Los comandos del modo de configuración de interfaz son parecidos a los que se usan para IPv4:

```
Router(config-if)# ipv6 hello-interval eigrp número-as segundos
```

```
Router(config-if)# ipv6 hold-time eigrp número-as segundos
```

En la figura 3, se muestra la configuración de los tiempos de intervalo de saludo y de espera para el R1 y el R2 con EIGRP para IPv6.

## Configuración de los temporizadores de saludo y de espera de EIGRP para IPv4

```
R1(config)# interface s0/0/0
R1(config-if)# ip hello-interval eigrp 1 50
R1(config-if)# ip hold-time eigrp 1 150
```

Intervalos de saludo y tiempos de espera predeterminados para EIGRP

Ancho de banda	Enlace de ejemplo	Intervalo de saludo predeterminado	Tiempo de espera predeterminado
1.544 Mbps	Frame relay multipunto	60segundos	180segundos
Mayor que 1.544 Mbps	T1, Ethernet	5segundos	15segundos

## Configuración de los temporizadores en el R2

Configure la interfaz serial 0/0/0 del R2 para que use un intervalo de saludo de 50 segundos y un tiempo de espera de 150 segundos para el AS 1. Realice las tareas en el siguiente orden:

- Configure el intervalo de saludo.
- Configure el tiempo de espera.

```
R2(config)# interface serial 0/0/0
R2(config-if)# ip hello-interval eigrp 1 50
R2(config-if)# ip hold-time eigrp 1 150
Configuró correctamente los temporizadores en el R2.
```

## Configuración de los temporizadores de saludo y de espera de EIGRP para IPv6

```
R1(config)# inter serial 0/0/0
R1(config-if)# ipv6 hello-interval eigrp 2 50
R1(config-if)# ipv6 hold-time eigrp 2 150
```

```
R2(config)# inter serial 0/0/0
R2(config-if)# ipv6 hello-interval eigrp 2 50
R2(config-if)# ipv6 hold-time eigrp 2 150
```

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.4.3 Balanceo de carga de IPv4

El balanceo de carga de igual costo es la capacidad de un router de distribuir tráfico saliente a través de todas las interfaces que tienen la misma métrica desde la dirección de destino. El

balanceo de carga usa los segmentos de red y el ancho de banda de manera más eficiente. En el caso de IP, el software IOS de Cisco aplica de manera predeterminada el balanceo de carga con hasta cuatro rutas de igual costo.

En la figura 1, se muestra la topología de la red EIGRP para IPv4. En esta topología, el R3 tiene dos rutas EIGRP de igual costo para la red entre el R1 y el R2, 172.16.3.0/30. Una ruta es a través del R1 en 192.168.10.4/30, y la otra es a través del R2 en 192.168.10.8/30.

El comando **show ip protocols** se puede usar para verificar la cantidad de rutas de igual costo que actualmente están configuradas en el router. El resultado de la figura 2 muestra que el R3 usa la opción predeterminada de cuatro rutas de igual costo.

La tabla de routing mantiene ambas rutas. En la figura 3, se muestra que el R3 tiene dos rutas EIGRP de igual costo para la red 172.16.3.0/30. Una ruta es a través del R1 en 192.168.10.5, y la otra es a través del R2 en 192.168.10.9. Si se observa la topología de la figura 1, puede parecer que la ruta a través del R1 es la mejor ruta, porque hay un enlace de 1544 kb/s entre el R3 y el R1, mientras que el enlace al R2 es solo de 1024 kb/s. Sin embargo, EIGRP solo usa el ancho de banda más lento en la métrica compuesta, que es el enlace de 64 kb/s entre el R1 y el R2. Las dos rutas tienen el mismo enlace de 64 kb/s como el ancho de banda más lento, lo que da como resultado que ambas rutas sean iguales.

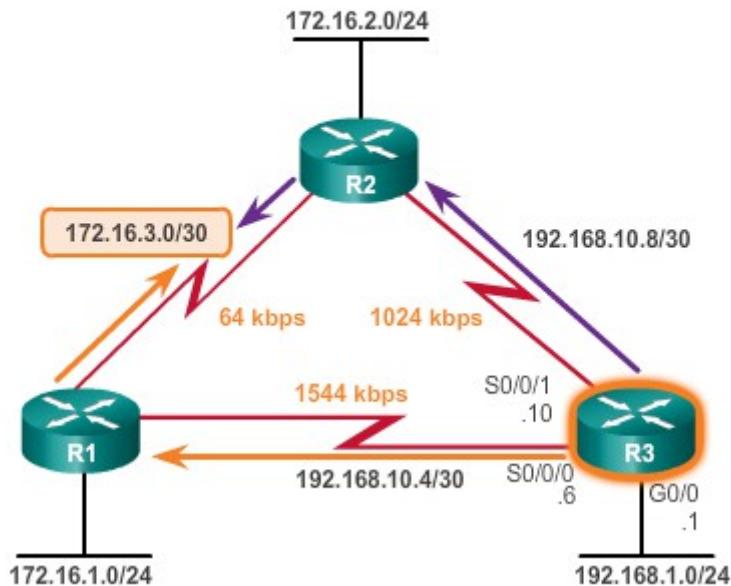
Cuando se aplica switching de procesos a un paquete, el balanceo de carga de rutas de igual costo se produce por paquete. Cuando se aplica switching rápido a los paquetes, el balanceo de carga de rutas de igual costo se produce por destino. Cisco Express Forwarding (CEF) puede realizar balanceo de carga tanto por paquete como por destino.

De manera predeterminada, el IOS de Cisco permite que el balanceo de carga use hasta cuatro rutas de igual costo. Sin embargo, esto se puede modificar. Con el comando **maximum-paths** del modo de configuración del router, pueden mantenerse hasta 32 rutas de igual costo en la tabla de routing.

```
Router(config-router)# maximum-paths valor
```

El argumento *valor* se refiere a la cantidad de rutas que deben mantenerse para el balanceo de carga. Si el valor se establece en **1**, el balanceo de carga se deshabilita.

## Topología EIGRP para IPv4



Rutas máximas del R3

```

R3# show ip protocols
*** IP Routing is NSF aware ***

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-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 3.3.3.3
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

    Automatic Summarization: disabled
    Address Summarization:
      192.168.0.0/22 for Se0/0/0, Se0/0/1
        Summarizing 3 components with metric 2816
      Maximum path: 4
<resultado omitido>
  
```

### Tabla de routing IPv4 del R3

```
R3# show ip route eigrp
<resultado omitido>
Gateway of last resort is 192.168.10.9 to network 0.0.0.0

D*EX 0.0.0.0/0 [170/3139840] via 192.168.10.9, 00:14:24,
Serial0/0/1
    172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
D      172.16.1.0/24 [90/2170112] via 192.168.10.5,
00:14:28, Serial0/0/0
D      172.16.2.0/24 [90/3012096] via 192.168.10.9,
00:14:24, Serial0/0/1
D      172.16.3.0/30 [90/41024000] via 192.168.10.9,
00:14:24, Serial0/0/1
        [90/41024000] via 192.168.10.5, 00:14:24,
        Serial0/0/0
D      192.168.0.0/22 is a summary, 00:14:40, Null0
R3#
```

#### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.4.4 Balanceo de carga de IPv6

En la figura 1, se muestra la topología de la red EIGRP para IPv6. Los enlaces seriales en la topología tienen el mismo ancho de banda que se utiliza en la topología EIGRP para IPv4.

En forma similar a la situación anterior para IPv4, el R3 tiene dos rutas EIGRP de igual costo para la red entre el R1 y el R2, 2001:DB8:CAFE:A001::/64. Una ruta es a través del R1 en FE80::1, y la otra es a través del R2 en FE80::2.

En la figura 2, se muestra que las métricas de EIGRP para las redes 2001:DB8:CAFE:A001::/64 y 172.16.3.0/30 son las mismas en la tabla de routing IPv6 y en la tabla de routing IPv4. Esto se debe a que la métrica compuesta de EIGRP es la misma en EIGRP para IPv6 y para IPv4.

#### **Balanceo de carga con distinto costo**

EIGRP para IPv4 y para IPv6 también puede equilibrar el tráfico en varias rutas con métricas diferentes. Este tipo de balanceo se denomina “balanceo de carga con distinto costo”. La configuración de un valor con el comando **variance** en el modo de configuración del router permite que EIGRP instale varias rutas sin bucles y con distinto costo en una tabla de routing local.

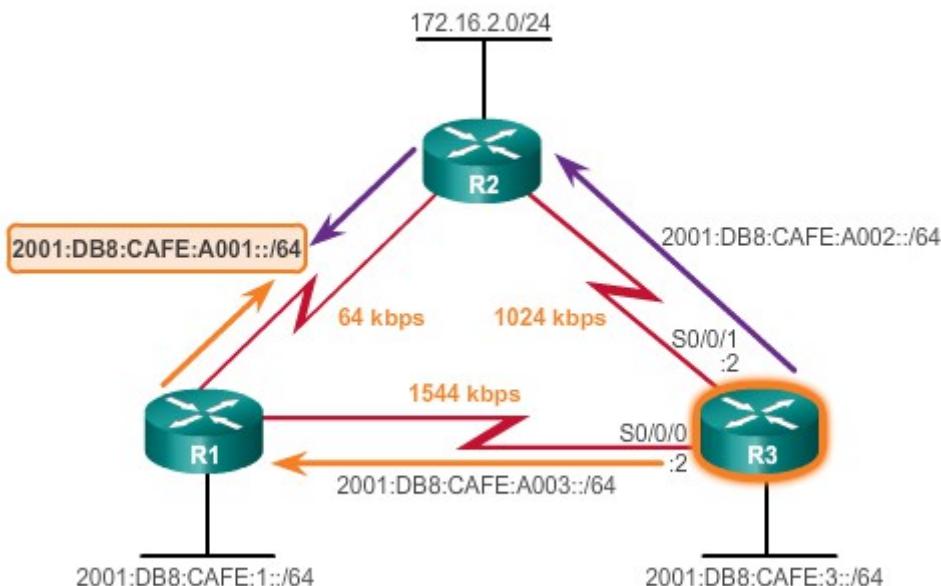
Para que se la instale en la tabla de routing local, una ruta que se descubre mediante EIGRP debe satisfacer dos criterios:

- La ruta no debe tener bucles y debe ser un sucesor factible o tener una distancia notificada inferior a la distancia total.
- La métrica de la ruta debe ser inferior a la métrica de la mejor ruta (el sucesor) multiplicada por la variación configurada en el router.

Por ejemplo, si la variación es de 1, solo se instalan en la tabla de routing local las rutas con la misma métrica que el sucesor. Si la variación es de 2, se instala en la tabla de routing local cualquier ruta descubierta mediante EIGRP con una métrica inferior al doble de la métrica del sucesor.

Para controlar la manera en que el tráfico se distribuye entre las rutas cuando hay varias rutas con distintos costos para la misma red de destino, use el comando **traffic-share balanced**. El tráfico se distribuye proporcionalmente de acuerdo con la proporción de los costos.

**Topología EIGRP para IPv6**



### Tabla de routing IPv6 del R3

```
R3# show ipv6 route eigrp
<resultado omitido>

EX  ::/0 [170/3011840]
    via FE80::2, Serial0/0/1
D  2001:DB8:ACAD::/48 [5/128256]
    via Null0, directly connected
D  2001:DB8:CAFE:1::/64 [90/2170112]
    via FE80::1, Serial0/0/0
D  2001:DB8:CAFE:2::/64 [90/3012096]
    via FE80::2, Serial0/0/1
D  2001:DB8:CAFE:A001::/64 [90/41024000]
    via FE80::2, Serial0/0/1
    via FE80::1, Serial0/0/0
R3#
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.4.5 Actividad:

#### Determinar los comandos para el ajuste de EIGRP

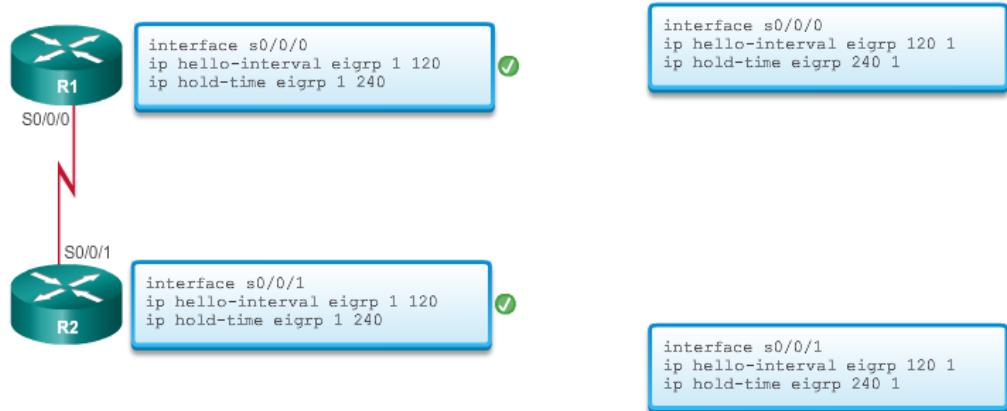
Actividad: Determinar los comandos de ajuste de EIGRP (situación 1)

La convergencia de EIGRP demora mucho en el enlace serial congestionado entre el router 1 (R1) y el router 2 (R2). Ajuste el ancho de banda de enlace máximo disponible para EIGRP en un 80% de utilización. Arrastre el comando hasta el campo correspondiente junto a cada router. No se utilizan todos los comandos. Haga clic en el botón 2 para continuar.



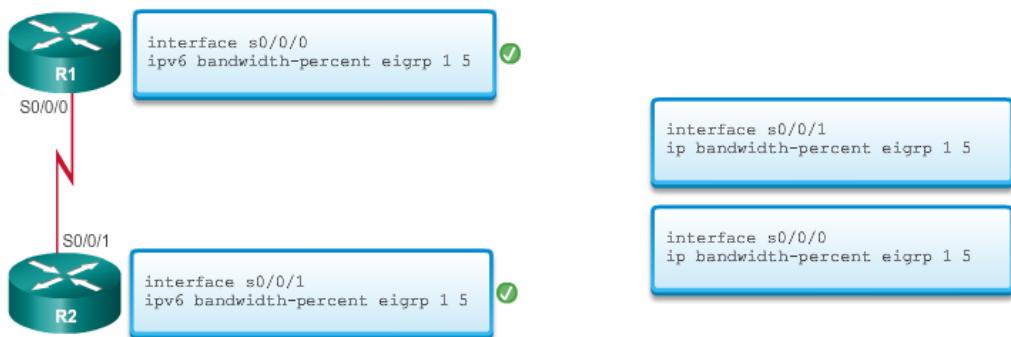
#### Actividad: Determinar los comandos de ajuste de EIGRP (situación 2)

El enlace serial entre el router 1 (R1) y el router 2 (R2) presenta un alto índice de errores, y EIGRP está perdiendo su adyacencia de vecino. Ajuste el intervalo de saludamiento máximo para EIGRP en 120 segundos y el temporizador de espera máximo para EIGRP en 240 segundos. Arrastre el comando hasta el campo correspondiente junto a cada router. No se utilizan todos los comandos. Haga clic en el botón 3 para continuar.



#### Actividad: Determinar los comandos de ajuste de EIGRP (situación 3)

El enlace serial entre el router 1 (R1) y el router 2 (R2) recientemente se actualizó a un enlace IPv6 de 2 gigabit. Ajuste el ancho de banda de enlace máximo disponible para EIGRP en un 5% de utilización. Arrastre el comando hasta el campo correspondiente junto a cada router. No se utilizan todos los comandos.



## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.5.1

### Descripción general de la autenticación del protocolo de enrutamiento

#### **Autenticación de protocolos de routing**

Los administradores de red deben tener en cuenta que los routers corren el mismo riesgo de sufrir ataques que los dispositivos para usuarios finales. Cualquier persona con un programa detector de paquetes, como Wireshark, puede leer la información que se propaga entre los routers. En general, los sistemas de routing se pueden atacar mediante la interrupción de dispositivos peer o la falsificación de información de routing.

La interrupción de peers es el ataque menos crítico de los dos, debido a que los protocolos de routing se reparan a sí mismos, lo que hace que la interrupción solo dure un poco más que el ataque propiamente dicho.

La falsificación de información de routing es una clase de ataque más sutil que tiene como objetivo la información que se transporta dentro del protocolo de routing. Las consecuencias de falsificar información de routing son las siguientes:

- Redireccionamiento del tráfico para crear bucles de routing
- Redireccionamiento del tráfico para el control en una línea no segura
- Redireccionamiento del tráfico para descartarlo

Un método para proteger la información de routing de la red es autenticar los paquetes del protocolo de routing mediante el algoritmo de síntesis del mensaje 5 (MD5). MD5 permite que los routers comparan firmas que deberían ser iguales, a fin de confirmar que provienen de un origen verosímil.

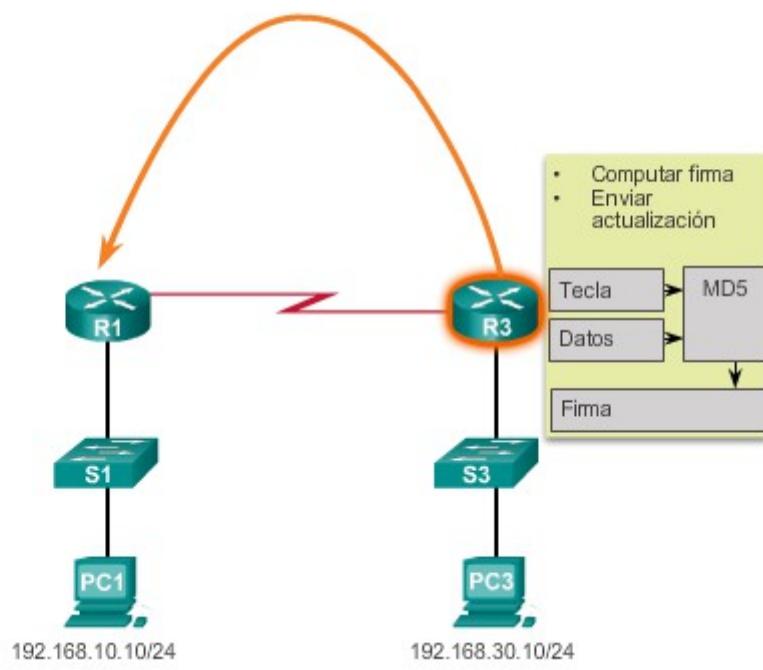
Los tres componentes de este sistema son los siguientes:

- Algoritmo de cifrado, generalmente de conocimiento público
- Clave que se usa en el algoritmo de cifrado, un secreto que comparten los routers que autentican los paquetes
- Contenido del paquete

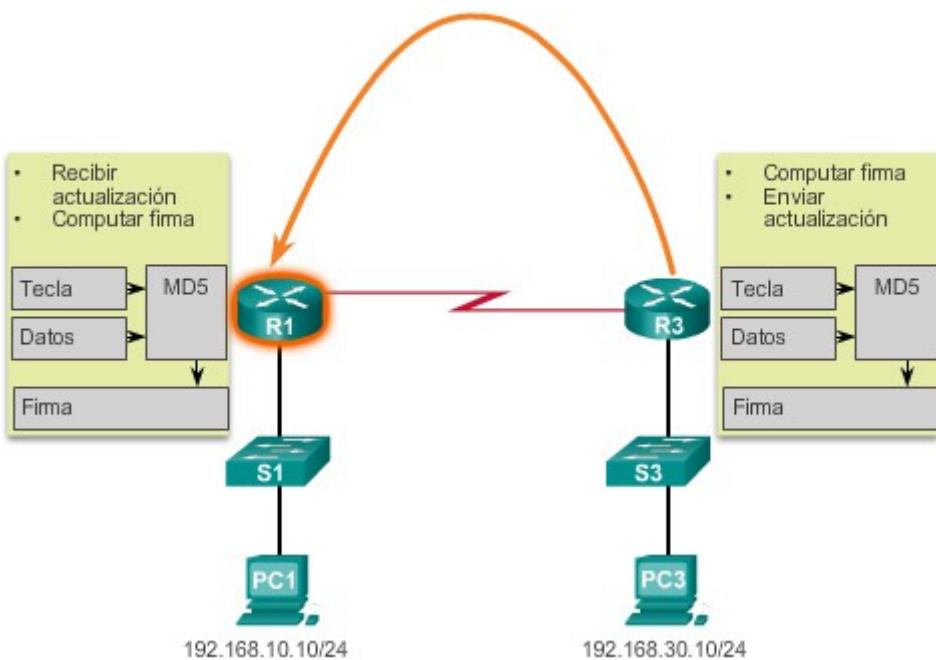
En la ilustración, haga clic en el botón Reproducir para ver una animación de la manera en que cada router autentica la información de routing. En general, el originador de la información de routing produce una firma con la clave y los datos de routing que está a punto de enviar como entradas al algoritmo de cifrado. El router que recibe los datos de routing luego repite el proceso con la misma clave y los mismos datos de routing que recibió. Si la firma que computa el receptor es la misma que computa el emisor, la actualización se autentica y se considera confiable.

Los protocolos de routing como RIPv2, EIGRP, OSPF, IS-IS y BGP admiten varias formas de autenticación MD5.

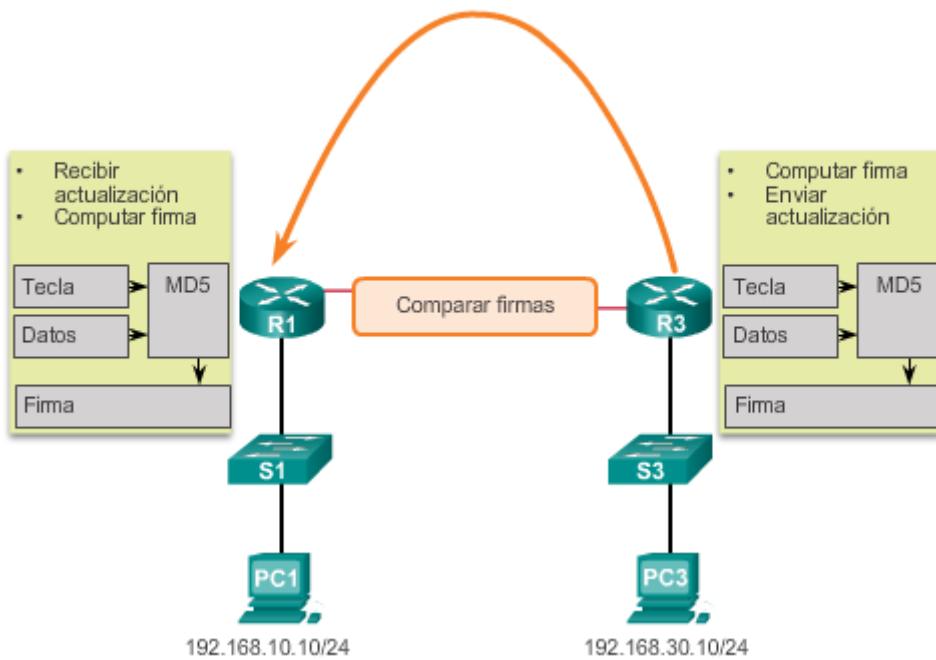
### Autenticación mediante MD5



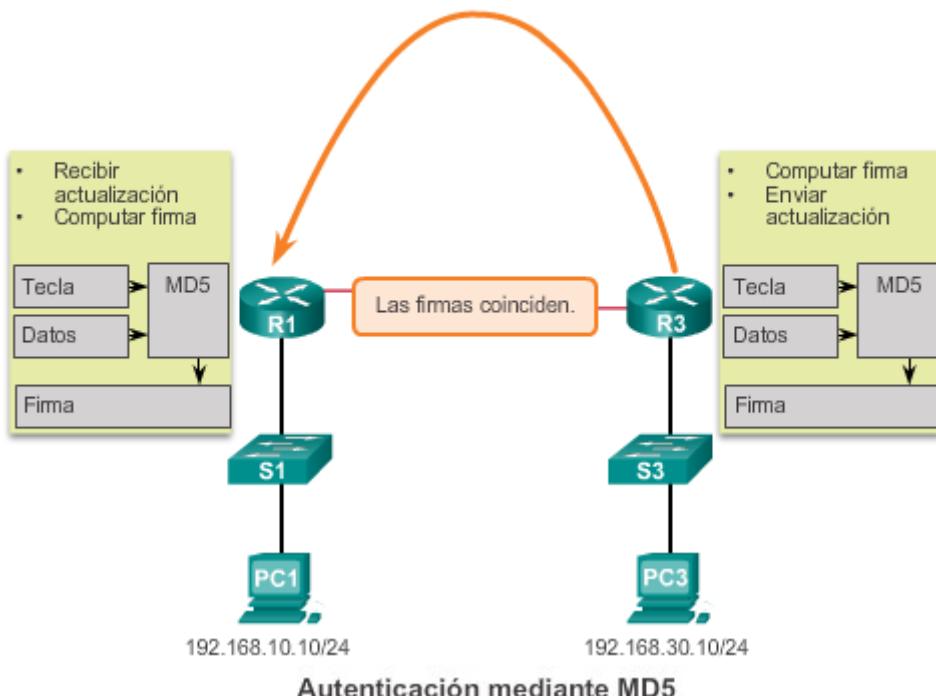
### Autenticación mediante MD5



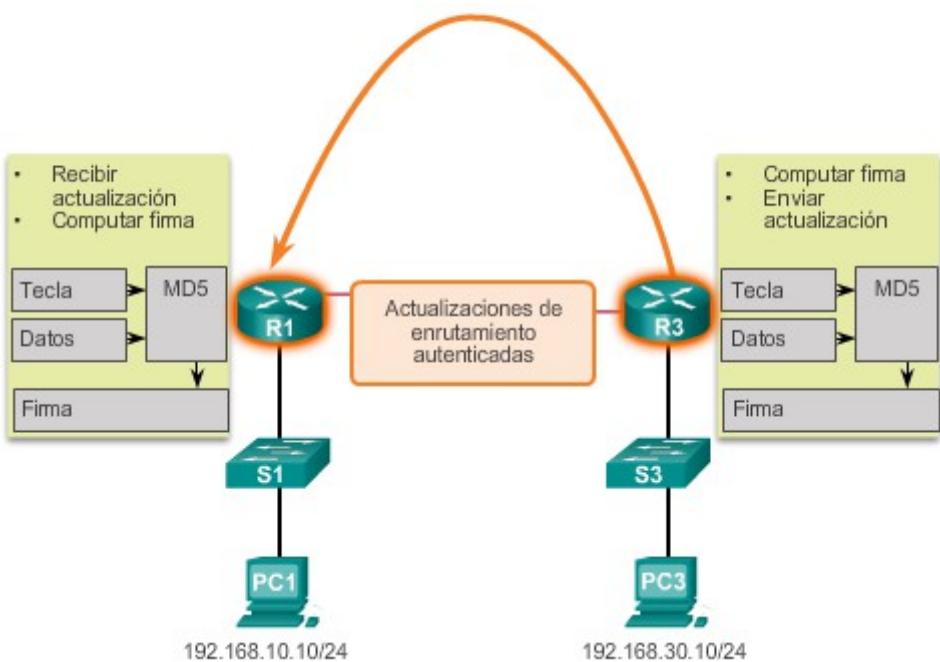
## Autenticación mediante MD5



### Autenticación mediante MD5



### Autenticación mediante MD5



Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.5.2

#### Configuración de EIGRP con autenticación MD5

La autenticación de mensajes EIGRP asegura que los routers solo acepten mensajes de routing de otros routers que conozcan la misma clave previamente compartida. Sin la autenticación configurada, si una persona no autorizada introduce en la red otro router con

información de ruta diferente o en conflicto, puede dañar las tablas de routing de los routers legítimos, lo que puede acompañarse de un ataque DoS. Entonces, cuando se agrega autenticación a los mensajes EIGRP que se envían entre routers, se evita que alguien agregue otro router a la red —a propósito o por accidente— y cause un problema.

EIGRP admite la autenticación de protocolos de routing mediante MD5. La configuración de la autenticación de mensajes EIGRP consta de dos pasos: la creación de un llavero y una clave, y la configuración de la autenticación de EIGRP para usar el llavero y la llave.

### Paso 1. Crear un llavero y una clave

Para funcionar, la autenticación del routing requiere una clave en un llavero. Para que se pueda habilitar la autenticación, cree un llavero y, al menos, una clave.

- a. En el modo de configuración global, cree el llavero. Aunque pueden configurarse varias claves, esta sección se centra en el uso de una sola clave.

```
Router(config)# key chain nombre-de-llavero
```

- b. Especifique la ID de la clave. La ID de la clave es el número que se usa para identificar una clave de autenticación dentro de un llavero. El intervalo de claves es de 0 a 2 147 483 647. Se recomienda que el número de clave sea el mismo en todos los routers en la configuración.

```
Router(config-keychain)# Clave id-clave
```

- c. Especifique la cadena de clave para la clave. La cadena de clave es parecida a una contraseña. Los routers que intercambian claves de autenticación deben configurarse con la misma cadena de clave.

```
Router(config-keychain-key )# key-string texto-cadena-clave
```

### Paso 2. Configurar la autenticación de EIGRP con el llavero y la clave

Configure EIGRP para realizar la autenticación de mensajes con la clave definida anteriormente. Complete esta configuración en todas las interfaces habilitadas para EIGRP.

- a. En el modo de configuración global, especifique la interfaz en la que configurará la autenticación de mensajes EIGRP.

```
Router(config)# interface tipo número
```

- b. Habilite la autenticación de mensajes EIGRP. La palabra clave **md5** indica que se usará el hash MD5 para la autenticación.

```
Router(config-if)# ip authentication mode eigrp número-asmd5
```

- c. Especifique el llavero que debe usarse para la autenticación. El argumento *nombre-de-llavero* especifica el llavero que se creó en el paso 1.

```
Router(config-if)# ip authentication key-chain eigrp número-as nombre-de-llavero
```

Cada clave tiene su propia ID de clave, que se almacena localmente. La combinación de la ID de la clave y la interfaz asociada al mensaje identifica de manera exclusiva el algoritmo de autenticación y la clave de autenticación MD5 en uso. El llavero y la actualización de routing se procesan con el algoritmo MD5 para producir una firma única.

### Autenticación de EIGRP con MD5

#### Paso 1: Creación de un llavero y una clave

```
Router(config)# key chain name-of-chain
Router(config-keychain)# key key-id
Router(config-keychain-key)# key-string key-string-text
```

#### Paso 2: Configuración de la autenticación de EIGRP con el llavero y la clave

```
Router(config)# interface type number
Router(config-if)# ip authentication mode eigrp as-number md5
Router(config-if)# ip authentication key-chain eigrp as-number
name-of-chain
```

[Capítulo](#)

#### Io 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.5.3 Ejemplo de autenticación de EIGRP

Para autenticar las actualizaciones de routing, todas las interfaces con EIGRP habilitado deben estar configuradas para admitir la autenticación. En la figura 1, se muestra la topología IPv4 y las interfaces que tienen autenticación configurada.

En la figura 2, se muestra la configuración para el router R1 con el llavero **EIGRP\_KEY** y la cadena de clave **cisco123**. Una vez que el R1 está configurado, los otros routers reciben actualizaciones de routing autenticadas. Las adyacencias se pierden hasta que se configura la autenticación del protocolo de routing en los vecinos.

En la figura 3, se muestra una configuración parecida para el router R2. Observe que la misma cadena de clave, **cisco123**, se usa para autenticar información con el R1 y, finalmente, el R3.

Utilice el verificador de sintaxis de la figura 4 para configurar la autenticación de EIGRP para el R3.

#### Configuración de la autenticación de EIGRP para IPv6

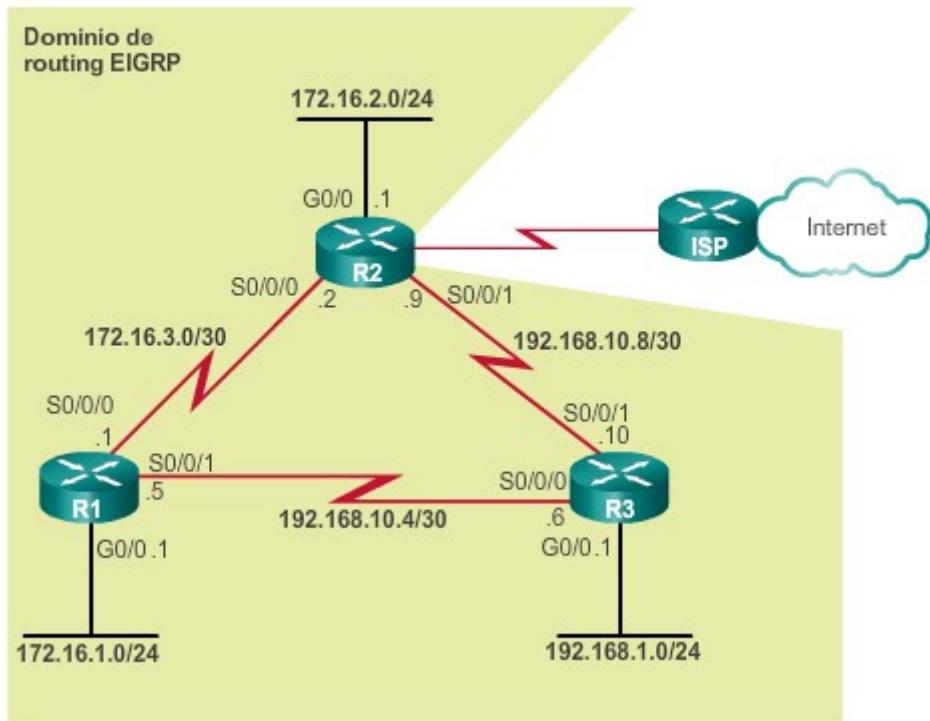
Los algoritmos y la configuración para autenticar mensajes EIGRP para IPv6 son los mismos que los correspondientes a EIGRP para IPv4. La única diferencia es que en los comandos del modo de configuración de interfaz se usa **ipv6** en lugar de **ip**.

```
Router(config-if)# ipv6 authentication mode eigrp número-asmd5
```

```
Router(config-if)# ipv6 authentication key-chain eigrp número-as nombre-de-llavero
```

En la figura 5, se muestran los comandos para configurar la autenticación de EIGRP para IPv6 en el router R1 por medio del llavero **EIGRP\_IPV6\_KEY** y la cadena de clave **cisco123**. En el R2 y el R3 se introducen configuraciones parecidas.

Topología EIGRP para IPv4



Configuración de la autenticación MD5 de EIGRP en el R1

```
R1(config)# key chain EIGRP_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco123
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# ip authentication mode eigrp 1 md5
R1(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R1(config-if)# end
R1#
```

## Configuración de la autenticación MD5 de EIGRP en el R2

```
R2(config)# key chain EIGRP_KEY
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string cisco123
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip authentication mode eigrp 1 md5
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# ip authentication mode eigrp 1 md5
R2(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R2(config-if)# end
R2#
```

## Configuración de la autenticación de EIGRP en el R3

Configure las interfaces seriales del R3 para la autenticación de EIGRP y vuelva al modo de configuración global después de cada sección de configuración.

Realice las tareas en el siguiente orden:

- Configure el llavero EIGRP\_KEY con la cadena de clave cisco123.
- Configure serial 0/0/0 para que use autenticación MD5.
- Configure serial 0/0/0 para que use el llavero EIGRP\_KEY.
- Configure serial 0/0/1 para que use autenticación MD5.
- Configure serial 0/0/1 para que use el llavero EIGRP\_KEY.

```
R3(config)# key chain EIGRP_KEY
R3(config-keychain)# key 1
R3(config-keychain-key)# key-string cisco123
R3(config-keychain-key)# exit
R3(config-keychain)# exit
R3(config)# interface serial 0/0/0
R3(config-if)# ip authentication mode eigrp 1 md5
R3(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config-if)# ip authentication mode eigrp 1 md5
R3(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY
Configuró correctamente la autenticación de IPv4 para EIGRP.
```

## Configuración de la autenticación MD5 de EIGRP para IPv6 en el R1

```
R1(config)# key chain EIGRP_IPV6_KEY
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string cisco123
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ipv6 authentication mode eigrp 2 md5
R1(config-if)# ipv6 authentication key-chain eigrp 2
    EIGRP_IPV6_KEY
R1(config-if)# exit
R1(config)# interface serial 0/0/1
R1(config-if)# ipv6 authentication mode eigrp 2 md5
R1(config-if)# ipv6 authentication key-chain eigrp 2
    EIGRP_IPV6_KEY
R1(config-if)#

```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.5.4

#### Verificación de la autenticación

Una vez que se configura la autenticación de mensajes EIGRP en un router, cualquier vecino adyacente que no se haya configurado para la autenticación deja de ser un vecino EIGRP. Por ejemplo, cuando la interfaz Serial 0/0/0 del R1 estaba configurada con autenticación MD5, pero el R2 todavía no estaba configurado, apareció el siguiente mensaje del IOS en el R1:

```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.3.2 (Serial0/0/0) is down:
authentication mode changed
```

Cuando se configura la interfaz Serial 0/0/0 adyacente en el R2, se vuelve a establecer la adyacencia y aparece el siguiente mensaje del IOS en el R1.

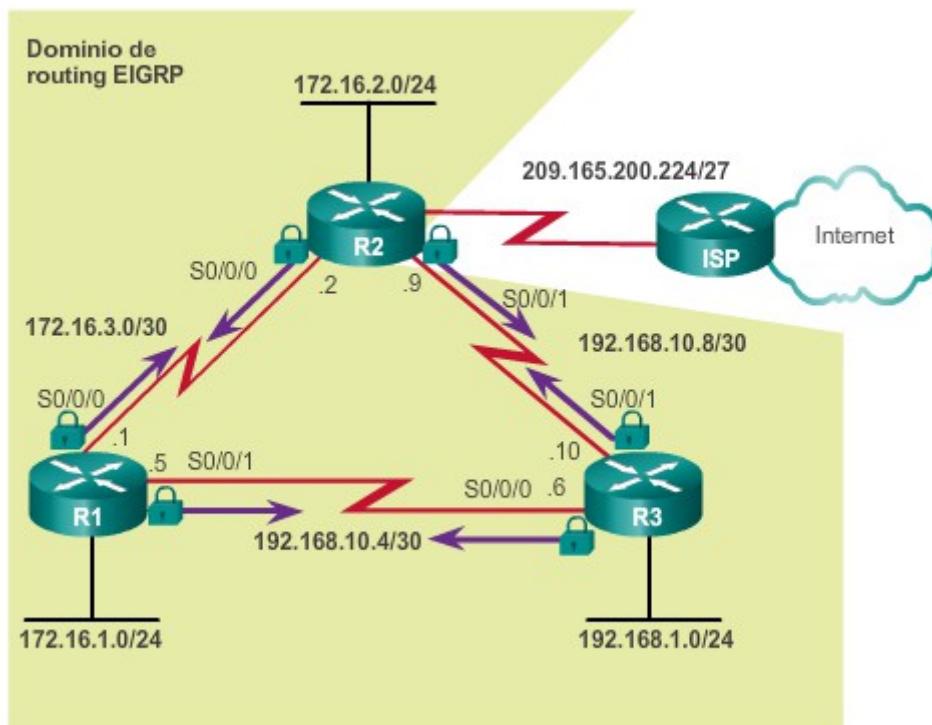
```
%DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 172.16.3.2 (Serial0/0/0) is up: new
adjacency
```

También aparecen mensajes parecidos en el R2.

Las adyacencias solo se forman cuando ambos dispositivos de conexión tienen configurada la autenticación, como se muestra en la figura 1. Para verificar que se hayan formado las adyacencias EIGRP correctas después de configurarlas para la autenticación, utilice el comando **show ip eigrp neighbors** en cada router. En la figura 2, se muestra que los tres routers volvieron a establecer adyacencias de vecinos después de que se configuró la autenticación de EIGRP.

Para verificar las adyacencias de vecinos EIGRP para IPv6, use el comando **show ipv6 eigrp neighbors**.

### Topología EIGRP para IPv4



### Verificación de la autenticación MD5 de EIGRP en el R1

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
      H   Address       Interface      Hold Uptime      SRTT      RTO      Q      Seq
          (sec)           (ms)           Cnt Num
  1 172.16.3.2    Se0/0/0        140 03:28:12     96 2340 0 23
  0 192.168.10.6  Se0/0/1        14 03:28:27     49 294 0 24
R1#
```

```
R2# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
      H   Address       Interface      Hold Uptime      SRTT      RTO      Q      Seq
          (sec)           (ms)           Cnt Num
  1 172.16.3.1    Se0/0/0        136 00:22:50   1046 5000 0 32
  0 92.168.10.10  Se0/0/1        10 07:51:37     62 372 0 35
R2#
```

```
R3# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
      H   Address       Interface      Hold Uptime      SRTT      RTO      Q      Seq
          (sec)           (ms)           Cnt Num
  0 192.168.10.5  Se0/0/0        14 00:21:26   1297 5000 0 33
  1 192.168.10.9  Se0/0/1        14 07:51:50     43 258 0 36
R3#
```

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.1.5.5 Práctica

de laboratorio: Configuración de EIGRP avanzado para admitir características de IPv4

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y configurar los parámetros básicos de los dispositivos
- Parte 2: configurar EIGRP y verificar la conectividad.
- Parte 3: Configurar la sumarización para EIGRP
- Parte 4: Configurar y propagar una ruta estática predeterminada
- Parte 5: Ajustar EIGRP
- Parte 6: Configurar la autenticación de EIGRP

[Práctica de laboratorio: Configuración de EIGRP avanzado para admitir características de IPv4](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.1.1

Comandos para la resolución de problemas de EIGRP básico

EIGRP se usa generalmente en redes empresariales grandes. La resolución de problemas relacionados con el intercambio de información de routing es una habilidad fundamental para un administrador de red. Esto es particularmente cierto para los administradores que participan en la implementación y el mantenimiento de grandes redes empresariales enrutadas que usan EIGRP como el protocolo de gateway interior (IGP). Existen varios comandos útiles para la resolución de problemas en redes EIGRP.

Con el comando **show ip eigrp neighbors**, se verifica que el router reconozca a sus vecinos. El resultado de la figura 1 indica dos adyacencias de vecinos EIGRP correctas en el R1.

En la figura 2, se verifica que el router descubrió la ruta a una red remota mediante EIGRP con el comando **show ip route**. El resultado muestra que el R1 descubrió alrededor de cuatro redes remotas mediante EIGRP.

En la figura 3, se muestra el resultado del comando **show ip protocols**. Con este comando, se verifica que EIGRP muestre los valores configurados actualmente de varias propiedades de cualquier protocolo de routing habilitado.

## **EIGRP para IPv6**

También se aplican comandos y criterios de resolución de problemas similares en EIGRP para IPv6.

Los siguientes son los comandos equivalentes que se utilizan con EIGRP para IPv6:

- Router# **show ipv6 eigrp neighbors**
- Router# **show ipv6 route**
- Router# **show ipv6 protocols**

### Tabla de vecinos EIGRP del R1

```
R1# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
  H Address       Interface   Hold Uptime      SRTT    RTO    Q  Seq
                           (sec)          (ms)
  1 172.16.3.2     Se0/0/0     140 03:28:12    96    2340  0  23
  0 192.168.10.6   Se0/0/1      14 03:28:27    49    294   0  24
R1#
```

### Tabla de routing IPv4 del R1

```
R1# show ip route eigrp
Gateway of last resort is 192.168.10.6 to network 0.0.0.0

D*EX  0.0.0.0/0 [170/3651840] via 192.168.10.6, 05:32:02,
      Serial0/0/1
      172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
D      172.16.2.0/24 [90/3524096] via 192.168.10.6, 05:32:02,
      Serial0/0/1
D      192.168.0.0/22 [90/2170112] via 192.168.10.6, 05:32:02,
      Serial0/0/1
      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D      192.168.10.8/30 [90/3523840] via 192.168.10.6,
      05:32:02, Serial0/0/1
R1#
```

## Procesos del protocolo de routing del R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

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-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    Topology : 0 (base)
    Active Timer: 3 min
    Distance: internal 90 external 170
    Maximum path: 4
    Maximum hopcount 100
    Maximum metric variance 1

  Automatic Summarization: disabled
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.1.2

#### Componentes

En la ilustración, se muestra un diagrama de flujo para el diagnóstico de problemas de conectividad de EIGRP.

Después de configurar EIGRP, el primer paso es probar la conectividad a la red remota. Si el ping falla, confirme las adyacencias de vecinos EIGRP. Hay varias razones por las que es posible que no se forme una adyacencia de vecino, incluidas las siguientes:

- La interfaz entre los dispositivos está inactiva.
- Los dos routers tienen números de sistema autónomo (ID de proceso) EIGRP que no coinciden.
- No están habilitadas las interfaces adecuadas para el proceso EIGRP.
- Una interfaz está configurada como pasiva.

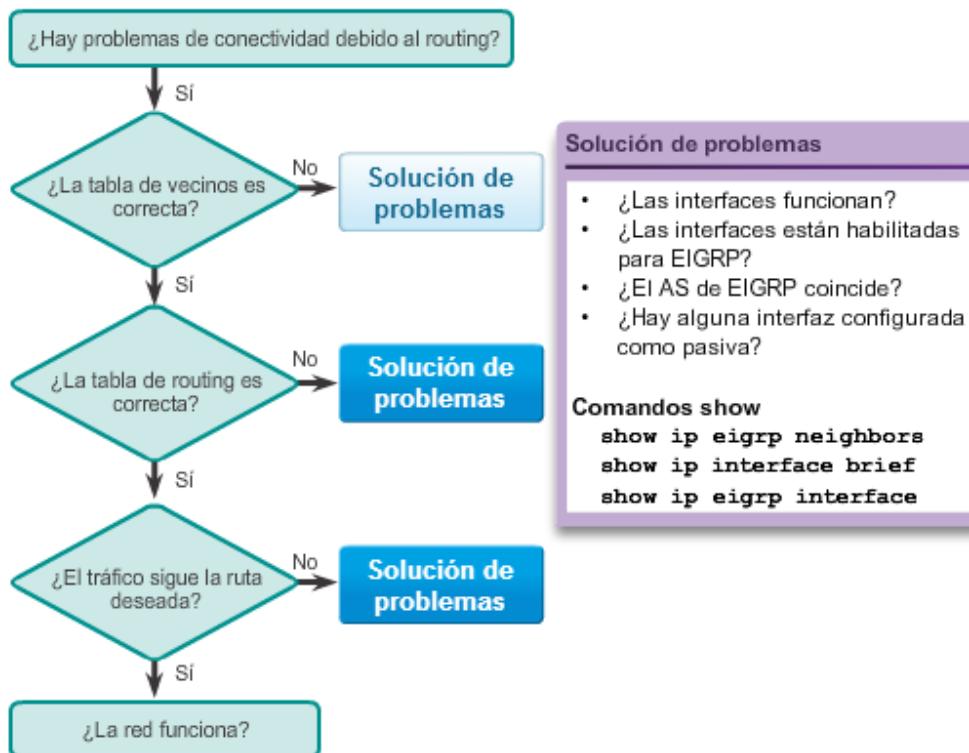
Aparte de estos problemas, existen otros más avanzados que pueden ocasionar que no se formen adyacencias de vecinos. Dos ejemplos son la configuración incorrecta de la autenticación de EIGRP y valores K incompatibles, que EIGRP usa para calcular su métrica.

Si se forma una adyacencia de vecinos EIGRP entre dos routers, pero todavía hay un problema de conexión, es posible que haya un problema de routing. Algunos de los problemas que pueden causar un problema de conectividad para EIGRP son los siguientes:

- No se anuncian las redes adecuadas en routers remotos.
- Una interfaz pasiva configurada incorrectamente, o una ACL, bloquea los anuncios de las redes remotas.
- La sumarización automática provoca un routing incongruente en una red no contigua.

Si todas las rutas requeridas están en la tabla de routing, pero la ruta que toma el tráfico es incorrecta, verifique los valores del ancho de banda de la interfaz.

#### Diagnóstico de problemas de conectividad de EIGRP

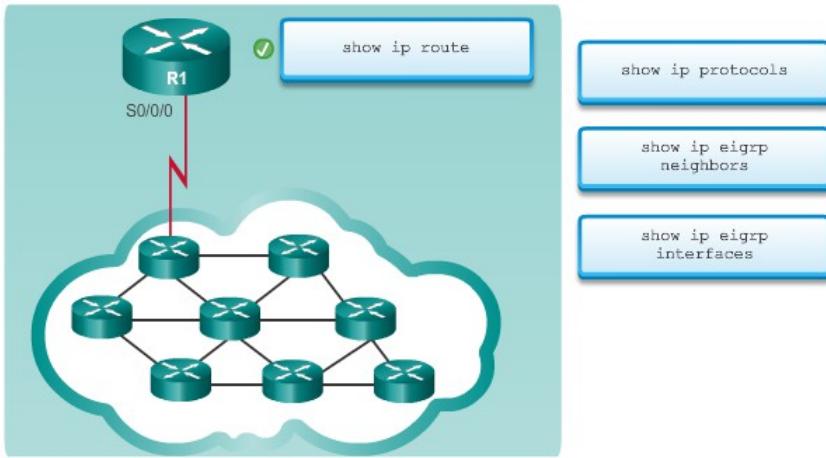


Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.1.3 Actividad:

Identificar el comando para la resolución de problemas

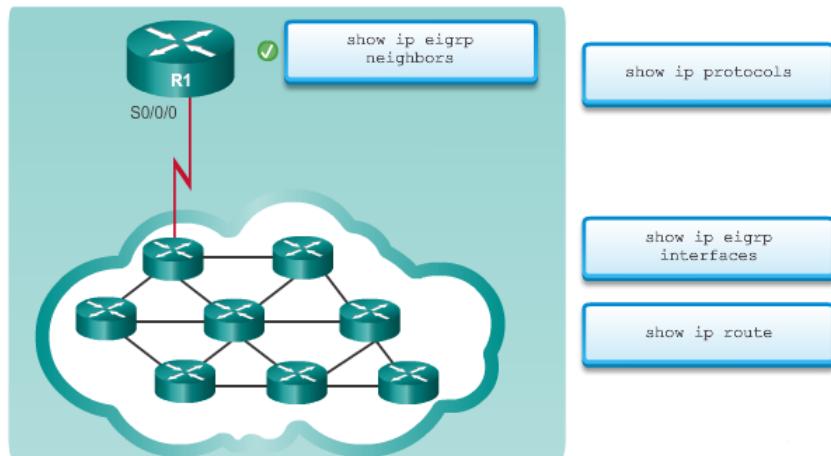
**Actividad: Identificar el comando para la resolución de problemas (situación 1)**

No puede llegar a la red 172.16.0.0 desde el router 1 y debe verificar que dicho router tenga una ruta EIGRP a esa red. Arrastre el comando correspondiente hasta el campo junto al R1. Haga clic en el botón 2 para continuar.

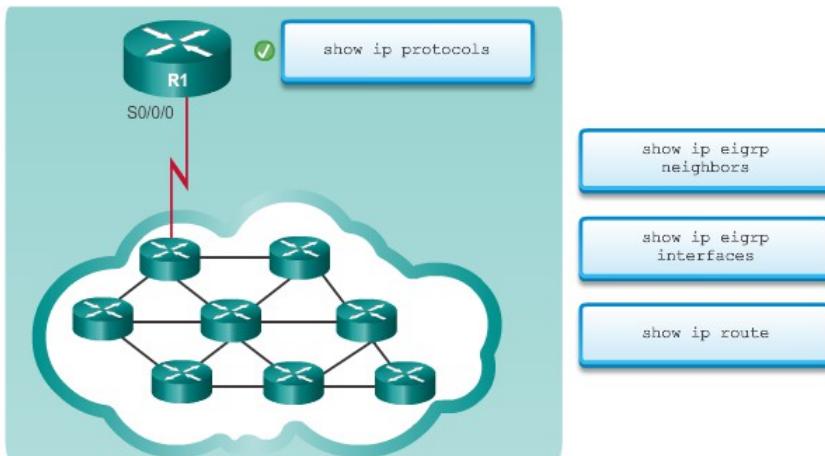


**Actividad: Identificar el comando para la resolución de problemas (situación 2)**

El R1 no puede hacer ping a través del enlace serial al router conectado directamente. Tiene que verificar que el router 1 (R1) esté conectado a otro router EIGRP, y la configuración de IP y del puerto de ese router. Arrastre el comando correspondiente hasta el campo junto al R1. Haga clic en el botón 3 para continuar.



**Actividad: Identificar el comando para la resolución de problemas (situación 3)**  
Faltan algunas redes conectadas directamente en las tablas de routing de los otros routers. Tiene que verificar que EIGRP anuncie todas sus redes conectadas directamente. Arrastre el comando correspondiente hasta el campo junto al R1.



## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.2.1

### Conecividad de capa 3

Un requisito para que se forme una adyacencia de vecinos entre dos routers conectados directamente es la conectividad de capa 3. Mediante el análisis del resultado del comando **show ip interface brief**, un administrador de red puede verificar que el estado de las interfaces de conexión y del protocolo de dichas interfaces sea activo. Un ping de un router a otro router conectado directamente debería confirmar la conectividad IPv4 entre los dispositivos. En la ilustración, se muestra el resultado del comando **show ip interface brief** para el R1. El R1 muestra conectividad al R2, y los pings se realizan correctamente.

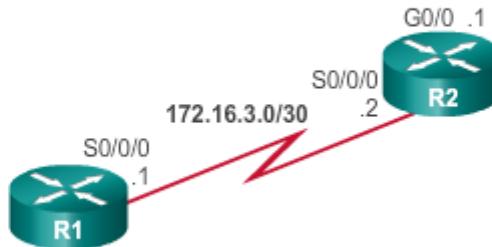
Si el ping no es correcto, revise el cableado y verifique que las interfaces de los dispositivos conectados estén en una subred común. Un mensaje de registro **not on common subnet**, que informa que los vecinos EIGRP no están en una subred común, indica que hay una dirección IPv4 incorrecta en una de las dos interfaces EIGRP vecinas.

### **EIGRP para IPv6**

También se aplican comandos y criterios de resolución de problemas similares en EIGRP para IPv6.

El comando equivalente que se usa con EIGRP para IPv6 es **show ipv6 interface brief**.

## Conecividad del R1 al R2



```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0          172.16.1.1    YES manual up
Serial0/0/0                 172.16.3.1    YES manual up
Serial0/0/1                 192.168.10.5  YES manual up
R1# ping 172.16.3.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
28/28/28 ms
R1#
```

## apítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.2.2 Parámetros

### EIGRP

En la resolución de problemas en una red EIGRP, una de las primeras cosas que hay que verificar es que todos los routers que participan en la red EIGRP estén configurados con el mismo número de sistema autónomo. El comando **router eigrp *número-as*** inicia el proceso EIGRP, y lo sigue el número de sistema autónomo. El valor del argumento **número-as** debe ser el mismo en todos los routers que están en el mismo dominio de routing EIGRP.

En la figura 1, se muestra que todos los routers deberían participar en el número de sistema autónomo 1. En la figura 2, con el comando **show ip protocols** se verifica que el R1, el R2 y el R3 usan el mismo número de sistema autónomo.

### **EIGRP para IPv6**

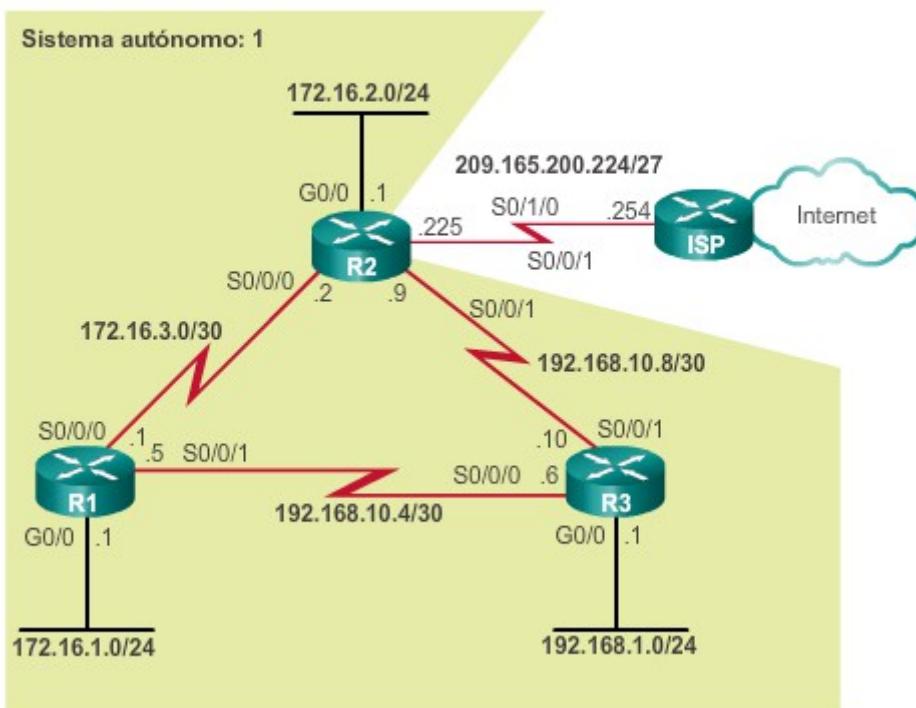
También se aplican comandos y criterios de resolución de problemas similares en EIGRP para IPv6.

Los siguientes son los comandos equivalentes que se utilizan con EIGRP para IPv6:

- Router(config)# **ipv6 router eigrp *número-as***
- Router# **show ipv6 protocols**

**Nota:** en la parte superior del resultado, el mensaje “IP Routing is NSF aware” (el routing IP reconoce NSF) se refiere a reenvío continuo (NSF). Esta capacidad permite que los peers EIGRP de un router defectuoso retengan la información de routing que este anunció y sigan usando esa información hasta que el router defectuoso vuelva a funcionar con normalidad y pueda intercambiar información de routing. Para obtener más información, consulte:[http://www.cisco.com/en/US/docs/ios-xml/ios/iproute\\_eigrp/configuration/15-mt/eigrp-nsf-awa.html](http://www.cisco.com/en/US/docs/ios-xml/ios/iproute_eigrp/configuration/15-mt/eigrp-nsf-awa.html)

### Topología EIGRP para IPv4



### Configuración inicial de la interfaz IPv4 y de EIGRP para IPv4

```
R1# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "eigrp 1"
```

```
<resultado omitido>
```

```
R2# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "eigrp 1"
```

```
<resultado omitido>
```

```
R3# show ip protocols
```

```
*** IP Routing is NSF aware ***
```

```
Routing Protocol is "eigrp 1"
```

```
<resultado omitido>
```

Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.2.3 Interfaces

EIGRP

Además de verificar el número de sistema autónomo, es necesario verificar que todas las interfaces participen en la red EIGRP. El comando **network** que se configura en el proceso de routing EIGRP indica qué interfaces del router participan en EIGRP. Este comando se aplica a la dirección de red con clase de la interfaz o a una subred, cuando se incluye la máscara wildcard.

En la figura 1, el comando **show ip eigrp interfaces** muestra qué interfaces están habilitadas para EIGRP en el R1. Si las interfaces conectadas no están habilitadas para EIGRP, los vecinos no forman una adyacencia.

En la figura 2, la sección “Routing for Networks” (Routing de redes) del comando **show ip protocols** indica qué redes se configuraron. Todas las interfaces en esas redes participan en EIGRP.

Si la red no está presente en esta sección, use **show running-config** para asegurarse de que se haya configurado el comando **network** correcto.

En la figura 3, el resultado del comando **show running-config** confirma que las interfaces con esas direcciones, o una subred de esas direcciones, están habilitadas para EIGRP.

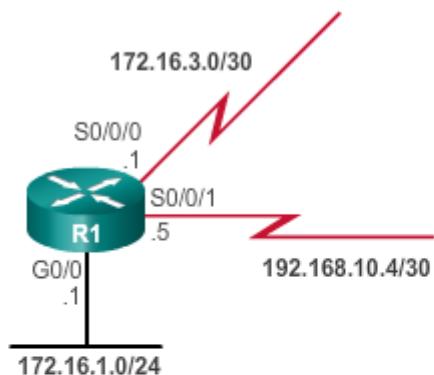
### EIGRP para IPv6

También se aplican comandos y criterios de resolución de problemas similares en EIGRP para IPv6.

Los siguientes son los comandos equivalentes que se utilizan con EIGRP para IPv6:

- Router# **show ipv6 protocols**
- Router# **show ipv6 eigrp interfaces**

### Interfaces EIGRP para IPv4



```
R1# show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(1)
      Xmit Queue   PeerQ      Mean   Facing Time
Interface Peers Un/Reliable Un/Reliable SRTT    Un/Reliable
Gi0/1      0       0/0       0/0       0       0/0
Se0/0/0    1       0/0       0/0      1295    0/23
Se0/0/1    1       0/0       0/0      1044    0/15
R1#
```

### Procesos del protocolo de routing del R1

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
<resultado omitido>

Routing for Networks:
  172.16.0.0
  192.168.10.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    192.168.10.6      90          00:42:31
    172.16.3.2        90          00:42:31
  Distance: internal 90 external 170
R1#
```

## Instrucciones network IPv4 EIGRP del R1

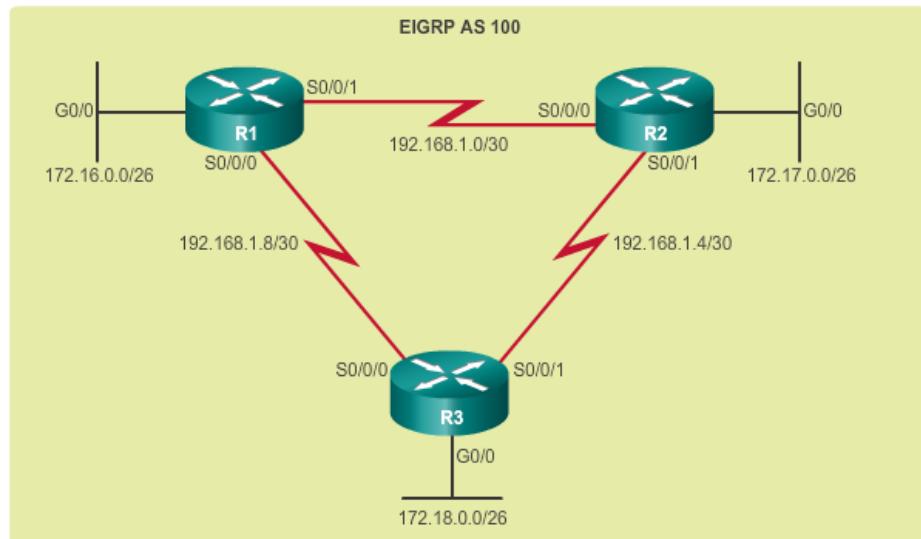
```
R1# show running-config | section eigrp 1
router eigrp 1
network 172.16.0.0
network 192.168.10.0
passive-interface GigabitEthernet0/0
eigrp router-id 1.1.1.1
R1#
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.2.4 Actividad:

#### Resolver problemas de vecinos EIGRP

##### Topología

Use este diagrama de topología como referencia para las situaciones. Haga clic en el botón 2 para continuar.



##### Actividad: resolver problemas de vecinos EIGRP (situación 1)

EIGRP tiene un problema de adyacencia de vecino y no puede obtener actualizaciones de la ruta del router 3 (R3). Utilice el diagrama de topología y el resultado del comando para determinar la causa más probable de este problema. Arrastre el motivo más probable de este problema de EIGRP hasta el campo junto al router 1 (R1). Haga clic en el botón 3 para continuar.

Dirección IP faltante

R1# sh ip interface brief
Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0 172.16.0.1 YES manual up up
Serial0/0/0 unassigned YES manual up up
Serial0/0/1 192.168.1.1 YES manual up up

Dirección IP incorrecta  
 Cable desconectado  
 EIGRP no configurado

**Actividad: resolver problemas de vecinos EIGRP (situación 2)**

EIGRP tiene un problema de adyacencia de vecino y no puede obtener actualizaciones de la ruta del router 1 (R1) y el router 3 (R3). Utilice el diagrama de topología y el resultado del comando para determinar la causa más probable de este problema. Arrastre el motivo más probable de este problema de EIGRP hasta el campo junto al router 2 (R2).

```
R2# sh ip protocols
Routing Protocol is "eigrp 101"
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 101
    Automatic network summarization is in effect
    Automatic address summarization:
      192.168.1.0/24 for FastEthernet0/0
        Summarizing with metric 2169856
      172.17.0.0/16 for Serial0/0/0, Serial0/0/1
        Summarizing with metric 28160
    Maximum path: 4
    Routing for Networks:
      172.17.0.0
      192.168.1.0
```

#### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.1 Interfaz pasiva

##### pasiva

Una razón por la que es posible que en las tablas de rutas no se muestren las rutas correctas es el comando **passive-interface**. Con EIGRP en ejecución en una red, el comando **passive-interface** detiene las actualizaciones de routing salientes y entrantes. Por esa razón, los routers no se convierten en vecinos.

Para verificar si alguna interfaz en un router está configurada como pasiva, use el comando **show ip protocols** en el modo EXEC privilegiado. En la figura 1, se muestra que la interfaz GigabitEthernet 0/0 del R2 está configurada como interfaz pasiva, porque no hay vecinos en ese enlace.

Además de estar configurada en interfaces que no tienen vecinos, una interfaz pasiva puede habilitarse en interfaces por motivos de seguridad. En la figura 2, observe que el sombreado del dominio de routing EIGRP es diferente de las topologías anteriores. La red 209.165.200.224/27 ahora está incluida en las actualizaciones de EIGRP del R2. Sin embargo, por motivos de seguridad, el administrador de red no desea que el R2 forme una adyacencia de vecino EIGRP con el router ISP.

En la figura 3, se muestra la incorporación del comando **network 209.165.200.224/27** en el R2. El R2 ahora anuncia esta red a los otros routers en el dominio de routing EIGRP.

El comando **passive-interface** del modo de configuración del router está configurado en Serial 0/1/0 para evitar que se envíen actualizaciones de EIGRP del R2 al router ISP. El comando **show ip eigrp neighbors** en el R2 verifica que ese router no haya establecido una adyacencia de vecino con ISP.

En la figura 4, se muestra que el R1 tiene una ruta EIGRP a la red 209.165.200.224/27 en su tabla de routing IPv4 (el R3 también tiene una ruta EIGRP a esa red en la tabla de routing IPv4). Sin embargo, el R2 no tiene una adyacencia de vecino con el router ISP.

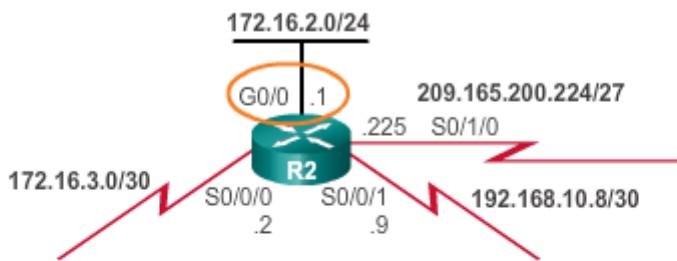
## EIGRP para IPv6

También se aplican comandos y criterios de resolución de problemas similares en EIGRP para IPv6.

Los siguientes son los comandos equivalentes que se utilizan con EIGRP para IPv6:

- Router# **show ipv6 protocols**
- Router(config-rtr)# **passive-interface tipo número**

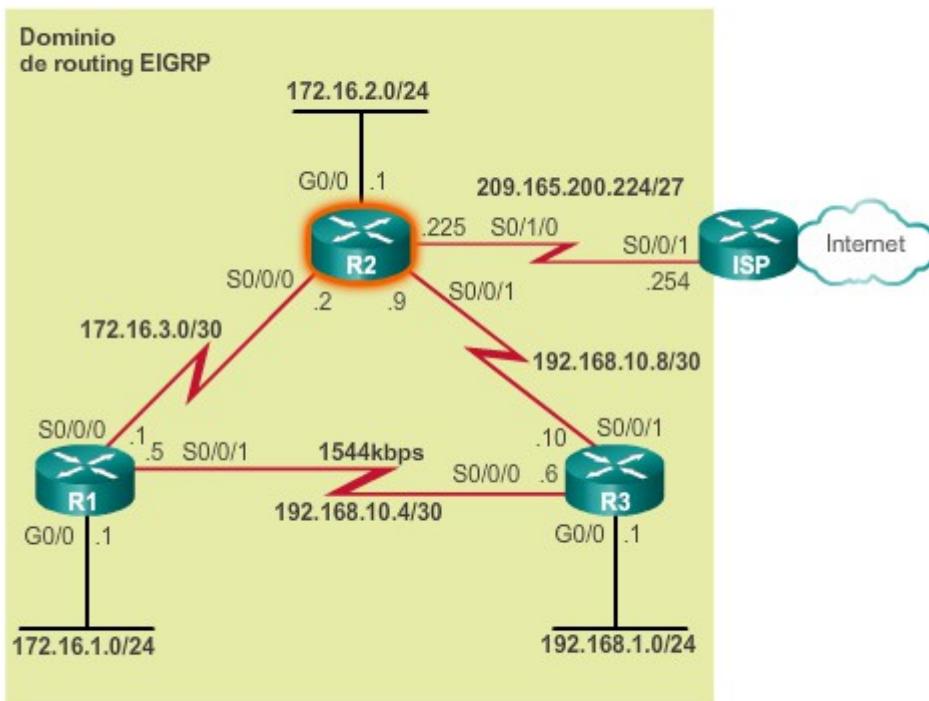
### Interfaz pasiva GigabitEthernet 0/0 del R2



```

R2# show ip protocols
*** IP Routing is NSF aware ***
Routing Protocol is "eigrp 1"
<resultado omitido>
Routing for Networks:
  172.16.0.0
  192.168.10.8/30
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway          Distance      Last Update
  192.168.10.10    90           00:08:59
  172.16.3.1       90           00:08:59
  Distance: internal 90 external 170
R2#
    
```

### Topología EIGRP para IPv4



## Configuración de una red al ISP como interfaz pasiva

```
R2(config)# router eigrp 1
R2(config-router)# network 209.165.200.0
R2(config-router)# passive-interface serial 0/1/0
R2(config-router)# end
R2# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
  H   Address       Interface   Hold Uptime    SRTT    RTO    Q    Seq
                (sec)          (ms)          Cnt Num
  1   172.16.3.1    Se0/0/0     175 01:09:18    80  2340  0  16
  0   192.168.10.10 Se0/0/1     11  01:09:33  1037 5000  0  17
R2#
```

## Verificación de una red propagada como ruta EIGRP

```
R1# show ip route | include 209.165.200.224
D 209.165.200.224 [90/3651840] via 192.168.10.6,
00:06:02, Serial0/0/1
R1#
```

### Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.2

#### Instrucción network faltante

En la figura 1, se muestra que la interfaz GigabitEthernet 0/1 del R1 ahora está configurada con la dirección 10.10.10.1/24 y está activa.

El R1 y el R3 todavía tienen adyacencias de vecinos, pero una prueba de ping del router R3 a la interfaz G0/1 del R1 de 10.10.10.1 es incorrecta. En la figura 2, se muestra una prueba fallida de conectividad del R3 a la red de destino 10.10.10.0/24.

En la figura 3, con el comando **show ip protocols** en el router R1 se muestra que la red 10.10.10.0/24 no se anuncia a los vecinos EIGRP.

Como se muestra en la figura 4, el proceso EIGRP del R1 está configurado para incluir el anuncio de la red 10.10.10.0/24.

En la figura 5, se muestra que ahora hay una ruta en la tabla de routing del R3 para la red 10.10.10.0/24, y la posibilidad de conexión se verifica mediante un ping a la interfaz GigabitEthernet 0/1 del R1.

#### **EIGRP para IPv6**

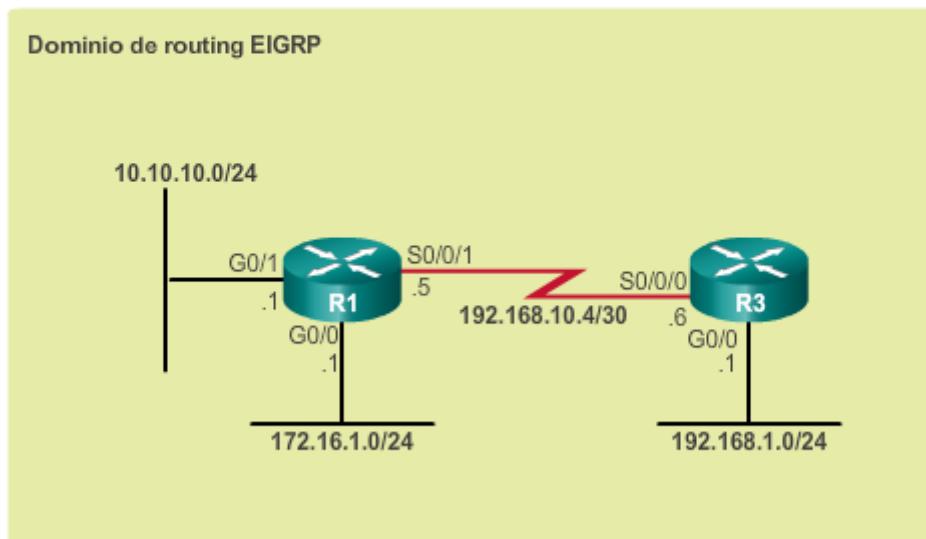
También se aplican comandos y criterios de resolución de problemas similares en EIGRP para IPv6.

Los siguientes son los comandos equivalentes que se utilizan con EIGRP para IPv6:

- Router# **show ipv6 protocols**
- Router# **show ipv6 route**
- Router(config-rtr)# **networkprefijo-ipv6/longitud-prefijo**

**Nota:** es posible que el filtrado que el router hace de actualizaciones de routing entrantes y salientes produzca otra forma de ruta faltante. Las ACL proporcionan filtrado para diferentes protocolos y es posible que afecten el intercambio de los mensajes de protocolo de routing que ocasionan que las rutas no aparezcan en la tabla de routing. El comando **show ip protocols** muestra si hay ACL aplicadas a EIGRP.

#### Topología EIGRP para IPv4



No se puede llegar a 10.10.10.0/24 desde el R3

```
R3# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2
seconds:
.....
Success rate is 0 percent (0/5)
R3#
```

## Actualizaciones de 10.10.100/24 en el R1

```
R1# show ip protocols | begin Routing for Networks
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Passive Interface(s):
    GigabitEthernet0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    192.168.10.6      90          01:34:19
    172.16.3.2       90          01:34:19
  Distance: internal 90 external 170

R1#
```

## Configuración de una red

```
R1(config)# router eigrp 1
R1(config-router)# network 10.0.0.0
```

## Verificación de una red propagada como ruta EIGRP

```
R3# show ip route | include 10.10.10.0
D        10.10.10.0 [90/2172416] via 192.168.10.5, 00:04:14,
      Serial0/0/0
R3#
R3# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
24/27/28 ms
R3#
```

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.3

### Sumarización automática

Otra cuestión que es posible que cree problemas para el administrador de red es la sumarización automática de EIGRP.

En la figura 1, se muestra una topología de red diferente de la que se usó en este capítulo. No hay ninguna conexión entre el R1 y el R3. La LAN del R1 tiene la dirección de red 10.10.10.0/24, y la LAN del R3 es 10.20.20.0/24. Las conexiones seriales entre ambos routers y el R2 tienen el mismo ancho de banda: 1024 kb/s.

El R1 y el R3 tienen las interfaces seriales y las LAN habilitadas para EIGRP, como se muestra en la figura 2. Ambos routers realizan summarización automática de EIGRP.

EIGRP para IPv4 puede configurarse para que resuma automáticamente las rutas en límites con clase. Si hay redes no contiguas, la summarización automática provoca un routing incongruente.

En la figura 3, la tabla de routing del R2 muestra que no recibe rutas individuales para las subredes 10.10.10.0/24 y 10.20.20.0/24. El R1 y el R3 resumen automáticamente esas subredes al límite con clase 10.0.0.0/8 cuando envían paquetes de actualización de EIGRP al R2. El resultado es que el R2 tiene dos rutas de igual costo a 10.0.0.0/8 en la tabla de routing, lo que puede ocasionar routing impreciso y pérdida de paquetes. Según se use balanceo de carga por paquete, por destino o CEF, es posible que los paquetes se reenvíen por la interfaz correcta o no.

En la figura 4, con el comando **show ip protocols** se verifica que se lleva a cabo summarización automática en el R1 y el R3. Observe que ambos routers resumen la red 10.0.0.0/8 con la misma métrica.

El comando **auto-summary** está deshabilitado de manera predeterminada en las versiones 15 y en las versiones más nuevas de 12.2(33) del software IOS de Cisco. El software más antiguo tiene habilitada la summarización automática de manera predeterminada. Para deshabilitar la summarización automática, introduzca el comando **no auto-summary** en el modo de configuración del **router EIGRP**.

Para corregir este problema, el R1 y el R3 tienen deshabilitada la summarización automática:

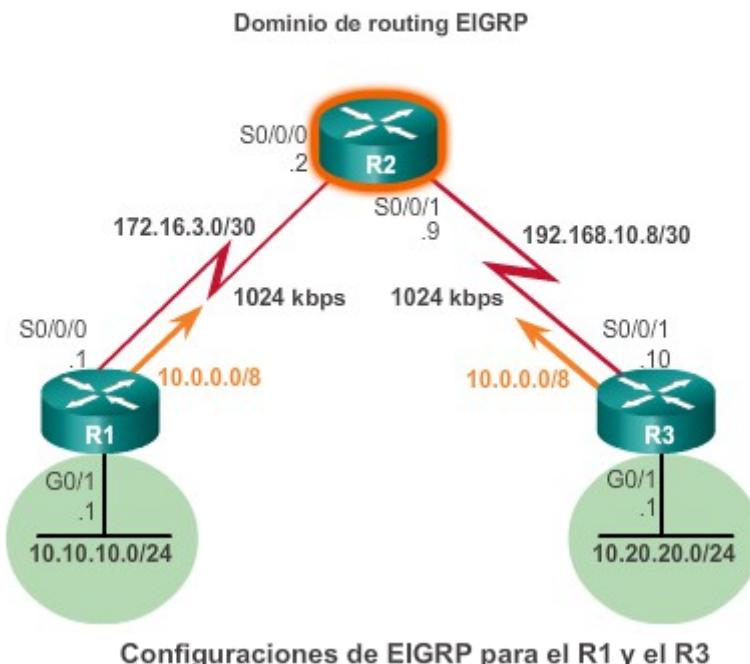
```
R1(config)# router eigrp 1  
R1(config-router)# no auto-summary  
  
R3(config)# router eigrp 1  
R3(config-router)# no auto-summary
```

Después de deshabilitar la summarización automática en el R1 y el R3, la tabla de routing del R2 indica que recibe las subredes individuales 10.10.10.0/24 y 10.20.20.0/24 del R1 y el R3, respectivamente, como se muestra en la figura 5. Se restauró el routing preciso y la conectividad en ambas subredes.

## EIGRP para IPv6

En IPv6 no existen las redes con clase, por lo tanto, EIGRP para IPv6 no admite la summarización automática. Toda la summarización debe realizarse mediante rutas resumidas manuales EIGRP.

## Topología EIGRP para IPv4



Configuraciones de EIGRP para el R1 y el R3

```
R1(config)# router eigrp 1
R1(config-router)# network 10.0.0.0
R1(config-router)# network 172.16.0.0
R1(config-router)# auto-summary
```

```
R3(config)# router eigrp 1
R3(config-router)# network 10.0.0.0
R3(config-router)# network 192.168.10.0
R3(config-router)# auto-summary
```

Reenvío incongruente desde el R2

```
R2# show ip route
<resultado omitido>

  10.0.0.0/8 is subnetted, 1 subnets
D      10.0.0.0 [90/3014400] via 192.168.10.10, 00:02:06,
          Serial0/0/1
          [90/3014400] via 172.16.3.1, 00:02:06,
          Serial0/0/0
```

### Verificación del estado de la summarización automática

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"

    Automatic Summarization: enabled
    10.0.0.0/8 for Se0/0/0
        Summarizing 1 component with metric 28160

<resultado omitido>
```

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"

    Automatic Summarization: enabled
    10.0.0.0/8 for Se0/0/1
        Summarizing 1 component with metric 28160

<resultado omitido>
```

Se puede llegar a todas las redes desde el R2

```
R2# show ip route
<resultado omitido>

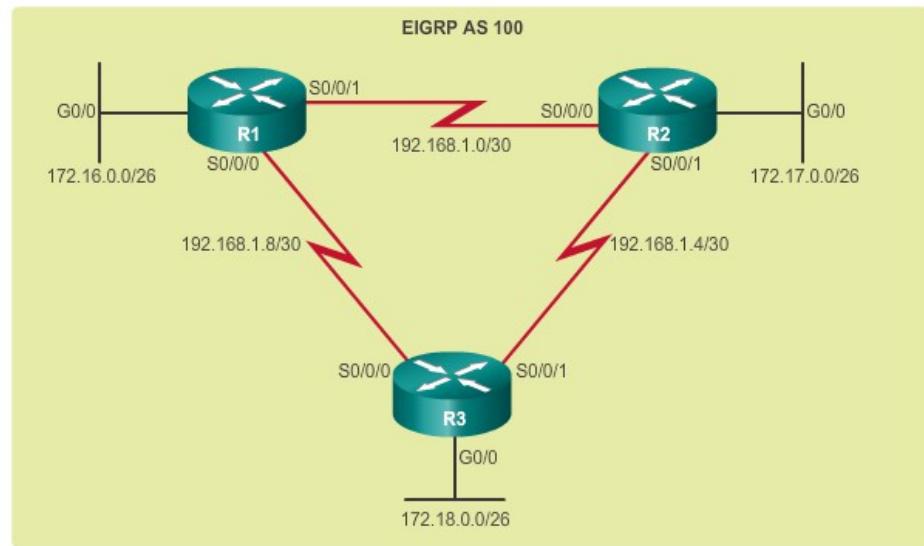
  10.0.0.0/24 is subnetted, 2 subnets
D  10.10.10.0 [90/3014400] via 172.16.3.1, 00:00:27,
    Serial0/0/0
D  10.20.20.0 [90/3014400] via 192.168.10.10, 00:00:11,
    Serial0/0/1
```

Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.4 Actividad:

Resolver problemas de tabla de routing EIGRP

## Topología

Use este diagrama de topología como referencia para las situaciones 1 a 3. Haga clic en el botón 2 para continuar.



### Actividad: resolver problemas de la tabla de routing EIGRP (situación 1)

El R1 no puede llegar a la red 172.17.0.0. Utilice el diagrama de topología y la tabla de routing para determinar la causa más probable de este problema. Arrastre el motivo más probable de este problema de la tabla de routing EIGRP hasta el campo junto al Router1 (R1). Haga clic en el botón 3 para continuar.

Router1 (R1) no alcanza la red 172.17.0.0.

Causas probables:

- El R3 no anuncia 172.17.0.0.
- La ruta estática 172.17.0.0 es incorrecta.
- La interfaz loopback 172.17.0.1 es incorrecta.

```
R1# sh ip route
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D   172.16.0.0/16 is a summary, 01:26:41, Null0
C     172.16.0.0/26 is directly connected, GigabitEthernet0/0
      172.18.0.0/26 is subnetted, 1 subnets
D       172.18.0.0 [90/2172416] via 192.168.1.10, 01:26:32, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
D         192.168.1.0/24 is a summary, 01:26:41, Null0
C           192.168.1.0/30 is directly connected, Serial0/0/1
D             192.168.1.4/30 [90/2681856] via 192.168.1.10, 01:26:32, Serial0/0/0
[90/2681856] via 192.168.1.2, 00:01:03, Serial0/0/1
C               192.168.1.8/30 is directly connected, Serial0/0/0
```

### Actividad: resolver problemas de la tabla de routing EIGRP (situación 2)

El R1 no puede llegar a la red 172.17.0.0. Utilice el diagrama de topología y la tabla de routing para determinar la causa más probable de este problema. Arrastre el motivo más probable de este problema de la tabla de routing EIGRP hasta el campo junto al Router1 (R1). Haga clic en el botón 4 para continuar.

Router1 (R1) no alcanza la red 172.17.0.0.

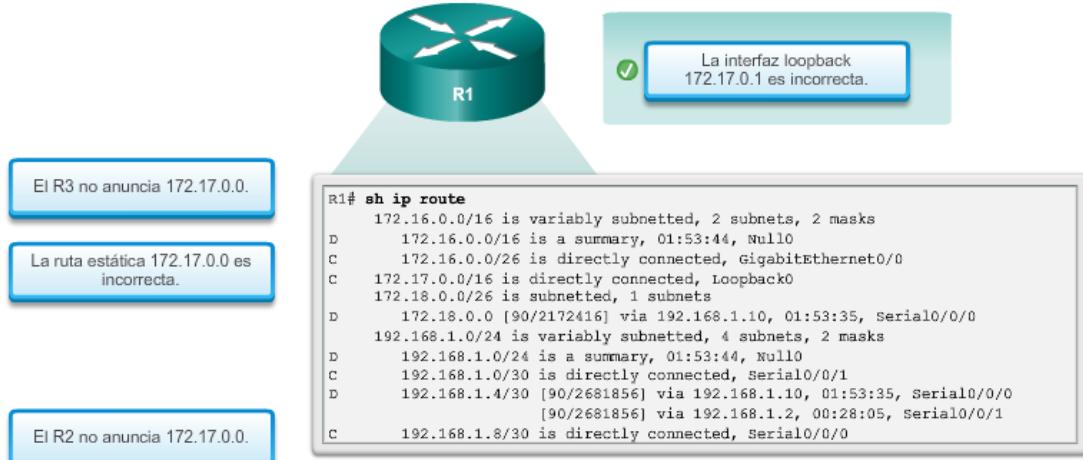
Causas probables:

- El R3 no anuncia 172.17.0.0.
- La ruta estática 172.17.0.0 es incorrecta.
- La interfaz loopback 172.17.0.1 es incorrecta.
- El R2 no anuncia 172.17.0.0.

```
R1# sh ip route
 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D   172.16.0.0/16 is a summary, 01:44:06, Null0
C     172.16.0.0/26 is directly connected, GigabitEthernet0/0
S       172.17.0.0/16 [1/0] via 172.16.0.2
      172.18.0.0/26 is subnetted, 1 subnets
D         172.18.0.0 [90/2172416] via 192.168.1.10, 01:43:57, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
D           192.168.1.0/24 is a summary, 01:44:06, Null0
C             192.168.1.0/30 is directly connected, Serial0/0/1
D               192.168.1.4/30 [90/2681856] via 192.168.1.10, 01:43:57, Serial0/0/0
[90/2681856] via 192.168.1.2, 00:18:27, Serial0/0/1
C                 192.168.1.8/30 is directly connected, Serial0/0/0
```

**Actividad: resolver problemas de la tabla de routing EIGRP (situación 3)**

El R1 no puede llegar a la red 172.17.0.0. Utilice el diagrama de topología y la tabla de routing para determinar la causa más probable de este problema. Arrastre el motivo más probable de este problema de la tabla de routing EIGRP hasta el campo junto al Router1 (R1).



## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.5 Packet

### Tracer: Resolución de problemas de EIGRP para IPv4

#### **Información básica/situación**

En esta actividad, resolverá problemas de vecinos EIGRP. Utilice los comandos **show** para identificar errores en la configuración de red. A continuación, registrará los errores que detecte e implementará una solución apropiada. Por último, verificará que se haya restaurado la plena conectividad de extremo a extremo.

[Packet Tracer: Resolución de problemas de EIGRP para IPv4 \(instrucciones\)](#)

[Packet Tracer: Resolución de problemas de EIGRP para IPv4 \(PKA\)](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.6 Práctica

### de laboratorio: Resolución de problemas de EIGRP básico para IPv4 e IPv6

#### **En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de conectividad de capa 3
- Parte 3: Resolver problemas de EIGRP para IPv4
- Parte 4: Resolver problemas de EIGRP para IPv6

[Práctica de laboratorio: Resolución de problemas de EIGRP básico para IPv4 e IPv6](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.2.3.7 Práctica

### de laboratorio: Resolución de problemas de EIGRP avanzado

**En esta práctica de laboratorio se cumplirán los siguientes objetivos:**

- Parte 1: armar la red y cargar las configuraciones de los dispositivos
- Parte 2: Resolver problemas de EIGRP

### [Práctica de laboratorio: Resolución de problemas de EIGRP avanzado](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.3.1.1 Actividad

### de clase: Ajuste de EIGRP

**Ajuste de EIGRP**

El objetivo de esta actividad es revisar los conceptos de ajuste del protocolo de routing EIGRP.

Trabajará con un compañero para diseñar una topología de EIGRP. Esta topología es la base para dos partes de la actividad. En la primera, se usan los parámetros predeterminados para todas las configuraciones, y en la segunda se incorporan, al menos, tres de las siguientes opciones de ajuste de EIGRP:

- Ruta resumida manual
- Rutas predeterminadas
- Propagación de rutas predeterminadas
- Configuración del temporizador de intervalo de saludo

Consulte las prácticas de laboratorio, las actividades de Packet Tracer y las actividades interactivas para obtener ayuda a medida que avanza en esta actividad de creación de modelos.

Las direcciones se indican en el archivo PDF de esta actividad. Comparta el trabajo completo con otro grupo. Quizá desee guardar una copia de esta actividad en una cartera.

### [Actividad de clase: Ajuste de EIGRP](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.3.1.2 Packet

### Tracer: desafío de integración de habilidades

## Información básica/situación

En esta actividad, debe implementar EIGRP para IPv4 e IPv6 en dos redes diferentes. Parte de su tarea consiste en habilitar EIGRP, asignar las ID de los routers, cambiar los temporizadores de saludo, configurar las rutas resumidas EIGRP y limitar los anuncios de EIGRP.

[Packet Tracer: Reto de habilidades de integración \(instrucciones\)](#)

[Packet Tracer: desafío de integración de habilidades \(PKA\)](#)

## Capítulo 8: Configuraciones avanzadas y resolución de problemas de EIGRP 8.3.1.3 Resumen

EIGRP es uno de los protocolos de routing comúnmente utilizados en redes empresariales grandes. La modificación de características de EIGRP y la resolución de problemas son algunas de las habilidades más indispensables para un ingeniero de red dedicado a la implementación y el mantenimiento de grandes redes empresariales enrutadas que usan EIGRP.

La summarización disminuye la cantidad de entradas en las actualizaciones de enrutamiento y reduce la cantidad de entradas en las tablas de enrutamiento locales. Reduce, además, el uso del ancho de banda para las actualizaciones de enrutamiento y acelera las búsquedas en las tablas de enrutamiento. La summarización automática de EIGRP para IPv4 está deshabilitada de manera predeterminada a partir de las versiones 15.0(1)M y 12.2(33) del IOS de Cisco. Antes de esto, la summarización automática estaba habilitada de manera predeterminada. Para habilitar la summarización automática de EIGRP, use el comando **auto-summary** en el modo de configuración del router. Utilice el comando **show ip protocols** para verificar el estado de la summarización automática. Examine la tabla de routing para verificar que la summarización automática funcione.

EIGRP incluye automáticamente rutas resumidas a Null0 para evitar bucles de routing a destinos que se incluyen en el resumen, pero que no existen realmente en la tabla de routing. La interfaz Null0 es una interfaz virtual del IOS que constituye una ruta hacia ninguna parte, comúnmente conocida como “el limbo electrónico”. Los paquetes que vinculan una ruta con una interfaz de salida Null0 se descartan.

Para establecer la summarización manual EIGRP en una interfaz EIGRP específica, utilice el siguiente comando del modo de configuración de interfaz:

```
Router(config-if)# ip summary-address eigrp as-number network-address subnet-mask
```

Para configurar la summarización manual de EIGRP para IPv6 en una interfaz EIGRP específica, utilice el siguiente comando del modo de configuración de interfaz:

```
Router(config-if)# ipv6 summary-address eigrp as-number prefix/prefix-length
```

Un método para propagar una ruta predeterminada dentro del dominio de routing EIGRP es mediante el comando **redistribute static**. Este comando le indica a EIGRP que incluya esta ruta estática en las actualizaciones de EIGRP a otros routers. El comando **show ip protocols** verifica que se redistribuyan las rutas estáticas dentro del dominio de routing EIGRP.

Use el comando **ip bandwidth-percent eigrp *número-as* porcentaje** del modo de configuración de interfaz para configurar el porcentaje del ancho de banda que EIGRP puede utilizar en una interfaz.

Para configurar el porcentaje del ancho de banda que puede utilizar EIGRP para IPv6 en una interfaz, utilice el comando **ipv6 bandwidth-percent eigrp** en el modo de configuración de interfaz. Para restaurar el valor predeterminado, utilice la versión **no** de este comando.

En EIGRP, los intervalos de saludo y los tiempos de espera se pueden configurar por interfaz y no tienen que coincidir con otros routers EIGRP para establecer o mantener adyacencias.

En el caso de IP en EIGRP, el software IOS de Cisco aplica de manera predeterminada el balanceo de carga con hasta cuatro rutas de igual costo. Con el comando **maximum-paths** del modo de configuración del router, pueden mantenerse hasta 32 rutas de igual costo en la tabla de routing.

EIGRP admite la autenticación de protocolos de routing mediante MD5. Los algoritmos y la configuración para autenticar mensajes EIGRP para IPv4 son los mismos que los correspondientes a EIGRP para IPv6. La única diferencia es que en los comandos del modo de configuración de interfaz se usa **ip** en lugar de **ipv6**.

```
Router(config-if)# ip authentication mode eigrp número-as md5
```

```
Router(config-if)# ipv6 authentication key-chain eigrp número-as nombre-de-llavero
```

Para verificar que se hayan formado las adyacencias EIGRP correctas después de configurarlas para la autenticación, utilice el comando **show ip eigrp neighbors** en cada router.

El comando **show ip route** verifica que el router haya descubierto rutas EIGRP. El comando **show ip protocols** se usa para verificar que EIGRP muestre los valores configurados actualmente.

## Sumarización automática en el límite de una red con clase



Redes con clase	
Clase A: de 0.0.0.0 a 127.255.255.255	Máscara predeterminada: 255.0.0.0 o /8
<b>Clase B: de 128.0.0.0 a 191.255.255.255</b>	<b>Máscara predeterminada: 255.255.0.0 o /16</b>
Clase C: de 192.0.0.0 a 223.255.255.255	Máscara predeterminada: 255.255.255.0 o /24

### Capítulo 9: Imágenes y licencias del IOS 9.0.1.1 Introducción

IOS de Cisco (initialmente sistema operativo Internetwork) es un software que se utiliza en la mayoría de los routers y switches Cisco. IOS es un paquete de routing, switching, seguridad y otras tecnologías de internetworking integradas en un único sistema operativo multitarea.

La cartera del IOS de Cisco admite una amplia gama de tecnologías y características. Los clientes eligen un IOS basado en un grupo de protocolos y características admitidas por una imagen determinada. Comprender la cartera de conjuntos de características del IOS de Cisco es útil al seleccionar el IOS adecuado para que satisfaga las necesidades de una organización.

Cisco realizó cambios significativos en los paquetes y las licencias del software IOS al llevar a cabo la transición de IOS 12.4 a 15.0. En este capítulo, se explican las convenciones de nomenclatura y los paquetes del IOS 12.4 y 15. Comenzando por IOS 15, Cisco también implementó un nuevo formato de paquetes y proceso activación de licencias para IOS. En este capítulo, se analiza el proceso de obtención, instalación y administración de licencias del software IOS de Cisco 15.

**Nota:** la versión del IOS que sigue a la 12.4 es la 15.0. No existen las versiones 13 o 14 del software IOS.

**Al finalizar este capítulo, podrá hacer lo siguiente:**

- Explicar las convenciones de nomenclatura de la imagen del IOS implementadas por Cisco.
- Administrar los archivos de imagen de sistema del IOS de Cisco para admitir requisitos de red en redes de pequeña a mediana empresa.
- Explicar el proceso de activación de licencias para el software IOS de Cisco en una red de una pequeña a mediana empresa.
- Configurar un router para instalar una licencia de la imagen del software IOS de Cisco.

[Capítulo 9: Imágenes y licencias del IOS 9.0.1.2 Actividad de clase: Detección del IOS](#)

### **Detección del IOS**

Su lugar de estudios o universidad acaba de recibir una donación de routers y switches Cisco. Usted los transporta desde el departamento de envíos y recepción hasta el laboratorio de redes de Cisco y comienza a clasificarlos en grupos de switches y de routers.

Consulte el PDF correspondiente para obtener las instrucciones sobre cómo continuar con esta actividad de creación de modelos. Guarde el trabajo y comparta con otro grupo o con toda la clase la información que encontró.

[Actividad de clase: Detección del IOS](#)

[Capítulo 9: Imágenes y licencias del IOS 9.1.1.1 Trenes y familias de versiones del software IOS de Cisco](#)

El software IOS de Cisco evolucionó de un sistema operativo de plataforma única para routing a un sistema operativo sofisticado que admite una amplia matriz de características y tecnologías, como VoIP, NetFlow e IPsec. Para cumplir mejor con los requisitos de los distintos segmentos del mercado, el software está organizado en familias de versiones de software y trenes de software.

Una familia de versiones del software consta de varias versiones del software IOS que presentan las siguientes características:

- Comparten una base de código.
- Se aplican a plataformas de hardware relacionadas.
- Se superponen en la cobertura de la compatibilidad (cuando concluye la vida útil de un OS, se introduce y admite otro OS).

Entre los ejemplos de versiones del software IOS de Cisco, dentro de una familia de versiones del software, se encuentran 12.3, 12.4, 15.0 y 15.1.

Junto con cada versión del software, hay nuevas versiones del software creadas para implementar correcciones de errores y nuevas características. En IOS, estas versiones se denominan “trenes”.

Un tren del IOS de Cisco se utiliza para lanzar versiones con una base de código común a un conjunto específico de plataformas y características. Un tren puede contener varias versiones, y cada versión es una instantánea de la base de código del tren en el momento del lanzamiento. Debido a que distintas familias de versiones del software pueden aplicarse a diversas plataformas o segmentos del mercado, varios trenes pueden estar vigentes en cualquier momento.

En este capítulo, se analizan los trenes del IOS 12.4 y del IOS 15.

#### Capítulo 9: Imágenes y licencias del IOS 9.1.1.2 Trenes T y de línea principal del IOS de Cisco

#### 12.4

##### **Trenes 12.4**

En la ilustración, se muestra la migración de la versión del software 12.3 a la 12.4. Dentro de una familia de versiones del software, puede haber uno o dos trenes activos estrechamente relacionados. Por ejemplo, la familia de versiones del software IOS de Cisco 12.4 tiene dos trenes, los trenes 12.4T y los trenes de línea principal 12.4.

El tren del software IOS de Cisco 12.4 se considera el tren de línea principal. El tren de línea principal recibe mayormente correcciones de software (errores) con el objetivo de mejorar la calidad de este. Las versiones del tren de línea principal también se denominan “versiones de Implementación de mantenimiento (MD)”.

Un tren de línea principal siempre está asociado a un tren de tecnología (tren T). Un tren T, como 12.4T, recibe las mismas correcciones de errores de software que el tren de línea principal. El tren T también recibe nuevas características de compatibilidad de hardware y software. Las versiones en el tren 12.4T del software IOS de Cisco se consideran versiones de Implementación temprana (ED).

Puede haber otros trenes, según la familia de la versión del software. Por ejemplo, otro tren disponible es el tren de proveedor de servicios (tren S). Un tren S contiene características específicas diseñadas para cumplir con los requisitos de los proveedores de servicios.

Todos los trenes secundarios del tren de línea principal (T, S, etc.) suelen tener una letra mayúscula que designa el tipo de tren.

Tren de línea principal = 12.4

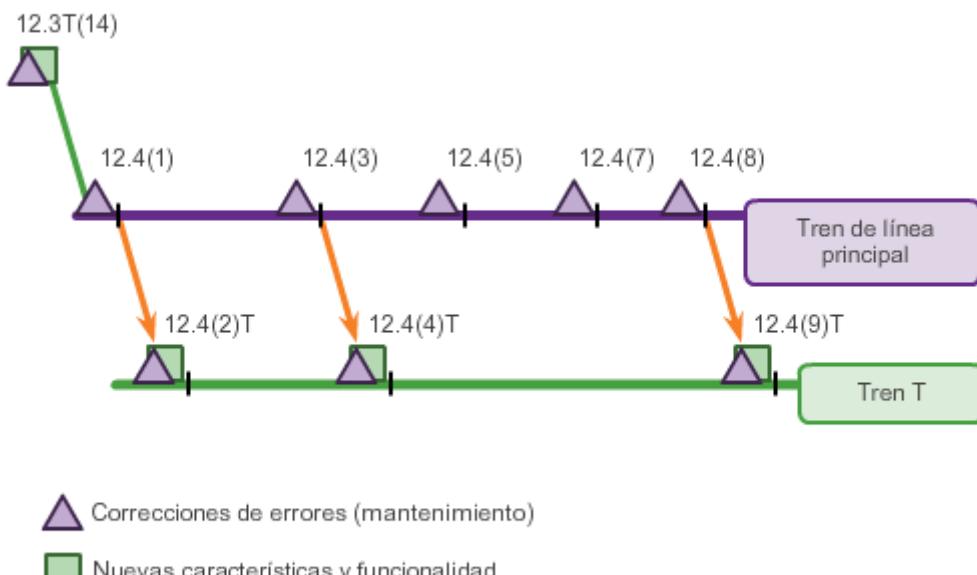
Tren T: 12.4T (12.4 + nuevas características de compatibilidad de hardware y software)

Hasta la familia de la versión 12.4 del software IOS de Cisco inclusive, los trenes de línea principal y los trenes T estaban separados. En otras palabras, desde el tren de línea principal, un tren T se ramificaba y se convertía en una base de código independiente que recibía nuevas características y compatibilidad de hardware. Con el tiempo, un nuevo tren de línea principal

evolucionaba de un tren T establecido, y el ciclo comenzaba nuevamente. El uso de varios trenes se modificó con la versión 15 del software IOS de Cisco.

En la ilustración, se muestran las relaciones entre la versión del tren de línea principal 12.4 y el tren 12.4T del software IOS de Cisco.

#### Familia de la versión 12.4 del software IOS de Cisco



\*Nota: este gráfico se centra en el tren T y en el tren de línea principal. 12.4(6) se utilizó en otro tren.

#### Capítulo 9: Imágenes y licencias del IOS 9.1.1.3 Numeración de trenes T y de línea principal

#### del IOS de Cisco 12.4

La convención de numeración de versiones del IOS de Cisco se utiliza para identificar la versión del software IOS, incluso correcciones de errores y nuevas características de software. En la ilustración, se muestra un ejemplo del esquema de numeración para los trenes de línea principal y para los trenes T:

- El esquema de numeración de versiones del software para un tren de línea principal consta de un número de tren, un identificador de mantenimiento y un identificador de recopilación. Por ejemplo, la versión 12.4(21a) del software IOS de Cisco es un tren de línea principal. La versión para un tren T consta de un número de tren, un identificador de mantenimiento, un identificador de tren y un identificador de recopilación. Por ejemplo, la versión 12.4(20)T1 del software IOS de Cisco pertenece al tren 12.4T del software IOS de Cisco.
- Cada identificador de mantenimiento de la línea principal del software IOS de Cisco 12.4, como 12.4(7), incluye correcciones de mantenimiento y de software adicionales.

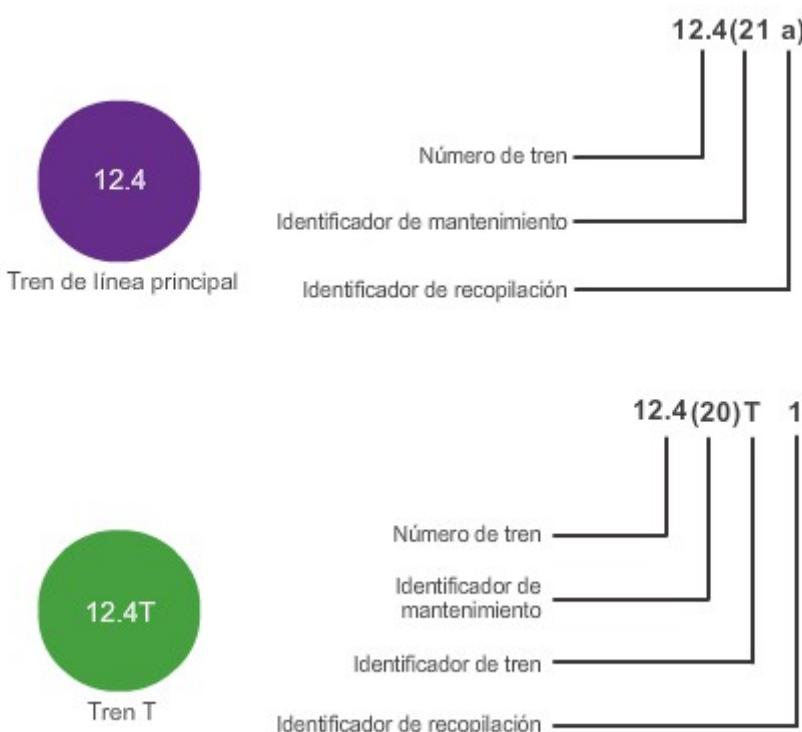
Este cambio se indica con el número entre paréntesis. Cada versión de mantenimiento del software IOS de Cisco 12.4T, como 12.4(20)T, incluye estas mismas correcciones de software, junto con características de software adicionales y compatibilidad de hardware.

- Cisco utiliza recopilaciones de una versión individual para integrar correcciones de problemas importantes. Esto reduce el posible impacto en los clientes que ya implementaron y certificaron una versión individual. Una recopilación típicamente incluye correcciones para una cantidad limitada de defectos de software, conocidos como advertencias. Se indica con una letra minúscula dentro del paréntesis de los trenes de línea principal o con un número final en otros trenes. Por ejemplo, la versión 12.4(21) del software IOS de Cisco recibió algunas correcciones de advertencias, y la recopilación resultante se denominó 12.4(21a). De manera similar, 12.4(15)T8 es la octava recopilación de 12.4(15)T. Cada nueva recopilación aumenta el identificador de recopilación y entrega correcciones de software adicionales en un programa acelerado, antes de la siguiente versión individual planeada. Los criterios para realizar cambios en una recopilación son estrictos.

Se utiliza un conjunto único de números de versión individual para todos los trenes 12.4 del software IOS de Cisco. La versión de mantenimiento 12.4 y la versión 12.4T del software IOS de Cisco utilizan un pool de números de versión individual que se comparten en toda la familia de la versión 12.4 de dicho software. A la versión 12.4(6)T del software IOS de Cisco le siguió la versión 12.4(7)T y la versión 12.4(8)T. Esto permite que el administrador rastree cambios introducidos en el código.

**Nota:** cualquier advertencia que se corrija en una versión de tren T debe implementarse en la siguiente versión de trenes de línea principal.

#### Numeración de los trenes T y de línea principal del software IOS de Cisco 12



## Capítulo 9: Imágenes y licencias del IOS 9.1.1.4 Paquetes de imagen de sistema del IOS de Cisco 12.4

### Cisco 12.4

Antes de la versión 15.0 del software IOS de Cisco, dicho software contaba con ocho paquetes para los routers Cisco, como se muestra en la ilustración. El esquema de paquetes se introdujo con el tren de línea principal 12.3 del software IOS de Cisco, y posteriormente se utilizó en otros trenes. Los paquetes de imágenes constan de ocho imágenes del IOS, tres de las cuales se consideran paquetes superiores.

Los cinco paquetes no superiores son los siguientes:

- **IP Base:** es la imagen básica del software IOS de Cisco.
- **Voz sobre IP:** voz y datos convergentes, VoIP, VoFR y telefonía IP.
- **Advanced Security:** características de VPN y de seguridad, incluido el firewall del IOS de Cisco, IDS/IPS, IPsec, 3DES y VPN.
- **Servicios de proveedor de servicios (SP):** agrega SSH/SSL, ATM, VoATM y MPLS a Voz sobre IP.
- **Base para empresas:** protocolos para empresas (Appletalk, IPX e IBM Support).

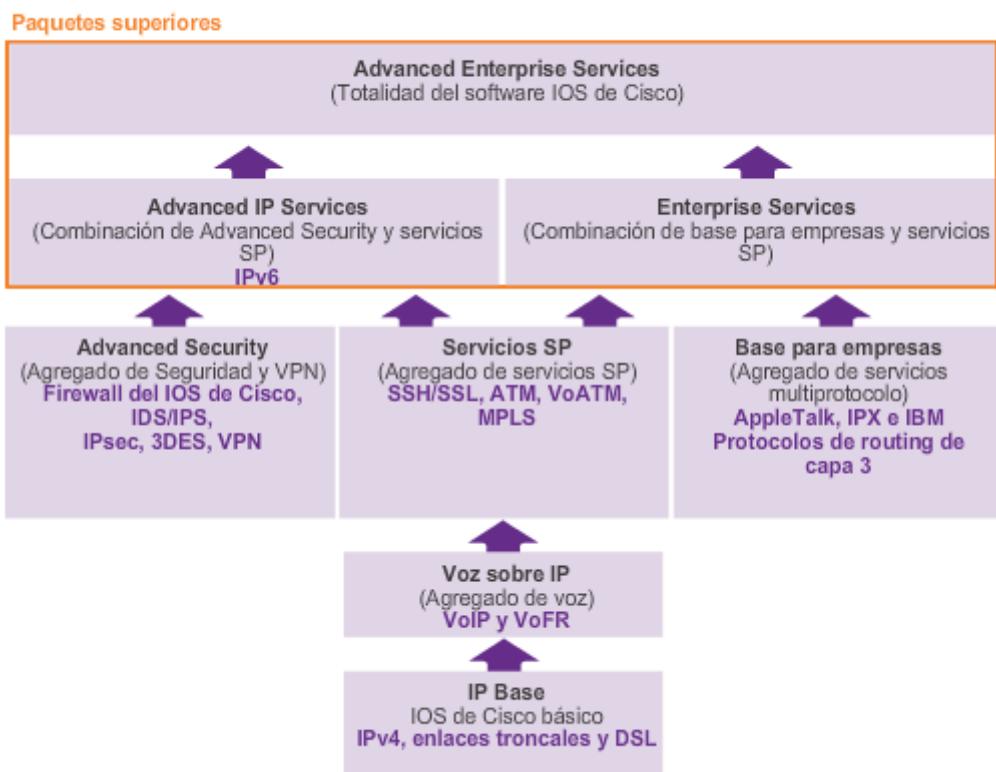
**Nota:** comenzando con la familia de la versión 12.4 del software IOS de Cisco, SSH se encuentra disponible en todas las imágenes.

Otros tres paquetes superiores ofrecen combinaciones adicionales de características del software IOS que abordan requisitos de red más complejos. Todas las características se fusionan en el paquete Advanced Enterprise Services. Este paquete integra compatibilidad para todos los protocolos de routing con capacidades de Voz, Seguridad y VPN:

- **Advanced Enterprise Services:** conjunto completo de características del software IOS de Cisco
- **Enterprise Services:** base para empresas y servicios de proveedor de servicios
- **Advanced IP Services:** seguridad avanzada, servicios de proveedor de servicios y compatibilidad con IPv6

**Nota:** Cisco Feature Navigator es una herramienta que se utiliza para encontrar el sistema operativo Cisco adecuado según las características y las tecnologías que se necesiten.

## Paquetes de imagen de sistema de Cisco



### Capítulo 9: Imágenes y licencias del IOS 9.1.1.5 Trenes M y T del IOS de Cisco 15.0

Después de la versión 12.4(24)T del IOS de Cisco, la siguiente versión del software IOS de Cisco fue 15.0.

IOS 15.0 proporciona varias mejoras al sistema operativo, por ejemplo:

- Nueva compatibilidad de hardware y de características
- Mayor coherencia de características con otras versiones principales del IOS
- Versión de nuevas características y programas de recopilación más predecibles
- Políticas de compatibilidad de versiones individuales proactivas
- Numeración de versión simplificada
- Pautas de migración e implementación de software más claras

Como se muestra en la ilustración, el IOS de Cisco 15.0 utiliza un modelo de versión distinto de los trenes T y de línea principal independientes de 12.4 tradicionales. En lugar de dividirse en trenes independientes, los trenes T y de línea principal del software IOS de Cisco 15 tendrán versión de mantenimiento extendido (versión de EM) y versión de mantenimiento estándar (versión T). Con el nuevo modelo de versión del IOS, las versiones de línea principal del IOS de Cisco 15 se denominan “trenes M”.

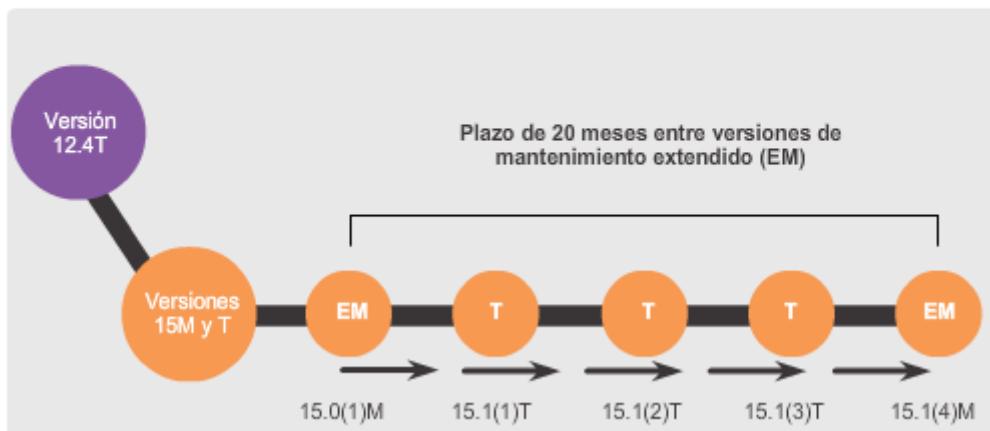
Comenzando por 15.0, las nuevas versiones en la forma de un tren T se encuentran disponibles aproximadamente de dos a tres veces por año. Las versiones de EM están disponibles aproximadamente cada 16 a 20 meses. Las versiones T permiten recibir la característica de Cisco más rápidamente, antes de que la siguiente versión de EM esté disponible.

Una versión de EM incorpora la compatibilidad de características y de hardware de todas las versiones T anteriores. Esto hace que las últimas versiones de EM contengan la funcionalidad total del tren en el momento del lanzamiento.

En resumen, entre los beneficios del nuevo modelo de versión del IOS de Cisco se incluyen los siguientes:

- Legado de características de las versiones 12.4T y 12.4 de línea principal del software IOS de Cisco
- Nuevas versiones de características aproximadamente cada dos a tres veces por año que se entregan en forma secuencial desde un único tren
- Versiones de EM aproximadamente cada 16 a 20 meses e inclusión de nuevas características
- Versiones T para las características más recientes y compatibilidad de hardware antes de que la siguiente versión de EM se encuentre disponible en Cisco.com
- Las recopilaciones de mantenimiento de versiones T y M solo contienen correcciones de errores.

#### Familia de la versión 15 del software IOS de Cisco



#### Capítulo 9: Imágenes y licencias del IOS 9.1.1.6 Numeración de trenes del IOS de Cisco 15

La convención de numeración de versión para el IOS 15 permite identificar la versión del IOS específica, incluso correcciones de errores y nuevas características de software, de manera

similar a familias de versiones del IOS anteriores. En la ilustración, se muestran ejemplos de esta convención para la versión de EM y la versión T.

### **Versión de mantenimiento extendido**

La versión de EM es ideal para el mantenimiento a largo plazo, y permite a los clientes cumplir con los requisitos, implementar la versión y mantenerla durante un período extendido. El tren de línea principal incorpora características proporcionadas en versiones anteriores y nuevas mejoras de características incrementales y compatibilidad de hardware.

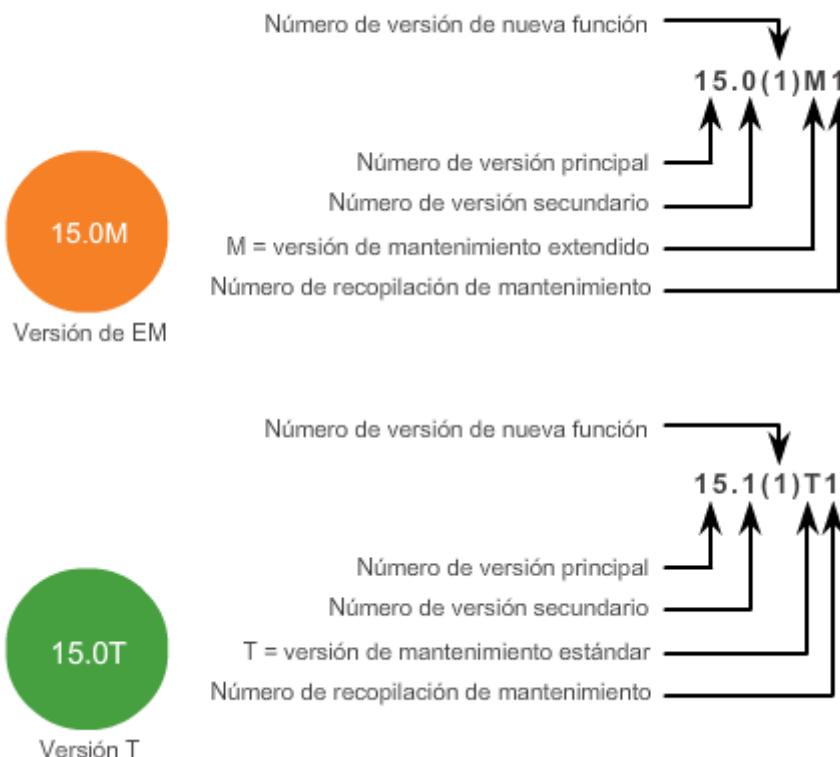
La primera recopilación de mantenimiento (para correcciones de errores solamente, sin nuevas características ni nueva compatibilidad de hardware) de la versión 15.0(1)M lleva el número 15.0(1)M1. Las versiones de mantenimiento posteriores se definen por un incremento del número de recopilación de mantenimiento (p. ej., M2, M3, etc.).

### **Versión de mantenimiento estándar**

La versión T se utiliza para versiones de implementación cortas ideales para las características más recientes y la compatibilidad de hardware antes de que la siguiente versión de EM se encuentre disponible. La versión T proporciona recopilaciones de mantenimiento de corrección de errores regulares y soporte de errores crítico para errores que afectan la red, como problemas del Equipo de informes de incidentes de seguridad del producto (PSIRT).

La primera versión de nuevas características 15 T planeada lleva el número de versión 15.1(1)T. La primera recopilación de mantenimiento (para correcciones de errores solamente, sin nuevas características o nueva compatibilidad de hardware) de la versión 15.1(1)T llevará el número 15.1(1)T1. Las versiones posteriores se definen por un incremento del número de recopilación de mantenimiento (p. ej., T2, T3, etc.).

## Numeración de trenes del software IOS de Cisco 15



### Capítulo 9: Imágenes y licencias del IOS 9.1.1.7 Paquetes de imagen de sistema del IOS 15

Las series de routers de servicios integrados Cisco de segunda generación (ISR G2) 1900, 2900 y 3900 admiten servicios a petición mediante el uso de licencias de software. El proceso de Servicios a petición permite que los clientes logren ahorros operativos mediante la facilidad de pedido y administración del software. Cuando se realiza un pedido de una nueva plataforma de ISR G2 de Cisco, el router se envía con una imagen única y universal del software IOS de Cisco, y se utiliza una licencia para habilitar los paquetes de conjuntos de características específicos, como se muestra en la figura 1.

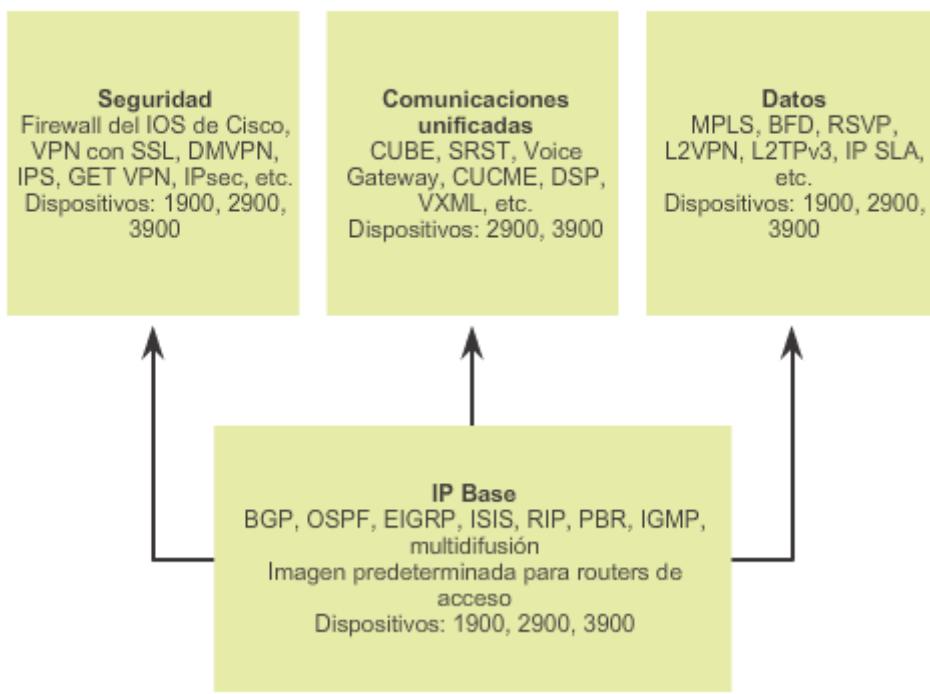
Existen dos tipos de imágenes universales admitidas en ISR G2:

- **Imágenes universales con la designación “universalk9” en el nombre de la imagen:** esta imagen universal ofrece todas las características del software IOS de Cisco, incluso características de criptografía del contenido seguras, como IPsec VPN, SSL VPN y comunicaciones unificadas seguras.
- **Imágenes universales con la designación “universalk9\_npe” en el nombre de la imagen:** el cumplimiento seguro de las capacidades de cifrado que proporciona Cisco Software Activation satisface los requisitos para la exportación de capacidades de cifrado. Sin embargo, algunos países tienen requisitos de importación que exigen que la plataforma no admita ninguna funcionalidad de criptografía segura, como la criptografía del contenido. Para satisfacer los requisitos de importación de dichos países, la imagen universal npe no admite ningún cifrado del contenido seguro.

Con los dispositivos ISR G2, se facilitó la selección de la imagen del IOS, debido a que se incluyen todas las características dentro de la imagen universal. Las características se activan mediante licencias. Cada dispositivo se envía con imagen universal. Los paquetes de tecnología IP Base, Datos, UC (Comunicaciones unificadas) y SEC (Seguridad) se habilitan en la imagen universal mediante las claves de licencia de Cisco Software Activation. Cada clave de licencia es exclusiva de un dispositivo en particular y se obtiene de Cisco al proporcionar la ID del producto, el número de serie del router y una clave de activación del producto (PAK). Cisco proporciona la PAK en el momento de la compra del software. IP Base se instala de manera predeterminada.

En la figura 2, se muestra la migración sugerida para los ISR de la siguiente generación del IOS 12 (paquetes de reforma del IOS) al IOS 15 (paquetes simplificados).

## Modelo de paquetes del IOS para los routers ISR G2



Transición sugerida del IOS 12 al 15

Paquetes de reforma	Transición sugerida a paquetes simplificados
Base IP	Base IP
Voz sobre IP	Comunicaciones unificadas
Base para empresas	Datos
Servicios empresariales	Datos + Comunicaciones unificadas
Servicios SP	Datos + Comunicaciones unificadas (para la paridad de características y características empresariales)
Advanced Security	Seguridad
Advanced IP Services	Seguridad + Comunicaciones unificadas + Datos (para la paridad de características y características empresariales)
Advanced Enterprise Services	Seguridad + Comunicaciones unificadas + Datos

### Capítulo 9: Imágenes y licencias del IOS 9.1.1.8 Nombres de archivo de imagen del IOS

Al seleccionar o actualizar un router con IOS de Cisco, es importante elegir la imagen del IOS adecuada con el conjunto de características y la versión correctos. El archivo de imagen del IOS de Cisco está basado en una convención de nomenclatura especial. El nombre del archivo de imagen del IOS de Cisco contiene varias partes, cada una con un significado específico. Es importante comprender esta convención de nomenclatura al actualizar y seleccionar un software IOS de Cisco.

Como se muestra en la figura 1, el comando **show flash** muestra los archivos almacenados en la memoria flash, incluso los archivos de imagen de sistema.

En la figura 2, se muestra un ejemplo de un nombre de imagen del software IOS 12.4.

- **Nombre de la imagen (c2800nm):** identifica la plataforma en la que se ejecuta la imagen. En este ejemplo, la plataforma es un router Cisco 2800 con un módulo de red.
- **advipservicesk9:** especifica el conjunto de características. En este ejemplo, advipservicesk9 se refiere al conjunto de características de Advanced IP Services, que incluye los paquetes de proveedor de servicios y de seguridad avanzada junto con IPv6.
- **mz:** indica dónde se ejecuta la imagen y si el archivo está comprimido. En este ejemplo, "mz" indica que el archivo se ejecuta desde la RAM y está comprimido.
- **124-6.T:** indica el formato del nombre del archivo para la imagen 12.4(6)T. Este es el número de tren, el número de versión de mantenimiento y el identificador de tren.
- **bin:** la extensión de archivo. Esta extensión indica que este es un archivo binario ejecutable.

En la figura 3, se ilustran las distintas partes de un archivo de imagen de sistema del IOS 15 en un dispositivo ISR G2:

- **Nombre de la imagen (c1900):** identifica la plataforma en la que se ejecuta la imagen. En este ejemplo, la plataforma es un router Cisco 1900.
- **universalk9:** especifica la designación de la imagen. Las dos designaciones para un ISR G2 son universalk9 y universalk9\_npe. Universalk9\_npe no contiene cifrado seguro y está pensado para países con restricciones de cifrado. Las características se controlan mediante licencias y pueden dividirse en cuatro paquetes de tecnología. Estos son IP Base, Seguridad, Comunicaciones unificadas y Datos.
- **mz:** indica dónde se ejecuta la imagen y si el archivo está comprimido. En este ejemplo, "mz" indica que el archivo se ejecuta desde la RAM y está comprimido.
- **SPA:** indica que el archivo está firmado digitalmente por Cisco.
- **152-4.M3:** especifica el formato del nombre del archivo para la imagen 15.2(4)M3. Esta es la versión del IOS, que incluye los números de la versión principal, de la versión secundaria, de la versión de mantenimiento y de la recopilación de mantenimiento. La M indica que se trata de una versión de mantenimiento extendido.
- **bin:** la extensión de archivo. Esta extensión indica que este es un archivo binario ejecutable.

La designación más común para ubicación de memoria y formato de compresión es mz. La primera letra indica la ubicación donde se ejecuta la imagen en el router. Las ubicaciones pueden incluir las siguientes:

- **f:** flash

- **m:** RAM
- **r:** ROM
- **I:** reubicable

El formato de compresión puede ser z para zip o x para mzip. La compresión de archivos es un método que utiliza Cisco para comprimir algunas imágenes ejecutadas desde la RAM que es eficaz para reducir el tamaño de la imagen. Se autodescomprime, de modo que cuando la imagen se carga en la RAM para ejecutarse, la primera acción es la descompresión.

**Nota:** las convenciones de nomenclatura, el significado de los campos, el contenido de la imagen y otros detalles del software IOS de Cisco están sujetos a cambios.

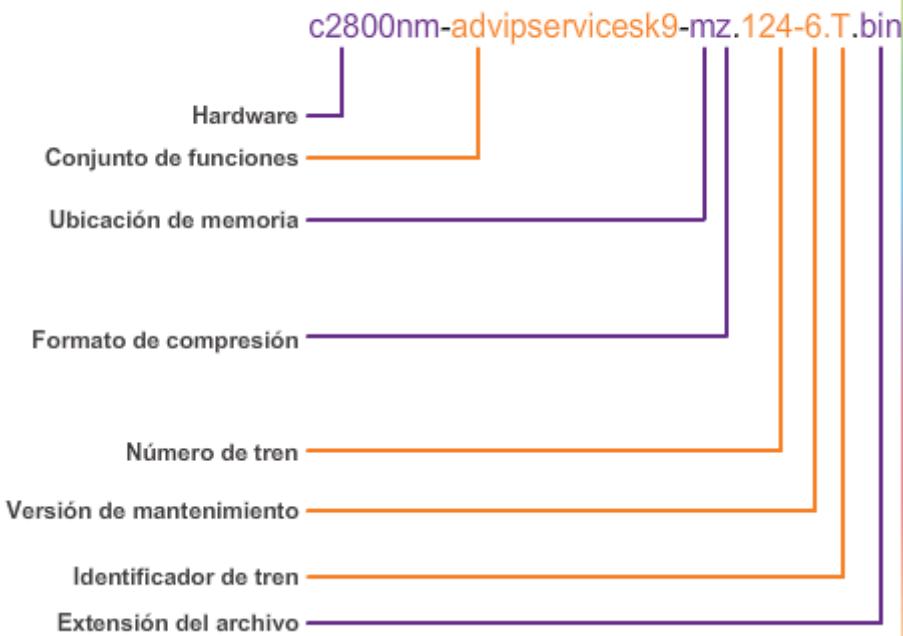
### **Requisitos de memoria**

En la mayoría de los routers Cisco, incluso en los routers de servicios integrados, el IOS se almacena en la memoria CompactFlash como una imagen comprimida y se carga en la DRAM durante el arranque. Las imágenes de la versión 15.0 del software IOS de Cisco disponibles para los ISR Cisco 1900 y 2900 requieren 256 MB de memoria flash y 512 MB de memoria RAM. El ISR 3900 requiere 256 MB de memoria flash y 1 GB de RAM. Esto no incluye herramientas de administración adicionales, como Cisco Configuration Professional (Cisco CP). Para obtener detalles completos, consulte la ficha técnica del producto para el router específico.

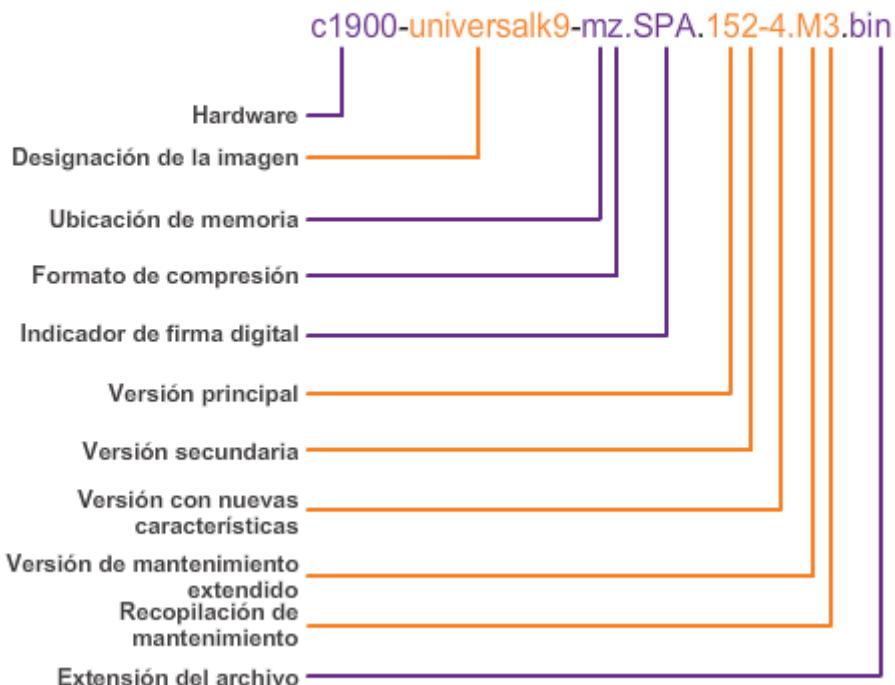
## Visualización de la imagen del IOS de Cisco

```
R1# show flash0:  
-# - --length-- -----date/time----- path  
  
8 68831808 Apr 2 2013 21:29:58 +00:00 c1900-universalk9-  
mz.SPA.152-4.M3.bin  
182394880 bytes available (74092544 bytes used)  
R1#
```

### Ejemplo de un nombre de imagen del software IOS de Cisco 12.4



### Ejemplo de un nombre de imagen del software IOS de Cisco 15.2 en un dispositivo ISR G2



Capítulo 9: Imágenes y licencias del IOS 9.1.1.9 Packet Tracer: Decodificación de nombres de la imagen del IOS

#### Información básica/situación

Como técnico de red, es importante que conozca la convención de nomenclatura de la imagen del IOS, de modo que pueda determinar con rapidez la información importante sobre los sistemas operativos que se ejecutan actualmente en un dispositivo. En esta situación, la Company A (Empresa A) se fusionó con la Company B (Empresa B). La Company A heredó el equipo de red de la Company B. Se le asignó que registre las características para las imágenes del IOS en estos dispositivos.

[Packet Tracer: Decodificación de nombres de la imagen del IOS \(instrucciones\)](#)

[Packet Tracer: Decodificación de nombres de la imagen del IOS \(PKA\)](#)

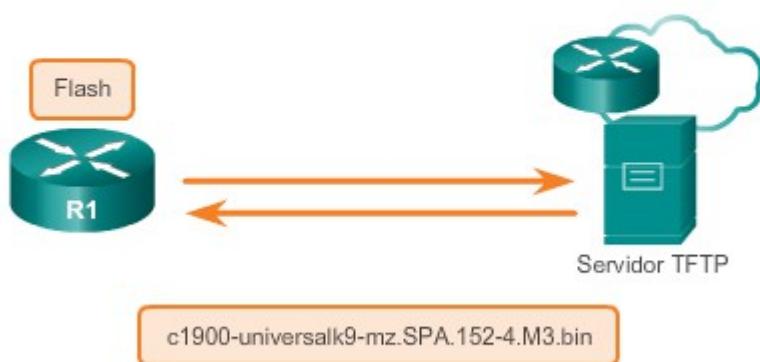
Capítulo 9: Imágenes y licencias del IOS 9.1.2.1 Servidores TFTP como ubicación de copia de seguridad

A medida que una red crece, las imágenes y los archivos de configuración del software IOS de Cisco pueden almacenarse en un servidor TFTP central. Esto ayuda a controlar la cantidad de imágenes del IOS y las revisiones a dichas imágenes del IOS, así como los archivos de configuración que deben mantenerse.

Las internetworks de producción suelen abarcar áreas extensas y contienen varios routers. Para cualquier red, es aconsejable tener una copia de seguridad de la imagen del software IOS de Cisco en caso de que la imagen de sistema en el router se dañe o se elimine accidentalmente.

Los routers distribuidos ampliamente necesitan una ubicación de origen o de copia de seguridad para las imágenes del software IOS de Cisco. El uso de un servidor TFTP de red permite las cargas y descargas de la imagen y la configuración a través de la red. El servidor TFTP de red puede ser otro router, una estación de trabajo o un sistema host.

#### **Servidor TFTP central utilizado como ubicación de copia de seguridad**



#### [Capítulo 9: Imágenes y licencias del IOS 9.1.2.2 Creación de copias de seguridad de la imagen del IOS de Cisco](#)

Para mantener las operaciones de red con el mínimo tiempo de inactividad, es necesario implementar procedimientos para realizar copias de seguridad de las imágenes del IOS de Cisco. Esto permite que el administrador de red copie rápidamente una imagen a un router en caso de que la imagen esté dañada o borrada.

En la figura 1, el administrador de red desea realizar una copia de seguridad del archivo de imagen actual en el router (c1900-universalk9-mz.SPA.152-4.M3.bin) en el servidor TFTP en 172.16.1.100.

Para realizar una copia de seguridad de la imagen del IOS de Cisco en un servidor TFTP, siga estos tres pasos:

**Paso 1.** Asegúrese de que haya acceso al servidor TFTP de red. Haga ping en el servidor TFTP para probar la conectividad, como se muestra en la figura 2.

**Paso 2.** Verifique que el servidor TFTP tenga suficiente espacio en disco para admitir la imagen del software IOS de Cisco. Utilice el comando **show flash0:** en el router para determinar el tamaño del archivo de imagen del IOS de Cisco. El archivo del ejemplo tiene 68831808 bytes de longitud.

**Paso 3.** Copie la imagen en el servidor TFTP mediante el comando **copy url-origen url-destino**, como se muestra en la figura 3.

Después de emitir el comando utilizando los URL de origen y de destino especificados, se solicita al usuario que introduzca el nombre del archivo de origen, la dirección IP del host remoto y el nombre del archivo de destino. A continuación, se inicia la transferencia.

Utilice el verificador de sintaxis de la figura 4 en el R2 para copiar el IOS en un servidor TFTP.

## Creación de copias de seguridad de la imagen del IOS de Cisco



### Verificación de la conectividad y del tamaño de la imagen

Verificación de la conectividad al servidor.

```
R1# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

Verifique el tamaño de la imagen.

```
R1# show flash0:
-# - --length-- -----date/time----- path
8 68831808 Apr 2 2013 21:29:58 +00:00
                           c1900-universalk9-mz.SPA.152-4.M3.bin
<resultado omitido>
```

### Comando copy

Copie la imagen en el servidor TFTP.

```
R1# copy flash0: tftp:  
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin  
Address or name of remote host []? 172.16.1.100  
Destination filename [c1900-universalk9-mz.SPA.152-4.M3.bin]?  
Writing c1900-universalk9-mz.SPA.152-4.M3.bin...  
!!!!!!!!!!!!!!  
<resultado omitido>  
68831808 bytes copied in 363.468 secs (269058 bytes/sec)
```

### Realización de una copia de seguridad del IOS de Cisco en el servidor TFTP

Copie la imagen del IOS c1900-universalk9-mz.SPA.152-4.M3.bin de la memoria flash0 en un servidor TFTP ubicado en 172.16.1.100. El nombre del archivo distingue mayúsculas de minúsculas.

```
R2# copy flash0: tftp:  
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin  
Address or name of remote host []? 172.16.1.100  
Destination filename [c1900-universalk9-mz.SPA.152-4.M3.bin]?  
!!!!!!  
<resultado omitido>  
68831808 bytes copied in 363.468 secs (269058 bytes/sec)  
R2#
```

Realizó correctamente una copia de seguridad del IOS de Cisco en el servidor TFTP.

### Capítulo 9: Imágenes y licencias del IOS 9.1.2.3 Copia de una imagen del IOS de Cisco

Cisco lanza sistemáticamente nuevas versiones del software IOS de Cisco para resolver advertencias y proporcionar nuevas características. En este ejemplo, se utiliza IPv6 para la transferencia, a fin de mostrar que TFTP también puede utilizarse a través de redes IPv6.

En la figura 1, se ilustra cómo copiar una imagen del software IOS de Cisco desde un servidor TFTP. Se copiará un nuevo archivo de imagen (c1900-universalk9-mz.SPA.152-4.M3.bin) del servidor TFTP en 2001:DB8:CAFE:100::99 al router.

Siga estos pasos para actualizar el software en el router Cisco:

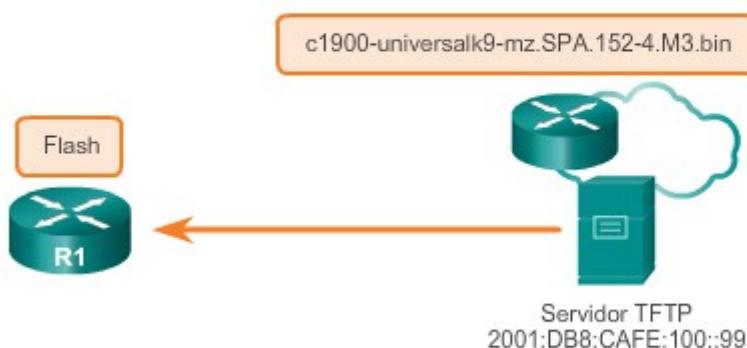
**Paso 1.** Seleccione un archivo de imagen del IOS de Cisco que satisfaga los requisitos en términos de plataforma, características y software. Descargue el archivo de cisco.com y transfíralo al servidor TFTP.

**Paso 2.** Verifique la conectividad al servidor TFTP. Haga ping al servidor TFTP desde el router. En el resultado de la figura 2, se muestra que se puede acceder al servidor TFTP desde el router.

**Paso 3.** Asegúrese de que haya suficiente espacio en la memoria flash en el router que se actualiza. Se puede verificar la cantidad de memoria flash disponible mediante el comando **show flash0**. Compare el espacio disponible en la memoria flash con el tamaño del nuevo archivo de imagen. El comando **show flash0** en la figura 3 se utiliza para verificar el espacio disponible en la memoria flash. En el ejemplo, el espacio disponible en la memoria flash es de 182.394.880 bytes.

**Paso 4.** Copie el archivo de imagen del IOS del servidor TFTP al router con el comando **copy** que se muestra en la figura 4. Después de emitir este comando con los URL de destino y de origen especificados, se solicitará al usuario que introduzca la dirección IP del host remoto, el nombre del archivo de origen y el nombre del archivo de destino. Se iniciará la transferencia del archivo.

#### Copia del IOS de Cisco



#### Verificación de la conectividad

Verificación de la conectividad al servidor.

```
R1# ping 2001:DB8:CAFE:100::99
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:CAFE:100::99,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

## Verificación del espacio disponible en la memoria flash

Verifique el espacio disponible en la memoria flash.

```
R1# show flash0:  
-# - --length-- -----date/time----- path  
<resultado omitido>  
  
182394880 bytes available (74092544 bytes used)  
  
R1#
```

## Realización de una copia de seguridad de la imagen

Copie la imagen del servidor TFTP.

```
R1# copy tftp: flash0:  
Address or name of remote host []? 2001:DB8:CAFE:100::99  
Source filename []? c1900-universalk9-mz.SPA.152-4.M3.bin  
Destination filename []?  
c1900-universalk9-mz.SPA.152-4.M3.bin  
Accessing tftp://2001:DB8:CAFE:100::99/c1900-universalk9-  
mz.SPA.152-4.M3.bin...  
Loading c1900-universalk9-mz.SPA.152-4.M3.bin from  
2001:DB8:CAFE:100::99 (via  
GigabitEthernet0/0): !!!!!!!!!!!!!!!  
<resultado omitido>  
[OK - 68831808 bytes]  
68831808 bytes copied in 368.128 secs (265652 bytes/sec)
```

## Capítulo 9: Imágenes y licencias del IOS 9.1.2.4 Comando boot system

Para actualizar a la imagen del IOS copiada una vez que esa imagen se guarda en la memoria flash del router, configure este último para que cargue a nueva imagen durante el arranque mediante el comando **boot system**. Guarde la configuración. Vuelva a cargar el router para que arranque con la nueva imagen. Una vez que arranque el router, utilice el comando **show version** para verificar que se cargó la nueva imagen.

Durante el arranque, el código bootstrap analiza el archivo de configuración de inicio en la NVRAM para detectar los comandos **boot system** que especifican el nombre y la ubicación de la imagen del software IOS de Cisco que se debe cargar. Se pueden introducir varios comandos **boot system** de manera secuencial para proporcionar un plan de arranque que tenga tolerancia a fallas.

Como se muestra en la figura 1, el comando **boot system** es un comando de configuración global que permite que el usuario especifique el origen para que se cargue la imagen del software IOS de Cisco. Entre las opciones de sintaxis disponibles se encuentran las siguientes:

- Especificar el dispositivo flash como el origen de la imagen del IOS de Cisco.

```
Router(config)# boot system flash0://c1900-universalk9-mz.SPA.152-4.M3.bin
```

- Especificar el servidor TFTP como el origen de la imagen del IOS de Cisco, con ROMmon como copia de seguridad.

```
Router(config)# boot system tftp://c1900-universalk9-mz.SPA.152-4.M3.bin
```

Si no hay comandos **boot system** en la configuración, de manera predeterminada, el router carga y ejecuta la primera imagen válida del IOS de Cisco en la memoria flash.

Como se muestra en la figura 2, el comando **show version** puede utilizarse para verificar el archivo de imagen del software.

## Uso del comando boot system

Establezca la imagen para arrancar y volver a cargar el sistema.

```
R1# configure terminal
R1(config)# boot system
  flash0:/c1900-universalk9-mz.SPA.152-4.M3.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

### Verificación de la nueva imagen

```
R1# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.2(4)M3, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Tue 26-Feb-13 02:11 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE
(fc1)

R1 uptime is 1 hour, 2 minutes
System returned to ROM by power-on
System image file is "flash0:
c1900-universalk9-mz.SPA.152-4.M3.bin"
```

Capítulo 9: Imágenes y licencias del IOS 9.1.2.5 Packet Tracer: Uso de un servidor TFTP para actualizar una imagen del IOS de Cisco

### Información básica/situación

Un servidor TFTP puede contribuir a administrar el almacenamiento y las revisiones de las imágenes del IOS. Para cualquier red, es aconsejable tener una copia de seguridad de la imagen del software IOS de Cisco en caso de que la imagen de sistema en el router se dañe o se elimine accidentalmente. Un servidor TFTP también se puede utilizar para almacenar nuevas actualizaciones del IOS y, luego, se puede implementar en la red donde sea necesario. En esta actividad, actualizará las imágenes del IOS en los dispositivos de Cisco mediante un servidor TFTP. También realizará copias de seguridad de una imagen del IOS con el uso de un servidor TFTP.

[Packet Tracer: Uso de un servidor TFTP para actualizar una imagen del IOS de Cisco \(instrucciones\)](#)

[Packet Tracer: Uso de un servidor TFTP para actualizar una imagen del IOS de Cisco \(PKA\)](#)

#### Capítulo 9: Imágenes y licencias del IOS 9.2.1.1 Descripción general de licencias

A partir de la versión 15.0 del software IOS de Cisco, Cisco modificó el proceso para habilitar las nuevas tecnologías dentro de los conjuntos de características del IOS. La versión 15.0 del software IOS de Cisco incorpora conjuntos de características interplataforma para simplificar el proceso de selección de imágenes. Lo hace proporcionando funciones similares a través de los límites de las plataformas. Cada dispositivo se envía con la misma imagen universal. Los paquetes de tecnología se habilitan en la imagen universal mediante claves de licencia de Cisco Software Activation. La característica Cisco IOS Software Activation permite que el usuario habilite características con licencia y registre licencias. La característica Cisco IOS Software Activation es un conjunto de procesos y componentes que se utilizan para activar los conjuntos de características del software IOS de Cisco mediante la obtención y validación de licencias del software de Cisco.

En la figura 1, se muestran los paquetes de tecnología disponibles:

- IP Base
- Datos
- Comunicaciones unificadas (UC)
- Seguridad (SEC)

Haga clic en los botones en la figura 2 para obtener más información sobre los paquetes de tecnología.

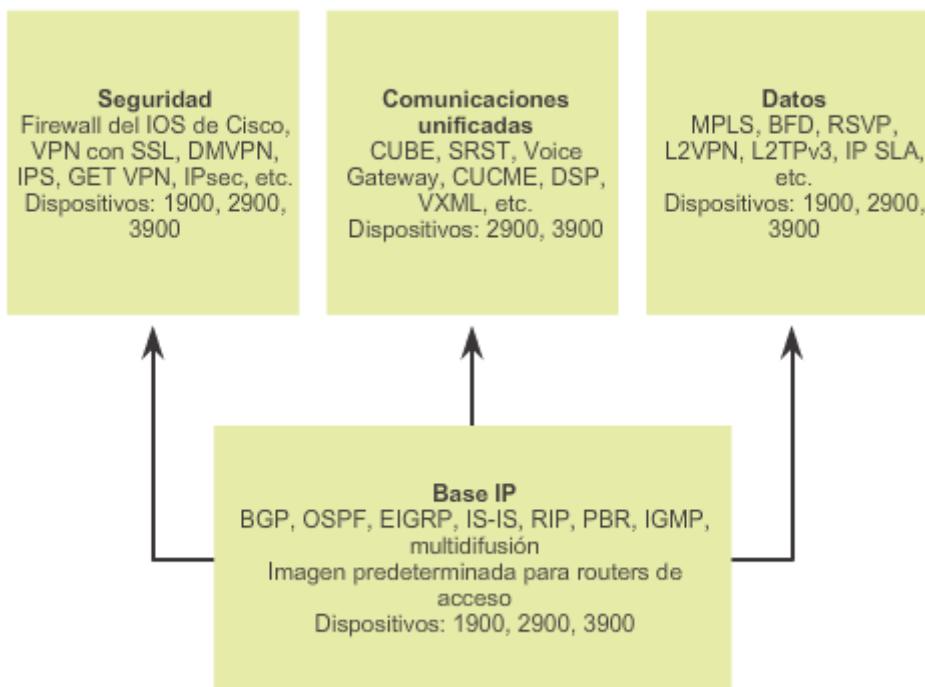
**Nota:** la licencia de IP Base es un requisito previo para instalar las licencias de Datos, Seguridad y Comunicaciones unificadas. No se encuentra disponible una imagen universal para plataformas de router anteriores que pueden admitir la versión 15.0 del software IOS de Cisco. Es necesario descargar otra imagen que contenga las características deseadas.

#### **Licencias de paquetes de tecnología**

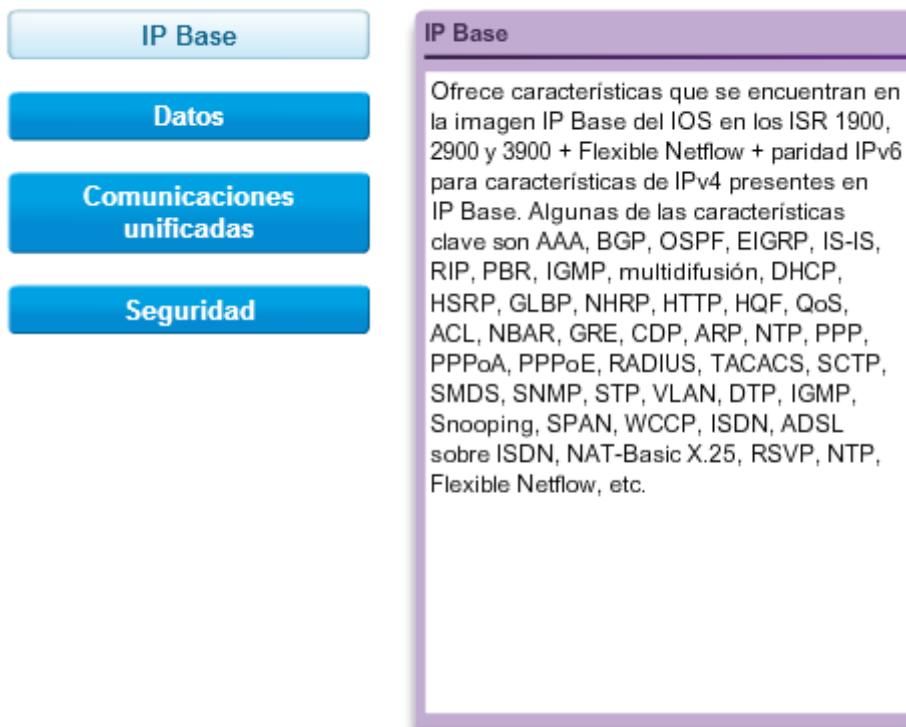
Las licencias de paquetes de tecnología se admiten en plataformas ISR G2 de Cisco (routers Cisco de las series 1900, 2900 y 3900). La imagen universal del IOS de Cisco contiene todos los paquetes y características en una imagen. Cada paquete es un conjunto de características específicas de la tecnología. Se pueden activar varias licencias de paquetes de tecnología en las plataformas ISR Cisco de las series 1900, 2900 y 3900.

**Nota:** utilice el comando **show license feature** para ver las licencias de paquetes de tecnología y las licencias de características admitidas en el router.

## Modelo de paquetes del IOS para los routers ISR G2



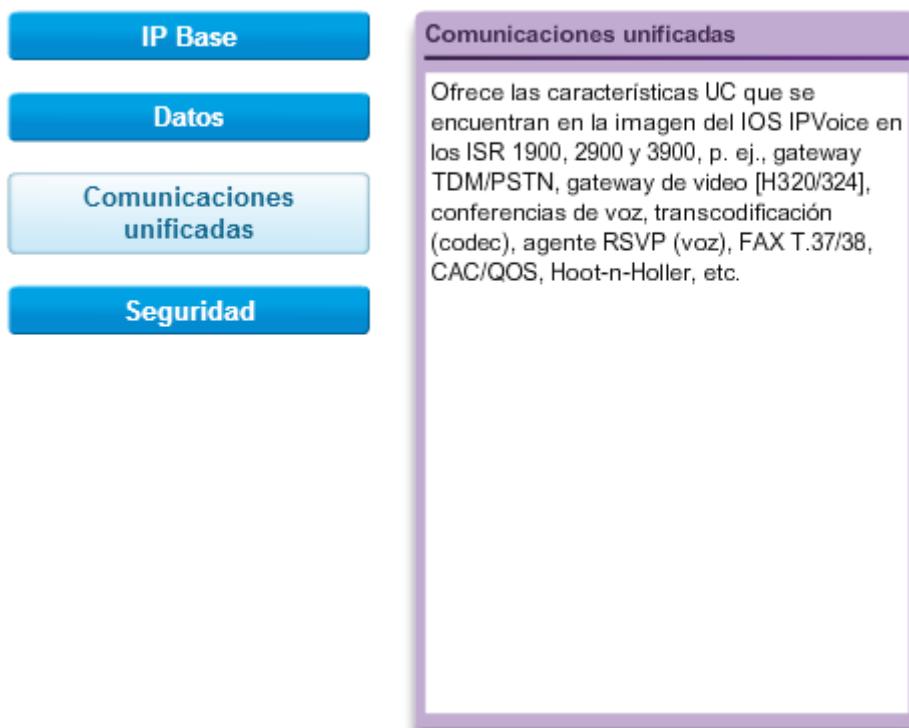
## Licencias de paquetes de tecnología



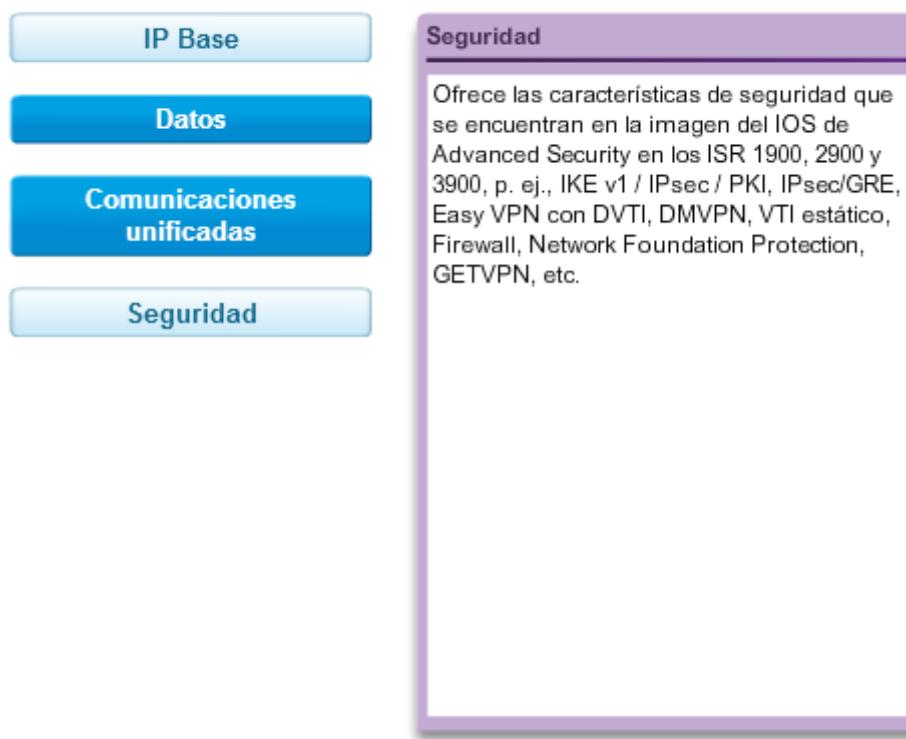
## Licencias de paquetes de tecnología

<b>IP Base</b>	Datos
<b>Datos</b>	
<b>Comunicaciones unificadas</b>	
<b>Seguridad</b>	

## Licencias de paquetes de tecnología



## Licencias de paquetes de tecnología



Cuando se envía un router nuevo, vienen preinstaladas la imagen del software y las licencias permanentes correspondientes para los paquetes y características especificadas por el cliente.

El router también viene con la licencia de evaluación, conocida como licencia temporal, para la mayoría de los paquetes y características admitidas en el router especificado. Esto permite que los clientes prueben una nueva característica o un nuevo paquete de software mediante la activación de una licencia de evaluación específica. Si los clientes desean activar de forma permanente una característica o un paquete de software en el router, deben obtener una licencia de software nueva.

En la ilustración, se muestran los tres pasos para activar de forma permanente una nueva característica o un nuevo paquete de software en el router.



Capítulo 9: Imágenes y licencias del IOS 9.2.1.3 Paso 1. Adquirir las características o el

paquete de software para instalar

#### **Paso 1. Adquirir la característica o el paquete de software que desea instalar.**

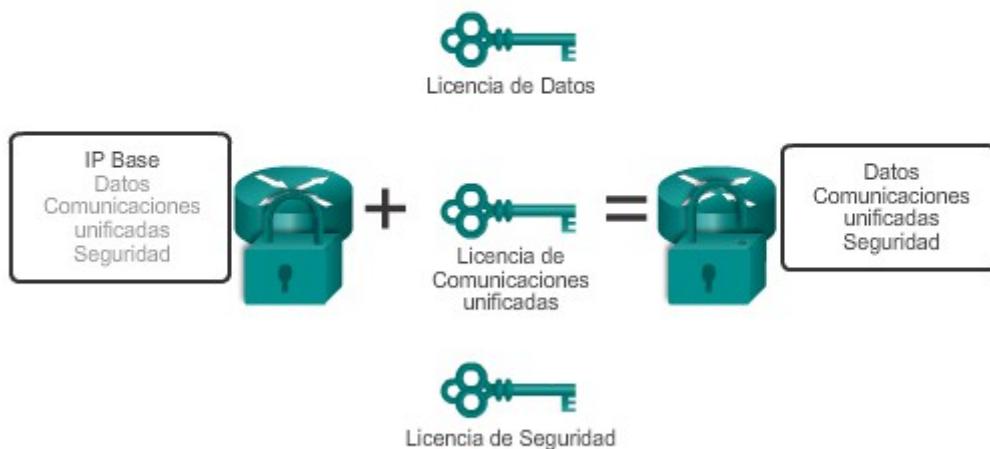
El primer paso es adquirir la característica o el paquete de software necesario. Esto puede ser la licencia de IP Base para una versión de software específica o el agregado de un paquete a IP Base, como Seguridad.

Los Certificados de reclamación de software se utilizan para licencias que requieren activación de software. El certificado de reclamación proporciona la clave de activación del producto (PAK) para la licencia e información importante acerca del Contrato de licencia para el usuario final (EULA) de Cisco. En la mayoría de los casos, Cisco o el socio del canal de Cisco ya contarán

con licencias activadas pedidas en el momento de la compra, y no se proporciona un Certificado de reclamación de software.

En cualquier caso, los clientes reciben una PAK con su compra. La PAK sirve como recibo y se utiliza para obtener una licencia. Una PAK es una clave alfanumérica de 11 dígitos creada por el equipo de producción de Cisco. Define el conjunto de características asociadas a la PAK. Una PAK no se relaciona con un dispositivo específico hasta que se crea la licencia. Se puede adquirir una PAK que genera cualquier cantidad especificada de licencias. Como se muestra en la ilustración, se requiere una licencia independiente para cada paquete, IP Base, Datos, UC y SEC.

#### Adquisición de una licencia para una característica



#### Capítulo 9: Imágenes y licencias del IOS 9.2.1.4 Paso 2. Obtener una licencia

##### Paso 2. Obtener una licencia.

El siguiente paso es obtener una licencia, que en realidad es un archivo de licencia. Un archivo de licencia, también conocido como Licencia de activación de software, se obtiene mediante una de las siguientes opciones:

- **Cisco License Manager (CLM):** esta es una aplicación de software gratuita disponible en <http://www.cisco.com/go/clm>. Cisco License Manager es una aplicación autónoma de Cisco que ayuda a los administradores de red a implementar rápidamente varias licencias de software de Cisco a través de las redes. Cisco License Manager puede detectar dispositivos de red, ver su información de licencia y adquirir e implementar licencias de Cisco. La aplicación proporciona una GUI que simplifica la instalación y ayuda a automatizar la obtención de licencias, además de llevar a cabo varias tareas de licencia desde una ubicación central. CLM es gratuito y puede descargarse de CCO.

- **Cisco License Registration Portal:** este es un portal basado en Web para obtener y registrar licencias de software individuales, disponibles en <http://www.cisco.com/go/license>.

Ambos procesos requieren un número de PAK y un Identificador de dispositivo único (UDI).

La PAK se recibe al efectuar la compra.

El UDI es una combinación de la ID del producto (PID), el número de serie (SN) y la versión de hardware. El SN es un número de 11 dígitos que identifica exclusivamente un dispositivo. La PID identifica el tipo de dispositivo. Para la creación de licencias, solo se utilizan la PID y el SN. El UDI puede mostrarse mediante el comando **show license udi**, que se muestra en la figura 1. Esta información también está disponible en una bandeja de etiquetas extraíble que se encuentra en el dispositivo. En la figura 2, se muestra un ejemplo de la etiqueta extraíble en un router Cisco 1941.

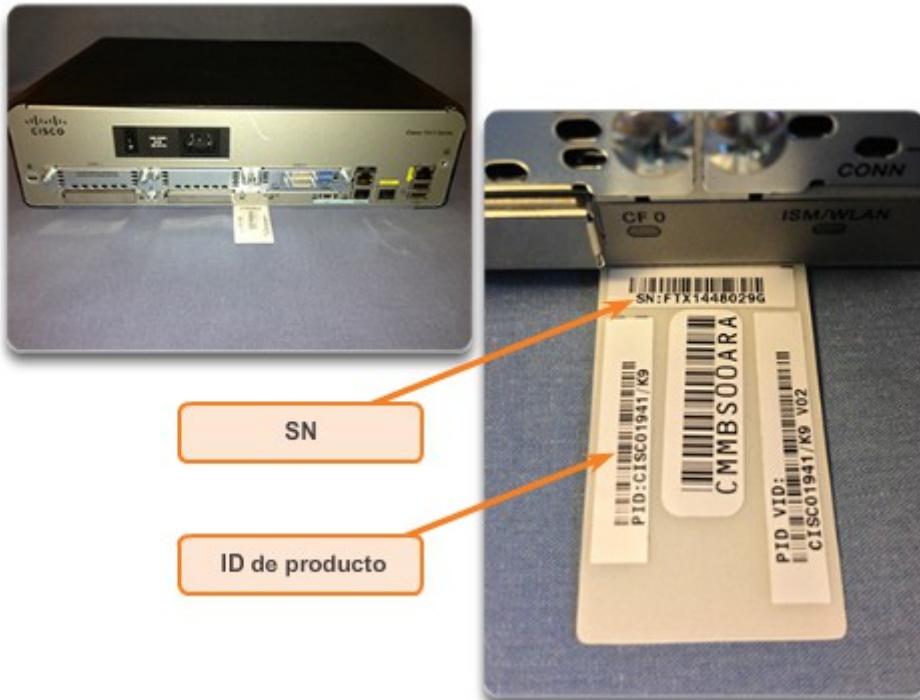
Después de introducir la información adecuada, el cliente recibe un correo electrónico con la información de licencia para instalar el archivo de licencia. El archivo de licencia es un archivo de texto XML con la extensión .lic.

Utilice el verificador de sintaxis de la figura 3 para determinar el UDI en el router R2.

## Visualización del UDI

```
R1# show license udi
Device# PID           SN          UDI
-----*
*0      CISCO1941/K9  FTX1636848Z  CISCO1941/K9:FTX1636848Z
R1#
```

## Visualización del UDI (PID/SN) en una etiqueta extraíble



## Visualización del UDI de la licencia en el R2

Muestre el Identificador de dispositivo único (UDI) para el R2.

```
R2# show license udi
Device# PID           SN          UDI
-----*
*0      CISCO1941/K9  FTX16368491  CISCO1941/K9:FTX16368491
R2#
```

Mostró correctamente el UDI para el R2.

Capítulo 9: Imágenes y licencias del IOS 9.2.1.5 Paso 3. Instalar la licencia

**Paso 3. Instalar la licencia.**

Una vez que se adquiere la licencia, el cliente recibe un archivo de licencia, que es un archivo de texto XML con la extensión .lic. La instalación de una licencia permanente requiere dos pasos:

**Paso 1.** Utilice el comando del modo EXEC privilegiado **license install url-ubicación-almacenamiento** para instalar un archivo de licencia.

**Paso 2.** Vuelva a cargar el router mediante el comando del modo EXEC privilegiado **reload**. Si una licencia de evaluación esta activa, no es necesario volver a cargar el router.

En la figura 1, se muestra la configuración para instalar la licencia permanente para el paquete de seguridad en el router.

**Nota:** no se admite Comunicaciones unificadas en los routers 1941.

Una licencia permanente es una licencia que nunca caduca. Después de que se instala una licencia permanente en un router, sirve para ese conjunto características específico durante la vida útil del router, incluso en distintas versiones del IOS. Por ejemplo, cuando se instala una licencia de UC, SEC o Datos en un router, las características posteriores para esa licencia se activan incluso si se actualiza el router a una nueva versión del IOS. La licencia permanente es el tipo de licencia habitual cuando se compra un conjunto de funciones para un dispositivo.

**Nota:** el equipo de producción de Cisco preinstala la licencia permanente adecuada para el conjunto de características adquirido en el dispositivo pedido. No se requiere interacción del cliente con los procesos de Cisco IOS Software Activation para habilitar esa licencia en hardware nuevo.

Utilice el verificador de sintaxis de la figura 2 para instalar un archivo de licencia permanente en el router R2.

## Instalación de la licencia permanente

```
R1# license install flash0:securityk9-CISCO1941-FHH12250057.xml
Installing licenses from "flash0:securityk9-CISCO1941-
FHH12250057.xml"
Installing...Feature:securityk9...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
R1#
*Jul 30 10:47:41.648: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name - c1941 Next reboot level - securityk9 and License -
securityk9
*Jul 30 10:47:42.036: %LICENSE-6-INSTALL: Feature securityk9 1.0 was
installed in this device. UDI-CISCO1941:FHH12250057;
StoreIndex-0:Primary License Storage
R1# reload
```

## Instalación de la licencia de Seguridad en el R2

```
Instale la licencia de seguridad seck9-C1900-SPE150_K9-FAB12340099.xml de
flash0 y vuelva a cargar el router.
R2# license install flash0:seck9-c1900-SPE150_K9-FAB12340099.xml
Installing licenses from "seck9-c1900-SPE150_K9-FAB12340099.xml"
Installing...Feature:seck9...Successful:Supported
1/1 licenses were successfully installed
0/1 licenses were existing licenses
0/1 licenses were failed to install
R2#
*May 27 17:24:57.391: %LICENSE-6-INSTALL: Feature seck9 1.0 was
installed in this
device.
UDI-1900-SPE150/K9:FAB12340099; StoreIndex-15:Primary License
Storage
*May 27 17:24:57.615: %IOS_LICENSE_IMAGE_APPLICATION-6-
LICENSE LEVEL: Module
name - c1900
Next reboot level - seck9 and License - seck9
R2# reload
Instaló correctamente la licencia de Seguridad en el R2.
```

## Capítulo 9: Imágenes y licencias del IOS 9.2.2.1 Verificación de la licencia

Después de que se instala una nueva licencia, se debe reiniciar el router mediante el comando **reload**. Como se muestra en la figura 1, el comando **show version** se utiliza una vez que se vuelve a cargar el router para verificar que se instaló la licencia.

El comando **show license** de la figura 2 se utiliza para mostrar información adicional sobre las licencias del software IOS de Cisco. Este comando muestra información de licencia que se utiliza para ayudar con cuestiones de resolución de problemas relacionados con licencias del software IOS de Cisco. Este comando muestra todas las licencias instaladas en el sistema. En este ejemplo, se activaron las licencias de Seguridad y de IP Base. Este comando también muestra las características que se encuentran disponibles, pero que no tienen licencia para ejecutarse, como el conjunto de características de Datos. El resultado se agrupa según la forma en que se guardan las características en el almacenamiento de licencias.

La siguiente es una breve descripción del resultado:

- **Feature:** nombre de la característica
- **License Type:** tipo de licencia, como Permanent (Permanente) o Evaluation (Evaluación)
- **License State:** estado de la licencia, como Active (Activa) o In Use (En uso)
- **License Count:** cantidad de licencias disponibles y en uso, si se cuentan. Si se indica que no se cuentan, la licencia es sin restricciones.
- **License Priority:** prioridad de la licencia, como High (Alta) o Low (Baja)

**Nota:** consulte la guía de referencia de comandos del IOS de Cisco 15 para obtener detalles completos sobre la información que se muestra en el comando **show license**.

#### Verificación de la licencia permanente

R1# show version <resultado omitido> License Info: License UDI:			
Device#	PID	SN	
*0	CISCO1941/K9	FTX1636848Z	
Technology Package License Information for Module:'c1900'			
Technology	Technology-package	Technology-package	
	Current	Type	Next reboot
ipbase	ipbasek9	Permanent	ipbasek9
security	seck9	Permanent	seck9
uc	None	None	None
data	None	None	None

Capítulo 9: Imágenes y licencias del IOS 9.2.2.2 Activación de una licencia de Right-to-Use de evaluación

El proceso de licencia de evaluación pasó por tres revisiones en los dispositivos ISR G2. En la revisión más reciente, comenzando con las versiones del IOS de Cisco 15.0(1)M6, 15.1(1)T4, 15.1(2)T4, 15.1(3)T2 y 15.1(4)M, las licencias de evaluación se reemplazan por licencias de Right-to-Use (RTU) de evaluación después de 60 días. Una licencia de evaluación es válida durante un período de evaluación de 60 días. Despues de 60 días, se lleva a cabo la transición de esta licencia a una licencia de RTU de forma automática. Estas licencias se encuentran disponibles en el sistema de honor y requieren que el cliente acepte el EULA. El EULA se aplica automáticamente a todas las licencias del software IOS de Cisco.

El comando del modo de configuración **globallicense accept end user agreement** se utiliza para configurar una aceptación única del EULA para todas las características y paquetes del software IOS de Cisco. Una vez que se emite el comando y que se acepta el EULA, este último se aplica automáticamente a todas las licencias del software IOS de Cisco, y no se le solicita al usuario que acepte el EULA durante la instalación de la licencia.

En la figura 1, se muestra cómo configurar una aceptación única del EULA:

```
Router(config)# license accept end user agreement
```

Además, en la figura 1 se muestra el comando para activar una licencia de RTU de evaluación:

```
Router# license boot module module-name technology-package package-name
```

Use **?** en lugar de los argumentos para determinar qué nombres de módulos y paquetes de software admitidos se encuentran disponibles en el router. Los nombres de los paquetes de tecnología para las plataformas de ISR G2 de Cisco son los siguientes:

- ipbasek9:paquete de tecnología IP Base
- securityk9:paquete de tecnología de Seguridad
- datak9: paquete de tecnología de Datos
- uck9: paquete de tecnología de Comunicaciones unificadas (no disponible en la serie 1900)

**Nota:** para activar el paquete de software, se requiere volver a cargar mediante el comando **reload**.

Las licencias de evaluación son temporales, y se utilizan para evaluar un conjunto de características en hardware nuevo. Las licencias temporales se limitan a un período de uso específico (por ejemplo, 60 días).

Una vez que se instala correctamente una licencia, vuelva a cargar el router mediante el comando **reload**. El comando **show licensede** la figura 2 verifica si se instaló la licencia.

Utilice el verificador de sintaxis de la figura 3 para aceptar el EULA y activar una licencia de paquetes de datos de RTU de evaluación en el router 1900.

## Instalación de la licencia de evaluación

```
R1(config)# license accept end user agreement
< Se omiten detalles del Acuerdo de licencia para el usuario final >

ACCEPT? [yes/no]: yes
R1(config)#
*Apr 12 11:05:43.775: %LICENSE-6-EULA_ACCEPT_ALL: The Right to
Use End User License Agreement is accepted
R1(config)# license boot module c1900 technology-package datak9
% use 'write' command to make license boot config take effect
on next boot

R1(config)#
*Apr 12 11:06:19.851: %IOS_LICENSE_IMAGE_APPLICATION-6-
LICENSE_LEVEL:
Module name = c1900 Next reboot level = datak9 and License =
datak9
R1(config)#

```

## Verificación de la licencia de evaluación

```
R1# show license
Index 1 Feature: ipbasek9
    Period left: Life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
Index 2 Feature: securityk9
    Period left: Life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
Index 3 Feature: datak9
    Period left: 8 weeks 4 days
    Period Used: 0 minute 0 second
    License Type: EvalRightToUse
    License State: Active, Not in Use, EULA accepted
    License Count: Non-Counted
    License Priority: Low
<resultado omitido>
```

**En el router R2, realice las siguientes tareas:**

- Acepte el Contrato de licencia para el usuario final.
- Instale el paquete de tecnología de Datos para la evaluación: "datak9".
- Vuelva al modo EXEC privilegiado.

```
R2(config)# license accept end user agreement
R2(config)# license boot module c1900 technology-package datak9
% use 'write' command to make license boot config take effect on
next boot
*Apr 27 01:27:01.703: %IOS LICENSE_IMAGE_APPLICATION-6-
LICENSE_LEVEL: Module name = c1900 Next reboot level = datak9
and license = datak9
*Apr 27 01:27:02.331: %LICENSE-6-EULA_ACCEPTED: EULA for feature
datak9 1.0 has been accepted. UDI-CISCO1941/K9:FTX16368491;
StoreIndex-1:Built-In License Storage
R2(config)# end
R2#
*Apr 27 01:27:20.811: %SYS-5-CONFIG_I: Configured from console by
console
```

**Verifique la instalación del paquete.**

```
R2# show license
Index 1 Feature: ipbasek9
    Period left: Life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
Index 2 Feature: securityk9
    Period left: Not Activated
    Period Used: 0 minute 0 second
    License Type: EvalRightToUse
    License State: Not in Use, EULA not accepted
    License Count: Non-Counted
    License Priority: None
Index 3 Feature: datak9
    Period left: 8 weeks 4 days
    Period Used: 0 minute 0 second
    License Type: EvalRightToUse
    License State: Active, Not in Use, EULA accepted
    License Count: Non-Counted
    License Priority: Low
Index 4 Feature: SSL_VPN
    Period left: Not Activated
    Period Used: 0 minute 0 second
```

```
R2#
```

**Activó correctamente una licencia de Right-to-Use de evaluación.**

Capítulo 9: Imágenes y licencias del IOS 9.2.2.3 Realización de copias de seguridad de la licencia

El comando **license save** se utiliza para copiar todas las licencias en un dispositivo y almacenarlas en un formato requerido por la ubicación de almacenamiento especificada. Las licencias guardadas se restablecen mediante el comando **license install**.

El comando para realizar una copia de seguridad de las licencias en un dispositivo es el siguiente:

```
Router# license save file-sys://lic-location
```

Utilice el comando **show flash0**: para verificar que las licencias se hayan guardado (figura 1).

La ubicación de almacenamiento de licencias puede ser un directorio o un URL que corresponda a un sistema de archivos. Utilice el comando ? para ver las ubicaciones de almacenamiento que admite un dispositivo.

Utilice el verificador de sintaxis de la figura 2 para guardar todos los archivos de licencia en el router R2.

## Creación de una copia de seguridad de la licencia



```
R1# license save flash0:all_licenses.lic
license lines saved ..... to flash0:all_licenses.lic

R1# show flash0:
-# - --length-- -----date/time----- path
<resultado omitido>
8 68831808 Apr 2 2013 21:29:58 +00:00
  c1900-universalk9-mz.SPA.152-4.M3.bin
9      1153 Apr 26 2013 02:24:30 +00:00 all_licenses.lic

182390784 bytes available (74096640 bytes used)

R1#
```

### En el router R2, realice las siguientes tareas:

- Guarde todas las licencias en flash0:R2\_license\_files.
- Verifique que el archivo se haya guardado en flash0.

```
R2# license save flash0:R2_license_files
license lines saved ..... to flash0:R2_license_files

R2# show flash0:
-#- --length-- -----date/time----- path
1      68831808 Apr 2 2013 21:50:32 +00:00 c1900-universalk9-
-mz.SPA.152-4.M3.bin
2      1153 Apr 27 2013 01:34:32 +00:00 R2_license_files

182398976 bytes available (68832961 bytes used)
```

```
R2#
```

You successfully backed up the license on R2.

## Capítulo 9: Imágenes y licencias del IOS 9.2.2.4 Desinstalación de la licencia

Para borrar una licencia permanente activa de los routers Cisco de las series 1900, 2900 y 3900, realice los siguientes pasos:

### Paso 1. Deshabilitar el paquete de tecnología.

- Deshabilite la licencia activa mediante el comando:

```
Router(config)# license boot module nombre-módulo technology-package nombre-paquete disable
```

- Vuelva a cargar el router mediante el comando **reload**. Se requiere volver a cargarlo para que el paquete de software esté inactivo.

#### Paso 2. Borrar la licencia.

- Borre la licencia de paquete de tecnología del almacenamiento de licencias.

```
Router# license clear nombre-característica
```

- Borre el comando **license boot module *nombre-módulo* technology-package *nombre-paquete* disable** que se utiliza para deshabilitar la licencia activa:

```
Router(config)# no license boot module nombre-módulo technology-package nombre-paquete disable
```

**Nota:** algunas licencias, como las licencias incorporadas, no pueden borrarse. Solo se eliminan las licencias que se agregaron mediante el comando **license install**. Las licencias de evaluación no se eliminan.

En la figura 1, se muestra un ejemplo de eliminación de una licencia activa.

Utilice el verificador de sintaxis de la figura 2 para desinstalar la licencia de seguridad en el router R2.

## Eliminación de una licencia permanente y activa



Paso 1. Deshabilitar el paquete de tecnología.

```
R1(config)# license boot module c1900 technology-package  
seck9 disable  
R1(config)# exit  
R1# reload
```

Paso 2. Borrar la licencia.

```
R1# license clear seck9  
R1# configure terminal  
R1(config)# no license boot module c1900 technology-package  
seck9 disable  
R1(config)# exit  
R1# reload
```

## Desinstalación de la licencia en el R2

En el router R2, realice las siguientes tareas:

- Deshabilite el paquete de tecnología "seck9".
- Vuelva al modo EXEC privilegiado con el comando "exit".
- Vuelva a cargar el router para que se apliquen los cambios.

```
R2(config)# license boot module c1900 technology-package seck9 disable  
R2(config)# exit  
R2# reload  
<Recarga simulada>
```

Ahora realice las siguientes tareas:

- Borre la licencia "seck9".
- Ingrese al modo de configuración y elimine la opción de arranque para la licencia.
- Vuelva al modo EXEC privilegiado con el comando "exit".
- Vuelva a cargar el router para que se apliquen los cambios.

```
R2# license clear seck9  
R2# configure terminal  
R2(config)# no license boot module c1900 technology-package seck9  
disable  
R2(config)# exit  
R2# reload  
<Simulated reload>
```

Desinstaló correctamente la licencia de seguridad en el R2.

## **Protocolos eficaces**

Al final de este curso, se le solicita que complete dos proyectos finales en los que creará, configurará y verificará dos topologías de red con los dos protocolos de routing principales que se abordaron en este curso: EIGRP y OSPF.

Para simplificar las cosas, decide crear un cuadro de los comandos de configuración y verificación que utilizará para estos dos proyectos de diseño. Solicite ayuda a otro estudiante de la clase para elaborar los gráficos de protocolos.

Consulte el PDF correspondiente a este capítulo para obtener las instrucciones sobre cómo crear un diseño para este proyecto de creación de modelos. Cuando termine, comparta el trabajo con otro grupo o con la clase. También puede guardar los archivos que creó para este proyecto en una cartera de red para referencia futura.

### [Actividad de clase: Protocolos eficaces](#)

#### Capítulo 9: Imágenes y licencias del IOS 9.3.1.2 Packet Tracer: Proyecto final de EIGRP

**En esta actividad de proyecto final, demostrará su capacidad para lo siguiente:**

- Diseñar, configurar, verificar y proteger EIGRP, IPv4 o IPv6 en una red.
- Diseñar un esquema de direccionamiento VLSM para los dispositivos conectados a las LAN.
- Presentar su diseño con la documentación de red de su proyecto final.

### [Packet Tracer: Proyecto final de EIGRP \(instrucciones\)](#)

#### Capítulo 9: Imágenes y licencias del IOS 9.3.1.3 Packet Tracer: Proyecto final de OSPF

**En esta actividad de proyecto final, demostrará su capacidad para lo siguiente:**

- Configurar OSPFv2 básico para habilitar las comunicaciones de internetwork en una red IPv4 de una pequeña a mediana empresa.
- Implementar características avanzadas de OSPF para mejorar el funcionamiento en una red de una pequeña a mediana empresa.
- Implementar OSPF multiárea para IPv4 para habilitar las comunicaciones de internetwork en una red de una pequeña a mediana empresa.
- Configurar OSPFv3 básico para habilitar las comunicaciones de internetwork en una red IPv6 de una pequeña a mediana empresa.

### [Packet Tracer: Proyecto final de OSPF \(instrucciones\)](#)

## Capítulo 9: Imágenes y licencias del IOS 9.3.1.4 Packet Tracer: Desafío de integración de

### habilidades

#### **Información básica/situación**

Como técnico de red familiarizado con el direccionamiento, el routing y la seguridad de red IPv4, ya está preparado para aplicar sus conocimientos y habilidades a una infraestructura de red. Su tarea es terminar de diseñar el esquema de direccionamiento IPv4 VLSM, implementar OSPF multiárea y proteger el acceso a las líneas VTY mediante listas de control de acceso.

[Packet Tracer: Desafío de integración de habilidades \(instrucciones\)](#)

[Packet Tracer: Desafío de integración de habilidades \(PKA\)](#)

## Capítulo 9: Imágenes y licencias del IOS 9.3.1.5 Resumen

Entre los ejemplos de versiones del software IOS de Cisco se incluyen 12.3, 12.4, 15.0 y 15.1. Junto con cada versión del software, hay nuevas versiones que se utilizan para implementar correcciones de errores y nuevas características.

El software IOS de Cisco 12.4 incorpora nuevas características de software y compatibilidad de hardware introducidas en el tren 12.3T del software IOS de Cisco y correcciones de software adicionales. Las versiones de línea principal (también llamadas "versiones de mantenimiento") no contienen una letra mayúscula en la designación de la versión y heredan la funcionalidad del nuevo software IOS de Cisco y hardware de versiones T con números más bajos. Hasta la versión 12.4 inclusive, el tren "M" de línea principal recibía solamente correcciones de errores. El tren "T" de tecnología incluye correcciones y nuevas características y plataformas. El tren 12.4T proporciona la funcionalidad del software IOS de Cisco y la adopción de hardware que introduce nueva tecnología, funcionalidad y avances de hardware que no se encuentran disponibles en el tren de línea principal del software IOS de Cisco 12.4.

En la familia de la versión 15.0 del software IOS de Cisco se aplica una nueva estrategia. La familia de la versión 15.0 del IOS de Cisco no se divide en trenes T y M independientes, sino que lo hace en versiones T y M en el mismo tren. Por ejemplo, la primera versión de la familia de versiones 15.0 del software IOS de Cisco es 15.0(1)M, donde M indica que se trata de una versión de mantenimiento extendido. Una versión de mantenimiento extendido es ideal para el mantenimiento a largo plazo. No todas las versiones de la familia de versiones 15.0 del software IOS de Cisco son de mantenimiento extendido; también hay versiones de mantenimiento estándar que reciben las características y la compatibilidad de hardware más recientes. Las versiones de mantenimiento estándar tienen una T mayúscula en su designación.

Al seleccionar o actualizar un router con IOS de Cisco, es importante elegir la imagen del IOS adecuada con el conjunto de características y la versión correctos. El archivo de imagen del IOS de Cisco está basado en una convención de nomenclatura especial. El nombre del archivo de imagen del IOS de Cisco contiene varias partes, cada una con un significado específico. Ejemplo: c1900-universalk9-mz.SPA.152-4.M3.bin