



Fundamentos de enrutamiento y conmutación (Routing and Switching Essentials).

CCNA2 V5.

Material oficial de la Academia Cisco.

Válido para la preparación a los exámenes de las certificaciones 100-101 (ICND1), 200-101 (ICND2) y 200-120 (CCNA R&S).

Compilado por Nicolás Contador.

Agradecimientos a la comunidad de
elprofederedes.wordpress.com

Todos los derechos de copyright pertenecen a Cisco y su academia Netacad.

Contenido

0	Bienvenido a Principios básicos de routing y switching.....	8
0.1	Mensaje para el estudiante.....	8
1	Introducción a redes conmutadas	13

1.1	Introducción	13
1.2	Diseño de la LAN	14
1.2.1	Redes convergentes	14
1.2.2	Redes conmutadas	20
1.3	El entorno conmutado	25
1.3.1	Reenvío de tramas.....	25
1.3.2	Dominios de switching	32
1.4	Resumen.....	35
2	Configuración y conceptos básicos de switching	36
2.1	Introducción	36
2.2	Configuración de parámetros iniciales de un switch	36
2.3	Configuración de puertos de un switch	43
2.4	Seguridad de switches: administración e implementación	52
2.4.1	Acceso remoto seguro.....	52
2.4.2	Cuestiones de seguridad en redes LAN.....	57
2.4.3	Prácticas recomendadas de seguridad.....	63
2.5	Resumen.....	75
3	VLAN	78
3.1	Introducción	78
3.2	Segmentación de VLAN	79
3.2.1	Descripción general de las VLAN	¡Error! Marcador no definido.
3.2.2	Redes VLAN en un entorno conmutado múltiple	84
3.3	Implementaciones de VLAN	90
3.3.1	Asignación de red VLAN	90
3.3.2	Enlaces troncales de la VLAN	98
3.3.3	Protocolo de enlace troncal dinámico	101
3.3.4	Resolución de problemas de VLAN y enlaces troncales.....	104
3.4	Seguridad y diseño de redes VLAN.....	113
3.4.1	Ataques a redes VLAN	113
3.5	Prácticas recomendadas de diseño para las VLAN.....	117
3.6	Resumen.....	117
4	Conceptos de routing	120
4.1	Introducción	120

4.2	Configuración inicial de un router.....	121
4.2.1	Funciones de un router	121
4.2.2	Conexión de los Dispositivos	131
4.2.3	Configuración básica de un router	140
4.2.4	Verificación de la conectividad de redes conectadas directamente.....	149
4.3	Decisiones de Routing	158
4.3.1	Switching de paquetes entre redes.....	158
4.3.2	Determinación de ruta	171
4.4	Funcionamiento del router	176
4.4.1	Análisis de la tabla de Routing	176
4.4.2	Rutas conectadas directamente.....	179
4.4.3	Rutas descubiertas estáticamente	187
4.4.4	Protocolos de enrutamiento dinámico	193
4.5	Resumen.....	198
5	Enrutamiento entre VLAN.....	200
5.1	Introducción	200
5.2	Configuración del routing entre VLAN	201
5.2.1	Funcionamiento del routing entre VLAN	201
5.2.2	Configuración de routing entre VLAN antiguo	206
5.2.3	Configurar un enrutamiento router-on-a-stick entre VLAN.....	213
5.3	Resolución de problemas de routing entre VLAN.....	225
5.3.1	Problemas de configuración entre VLAN	225
5.3.2	Problemas de direccionamiento IP	230
5.4	Comutación de capa 3.....	234
5.4.1	Funcionamiento y configuración del switching de capa 3	234
5.5	Comutación de capa 3.....	247
5.5.1	Resolución de problemas de switching de capa 3	247
5.6	Resumen.....	248
6	Enrutamiento estático.....	250
6.1	Introducción	250
6.2	Implementación del routing estático.....	251
6.2.1	Enrutamiento estático.....	251
6.2.2	Tipos de rutas estáticas.....	255

6.3	Configuración de rutas estáticas y predeterminadas	259
6.3.1	Configuración de rutas estáticas IPv4	259
6.3.2	Configuración de rutas predeterminadas IPv4.....	271
6.3.3	Configuración de rutas estáticas IPv6	273
6.3.4	Configuración de rutas IPv6 predeterminadas	287
6.4	Revisión de CIDR y VLSM.....	291
6.4.1	Direccionamiento con clase	291
6.4.2	CIDR	296
6.4.3	VLSM.....	300
6.5	Configuración de rutas resumidas y estáticas flotantes	312
6.5.1	Configuración de rutas resumidas IPv4.....	312
6.5.2	Configuración de rutas resumidas IPv6.....	318
6.5.3	Configuración de rutas estáticas flotantes.....	324
6.6	Resolución de problemas de rutas estáticas y predeterminadas	329
6.6.1	Procesamiento de paquetes con rutas estáticas.....	329
6.6.2	Resolución de problemas de configuración de rutas estáticas y predeterminadas IPv4	331
6.7	Resumen.....	337
7	Routing dinámico	339
7.1	Introducción	339
7.2	Protocolos de enrutamiento dinámico	340
7.2.1	Funcionamiento del protocolo de enrutamiento dinámico.....	340
7.2.2	Comparación entre routing dinámico y estático.....	343
7.2.3	Aspectos básicos de la operación de los protocolos de routing	346
7.2.4	Tipos de protocolos de routing	352
7.3	Routing dinámico vector distancia.....	370
7.3.1	Funcionamiento del protocolo de enrutamiento vector distancia	370
7.3.2	Tipos de protocolos de routing vector distancia.....	372
7.4	Routing RIP y RIPng	375
7.4.1	Configuración del protocolo RIP.....	375
7.4.2	Configuración del protocolo RIPng.....	386
7.5	Routing dinámico de estado de enlace	390
7.5.1	Funcionamiento del protocolo de routing de estado de enlace	390

7.5.2	Actualizaciones de estado de enlace	394
7.5.3	Razones para utilizar protocolos de routing de estado de enlace	407
7.6	La tabla de routing	410
7.6.1	Partes de una entrada de ruta IPv4.....	410
7.6.2	Rutas IPv4 descubiertas en forma dinámica	415
7.6.3	Proceso de búsqueda de rutas IPv4	422
7.6.4	Análisis de una tabla de routing IPv6	424
7.7	Resumen.....	429
8	OSPF de área única.....	432
8.1	Introducción	432
8.2	Características de OSPF	433
8.2.1	Open Shortest Path First	433
8.2.2	Mensajes OSPF	443
8.2.3	Funcionamiento de OSPF	448
8.3	Configuración de OSPFv2 de área única	455
8.3.1	ID del router OSPF	455
8.3.2	Configuración de OSPFv2 de área única.....	461
8.3.3	Costo OSPF	466
8.4	Configuración de OSPFv3 de área única	478
8.4.1	Comparación de los protocolos OSPFv2 y OSPFv3.....	478
8.4.2	Configuración de OSPFv3	482
8.4.3	Verificación de OSPFv3.....	491
8.5	Resumen.....	493
9	Listas de control de acceso	495
9.1	Funcionamiento de ACL de IP	496
9.1.1	Propósito de los ACLs	496
9.1.2	Comparación entre ACL de IPv4 estándar y extendidas	504
9.1.3	Máscaras wildcard en ACL.....	506
9.1.4	Pautas para la creación de ACL	513
9.1.5	Pautas para la colocación de ACL.....	515
9.2	ACL de IPv4 estándar.....	520
9.2.1	Configuración de ACL de IPv4 estándar	520
9.2.2	Modificación de ACL de IPv4	531

9.2.3	Protección de puertos VTY con una ACL de IPv4 estándar	539
9.3	ACL de IPv4 extendidas	541
9.3.1	Estructura de una ACL de IPv4 extendida	541
9.3.2	Configuración de ACL de IPv4 extendidas	543
9.4	Resolución de problemas de ACL.....	550
9.4.1	Procesamiento de paquetes con ACL.....	550
9.4.2	Errores comunes de ACL	553
9.5	ACL de IPv6.....	558
9.5.1	Creación de ACL de IPv6.....	558
9.6	Resumen.....	568
10	DHCP.....	571
10.1	Introducción	571
10.2	Protocolo de configuración dinámica de host v4.....	572
10.2.1	Funcionamiento de DHCPv4.....	572
10.2.2	Configuración de un servidor de DHCPv4 básico	580
10.2.3	Configuración de cliente DHCPv4.....	590
10.2.4	Resolución de problemas de DHCPv4	592
10.3	Protocolo de configuración dinámica de host v6.....	596
10.3.1	SLAAC y DHCPv6	596
10.3.2	DHCPv6 sin estado	605
10.3.3	Servidor de DHCPv6 con estado.....	611
10.3.4	Resolución de problemas de DHCPv6	616
10.4	Resumen.....	620
11	Traducción de direcciones de red para IPv4 NAT.....	623
11.1	Introducción	623
11.2	Funcionamiento de NAT.....	624
11.2.1	Características de NAT	624
11.2.2	Tipos de NAT	630
11.2.3	Beneficios de NAT	637
11.3	Configuración de NAT estática	639
11.3.1	Configuración de NAT dinámica.....	644
11.3.2	Configuración de la traducción de la dirección del puerto (PAT).....	652
11.3.3	Reenvío de puertos	661

11.3.4 Configuración de NAT e IPv6	666
11.4 Resolución de problemas de NAT	669
11.5 Resumen.....	674

0 Bienvenido a Principios básicos de routing y switching

0.1 Mensaje para el estudiante

Bienvenido al curso Principios básicos de routing y switching de CCNA. El objetivo de este curso es presentar los conceptos y tecnologías básicos de red. Este material del curso en línea lo ayudará a desarrollar las aptitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones. Las habilidades específicas desarrolladas en cada capítulo se describen al comienzo de cada uno de ellos.

Puede utilizar un smartphone, una tablet PC, una computadora portátil o una computadora de escritorio para acceder al curso, participar en debates con su instructor, ver sus calificaciones, leer o revisar textos y practicar con medios interactivos. Sin embargo, algunos medios son complejos y se deben ver en una PC, al igual que las actividades de Packet Tracer, los cuestionarios y los exámenes.

Cuando participa en Networking Academy, se suma a una comunidad global conectada por tecnologías y objetivos en común. En el programa, participan escuelas, institutos de enseñanza superior, universidades y otras entidades de más de 160 países. En <http://www.academynetspace.com>, puede acceder a una visualización de la comunidad global de Networking Academy.

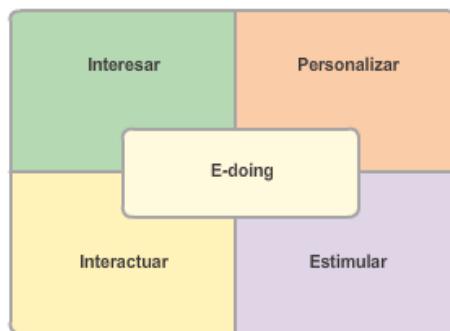
Busque el sitio oficial de Cisco Networking Academy en Facebook® y LinkedIn®. En el sitio de Facebook, puede encontrarse y relacionarse con otros estudiantes de Networking Academy de todo el mundo. El sitio de LinkedIn de Cisco Networking Academy lo conecta con ofertas de empleo, y puede ver la manera en que otras personas comunican sus aptitudes con eficacia.

El entorno de aprendizaje NetSpace es una parte importante de la experiencia general del curso para los alumnos e instructores de Networking Academy. Este material de curso en línea incluye el texto del curso y medios interactivos relacionados, actividades de simulación de Packet Tracer, prácticas de laboratorio con equipos reales, prácticas de laboratorio de acceso remoto y muchos tipos de cuestionarios diferentes. Este material proporciona comentarios pertinentes para ayudarlo a evaluar su progreso a lo largo del curso.

El material de este curso abarca una amplia variedad de tecnologías que facilitan la manera en la que las personas trabajan, viven, juegan y aprenden mediante comunicaciones de voz, video y otros datos. Las tecnologías de red e Internet afectan a las personas de distintas maneras en diferentes partes del mundo. Si bien trabajamos con instructores de todo el mundo para crear este material, es importante que trabaje con su instructor y sus compañeros de curso para asegurarse de que el contenido del curso se aplique a su situación local.

E-doing es una filosofía de diseño que aplica el principio de que se aprende mejor a través de la práctica. El currículo incluye actividades integradas y altamente interactivas de e-doing para ayudar a estimular el aprendizaje, aumentar la retención de conocimientos y enriquecer mucho más la experiencia integral de aprendizaje, lo que facilita mucho la comprensión de los contenidos.

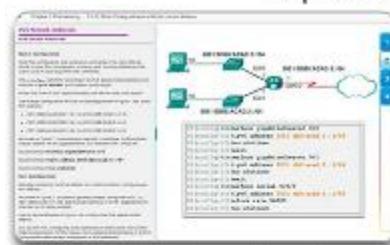
Cómo enseñamos



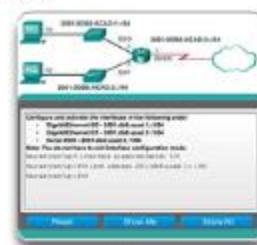
En una clase típica, después de estudiar un tema por primera vez, evaluará su comprensión con algunos elementos de medios interactivos. Si se deben aprender comandos nuevos, los practicará con el verificador de sintaxis antes de utilizarlos para configurar una red o llevar a cabo la resolución de problemas de una red en Packet Tracer, la herramienta de simulación de redes de Networking Academy. Luego, realizará actividades de práctica en equipos reales en el aula o mediante el acceso remoto por Internet.

Además, Packet Tracer le permite crear sus propias actividades para realizar prácticas adicionales en cualquier momento. También puede evaluar sus aptitudes en forma competitiva con sus compañeros de curso mediante juegos multiusuario. Las evaluaciones de habilidades y las prácticas de laboratorio de habilidades de integración de Packet Tracer le proporcionan sugerencias muy útiles sobre las capacidades que demuestra y son una excelente práctica para los exámenes de capítulos, de control y finales.

La práctica hace al maestro



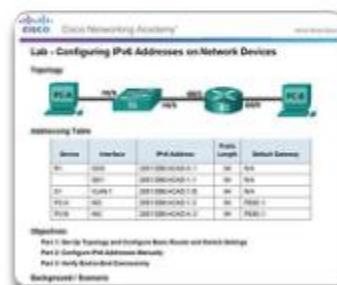
1. Mostrar: ejemplos prácticos (con texto y medios)



2. Probar: prácticas (con verificador de sintaxis)



3. Hacer: ejemplo práctico parcial (con Packet Tracer o equipos reales)



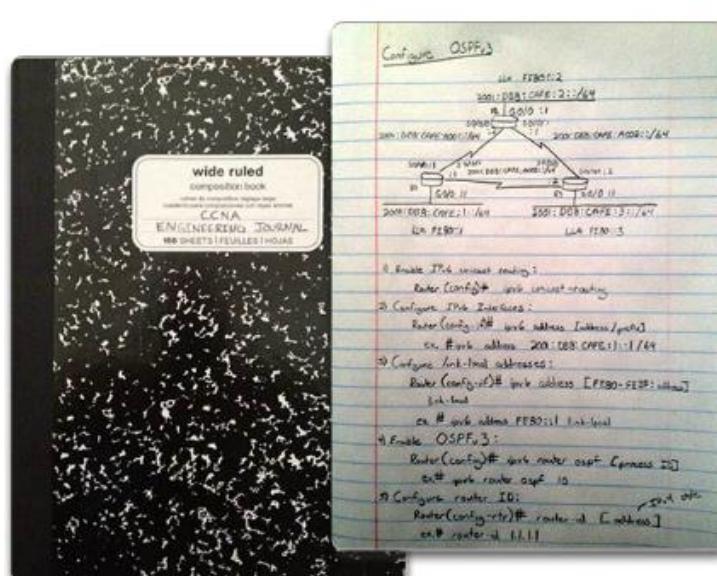
4. Sintetizar: resolución de problemas (con Packet Tracer o equipos reales)

Un objetivo importante de la capacitación es enriquecerlo a usted, el alumno, al ampliar lo que sabe y lo que puede hacer. No obstante, es importante tener en cuenta que el material de capacitación y el instructor solo pueden facilitar el proceso. Usted debe comprometerse a aprender nuevas aptitudes. En las siguientes páginas, se comparten algunas sugerencias para ayudarlo a aprender y a prepararse para trasladar sus nuevas aptitudes al lugar de trabajo.

Los profesionales del ámbito de redes suelen llevar diarios de ingeniería en los que anotan lo que observan y aprenden, por ejemplo, cómo utilizar protocolos y comandos. Llevar un diario de ingeniería crea una referencia que puede utilizar en su trabajo de ICT. Escribir —junto con leer, ver y practicar— es una forma de reforzar el aprendizaje.

Una entrada de muestra sobre la implementación de una tecnología podría incluir los comandos de software necesarios, el propósito de los comandos, las variables de comandos y un diagrama de topología que indique el contexto en el que se utilizan los comandos para configurar la tecnología.

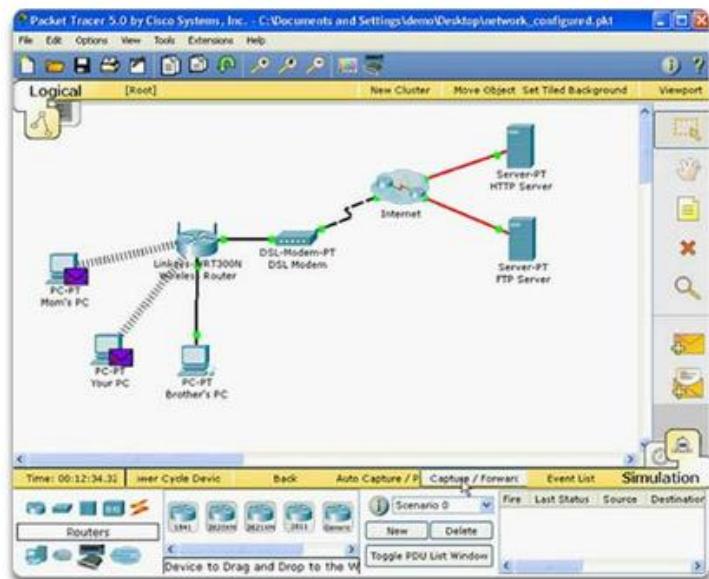
Diarios de ingeniería



Packet Tracer es una herramienta de aprendizaje de redes que admite una amplia gama de simulaciones físicas y lógicas. También proporciona herramientas de visualización para ayudarlo a comprender el funcionamiento interno de una red.

Las actividades ya preparadas de Packet Tracer constan de simulaciones de red, juegos, actividades y desafíos que proporcionan una amplia gama de experiencias de aprendizaje. Estas herramientas lo ayudarán a comprender la forma en que los datos fluyen en una red.

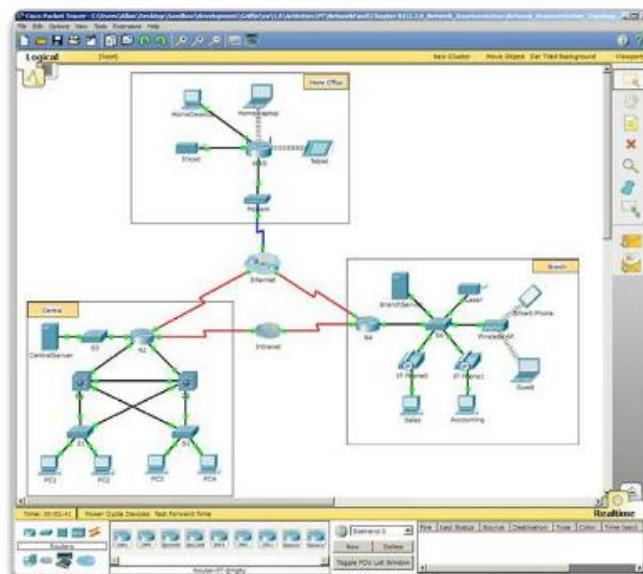
Exploración del mundo de las redes



También puede utilizar Packet Tracer para crear sus propios experimentos y situaciones de redes. Esperamos que, con el tiempo, considere la opción de utilizar Packet Tracer no solo para probar las actividades prediseñadas, sino también para crear, explorar y experimentar.

El material del curso en línea tiene actividades de Packet Tracer incorporadas que se pueden iniciar en PC con sistemas operativos Windows®, si Packet Tracer está instalado. Esta integración también puede funcionar en otros sistemas operativos que usan la emulación de Windows.

Cree sus propios mundos



Juegos educativos

Los juegos multiusuario de Packet Tracer le permiten a usted o a un equipo competir con otros estudiantes para ver quiénes pueden completar una serie de tareas de redes de la manera correcta.

y con la mayor rapidez. Es una excelente manera de practicar las habilidades que se aprenden con las actividades y las prácticas de laboratorio de Packet Tracer.

Cisco Aspire es un juego de simulación estratégico y autónomo para un solo jugador. Los jugadores prueban sus aptitudes de redes cumpliendo contratos en una ciudad virtual. La edición para Networking Academy se diseñó específicamente para ayudarlo a prepararse para el examen de certificación CCENT. También incorpora aptitudes para la comunicación y habilidades comerciales que los empleadores de la industria de ICT buscan en los postulantes.

Evaluaciones de Performance-Based

Las evaluaciones basadas en el rendimiento de Networking Academy le permiten realizar las actividades de Packet Tracer como siempre lo hizo, solo que ahora incorporan un motor de evaluación en línea que califica los resultados en forma automática y le proporciona comentarios inmediatos. Estos comentarios lo ayudan a identificar con mayor precisión los conocimientos y las aptitudes que logró dominar y aquello que necesita seguir practicando. En los cuestionarios y los exámenes de los capítulos, también hay preguntas que utilizan las actividades de Packet Tracer para proporcionarle comentarios adicionales con respecto a su progreso.

Tal como indica el título, este curso se centra en el aprendizaje de la arquitectura, los componentes y el funcionamiento de los routers y switches en una red pequeña. En este curso, aprenderá a configurar un router y un switch para obtener funcionalidad básica. En este curso:

- Describirá las tecnologías de switching mejoradas, como las VLAN, el protocolo de enlace troncal de VLAN (VTP), el protocolo de árbol de expansión rápido (RSTP), el protocolo de árbol de expansión por VLAN (PVSTP) y 802.1q.
- Configurará las operaciones básicas de una red comutada pequeña y resolverá problemas relacionados.
- Configurará y verificará el routing estático y el routing predeterminado.
- Configurará las operaciones básicas de los routers en una red enrutada pequeña, y resolverá problemas relacionados.
- Configurará VLAN y el routing entre VLAN, y resolverá problemas relacionados.
- Configurará y controlará ACL para IPv4 e IPv6, y resolverá problemas relacionados.
- Configurará y controlará ACL para IPv4 e IPv6, y resolverá problemas relacionados.

Al final de este curso, podrá configurar routers y switches, y resolver problemas relacionados, así como solucionar problemas frecuentes de RIPv1, de RIPv2, de OSPF de área única y OSPF multiárea, de LAN virtuales y de routing entre VLAN en redes IPv4 e IPv6.

1 Introducción a redes conmutadas

1.1 Introducción

Las redes modernas continúan evolucionando para adaptarse a la manera cambiante en que las organizaciones realizan sus actividades diarias. Ahora los usuarios esperan tener acceso instantáneo a los recursos de una compañía, en cualquier momento y en cualquier lugar. Estos recursos incluyen no solo datos tradicionales, sino también de video y de voz. También hay una necesidad creciente de tecnologías de colaboración que permitan el intercambio de recursos en tiempo real entre varias personas en sitios remotos como si estuvieran en la misma ubicación física.

Los distintos dispositivos deben trabajar en conjunto sin inconvenientes para proporcionar una conexión rápida, segura y confiable entre los hosts. Los switches LAN proporcionan el punto de conexión a la red empresarial para los usuarios finales y también son los principales responsables del control de la información dentro del entorno LAN. Los routers facilitan la transmisión de información entre redes LAN y, en general, desconocen a los hosts individuales. Todos los servicios avanzados dependen de la disponibilidad de una infraestructura sólida de routing y switching sobre la que se puedan basar. Esta infraestructura se debe diseñar, implementar y administrar cuidadosamente para proporcionar una plataforma estable necesaria.

En este capítulo, se comienza con un examen del flujo de tráfico en una red moderna. Se examinan algunos de los modelos actuales de diseño de red y el modo en que los switches LAN crean tablas de reenvío y usan la información de direcciones MAC para conmutar datos entre los hosts de forma eficaz.

Después de completar este capítulo, podrá hacer lo siguiente:

- Describir la convergencia de datos, voz y video en el contexto de las redes conmutadas.
- Describir una red conmutada en una pequeña a mediana empresa.
- Explicar el proceso de reenvío de tramas en una red conmutada.
- Comparar un dominio de colisiones con un dominio de difusión.

Enviar o recibir (instrucciones)

Analice de manera individual o grupal (según lo decida el instructor) las diversas formas en que los hosts envían y reciben datos, voz y transmisión de video.

Desarrolle una matriz (tabla) donde se enumeren los tipos de datos de red que se pueden enviar y recibir. Proporcione cinco ejemplos.

Nota: para ver un ejemplo de la matriz, consulte el documento elaborado para esta actividad de creación de modelos.

Conserve una copia impresa o electrónica de su trabajo. Esté preparado para explicar la matriz y las afirmaciones en clase.



Los switches funcionan para proporcionar...

- Calidad de servicio
- Transferencia de datos de voz y de video
- Seguridad

1.2 Diseño de la LAN

1.2.1 Redes convergentes

El mundo digital está cambiando. La capacidad de acceder a Internet y a la red corporativa ya no se limita a oficinas físicas, ubicaciones geográficas o zonas horarias. En el lugar de trabajo globalizado actual, los empleados pueden acceder a los recursos desde cualquier lugar del mundo, y la información debe estar disponible en cualquier momento y en cualquier dispositivo, como se muestra en la figura 1. Estos requisitos impulsan la necesidad de armar redes de última generación que sean seguras, confiables y de alta disponibilidad.

Estas redes de última generación no solo deben ser compatibles con las expectativas y el equipamiento actuales, sino que también deben ser capaces de integrar plataformas antiguas. En la figura 2, se muestran algunos dispositivos antiguos comunes que con frecuencia se deben incorporar al diseño de red. En la figura 3, se muestran algunas de las plataformas más modernas (redes convergentes) que contribuyen a proporcionar el acceso a la red en cualquier momento, en cualquier lugar y en cualquier dispositivo.





Para admitir la colaboración, las redes comerciales emplean soluciones convergentes mediante sistemas de voz, teléfonos IP, gateways de voz, soporte de video y videoconferencias (figura 1). Las redes convergentes con soporte de colaboración, incluidas las de servicio de datos, pueden incluir características como las siguientes:

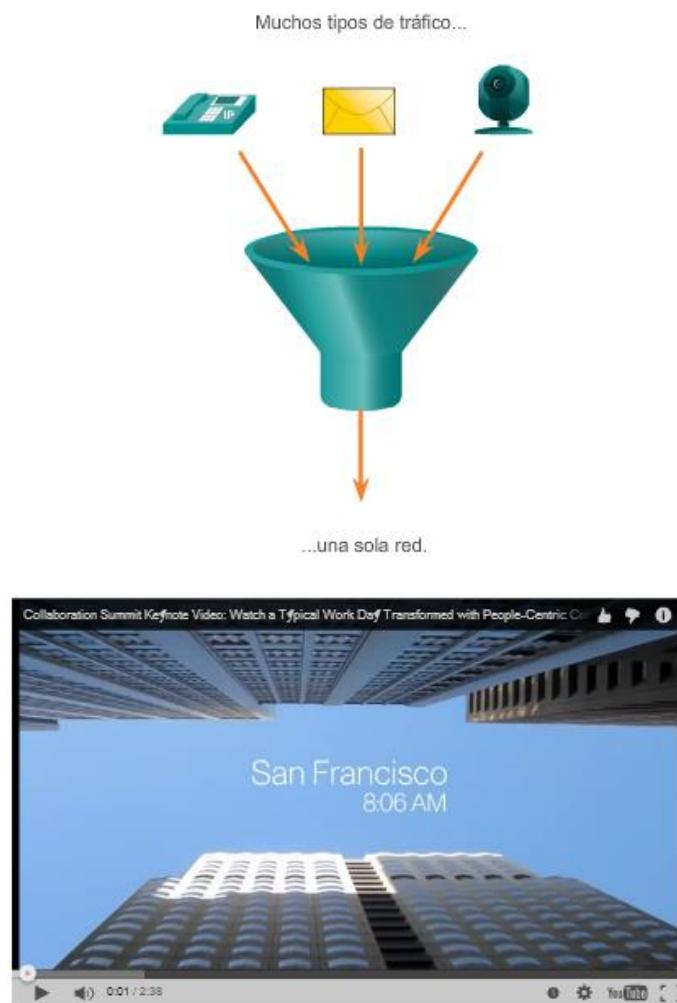
- **Control de llamadas:** procesamiento de llamadas telefónicas, identificador de llamadas, transferencia de llamadas, llamadas en espera y conferencias.
- **Mensajería de voz:** correo de voz.
- **Movilidad:** recepción de llamadas importantes en cualquier lugar.
- **Contestador automático:** se atiende a los clientes con mayor rapidez, ya que las llamadas se enrutan directamente al departamento o a la persona que corresponde.

Uno de los principales beneficios de la transición hacia una red convergente es que se debe instalar y administrar una sola red física. Esto permite ahorrar de manera considerable en la

instalación y la administración de las redes de voz, de video y de datos independientes. Estas soluciones de redes convergentes integran la administración de TI para que cada movimiento, adición y modificación se complete con una interfaz de administración intuitiva. Además, las soluciones de redes convergentes admiten las aplicaciones de softphone para PC, así como de video punto a punto, de modo que los usuarios puedan disfrutar de las comunicaciones personales con la misma facilidad de administración y de uso de una llamada de voz.

La convergencia de servicios en la red dio lugar a una evolución de las redes, de la función tradicional de transporte de datos a una gran autopista para la comunicación de datos, voz y video. Esta red física se debe diseñar e implementar correctamente para permitir el manejo confiable de los diversos tipos de información que debe transportar. Para permitir la administración de este entorno complejo, se requiere un diseño estructurado.

En la figura 2, reproduzca el video para ver algunos de los servicios de colaboración en acción.



Video: https://www.youtube.com/watch?feature=player_embedded&v=DTHHzSKdcaA

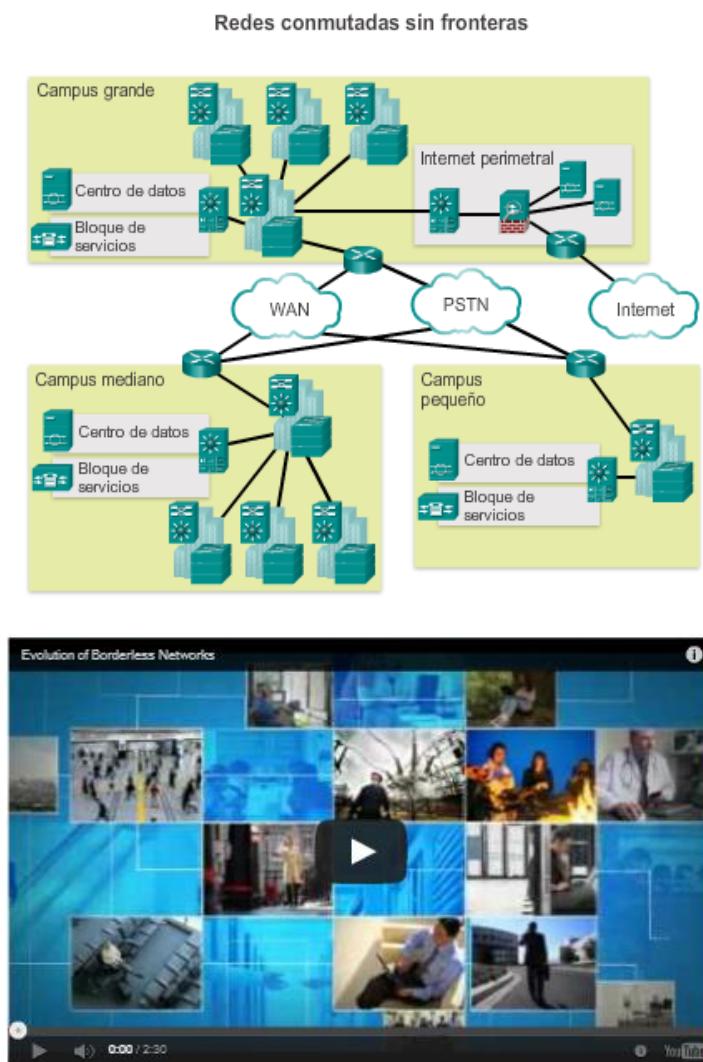
Con las crecientes demandas de las redes convergentes, la red se debe desarrollar con un enfoque arquitectónico que integre inteligencia, simplifique las operaciones y sea escalable para

satisfacer demandas futuras. La arquitectura Cisco Borderless Network, la cual se muestra en la figura 1, es un ejemplo de uno de los últimos desarrollos del diseño de red.

Cisco Borderless Network es una arquitectura de red que combina varias innovaciones y consideraciones de diseño para permitir que las organizaciones se conecten con cualquier persona, en cualquier lugar, en cualquier momento y en cualquier dispositivo de forma segura, con confianza y sin inconvenientes. Esta arquitectura está diseñada para enfrentar los desafíos comerciales y de TI, como la admisión de redes convergentes y el cambio de los patrones de trabajo.

La arquitectura Cisco Borderless Network se construye sobre una infraestructura de hardware y software escalable y resistente. Esta arquitectura permite que distintos elementos, desde switches de acceso hasta puntos de acceso inalámbrico, funcionen conjuntamente y permitan a los usuarios acceder a los recursos en cualquier momento y lugar, lo que proporciona optimización, escalabilidad y seguridad a la colaboración y la virtualización.

En la figura 2, reproduzca el video para conocer más sobre la evolución de Cisco Borderless Network.



Video: https://www.youtube.com/watch?feature=player_embedded&v=lCg2HctqvJE

La creación de una red conmutada sin fronteras requiere el uso de principios de diseño de red sólidos para asegurar la máxima disponibilidad, flexibilidad, seguridad y facilidad de administración. Las redes conmutadas sin fronteras deben funcionar según los requisitos actuales y los servicios y las tecnologías que se requerirán en el futuro. Las pautas de diseño de las redes conmutadas sin fronteras se basan en los siguientes principios:

- **Jerárquico:** facilita la comprensión de la función de cada dispositivo en cada nivel, simplifica la implementación, el funcionamiento y la administración, y reduce los dominios de error en cada nivel.
- **Modularidad:** permite la expansión de la red y la habilitación de servicios integrados sin inconvenientes y a petición.
- **Resistencia:** satisface las expectativas del usuario al mantener la red siempre activa.
- **Flexibilidad:** permite compartir la carga de tráfico de forma inteligente mediante el uso de todos los recursos de red.

Estos no son principios independientes. Es fundamental comprender cómo encaja cada principio en el contexto de los demás. El diseño jerárquico de una red conmutada sin fronteras sienta una base que permite que los diseñadores de red superpongan las características de seguridad, movilidad y comunicación unificada. Los modelos de capas de tres y dos niveles, como los que se muestran en la ilustración, son marcos de diseño jerárquico doblemente comprobados para las redes de campus.

Las tres capas fundamentales dentro de estos diseños con niveles son las capas de acceso, de distribución y de núcleo. Cada capa se puede considerar como un módulo estructurado bien definido, con funciones y roles específicos en la red de campus. La introducción de la modularidad en el diseño jerárquico de campus asegura aún más que la red de campus mantenga la resistencia y la flexibilidad suficientes para proporcionar servicios de red fundamentales. La modularidad también permite el crecimiento y los cambios que ocurren con el tiempo.

Capa de acceso

La capa de acceso representa el perímetro de la red, por donde entra o sale el tráfico de la red de campus. Tradicionalmente, la función principal de los switches de capa de acceso es proporcionar acceso de red al usuario. Los switches de capa de acceso se conectan a los switches de capa de distribución, que implementan tecnologías de base de red como el routing, la calidad de servicio y la seguridad.

Para satisfacer las demandas de las aplicaciones de red y de los usuarios finales, las plataformas de switching de última generación ahora proporcionan servicios más convergentes, integrados e inteligentes a diversos tipos de terminales en el perímetro de la red. La incorporación de inteligencia en los switches de capa de acceso permite que las aplicaciones funcionen de manera más eficaz y segura en la red.

Capa de distribución

La capa de distribución interactúa entre la capa de acceso y la capa de núcleo para proporcionar muchas funciones importantes, incluidas las siguientes:

- Agregar redes de armario de cableado a gran escala.

- Agregar dominios de difusión de capa 2 y límites de routing de capa 3.
- Proporcionar funciones inteligentes de switching, de routing y de política de acceso a la red para acceder al resto de la red.
- Proporcionar una alta disponibilidad al usuario final mediante los switches de capa de distribución redundantes, y rutas de igual costo al núcleo.
- Proporcionar servicios diferenciados a distintas clases de aplicaciones de servicio en el perímetro de la red.

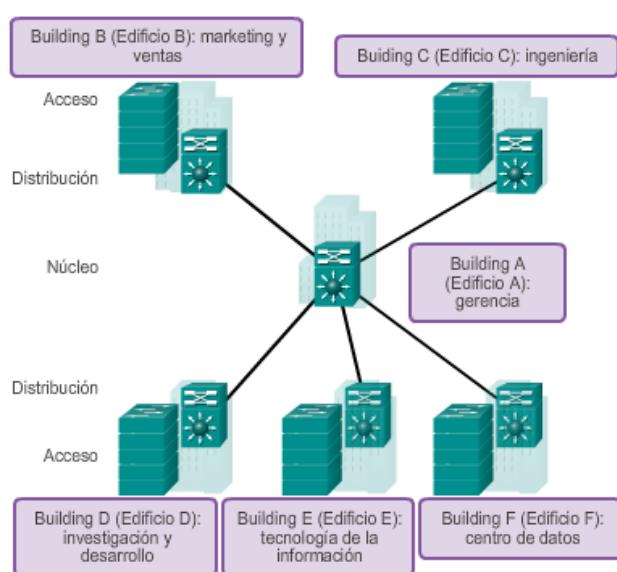
Capa núcleo

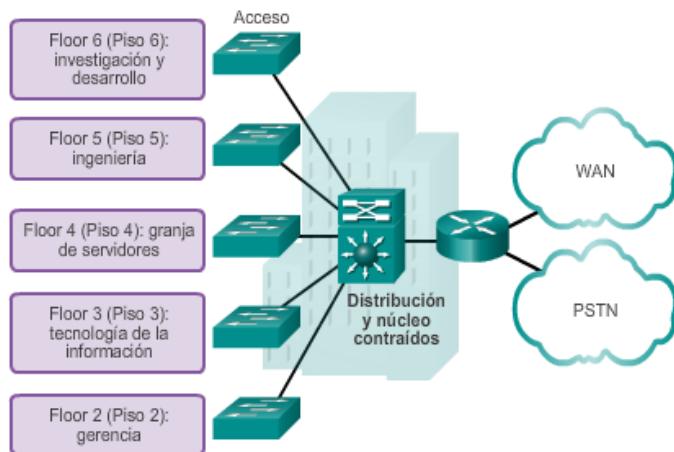
La capa de núcleo es el backbone de una red. Esta conecta varias capas de la red de campus. La capa de núcleo funciona como agregador para el resto de los bloques de campus y une el campus con el resto de la red. El propósito principal de la capa de núcleo es proporcionar el aislamiento de fallas y la conectividad de backbone de alta velocidad.

En la figura 1, se muestra un diseño de red de campus de tres niveles para organizaciones donde las capas de acceso, de distribución y de núcleo están separadas. Para armar un diseño de disposición de cables físicos simplificado, escalable, rentable y eficaz, se recomienda armar una topología de red física en estrella extendida desde una ubicación central en un edificio hacia el resto de los edificios en el mismo campus.

En algunos casos, debido a la falta de restricciones físicas o de escalabilidad de la red, no es necesario mantener las capas de distribución y de núcleo separadas. En las ubicaciones de campus más pequeñas donde hay menos usuarios que acceden a la red, o en los sitios de campus que constan de un único edificio, puede no ser necesario que las capas de núcleo y de distribución estén separadas. En esta situación, la recomendación es el diseño alternativo de red de campus de dos niveles, también conocido como “diseño de red de núcleo contraído”.

En la figura 2, se muestra un ejemplo de diseño de red de campus de dos niveles para un campus empresarial donde las capas de distribución y de núcleo se contraen en una única capa.





	Jerárquico	Modularidad	Capacidad de recuperación	Flexibilidad
Permite que la red siempre sea accesible.			✓	
Permite que las redes se expandan y proporcionen servicios a pedido.		✓		
Contribuye a que cada dispositivo de cada nivel cumpla una función específica.	✓			
Usa todos los recursos de red disponibles para compartir la carga de tráfico de datos.				✓

Capa núcleo	Capa de distribución	Capa de acceso
<p>Área backbone de red para el switching.</p> <p>Proporciona aislamiento de fallas y conectividad backbone de switch de alta velocidad.</p> <p>Puede combinarse con la capa de distribución para proporcionar un diseño contraido.</p>	<p>Admite dominios de difusión de capa 2 y límites de routing de capa 3.</p> <p>Permite que los datos fluyan en rutas de switching de igual costo al backbone.</p> <p>Incluye la redundancia como característica importante para el acceso a las redes commutadas.</p> <p>Interactúa con el backbone y los usuarios para proporcionar switching, routing y seguridad inteligentes.</p>	<p>Contribuye a que las aplicaciones funcionen en la red conmutada de forma más segura.</p> <p>Proporciona una conectividad directa y de red conmutada al usuario</p>

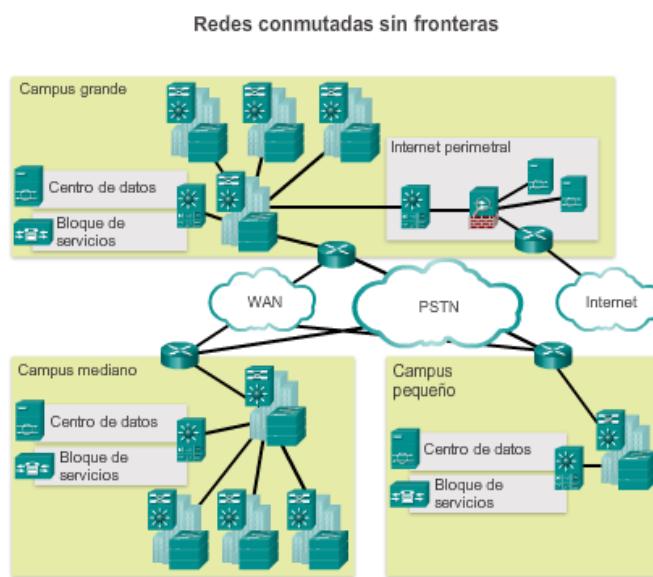
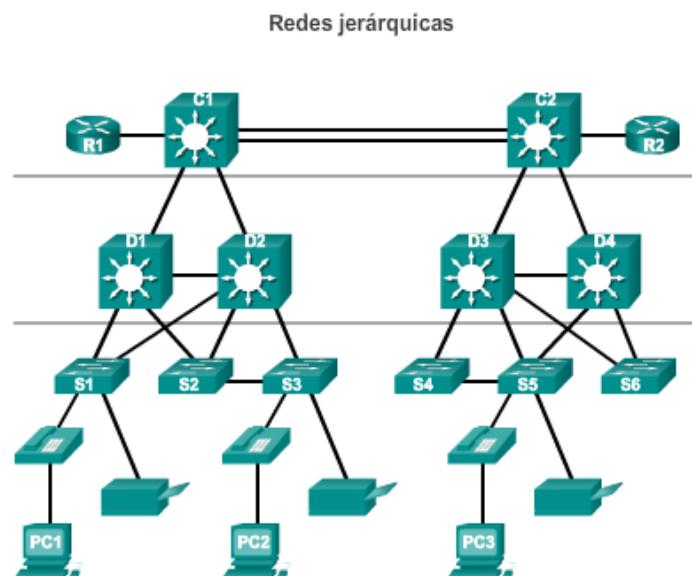
1.2.2 Redes conmutadas

La función de las redes conmutadas evolucionó notablemente en las dos últimas décadas. No hace mucho tiempo, las redes conmutadas planas de capa 2 eran lo habitual. Las redes de datos planas de capa 2 dependían de las propiedades básicas de Ethernet y del uso generalizado de los repetidores hub para propagar el tráfico LAN a través de una organización. Como se muestra en la figura 1, las redes se cambiaron básicamente por LAN conmutadas en las redes jerárquicas. Las

LAN comutadas brindan más flexibilidad, administración de tráfico y características adicionales, como las siguientes:

- Calidad de servicio
- Seguridad adicional
- Compatibilidad con tecnología de redes y conectividad inalámbricas
- Compatibilidad con tecnologías nuevas, como la telefonía IP y los servicios de movilidad

En la figura 2, se muestra el diseño jerárquico utilizado en las redes comutadas sin fronteras.



En las redes comerciales, se usan diversos tipos de switches: Es importante implementar los tipos de switches adecuados según los requisitos de la red. En la figura 1, se destacan algunas

consideraciones comerciales comunes que se deben tener en cuenta al seleccionar el equipo de switch.

Cuando se selecciona el tipo de switch, el diseñador de red debe elegir entre una configuración fija o una modular, y entre un dispositivo apilable o no apilable. Otra consideración es el grosor del switch, expresado en cantidad de unidades de rack. Esto es importante para los switches que se montan en un rack. Por ejemplo, los switches de configuración fija que se muestran en la figura 2 son todos de 1 unidad de rack (1U). Con frecuencia estas opciones se denominan factores de forma del switch.

Switches de configuración fija

Los switches de configuración fija no admiten características u opciones más allá de las que vienen originalmente con el switch (figura 2). El modelo específico determina las características y opciones disponibles. Por ejemplo, un switch gigabit fijo de 24 puertos no admite puertos adicionales. En general, existen diferentes opciones de configuración que varían según la cantidad y el tipo de puertos incluidos en un switch de configuración fija.

Switches de configuración modular

Los switches de configuración modular ofrecen más flexibilidad en su configuración. Generalmente, estos switches vienen con bastidores de diferentes tamaños que permiten la instalación de diferentes números de tarjetas de líneas modulares (figura 3). Las tarjetas de línea son las que contienen los puertos. La tarjeta de línea se ajusta al bastidor del switch de igual manera que las tarjetas de expansión se ajustan en la computadora. Cuanto más grande es el chasis, más módulos puede admitir. Es posible elegir entre muchos tamaños de bastidores diferentes. Un switch modular con una tarjeta de línea de 24 puertos admite una tarjeta de línea de 24 puertos adicional para hacer que la cantidad total de puertos ascienda a 48.

Switches de configuración apilable

Los switches de configuración apilable se pueden interconectar mediante un cable especial que proporciona un rendimiento de ancho de banda alto entre los switches (figura 4). La tecnología Cisco StackWise permite la interconexión de hasta nueve switches. Los switches se pueden apilar unos sobre otros con cables que conectan los switches en forma de cadena margarita. Los switches apilados operan con efectividad como un switch único más grande. Los switches apilables son convenientes cuando la tolerancia a fallas y la disponibilidad de ancho de banda son críticas y resulta costoso implementar un switch modular. El uso de conexiones cruzadas hace que la red pueda recuperarse rápidamente si falla un switch único. Los switches apilables usan un puerto especial para las interconexiones. Muchos switches apilables Cisco también admiten la tecnología StackPower, que permite compartir la alimentación entre los miembros de la pila.

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.

Switches de configuración fija



Las características y las opciones se limitan a aquéllas que originalmente vienen con el switch.

Switches de configuración modular



El chasis acepta tarjetas de línea que contienen los puertos.

Switches de configuración apilable



Los switches apilables, conectados por un cable especial, operan con eficacia como un gran switch.

Nombre de la categoría	Criterios de selección de switch
Densidad del puerto	Se ve afectado por la cantidad de dispositivos de red que debe admitir.
Alimentación	Redundancia mediante alimentación por Ethernet.
Velocidad del puerto	La velocidad con la que las interfaces procesan los datos de red.
Confiabilidad	Acceso continuo a la red.
Precio	Se ve afectado por la cantidad de interfaces, las características y la capacidad de expansión.
Buffers para tramas	La capacidad de almacenar tramas en la caché.
Escalabilidad	La capacidad de adaptarse al aumento de la cantidad de usuarios de la red.
Modulares	Switches con tarjetas de línea y de puerto de switching ajustables.
Configuración fija	Switches con características u opciones preestablecidas.
Apilable	Switches agrupados en cadena margarita con rendimiento de ancho de banda alto.

1.3 El entorno comutado

1.3.1 Reenvío de tramas

El concepto de switching y reenvío de tramas es universal en la tecnología de redes y en las telecomunicaciones. En las redes LAN, WAN y en la red pública de telefonía comutada (PSTN), se usan diversos tipos de switches. El concepto fundamental de switching hace referencia a un dispositivo que toma una decisión según dos criterios:

- Puerto de entrada
- Dirección de destino

La decisión sobre cómo un switch reenvía el tráfico se toma en relación con el flujo de ese tráfico. El término “entrada” se usa para describir el lugar de un puerto por donde ingresa una trama al dispositivo. El término “salida” se usa para describir las tramas que salen del dispositivo desde un puerto determinado.

Cuando un switch toma una decisión, lo hace sobre la base del puerto de entrada y la dirección de destino del mensaje.

Los switches LAN mantienen una tabla que usan para determinar cómo reenviar el tráfico a través del switch. Haga clic en el botón Reproducir de la ilustración para ver una animación del proceso de switching. En este ejemplo:

- Si un mensaje ingresa al puerto 1 del switch y la dirección de destino es EA, el switch reenvía el tráfico por el puerto 4.
- Si un mensaje ingresa al puerto 5 del switch y la dirección de destino es EE, el switch reenvía el tráfico por el puerto 1.
- Si un mensaje ingresa al puerto 3 del switch y la dirección de destino es AB, el switch reenvía el tráfico por el puerto 6.

La única inteligencia que poseen los switches LAN es la capacidad de usar la tabla para reenviar el tráfico según el puerto de entrada y la dirección de destino de un mensaje. Con los switches LAN, hay solamente una tabla de switching principal que describe una asociación estricta entre las direcciones y los puertos; por lo tanto, un mensaje con una dirección de destino determinada siempre sale por el mismo puerto de salida, independientemente del puerto de entrada por el que ingresa.

Los switches LAN Cisco reenvían tramas de Ethernet según la dirección MAC de destino de las tramas.

Los switches usan direcciones MAC para dirigir las comunicaciones de red a través del switch al puerto correspondiente hacia el destino. Un switch se compone de circuitos integrados y del software complementario que controla las rutas de datos a través del switch. Para definir qué puerto usar para transmitir una trama, el switch primero debe saber qué dispositivos existen en cada puerto. A medida que el switch descubre la relación entre puertos y dispositivos, crea una tabla denominada “tabla de direcciones MAC” o “tabla de memoria de contenido direccionable” (CAM). CAM es un tipo de memoria especial que se usa en las aplicaciones de búsqueda de alta velocidad.

Los switches LAN determinan cómo manejar las tramas de datos entrantes mediante una tabla de direcciones MAC. El switch genera la tabla de direcciones MAC mediante el registro de la dirección MAC de cada dispositivo conectado a cada uno de los puertos. El switch usa la información de la tabla de direcciones MAC para enviar las tramas destinadas a un dispositivo específico por el puerto que se asignó a ese dispositivo.

El switch completa la tabla de direcciones MAC según las direcciones MAC de origen. Cuando el switch recibe una trama entrante con una dirección MAC de destino que no figura en la tabla de direcciones MAC, este reenvía la trama por todos los puertos (saturación), excepto el puerto de entrada de la trama. Cuando el dispositivo de destino responde, el switch agrega la dirección MAC de origen de la trama y el puerto por donde se recibió la trama a la tabla de direcciones MAC. En las redes que cuentan con varios switches interconectados, la tabla de direcciones MAC contiene varias direcciones MAC para un único puerto conectado a los otros switches.

Los siguientes pasos describen el proceso de creación de una tabla de direcciones MAC:

1. El switch recibe una trama de la PC 1 en el puerto 1 (figura 1).
2. El switch examina la dirección MAC de origen y la compara con la tabla de direcciones MAC.
 - Si la dirección no está en la tabla de direcciones MAC, el switch asocia la dirección MAC de origen de la PC 1 al puerto de entrada (puerto 1) en la tabla de direcciones MAC (figura 2).
 - Si la tabla de direcciones MAC ya contiene una entrada para esa dirección de origen, restablece el temporizador de vencimiento. Por lo general, las entradas para las direcciones MAC se guardan durante cinco minutos.
3. Una vez que el switch registró la información de la dirección de origen, examina la dirección MAC de destino.

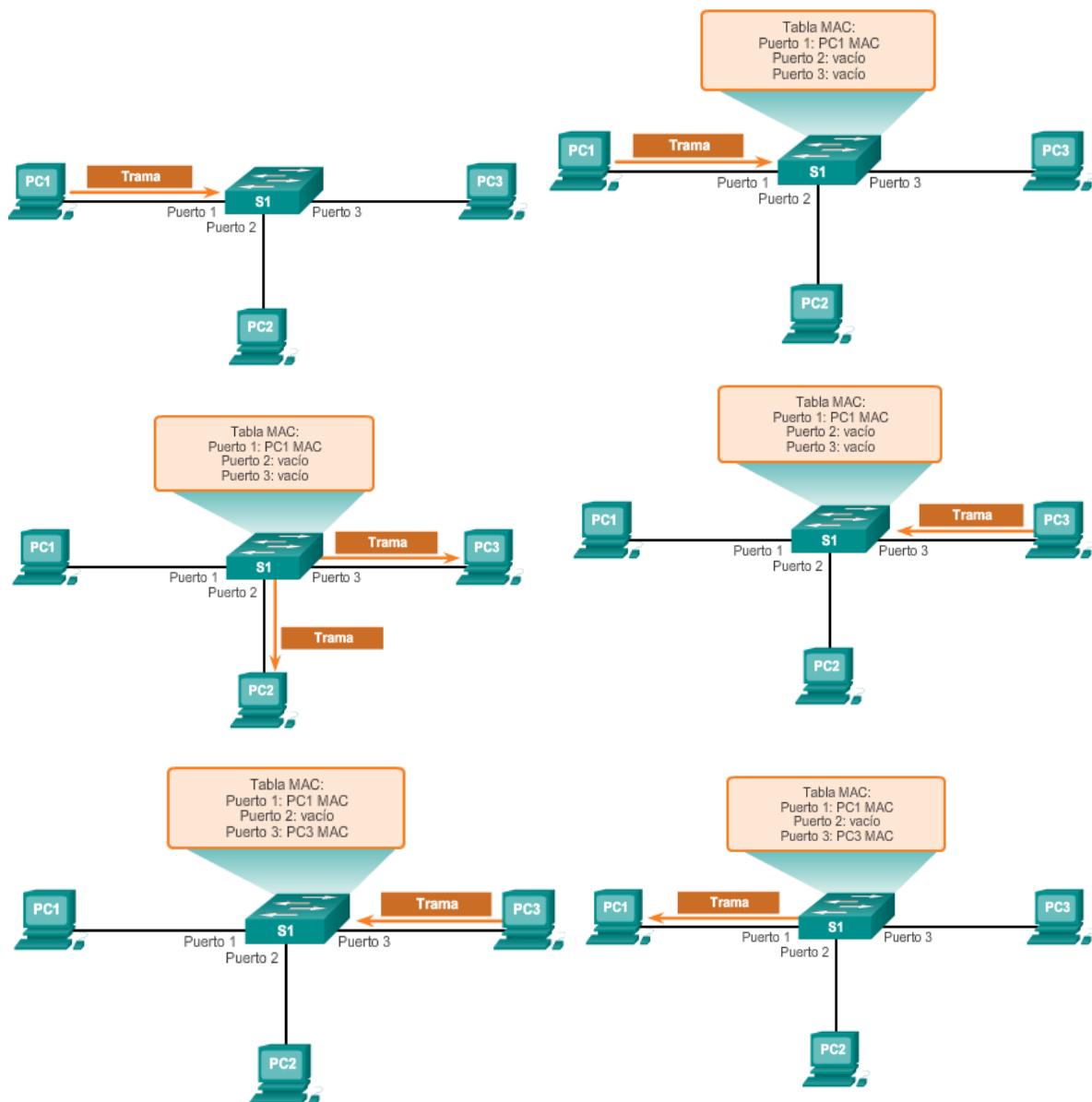
- Si la dirección de destino no figura en la tabla MAC o si es una dirección MAC de difusión, indicada por todas letras F, el switch satura todos los puertos con la trama, excepto el puerto de entrada (figura 3).

4. El dispositivo de destino (PC 3) responde a la trama con una trama de unidifusión dirigida a la PC 1 (figura 4).

5. El switch incorpora la dirección MAC de origen de la PC 3 y el número de puerto de entrada a la tabla de direcciones. En la tabla de direcciones MAC, se encuentran la dirección de destino de la trama y el puerto de salida asociado (figura 5).

6. Ahora el switch puede reenviar tramas entre estos dispositivos de origen y destino sin saturación, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados (figura 6).

Direccionamiento MAC y Tablas MAC de los switches

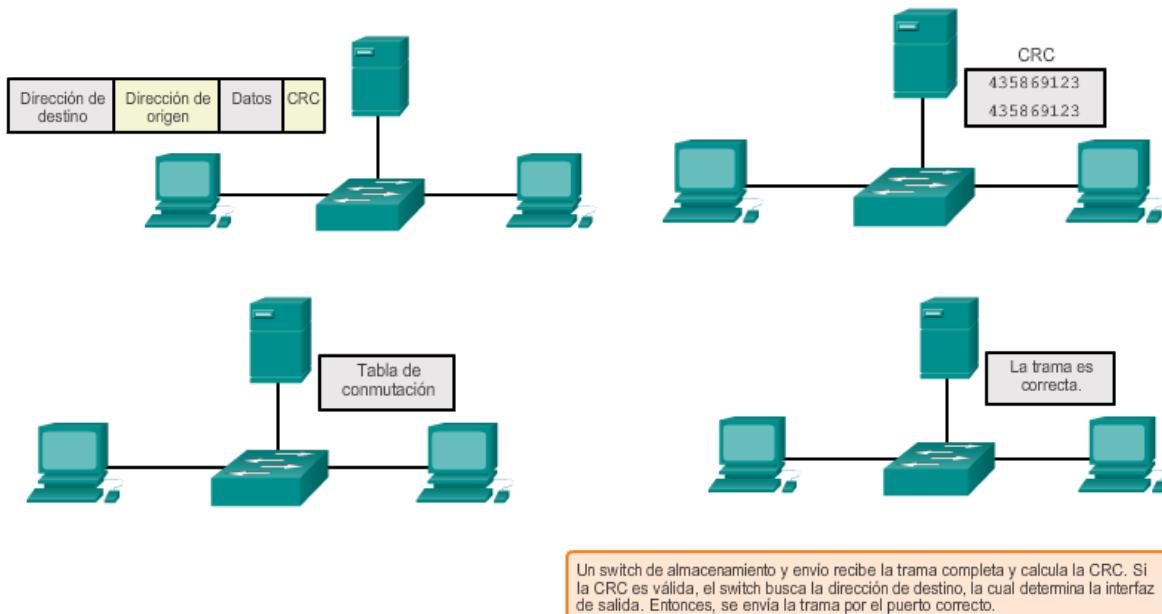


A medida que las redes fueron creciendo y las empresas comenzaron a experimentar un rendimiento de la red más lento, se agregaron puentes Ethernet (una versión anterior del switch) a las redes para limitar el tamaño de los dominios de colisiones. En la década de los noventa, los avances en las tecnologías de circuitos integrados permitieron que los switches LAN reemplazaran a los puentes Ethernet. Estos switches LAN podían transportar las decisiones de reenvío de capa 2 desde el software hasta los circuitos integrados de aplicación específica (ASIC). Los ASIC reducen el tiempo de manejo de paquetes dentro del dispositivo y permiten que el dispositivo pueda manejar una mayor cantidad de puertos sin disminuir el rendimiento. Este método de reenvío de tramas de datos en la capa 2 se denominaba “switching por almacenamiento y envío”. Este término lo diferenciaba del switching por método de corte.

Como se muestra en la figura 1, el método de almacenamiento y envío toma una decisión de reenvío en una trama después de recibir la trama completa y de revisarla para detectar errores.

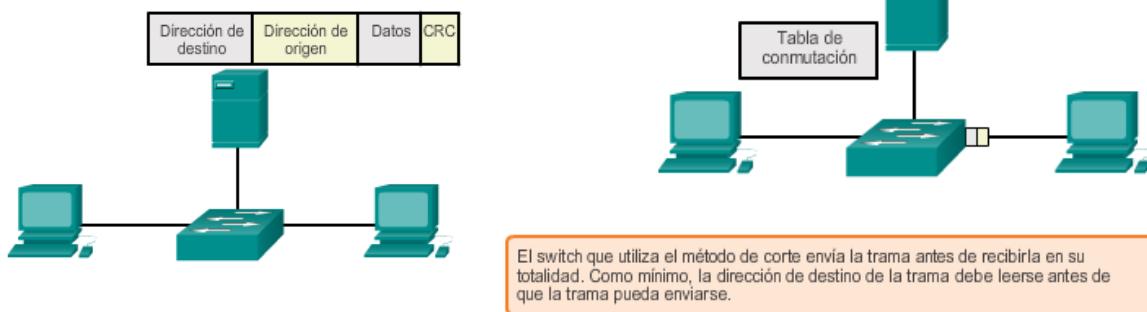
Por el contrario, el método de corte, como se muestra en la figura 2, inicia el proceso de reenvío una vez que se determinó la dirección MAC de destino de una trama entrante y se estableció el puerto de salida.

Comutación por almacenamiento y envío



El switching por almacenamiento y envío tiene dos características principales que lo diferencian del método de corte: la verificación de errores y el almacenamiento en buffer automático.

Comutación por método de corte



Verificación de errores

Los switches que usan switching por almacenamiento y envío realizan la verificación de errores de las tramas entrantes. Después de recibir la trama completa en el puerto de entrada, como se muestra en la ilustración, el switch compara el valor de secuencia de verificación de trama (FCS) en el último campo del datagrama con sus propios cálculos de FCS. FCS es un proceso de verificación de errores que contribuye a asegurar que la trama no contenga errores físicos ni de enlace de datos. Si la trama no posee errores, el switch la reenvía. De lo contrario, se la descarta.

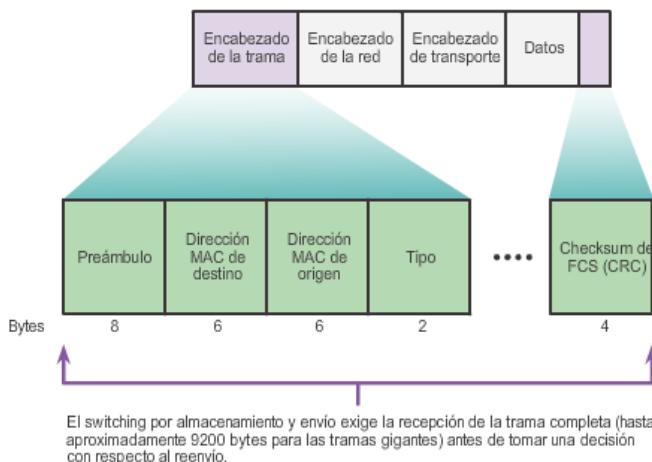
Almacenamiento en buffer automático

El proceso de almacenamiento en buffer del puerto de entrada que usan los switches de almacenamiento y envío proporciona la flexibilidad para admitir cualquier combinación de velocidades de Ethernet. Por ejemplo, el manejo de una trama entrante que se traslada a un puerto Ethernet de 100 Mb/s y que se debe enviar por una interfaz de 1 Gb/s requiere el uso del método de almacenamiento y envío. Ante cualquier incompatibilidad de las velocidades de los puertos de entrada y salida, el switch almacena la trama completa en un buffer, calcula la verificación de FCS, la reenvía al buffer del puerto de salida y después la envía.

El switching por almacenamiento y envío es el método principal de switching LAN de Cisco.

Los switches de almacenamiento y envío descartan las tramas que no pasan la verificación de FCS y, por lo tanto, no reenvían las tramas no válidas. Por el contrario, los switches que usan el método de corte pueden reenviar tramas no válidas, ya que no realizan la verificación de FCS.

Commutación por almacenamiento y envío



Una ventaja del switching por método de corte es que el switch tiene la capacidad de iniciar el reenvío de una trama antes que con el switching por almacenamiento y envío. El switching por método de corte tiene dos características principales: el reenvío rápido de tramas y el procesamiento de tramas no válidas.

Reenvío rápido de tramas

Como se indica en la ilustración, los switches que usan el método de corte pueden tomar una decisión de reenvío tan pronto como encuentran la dirección MAC de destino de la trama en la tabla de direcciones MAC. El switch no tiene que esperar a que el resto de la trama ingrese al puerto de entrada antes de tomar la decisión de reenvío.

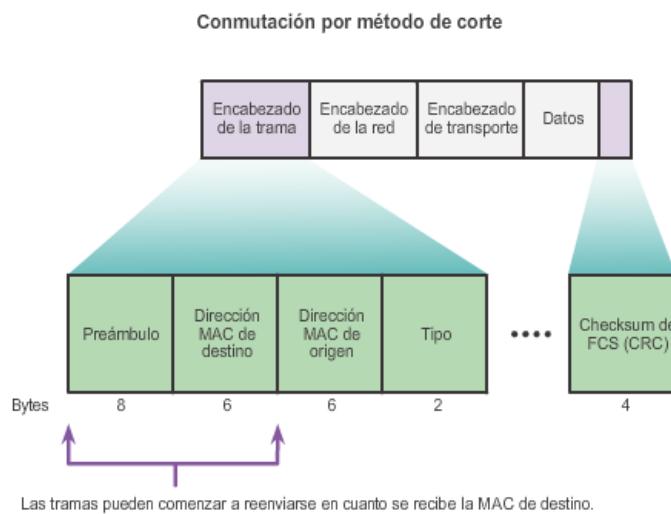
Con los controladores MAC y los ASIC actuales, los switches que usan el método de corte pueden decidir rápidamente si necesitan examinar una mayor parte de los encabezados de una trama para propósitos de filtrado adicional. Por ejemplo, el switch puede analizar más allá de los primeros 14 bytes (la dirección MAC de origen, la dirección MAC de destino y los campos de EtherType) y examinar 40 bytes adicionales para llevar a cabo las funciones más sofisticadas relacionadas con las capas 3 y 4 de IPv4.

El switching por método de corte no descarta la mayoría de las tramas no válidas. Las tramas con errores se reenvían a otros segmentos de la red. Si hay un índice de error alto (tramas no válidas) en la red, el switching por método de corte puede tener un impacto negativo en el ancho de banda; de esta forma, se obstruye el ancho de banda con las tramas dañadas y no válidas.

Libre de fragmentos

El switching libre de fragmentos es una forma modificada del switching por método de corte en la cual el switch espera a que pase la ventana de colisión (64 bytes) antes de reenviar la trama. Esto significa que cada trama se registra en el campo de datos para asegurarse de que no se produzca la fragmentación. El modo libre de fragmentos proporciona una mejor verificación de errores que el de corte, con prácticamente ningún aumento de latencia.

Con la ventaja de la velocidad de latencia más baja que la del switching por método de corte, este modo resulta más adecuado para las aplicaciones muy exigentes de tecnología informática de alto rendimiento (HPC) que requieren latencias de proceso a proceso de 10 microsegundos o menos.



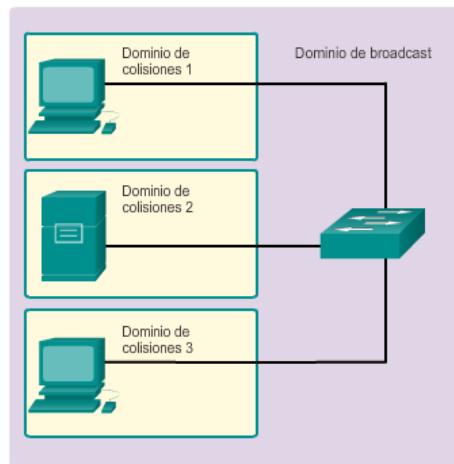
Almacenamiento y envío	Método de corte
1. Almacena las tramas en buffer hasta que el switch recibe la trama completa.	✓
2. Revisa la trama para detectar errores antes de liberarla por los puertos del switch. Si no se recibió la trama completa, el switch la descarta.	✓
3. El switch no realiza ninguna verificación de errores de la trama antes de liberarla a través de los puertos.	✓
4. Un excelente método para conservar el ancho de banda en la red.	✓
5. Con este método de reenvío de tramas, la tarjeta de interfaz de red (NIC) de destino descarta cualquier trama incompleta.	✓
6. Es el método de switching más rápido, pero puede producir más errores de integridad de los datos; por lo tanto, es posible que se consuma más ancho de banda.	✓

1.3.2 Dominios de switching

En los segmentos Ethernet basados en hubs, los dispositivos de red compiten por el medio, porque los dispositivos deben turnarse durante la transmisión. Los segmentos de red que comparten el mismo ancho de banda entre dispositivos se conocen como “dominios de colisiones”, ya que cuando hay dos o más dispositivos que intentan comunicarse dentro de ese segmento al mismo tiempo, pueden ocurrir colisiones.

Sin embargo, es posible usar otros dispositivos de red (por ejemplo, switches y routers) que funcionan en la capa de acceso a la red del modelo TCP/IP y superiores para segmentar la red y reducir el número de dispositivos que compiten por el ancho de banda. Cada segmento nuevo produce un nuevo dominio de colisiones. Hay más ancho de banda disponible para los dispositivos en un segmento, y las colisiones en un dominio de colisiones no interfieren en los demás segmentos. Esto también se conoce como “microsegmentación”.

Como se muestra en la ilustración, cada puerto del switch se conecta a un único servidor o una única computadora y representa un dominio de colisiones independiente.



Si bien los switches hacen pasar por un filtro a la mayoría de las tramas según las direcciones MAC, no hacen lo mismo con las tramas de broadcast. Para que otros switches en la LAN reciban las tramas de difusión, los switches deben saturar todos los puertos con estas tramas. Una serie de switches interconectados forma un dominio de broadcast simple. Solo los dispositivos de capa de red, como los routers, pueden dividir un dominio de difusión de capa 2. Los routers se usan para segmentar los dominios de colisiones y de difusión.

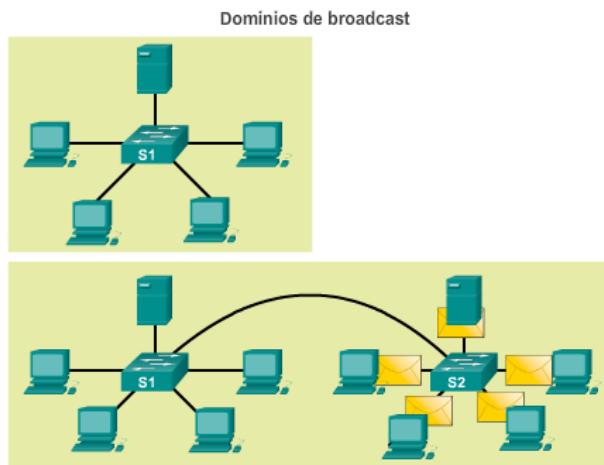
Cuando un dispositivo desea enviar una difusión de capa 2, la dirección MAC de destino de la trama se establece solo en números uno binarios. Todos los dispositivos en el dominio de difusión reciben una trama con una dirección MAC de destino, compuesta solo por números uno binarios.

El dominio de difusión de capa 2 se denomina “dominio de difusión MAC”. El dominio de difusión MAC consta de todos los dispositivos en la LAN que reciben tramas de difusión de un host.

Haga clic en Reproducir en la ilustración para verlo en la primera mitad de la animación.

Cuando un switch recibe una trama de difusión, la reenvía por cada uno de sus puertos, excepto el puerto de entrada en el que se recibió la trama de difusión. Cada dispositivo conectado al switch recibe una copia de la trama de difusión y la procesa. En ocasiones, las difusiones son necesarias para localizar inicialmente otros dispositivos y servicios de red, pero también reducen la eficacia de la red. El ancho de banda de red se usa para propagar el tráfico de difusión. Si hay demasiadas difusiones y una carga de tráfico intensa en una red, se puede producir una congestión: un rendimiento de la red más lento.

Cuando hay dos switches conectados entre sí, se aumenta el dominio de difusión, como se ve en la segunda mitad de la animación. En este caso, se reenvía una trama de difusión a todos los puertos conectados en el switch S1. El switch S1 está conectado al switch S2. Luego, la trama se propaga a todos los dispositivos conectados al switch S2.



Los switches LAN tienen características especiales que los hacen eficaces para aliviar la congestión de una red. En primer lugar, permiten la segmentación de una LAN en dominios de colisiones independientes. Cada puerto del switch representa un dominio de colisiones independiente y proporciona todo el ancho de banda a los dispositivos conectados a dicho puerto. En segundo lugar, proporcionan la comunicación full-duplex entre los dispositivos. Una conexión full-duplex puede transportar las señales transmitidas y recibidas al mismo tiempo. Las conexiones full-duplex aumentaron notablemente el rendimiento de las redes LAN y se requieren para velocidades de Ethernet de 1 Gb/s y superiores.

Los switches interconectan segmentos LAN (dominios de colisiones), usan una tabla de direcciones MAC para determinar el segmento al que deben enviar la trama y pueden reducir o eliminar las colisiones por completo. A continuación, se detallan algunas características importantes de los switches que contribuyen a aliviar la congestión de la red:

- **Alta densidad de puertos:** los switches tienen altas densidades de puertos; los switches de 24 y 48 puertos con frecuencia son de solo 1 unidad de rack (1,75 in) de altura y funcionan a velocidades de 100 Mb/s, 1 Gb/s y 10 Gb/s. Los switches empresariales grandes pueden admitir cientos de puertos.
- **Buffers grandes para tramas:** la capacidad de almacenar más tramas recibidas antes de comenzar a descartarlas es útil, especialmente cuando puede haber puertos congestionados conectados a servidores o a otras partes de la red.
- **Velocidad del puerto:** según el costo de un switch, es posible que admita una combinación de velocidades. Los puertos de 100 Mb/s y de 1 Gb/s o 10 Gb/s son comunes (también puede haber de 100 Gb/s).
- **Switching interno rápido:** la capacidad de reenvío interno rápido promueve un alto rendimiento. El método que se usa puede ser un bus interno o una memoria compartida de gran velocidad, lo que afecta el rendimiento general del switch.
- **Bajo costo por puerto:** los switches proporcionan una alta densidad de puertos a menor costo. Por este motivo, los switches LAN pueden admitir diseños de red que admiten menos usuarios por segmento y, por lo tanto, se aumenta el ancho de banda disponible para cada usuario.



1.4 Resumen

Vimos que la tendencia en redes es la convergencia mediante un único conjunto de cables y de dispositivos para administrar la transmisión de voz, de video y de datos. Además, hubo un cambio notable en el modo en el que las empresas realizan sus actividades. Los empleados ya no están limitados por oficinas físicas o límites geográficos. Los recursos ahora deben estar disponibles sin inconvenientes en cualquier momento y lugar. La arquitectura Cisco Borderless Network permite que distintos elementos, desde switches de acceso hasta puntos de acceso inalámbrico, funcionen conjuntamente y permitan a los usuarios acceder a los recursos en cualquier momento y desde cualquier lugar.

El modelo tradicional de diseño jerárquico de tres capas divide a la red en las capas de núcleo, de distribución y de acceso, y permite que cada parte de la red esté optimizada para una funcionalidad específica. Proporciona modularidad, resistencia y flexibilidad, lo cual sienta una base que permite que los diseñadores de red superpongan funciones de seguridad, movilidad y comunicación unificada. En algunas redes, no se requiere mantener las capas de distribución y de núcleo separadas. En estas redes, la funcionalidad de la capa de núcleo y de la capa de distribución a menudo se contrae en una sola.

Los switches LAN Cisco usan ASIC para reenviar tramas según la dirección MAC de destino. Antes de poder lograr esto, primero deben usar la dirección MAC de origen de las tramas entrantes para crear una tabla de direcciones MAC en la memoria de contenido direccionable (CAM). Si la dirección MAC de destino está en esta tabla, la trama se reenvía solamente al puerto de destino específico. En el caso de que la dirección MAC de destino no se encuentre en la tabla de direcciones MAC, se saturan todos los puertos con las tramas, excepto aquel en el que se recibió la trama.

Los switches usan switching por almacenamiento y envío o por método de corte. El switching por almacenamiento y envío lee la trama completa en un buffer y verifica la CRC antes de reenviar la trama. El switching por método de corte lee solo la primera parte de la trama e inicia el reenvío tan pronto como lee la dirección de destino. Si bien este proceso es sumamente rápido, no se realiza ninguna verificación de errores en la trama antes de reenviarla.

Cada puerto de un switch constituye un dominio de colisiones independiente que permite la comunicación full-duplex a velocidades extremadamente altas. Los puertos del switch no bloquean las difusiones, y la conexión de switches entre sí puede ampliar el tamaño del dominio de difusión, lo que generalmente provoca un deterioro del rendimiento de la red.

2 Configuración y conceptos básicos de switching

2.1 Introducción

Los switches se usan para conectar varios dispositivos en la misma red. En una red diseñada correctamente, los switches LAN son responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red.

Los switches de Cisco son de configuración automática y no necesitan ninguna configuración adicional para comenzar a funcionar. Sin embargo, los switches Cisco ejecutan Cisco IOS y se pueden configurar manualmente para satisfacer mejor las necesidades de la red. Esto incluye el ajuste de los requisitos de velocidad, de ancho de banda y de seguridad de los puertos.

Además, los switches Cisco se pueden administrar de manera local y remota. Para administrar un switch de forma remota, este se debe configurar con una dirección IP y un gateway predeterminado. Estos son solo dos de los parámetros de configuración que se analizan en este capítulo.

Los switches funcionan en lugares de la capa de acceso donde los dispositivos de red cliente se conectan directamente a la red y donde los departamentos de TI quieren que los usuarios accedan de forma simple a esta. Es una de las áreas más vulnerables de la red, ya que está muy expuesta al usuario. Los switches se deben configurar para que sean resistentes a los ataques de todo tipo y, al mismo tiempo, protejan los datos de los usuarios y permitan que haya conexiones de alta velocidad. La seguridad de puertos es una de las características de seguridad que proporcionan los switches administrados por Cisco.

En este capítulo, se analizan algunas de las opciones de configuración básica de switch que se requieren para mantener un entorno LAN comutado seguro y disponible.

Después de completar este capítulo, podrá hacer lo siguiente:

- Configurar los parámetros iniciales en un switch Cisco.
- Configurar los puertos de un switch para cumplir con los requisitos de red.
- Configurar la interfaz virtual de administración de un switch.
- Describir los ataques de seguridad básicos en un entorno comutado.
- Describir las prácticas recomendadas de seguridad en un entorno comutado.
- Configurar la característica de seguridad de puertos para restringir el acceso a la red.

2.2 Configuración de parámetros iniciales de un switch

Una vez que se enciende el switch Cisco, lleva a cabo la siguiente secuencia de arranque:

1. Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.

2. A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.

3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.

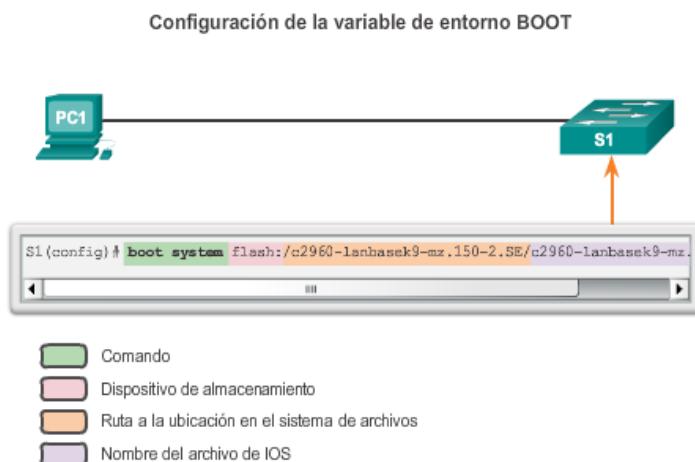
4. El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.

5. Por último, el cargador de arranque ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al IOS.

El cargador de arranque busca la imagen de Cisco IOS en el switch de la siguiente manera: el switch intenta arrancar automáticamente mediante la información de la variable de entorno BOOT. Si no se establece esta variable, el switch intenta cargar y ejecutar el primer archivo ejecutable que puede mediante una búsqueda recursiva y en profundidad en todo el sistema de archivos flash. Cuando se realiza una búsqueda en profundidad de un directorio, se analiza por completo cada subdirectorio que se encuentra antes de continuar la búsqueda en el directorio original. En los switches de la serie Catalyst 2960, el archivo de imagen generalmente se encuentra en un directorio que tiene el mismo nombre que el archivo de imagen (excepto la extensión de archivo .bin).

Luego, el sistema operativo IOS inicia las interfaces mediante los comandos del IOS de Cisco que se encuentran en el archivo de configuración, startup-config, que está almacenado en NVRAM.

En la ilustración, la variable de entorno BOOT se establece con el comando **boot system** del modo de configuración global. Observe que el IOS se ubica en una carpeta distinta y que se especifica la ruta de la carpeta. Use el comando **show bootvar**(**show boot** en versiones anteriores de IOS) para ver la configuración actual del archivo de arranque de IOS.



El cargador de arranque proporciona acceso al switch si no se puede usar el sistema operativo debido a la falta de archivos de sistema o al daño de estos. El cargador de arranque tiene una línea de comandos que proporciona acceso a los archivos almacenados en la memoria flash.

Se puede acceder al cargador de arranque mediante una conexión de consola con los siguientes pasos:

Paso 1. Conecte una computadora al puerto de consola del switch con un cable de consola. Configure el software de emulación de terminal para conectarse al switch.

Paso 2. Desconecte el cable de alimentación del switch.

Paso 3. Vuelva a conectar el cable de alimentación al switch, espere 15 segundos y, a continuación, presione y mantenga presionado el botón **Mode** (Modo) mientras el LED del sistema sigue parpadeando con luz verde.

Paso 4. Continúe oprimiendo el botón**Modo** hasta que el LED del sistema se torne ámbar por un breve instante y luego verde, después suelte el botón **Modo**.

Paso 5. Aparece la petición de entrada**switch#**: del cargador de arranque en el software de emulación de terminal en la computadora.

La línea de comandos de **boot loader** admite comandos para formatear el sistema de archivos flash, volver a instalar el software del sistema operativo y recuperarse de la pérdida o el olvido de una contraseña. Por ejemplo, el comando **dirse** puede usar para ver una lista de archivos dentro de un directorio específico, como se muestra en la ilustración.

Nota: observe que, en este ejemplo, el IOS se ubica en la raíz de la carpeta de la memoria flash.

```

Switch# dir flash:
Directory of flash:/

  2 -rwx    11607161 Mar 1 2013 03:10:47 +00:00 c2960-
lenbasek9-mz.150-2.SE.bin
  3 -rwx        1809 Mar 1 2013 00:02:48 +00:00 config.text
  5 -rwx        1919 Mar 1 2013 00:02:48 +00:00 private-
config.text
  6 -rwx       59416 Mar 1 2013 00:02:49 +00:00 multiple-fs

32514048 bytes total (20841472 bytes free)
Switch#

```

Los switches Cisco Catalyst tienen varios indicadores luminosos LED de estado. Puede usar los LED del switch para controlar rápidamente la actividad y el rendimiento del switch. Los diferentes modelos y conjuntos de características de los switches tienen diferentes LED, y la ubicación de estos en el panel frontal del switch también puede variar.

En la ilustración, se muestran los LED y el botón Mode de un switch Cisco Catalyst 2960. El botón Mode se utiliza para alternar entre el estado del puerto, el modo dúplex del puerto, la velocidad del puerto y el estado de alimentación por Ethernet (PoE [si se admite]) de los LED del puerto. A continuación, se describe el propósito de los indicadores LED y el significado de los colores:

- **LED del sistema:** muestra si el sistema recibe alimentación y funciona correctamente. Si el LED está apagado, significa que el sistema no está encendido. Si el LED es de color verde, el sistema funciona normalmente. Si el LED es de color ámbar, el sistema recibe alimentación pero no funciona correctamente.
- **LED del sistema de alimentación redundante (RPS):** muestra el estado del RPS. Si el LED está apagado, el RPS está apagado o no se conectó correctamente. Si el LED es de color verde, el RPS está conectado y listo para proporcionar alimentación de respaldo. Si el LED parpadea y es de color verde, el RPS está conectado pero no está disponible porque está proporcionando alimentación a otro dispositivo. Si el LED es de color ámbar, el RPS está en modo de reserva o presenta una falla. Si el LED parpadea y es de color ámbar, la fuente de

alimentación interna del switch presenta una falla, y el RPS está proporcionando alimentación.

- **LED de estado del puerto:** cuando el LED es de color verde, indica que se seleccionó el modo de estado del puerto. Éste es el modo predeterminado. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, no hay enlace, o el puerto estaba administrativamente inactivo. Si el LED es de color verde, hay un enlace presente. Si el LED parpadea y es de color verde, hay actividad, y el puerto está enviando o recibiendo datos. Si el LED alterna entre verde y ámbar, hay una falla en el enlace. Si el LED es de color ámbar, el puerto está bloqueado para asegurar que no haya un bucle en el dominio de reenvío y no reenvía datos (normalmente, los puertos permanecen en este estado durante los primeros 30 segundos posteriores a su activación). Si el LED parpadea y es de color ámbar, el puerto está bloqueado para evitar un posible bucle en el dominio de reenvío.
- **LED de modo dúplex del puerto:** cuando el LED es de color verde, indica que se seleccionó el modo dúplex del puerto. Al seleccionarlo, los LED del puerto que están apagados están en modo half-duplex. Si el LED del puerto es de color verde, el puerto está en modo full-duplex.
- **LED de velocidad del puerto:** indica que se seleccionó el modo de velocidad del puerto. Al seleccionarlo, los indicadores LED del puerto muestran colores con diferentes significados. Si el LED está apagado, el puerto funciona a 10 Mb/s. Si el LED es de color verde, el puerto funciona a 100 Mb/s. Si el LED parpadea y es de color verde, el puerto funciona a 1000 Mb/s.
- **LED de modo de alimentación por Ethernet:** si se admite alimentación por Ethernet, hay un LED de modo de PoE. Si el LED está apagado, indica que no se seleccionó el modo de alimentación por Ethernet, que a ninguno de los puertos se le negó el suministro de alimentación y ninguno presenta fallas. Si el LED parpadea y es de color ámbar, no se seleccionó el modo de alimentación por Ethernet, pero al menos a uno de los puertos se le negó el suministro de alimentación o uno de ellos presenta una falla de alimentación por Ethernet. Si el LED es de color verde, indica que se seleccionó el modo de alimentación por Ethernet, y los LED del puerto muestran colores con diferentes significados. Si el LED del puerto está apagado, la alimentación por Ethernet está desactivada. Si el LED del puerto es de color verde, la alimentación por Ethernet está activada. Si el LED del puerto alterna entre verde y ámbar, se niega la alimentación por Ethernet, ya que, si se suministra energía al dispositivo alimentado, se excede la capacidad de alimentación del switch. Si el LED parpadea y es de color ámbar, la alimentación por Ethernet está desactivada debido a una falla. Si el LED es de color ámbar, se inhabilitó la alimentación por Ethernet para el puerto.



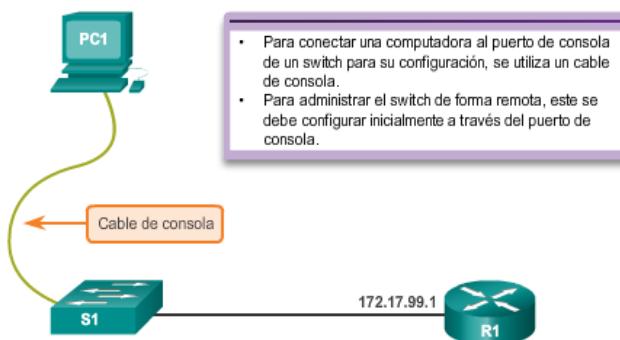
Para el acceso a la administración remota de un switch, este se debe configurar con una dirección IP y una máscara de subred. Recuerde que para administrar un switch desde una red remota, se lo debe configurar con un gateway predeterminado. Este es un proceso muy similar a la configuración de la información de dirección IP en los dispositivos host. En la ilustración, se debe asignar una dirección IP a la interfaz virtual del switch (SVI) de S1. La SVI es una interfaz virtual, no un puerto físico del switch.

SVI es un concepto relacionado con las VLAN. Las VLAN son grupos lógicos numerados a los que se pueden asignar puertos físicos. Los parámetros de configuración aplicados a una VLAN también se aplican a todos los puertos asignados a esa VLAN.

De manera predeterminada, el switch está configurado para que el control de la administración del switch se realice mediante la VLAN 1. Todos los puertos se asignan a la VLAN 1 de manera predeterminada. Por motivos de seguridad, se recomienda usar una VLAN de administración distinta de la VLAN 1.

Tenga en cuenta que el propósito de esta configuración IP es solamente obtener acceso a la administración remota del switch; la configuración IP no permite que el switch enrute paquetes de capa 3.

Preparación para la administración remota



Paso 1. Configurar la interfaz de administración

Se configura una dirección IP y una máscara de subred en la SVI de administración del switch desde el modo de configuración de interfaz VLAN. Como se muestra en la figura 1, el comando **interface vlan 99** se usa para ingresar al modo de configuración de interfaz. Para configurar la dirección IP, se usa el comando **ip address**. El comando **no shutdown** habilita la interfaz. En este ejemplo, la VLAN 99 se configuró con la dirección IP 172.17.99.11.

La SVI para la VLAN 99 no se muestra como “up/up” hasta que se cree la VLAN 99 y haya un dispositivo conectado a un puerto del switch asociado a la VLAN 99. Para crear una VLAN con la id_de_vlan 99 y asociarla a una interfaz, use los siguientes comandos:

```
S1(config)# vlan id_de_vlan
S1(config-vlan)# namenombre_de_vlan
S1(config-vlan)# exit
S1(config)# interfaceinterface_id
S1(config-if)# switchport access vlan id_de_vlan
```

Paso 2. Configuración del gateway predeterminado

Si el switch se va a administrar de forma remota desde redes que no están conectadas directamente, se debe configurar con un gateway predeterminado. El gateway predeterminado es el router al que está conectado el switch. El switch reenvía los paquetes IP con direcciones IP de destino fuera de la red local al gateway predeterminado. Como se muestra en la figura 2, R1 es el gateway predeterminado para S1. La interfaz en R1 conectada al switch tiene la dirección IP 172.17.99.1. Esta es la dirección de gateway predeterminado para S1.

Para configurar el gateway predeterminado del switch, use el comando **ip default-gateway**. Introduzca la dirección IP del gateway predeterminado. El gateway predeterminado es la dirección IP de la interfaz del router a la que está conectado el switch. Use el comando **copy running-config startup-config** para realizar una copia de seguridad de la configuración.

Paso 3. Verificar la configuración

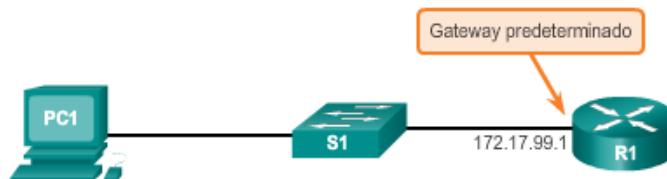
Como se muestra en la figura 3, el comando **show ip interface brief** es útil para determinar el estado de las interfaces virtuales y físicas. El resultado que se muestra confirma que la interfaz VLAN 99 se configuró con una dirección IP y una máscara de subred y que está en condiciones de funcionamiento.

Configuración de la interfaz de administración de un switch

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	S1# configure terminal
Ingrera al modo de configuración de interfaz para la SVI.	S1(config)# interface vlan 99
Configura la dirección IP de la interfaz de administración.	S1(config-if)# ip address 172.17.99.11 255.255.0.0
Habilita la interfaz de administración.	S1(config-if)# no shutdown
Vuelve al modo EXEC privilegiado.	S1(config-if)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

Configuración del gateway predeterminado de un switch

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	S1# configure terminal
Configura el gateway predeterminado del switch.	S1(config)# ip default-gateway 172.17.99.1
Vuelve al modo EXEC privilegiado.	S1(config)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config



Verificación de la configuración de la interfaz de administración de un switch

```
S1# show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
vlan99         172.17.99.11    YES manual up        down
<resultado omitido>
```



2.3 Configuración de puertos de un switch

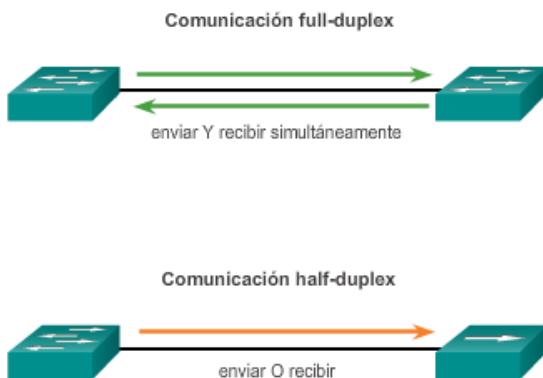
En la ilustración, se muestra la comunicación full-duplex y half-duplex.

La comunicación full-duplex mejora el rendimiento de una LAN conmutada. La comunicación full-duplex aumenta el ancho de banda eficaz al permitir que ambos extremos de una conexión transmitan y reciban datos simultáneamente. Esto también se conoce como “flujo de datos bidireccional”. Este método de optimización de rendimiento de la red requiere microsegmentación. Las LAN microsegmentadas se crean cuando un puerto de switch tiene solo un dispositivo conectado y funciona en modo full-duplex. Como resultado, se obtiene el dominio de colisiones de tamaño micro de un único dispositivo. Sin embargo, debido a que hay solamente un dispositivo conectado, en las LAN microsegmentadas no hay colisiones.

A diferencia de la comunicación full-duplex, la comunicación half-duplex es unidireccional. El envío y la recepción de datos no ocurren al mismo tiempo. La comunicación half-duplex genera problemas de rendimiento debido a que los datos fluyen en una sola dirección por vez, lo que a menudo provoca colisiones. Las conexiones half-duplex suelen verse en los dispositivos de hardware más antiguos, como los hubs. La comunicación full-duplex reemplazó a la half-duplex en la mayoría del hardware.

Actualmente, la mayoría de las tarjetas NIC Ethernet y Fast Ethernet disponibles en el mercado proporciona capacidad full-duplex. Las NIC Gigabit Ethernet y de 10 Gb requieren conexiones full-duplex para funcionar. En el modo full-duplex, el circuito de detección de colisiones de la NIC se encuentra inhabilitado. Las tramas enviadas por los dos dispositivos conectados no pueden colisionar, dado que estos utilizan dos circuitos independientes en el cable de red. Las conexiones full-duplex requieren un switch que admita la configuración full-duplex o una conexión directa entre dos dispositivos mediante un cable Ethernet.

En general, la eficacia de una configuración Ethernet compartida basada en hubs es del 50% al 60% del ancho de banda indicado. Full-duplex ofrece el 100% de eficacia en ambas direcciones (transmisión y recepción). Como resultado, se obtiene un uso potencial del 200% del ancho de banda indicado.



Dúplex y velocidad

Los puertos de switch se pueden configurar manualmente con parámetros específicos de dúplex y de velocidad. Use el comando **duplex** del modo de configuración de interfaz para especificar manualmente el modo dúplex de un puerto de switch. Use el comando **speed** del modo de

configuración de interfaz para especificar manualmente la velocidad de un puerto de switch. En la figura 1, el puerto F0/1 de los switches S1 y S2 se configura manualmente con la palabra clave **full** para el comando **duplex** y la palabra clave **100** para el comando **speed**.

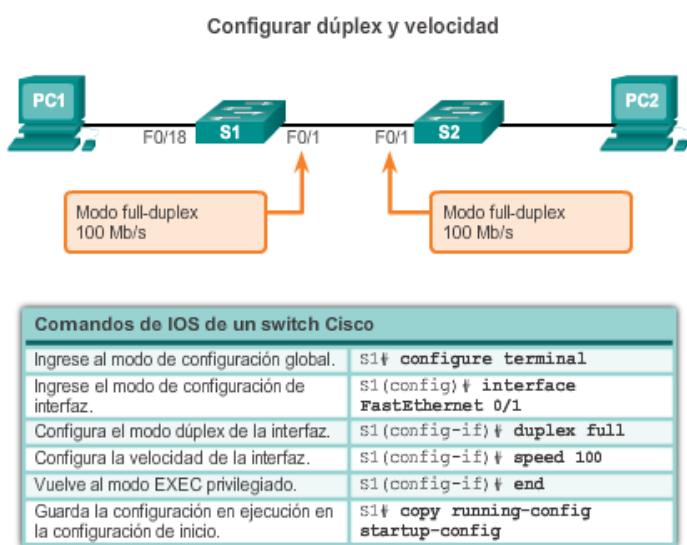
La configuración predeterminada de dúplex y velocidad para los puertos de switch en los switches Cisco Catalyst 2960 y 3560 es automática. Los puertos 10/100/1000 funcionan en el modo half-duplex o full-duplex cuando se establecen en 10 Mb/s o 100 Mb/s, pero solo funcionan en el modo full-duplex cuando se establecen en 1000 Mb/s (1 Gb/s). La autonegociación es útil cuando se desconoce la configuración de dúplex y de velocidad del dispositivo que se conecta al puerto o cuando es posible que dicha configuración cambie. Al conectarse a dispositivos conocidos, como servidores, estaciones de trabajo dedicadas o dispositivos de red, se recomienda establecer manualmente la configuración de dúplex y de velocidad.

Cuando se realiza la resolución de problemas de puertos de switch, se debe verificar la configuración de dúplex y de velocidad.

Nota: si la configuración para el modo dúplex y la velocidad de puertos del switch presenta incompatibilidades, se pueden producir problemas de conectividad. Una falla de autonegociación provoca incompatibilidades en la configuración.

Todos los puertos de fibra óptica, como los puertos 100BASE-FX, solo funcionan a una velocidad predefinida y siempre son full-duplex.

Use el verificador de sintaxis de la figura 2 para configurar el puerto F0/1 del switch S1.



```

Ingrese al modo de configuración y establezca el modo dúplex de
FastEthernet0/1 en full y la velocidad en 100.
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# interface FastEthernet0/1
S1(config-if)# duplex full
S1(config-if)# speed 100
Finalice el modo de configuración y guarde la configuración en la NVRAM.
S1(config-if)# end
S1#
SYS-5-CONFIG_I: Configured from console by console
S1# copy running-config startup-config
Configuró correctamente los parámetros de dúplex y velocidad del puerto del
switch.

```

Hasta hace poco, se requerían determinados tipos de cable (cruzado o directo) para conectar dispositivos. Las conexiones switch a switch o switch a router requerían el uso de diferentes cables Ethernet. Mediante el uso de la característica automática de conexión cruzada de interfaz dependiente del medio (auto-MDIX) en una interfaz, se elimina este problema. Al habilitar la característica auto-MDIX, la interfaz detecta automáticamente el tipo de conexión de cable requerido (directo o cruzado) y configura la conexión conforme a esa información. Al conectarse a los switches sin la característica auto-MDIX, se deben usar cables directos para conectarse a dispositivos como servidores, estaciones de trabajo o routers, y cables cruzados para conectarse a otros switches o repetidores.

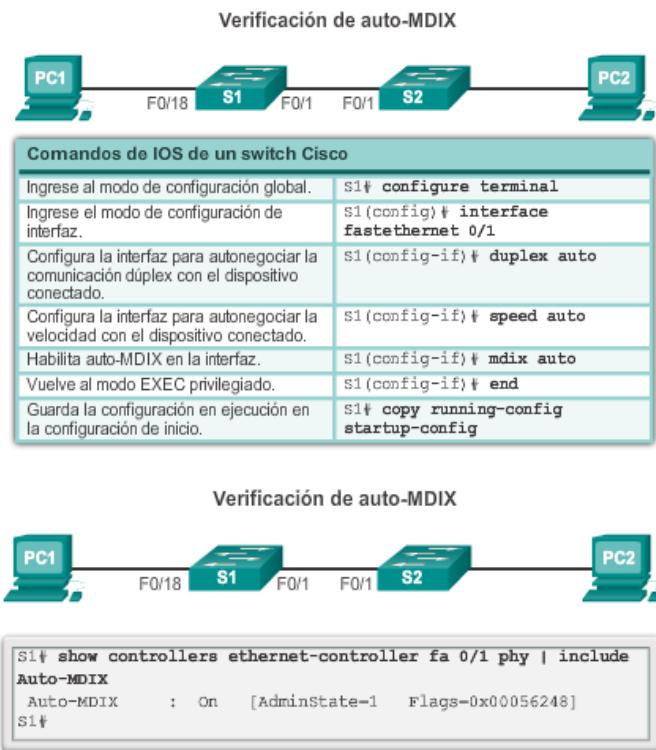
Con la característica auto-MDIX habilitada, se puede usar cualquier tipo de cable para conectarse a otros dispositivos, y la interfaz se ajusta de manera automática para proporcionar comunicaciones satisfactorias. En los routers y switches Cisco más modernos, el comando **mdix auto** del modo de configuración de interfaz habilita la característica. Cuando se usa auto-MDIX en una interfaz, la velocidad y el modo dúplex de la interfaz se deben establecer en **auto** para que la característica funcione correctamente.

Los comandos para habilitar auto-MDIX se muestran en la figura 1.

Nota: la característica auto-MDIX está habilitada de manera predeterminada en los switches Catalyst 2960 y Catalyst 3560, pero no está disponible en los switches más antiguos Catalyst 2950 y Catalyst 3550.

Para examinar la configuración de auto-MDIX de una interfaz específica, use el comando **show controllers ethernet-controller** con la palabra clave **phy**. Para limitar los resultados a las líneas que se refieren a auto-MDIX, use el filtro **include Auto-MDIX**. Como se muestra en la figura 2, el resultado indica On (Habilitada) u Off (Deshabilitada) para la característica.

Use el verificador de sintaxis de la figura 3 para configurar la interfaz FastEthernet 0/1 de S2 con auto-MDIX.



En la figura 1, se describen algunas de las opciones del comando **show** que son útiles para verificar las características configurables comunes de un switch.

En la figura 2, se muestra un resultado abreviado del comando **show running-config**. Use este comando para verificar que el switch se haya configurado correctamente. Como se observa en el resultado de S1, se muestra cierta información clave:

- Interfaz Fast Ethernet 0/18 configurada con la VLAN 99 de administración
- VLAN 99 configurada con la dirección IP 172.17.99.11 255.255.255.0
- Gateway predeterminado establecido en 172.17.99.1

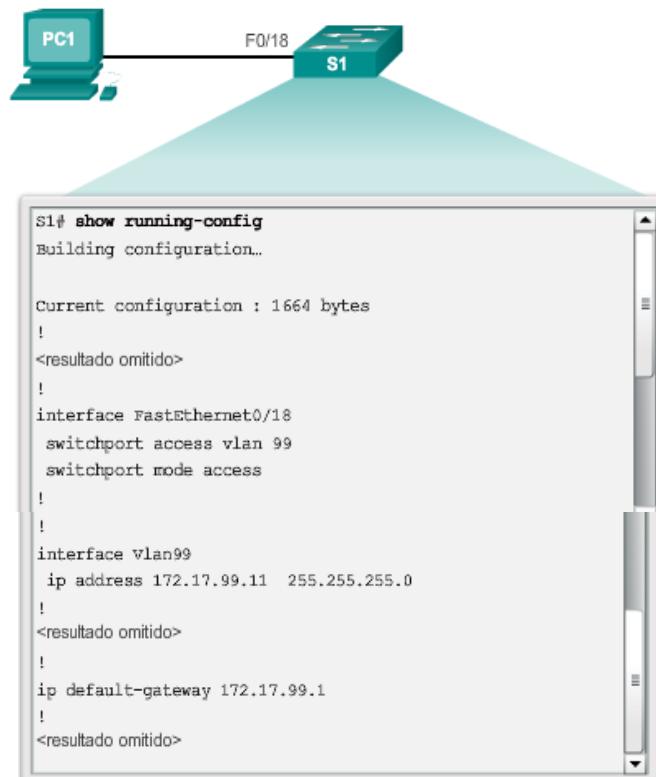
El comando **show interfaces** es otro comando de uso frecuente que muestra información estadística y de estado sobre las interfaces de red del switch. El comando **show interfaces** se usa habitualmente cuando se configuran y se controlan los dispositivos de red.

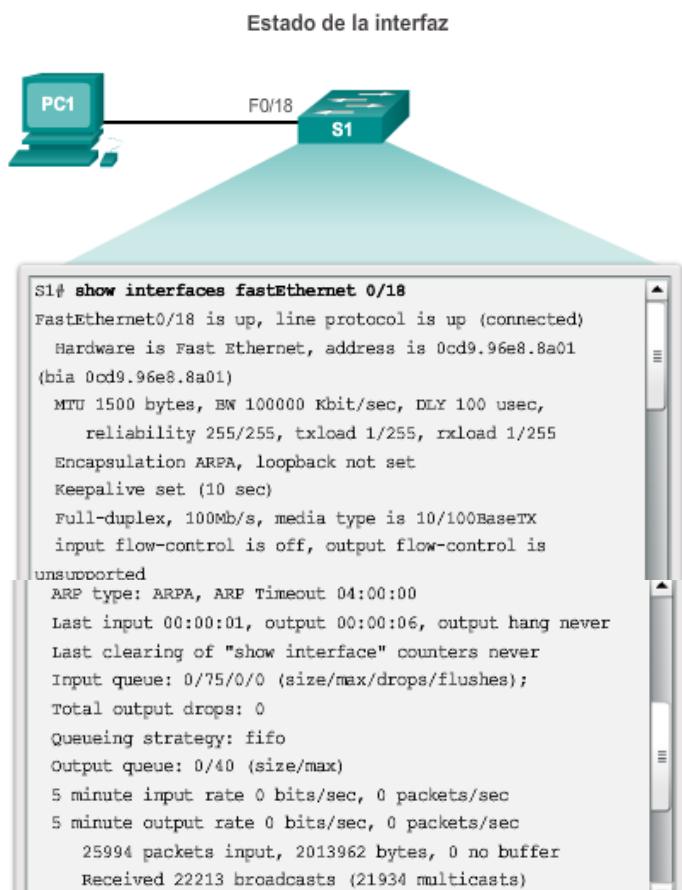
En la figura 3, se muestra el resultado del comando **show interfaces fastEthernet 0/18**. En la primera línea de la ilustración, se indica que la interfaz FastEthernet 0/18 está “up/up”, lo que significa que está en funcionamiento. Más abajo en el resultado, se muestra que el modo dúplex es full y la velocidad es de 100 Mb/s.

Comandos de verificación

Comandos de IOS de un switch Cisco	
Muestra el estado y la configuración de la interfaz.	S1# show interfaces [id-interfaz]
Muestra la configuración de inicio actual.	S1# show startup-config
Muestra la configuración de funcionamiento actual.	S1# show running-config
Muestra información sobre el sistema de archivos flash.	S1# show flash
Muestra el estado del hardware y el software del sistema.	S1# show version
Muestra el historial de comandos introducidos.	S1# show history
Muestra información de IP de una interfaz.	S1# show ip [id-interfaz]
Muestra la tabla de direcciones MAC.	S1# show mac-address-table O S1# show mac address-table

Configuración en ejecución





El resultado del comando **show interfaces** se puede usar para detectar problemas frecuentes de los medios. Una de las partes más importantes de este resultado es la visualización del estado del protocolo de línea y de enlace de datos. En la figura 1, se indica la línea de resumen para revisar el estado de una interfaz.

El primer parámetro (FastEthernet0/1 is up) se refiere a la capa de hardware y, básicamente, refleja si la interfaz recibe la señal de detección de portadora del otro extremo. El segundo parámetro (line protocol is up) se refiere a la capa de enlace de datos y refleja si se reciben los keepalives del protocolo de capa de enlace de datos.

Sobre la base del resultado del comando **show interfaces**, los posibles problemas se pueden reparar de la siguiente manera:

- Si la interfaz está activa y el protocolo de línea está inactivo, hay un problema. Puede haber una incompatibilidad en el tipo de encapsulación, la interfaz en el otro extremo puede estar inhabilitada por errores o puede haber un problema de hardware.
- Si el protocolo de línea y la interfaz están inactivos, hay un cable que no está conectado o existe algún otro problema de interfaz. Por ejemplo, en una conexión directa, el otro extremo de la conexión puede estar administrativamente inactivo.
- Si la interfaz se encuentra administrativamente inactiva, se inhabilitó manualmente en la configuración activa (se emitió el comando **shutdown**).

En la figura 2, se muestra un ejemplo del resultado del comando **show interfaces**. En el ejemplo, se muestran los contadores y las estadísticas de la interfaz FastEthernet0/1.

Algunos errores de medios no son lo suficientemente graves para provocar una falla en el circuito, pero sí provocan problemas en el rendimiento de la red. En la figura 3, se explican algunos de estos errores frecuentes, los cuales se pueden detectar mediante el comando **show interfaces**.

“Input errors” indica la suma de todos los errores en los datagramas que se recibieron en la interfaz que se analiza. Estos incluyen los recuentos de fragmentos de colisión, de fragmentos gigantes, de los que no están almacenados en buffer, de CRC, de tramas, de saturación y de ignorados. Los errores de entrada que se informan con el comando **show interfaces** incluyen lo siguiente:

- **Runt frames:** las tramas de Ethernet más cortas que la longitud mínima permitida de 64 bytes se denominan “runt frames” (fragmentos de colisión). La causa del exceso de fragmentos de colisión suele ser una NIC en mal funcionamiento, pero este puede deberse a los mismos problemas que causan el exceso de colisiones.
- **Giants:** las tramas Ethernet más largas que la longitud máxima permitida se denominan “giants” (fragmentos gigantes). Los fragmentos gigantes se deben a los mismos problemas que causan los fragmentos de colisión.
- **Errores de CRC:** en las interfaces Ethernet y seriales, los errores de CRC generalmente indican que hay errores en los medios o en los cables. Las causas comunes incluyen interferencia eléctrica, conexiones flojas o dañadas o el uso del tipo de cable incorrecto. Si aparecen muchos errores de CRC, hay demasiado ruido en el enlace, y se debe examinar el cable para conocer la longitud y detectar daños. También se deben buscar y eliminar las fuentes del ruido, si es posible.

“Output errors” indica la suma de todos los errores que impiden la transmisión final de los datagramas por la interfaz que se analiza. Los errores de salida que se informan con el comando **show interfaces** incluyen lo siguiente:

- **Collisions:** las colisiones en las operaciones half-duplex son completamente normales y no debe preocuparse por estas, siempre que esté satisfecho con el funcionamiento half-duplex. Sin embargo, nunca debe haber colisiones en una red correctamente diseñada y configurada que use la comunicación full-duplex. Se recomienda especialmente usar full-duplex, a menos que tenga un equipo más antiguo o heredado que requiera half-duplex.
- **Late collisions:** las colisiones tardías se refieren a las colisiones que ocurren después de que se transmitieron 512 bits (el preámbulo) de la trama. La longitud excesiva de los cables es la causa más frecuente de las colisiones tardías. Otra causa frecuente es la configuración incorrecta de dúplex. Por ejemplo, el extremo de una conexión puede estar configurado para full-duplex y el otro para half-duplex. Las colisiones tardías se verían en la interfaz que está configurada para half-duplex. En ese caso, debe configurar los mismos parámetros de dúplex en ambos extremos. Una red diseñada y configurada correctamente nunca debería tener colisiones tardías.

Verificación del estado de una interfaz

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia
0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<resultado omitido>
```

Estado de la interfaz	Estado del protocolo de línea	Estado de enlace
Up (Activo)	Up (Activo)	Operativo
Down (Inactivo)	Down (Inactivo)	Problema de interfaz

Visualización del estado y las estadísticas de una interfaz

```
S1# show interfaces FastEthernet0/1
FastEthernet0/1 is up, line protocol is up
Hardware is Fast Ethernet, address is 0022.91c4.0e01 (bia 0022.91c4.0e01)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<resultado omitido>
 2295197 packets input, 305539992 bytes, 0 no buffer
 Received 1925500 broadcasts, 0 runts, 0 giants, 0
 throttles
 3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 68 multicast, 0 pause input
 0 input packets with dribble condition detected
 3594664 packets output, 436549843 bytes, 0 underruns
 8 output errors, 1790 collisions, 10 interface resets
 0 unknown protocol drops
 0 babbles, 235 late collision, 0 deferred
<resultado omitido>
```

Problemas de la capa de acceso a la red

Tipo de error	Descripción
Errores de entrada	Cantidad total de errores. Incluye los recuentos de fragmentos de colisión, de fragmentos gigantes, de los que no están almacenados en buffer, de CRC, de tramas, de saturación y de ignorados.
Fragmentos de colisión	Paquetes que se descartan porque son más pequeños que el tamaño mínimo de paquete para el medio. Por ejemplo, cualquier paquete Ethernet que tenga menos de 64bytes se considera un fragmento de colisión.
Fragmentos gigantes	Paquetes que se descartan porque superan el tamaño máximo de paquete para el medio. Por ejemplo, cualquier paquete Ethernet que tenga más de 1518bytes se considera un fragmento gigante.
CRC	Se generan errores de CRC cuando el checksum calculado no es igual al checksum recibido.
Errores de salida	La suma de todos los errores que impiden la transmisión final de los datagramas por la interfaz que se analiza.
Colisiones	Cantidad de mensajes retransmitidos debido a una colisión de Ethernet.
Colisiones tardías	Una colisión que ocurre después de que se transmitieron 512bits de la trama.

La mayoría de los problemas que afectan a las redes commutadas se produce durante la implementación inicial. En teoría, una vez instaladas, las redes continúan funcionando sin problemas. Sin embargo, los cables se dañan, la configuración cambia, y se conectan al switch

nuevos dispositivos que requieren cambios de configuración en este. Se requiere el mantenimiento y la resolución de problemas de infraestructura de la red de forma permanente.

Para poder resolver estos problemas, si no cuenta con una conexión o tiene una conexión defectuosa entre un switch y otro dispositivo, siga este proceso general:

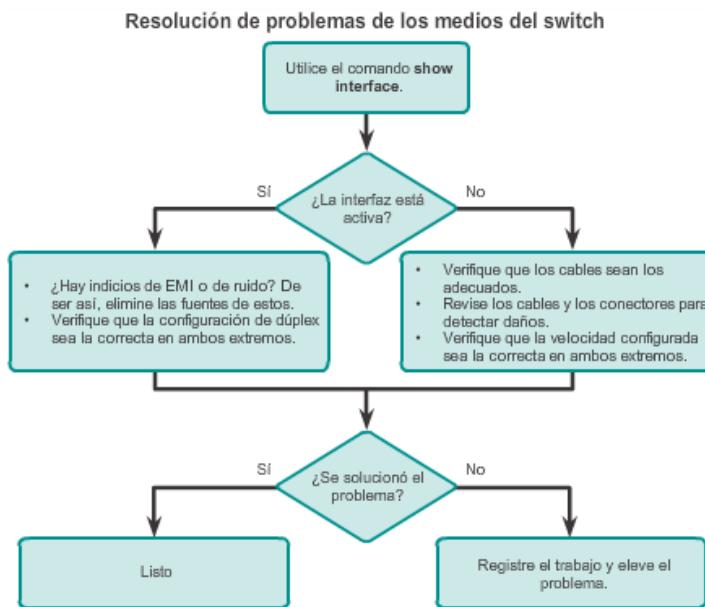
Para revisar el estado de la interfaz, use el comando **show interfaces**.

Si la interfaz está inactiva, realice lo siguiente:

- Verifique que se usen los cables adecuados. Además, revise los cables y los conectores para detectar daños. Si se sospecha que hay un cable defectuoso o incorrecto, reemplácelo.
- Si la interfaz continúa inactiva, el problema puede deberse a una incompatibilidad en la configuración de velocidad. En general, la velocidad de una interfaz se negocia automáticamente; por lo tanto, incluso si se configura manualmente, la interfaz que se conecta debe negociar automáticamente conforme a ello. Si se produce una incompatibilidad de velocidad debido a una configuración incorrecta o a un problema de hardware o de software, esto podría provocar que la interfaz quede inactiva. Establezca manualmente la misma velocidad en ambos extremos de la conexión si se sospecha que hay un problema.

Si la interfaz está activa pero aún hay problemas de conectividad, realice lo siguiente:

- Mediante el comando **show interfaces**, busque indicios de ruido excesivo. Los indicios pueden incluir un aumento en los contadores de fragmentos de colisión, de fragmentos gigantes y de errores de CRC. Si hay un exceso de ruido, primero busque el origen del ruido y, si es posible, elimínelo. Además, verifique qué tipo de cable se utiliza y que el cable no supere la longitud máxima. Para los cables de cobre, se recomienda que utilice, por lo menos, la categoría 5.
- Si no hay problemas de ruido, verifique si hay un exceso de colisiones. Si hay colisiones o colisiones tardías, verifique la configuración de dúplex en ambos extremos de la conexión. Al igual que la configuración de velocidad, la configuración de dúplex por lo general se negocia automáticamente. Si pareciera haber una incompatibilidad de dúplex, configúrela manualmente en ambos extremos de la conexión. Se recomienda usar full-duplex si ambos extremos lo admiten.



2.4 Seguridad de switches: administración e implementación

2.4.1 Acceso remoto seguro

Shell seguro (SSH) es un protocolo que proporciona una conexión de administración segura (cifrada) a un dispositivo remoto. SSH debe reemplazar a Telnet para las conexiones de administración. Telnet es un protocolo más antiguo que usa la transmisión no segura de texto no cifrado de la autenticación de inicio de sesión (nombre de usuario y contraseña) y de los datos transmitidos entre los dispositivos que se comunican. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro cuando se autentica un dispositivo (nombre de usuario y contraseña) y también para los datos transmitidos entre los dispositivos que se comunican. SSH se asigna al puerto TCP 22. Telnet se asigna al puerto TCP 23.

En la figura 1, un atacante puede controlar los paquetes mediante Wireshark. Se puede dirigir un flujo de Telnet para que capture el nombre de usuario y la contraseña.

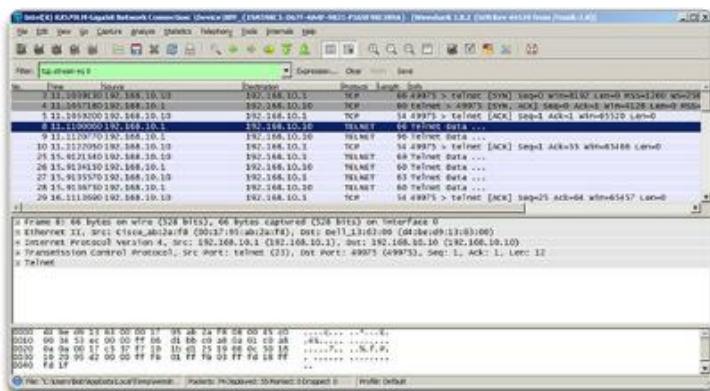
En la figura 2, el atacante puede capturar el nombre de usuario y la contraseña del administrador desde la sesión de Telnet de texto no cifrado.

En la figura 3, se muestra la vista de Wireshark de una sesión de SSH. El atacante puede hacer un seguimiento de la sesión mediante la dirección IP del dispositivo administrador.

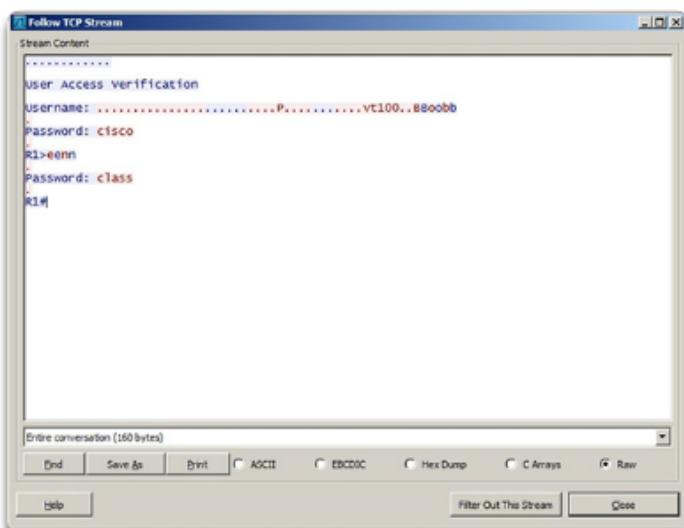
Sin embargo, en la figura 4, el nombre de usuario y la contraseña están cifrados.

Para habilitar SSH en un switch Catalyst 2960, el switch debe usar una versión del software IOS que incluya características y capacidades criptográficas (cifradas). En la figura 5, use el comando **show version** en el switch para ver qué IOS se ejecuta actualmente en el dispositivo y el nombre de archivo de IOS que incluye la combinación "k9" que admite características y capacidades criptográficas (cifradas).

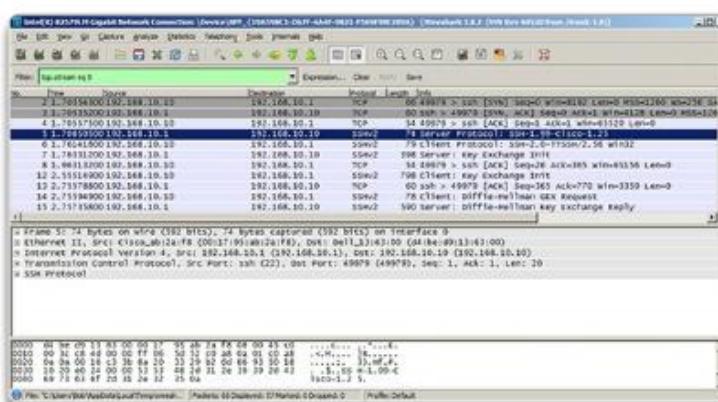
Captura de Telnet en Wireshark



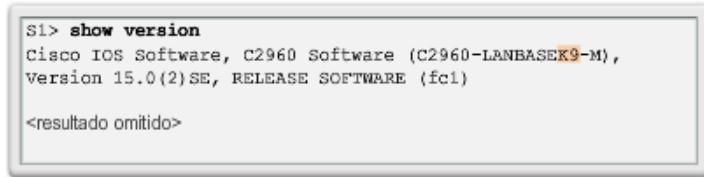
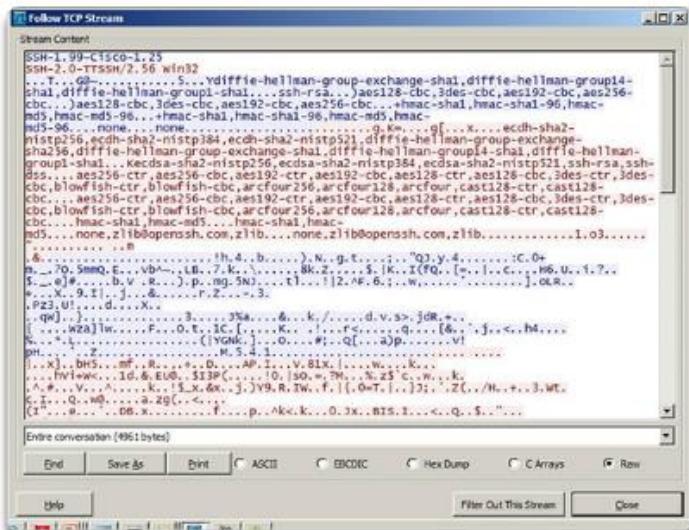
Captura de nombre de usuario y contraseña en texto no cifrado



Captura de SSH en Wireshark



Nombre de usuario y contraseña cifrados



Antes de configurar SSH, el switch debe tener configurado, como mínimo, un nombre de host único y los parámetros correctos de conectividad de red.

Paso 1. Verificar la compatibilidad con SSH

Use el comando **show ip ssh** para verificar que el switch admite SSH. Si el switch no ejecuta un IOS que admite características criptográficas, este comando no se reconoce.

Paso 2. Configurar el dominio IP

Configure el nombre de dominio IP de la red mediante el comando **ip domain-name nombre-del-dominio** del modo de configuración global. En la figura 1, el valor de *nombre-del-dominio* es **cisco.com**.

Paso 3. Generar pares de claves RSA

No todas las versiones del IOS utilizan la versión 2 de SSH de manera predeterminada, y la versión 1 de SSH tiene fallas de seguridad conocidas. Para configurar la versión 2 de SSH, emita el comando **ip ssh version 2** del modo de configuración global. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando **crypto key generate rsa** del modo de configuración global para habilitar el servidor SSH en el switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. Cisco recomienda un tamaño de módulo mínimo de 1024 bits (consulte la configuración de muestra en la figura 1). Una longitud de módulo mayor es más segura, pero se tarda más en generarlo y utilizarlo.

Nota: para eliminar el par de claves RSA, use el comando **crypto key zeroize rsa** del modo de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

Paso 4. Configurar la autenticación de usuario

El servidor SSH puede autenticar a los usuarios localmente o con un servidor de autenticación. Para usar el método de autenticación local, cree un nombre de usuario y una contraseña con el comando del modo de configuración global **username nombre-de-usuario secret contraseña**. En el ejemplo, se asignó la contraseña **ccna** al usuario **admin**.

Paso 5. Configurar las líneas vty

Habilite el protocolo SSH en las líneas vty mediante el comando **transport input ssh** del modo de configuración de línea. El switch Catalyst 2960 tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al switch a que acepte solo las conexiones SSH. Use el comando **line vty** del modo de configuración global y, luego, el comando **login local** del modo de configuración de línea para requerir la autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

Paso 6. Habilitar la versión 2 de SSH.

De manera predeterminada, SSH admite las versiones 1 y 2. Si se admiten ambas versiones, en el resultado de **show ip ssh** se muestra que se admite la versión 1.99. La versión 1 tiene vulnerabilidades conocidas. Por esta razón, se recomienda habilitar únicamente la versión 2. Habilite la versión de SSH mediante el comando de configuración global **ip ssh version 2**.

Use el verificador de sintaxis de la figura 2 para configurar SSH en el switch S1.



```

S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# end
*SYS-5-CONFIG_I: Configured from console by console

Configure S1 para usar SSH 2.0.

S1(config)# ip ssh version 2
S1(config)#
Configuró correctamente SSH en todas las líneas VTY.

```

En las computadoras, se usa un cliente SSH, como PuTTY, para conectarse a un servidor SSH. Para los ejemplos de las figuras 1 a 3, se configuró lo siguiente:

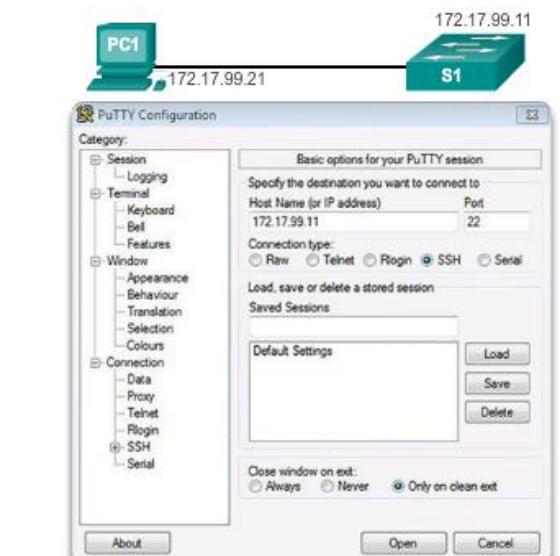
- Se habilitó SSH en el switch S1.
- Interfaz VLAN 99 (SVI) con la dirección IP 172.17.99.11 en el switch S1.
- PC1 con la dirección IP 172.17.99.21.

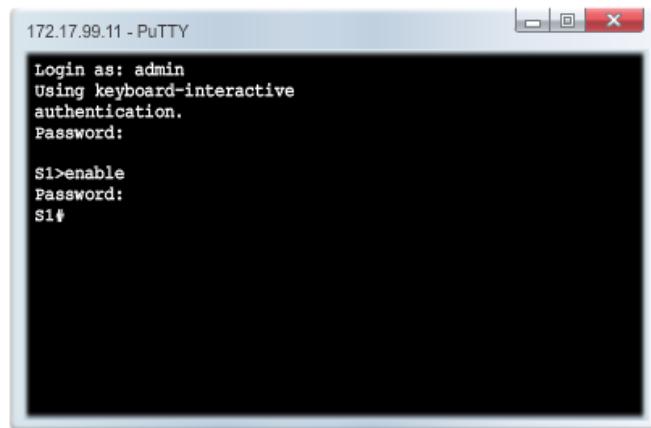
En la figura 1, la computadora inicia una conexión SSH a la dirección IP de la VLAN SVI de S1.

En la figura 2, se solicita al usuario que introduzca un nombre de usuario y una contraseña. Con la configuración del ejemplo anterior, se introduce el nombre de usuario **admin** y la contraseña **ccna**. Después de introducir la combinación correcta, el usuario se conecta a la CLI del switch Catalyst 2960 mediante SSH.

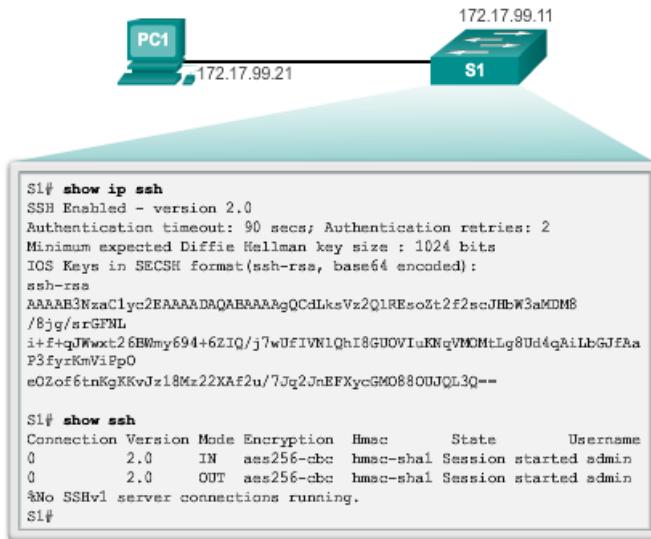
Para mostrar los datos de la versión y de configuración de SSH en el dispositivo que configuró como servidor SSH, use el comando **show ip ssh**. En el ejemplo, se habilitó la versión 2 de SSH. Para revisar las conexiones SSH al dispositivo, use el comando **show ssh** (consulte la figura 3).

Configuración de los parámetros de conexión de cliente SSH PuTTY





Verificación del estado y la configuración de SSH



SSH debe reemplazar a Telnet para las conexiones de administración. Telnet usa comunicaciones inseguras de texto no cifrado. SSH proporciona seguridad para las conexiones remotas mediante el cifrado seguro de todos los datos transmitidos entre los dispositivos.

2.4.2 Cuestiones de seguridad en redes LAN

La seguridad básica del switch no evita los ataques malintencionados. La seguridad es un proceso en capas que, básicamente, nunca está completo. Cuanto más consciente sea el equipo de profesionales de redes de una organización sobre los ataques de seguridad y los peligros que presentan, mejor. Algunos tipos de ataques de seguridad se describen aquí, pero los detalles sobre cómo funcionan algunos de estos ataques exceden el ámbito de este curso. Encontrará información más detallada en los cursos de tecnologías WAN y de seguridad de CCNA.

Saturación de direcciones MAC

La tabla de direcciones MAC de un switch contiene las direcciones MAC relacionadas con cada puerto físico y la VLAN asociada para cada puerto. Cuando un switch de la Capa 2 recibe una trama, el switch busca en la tabla de direcciones MAC la dirección MAC de destino. Todos los modelos de switches Catalyst utilizan una tabla de direcciones MAC para la conmutación en la Capa 2. A medida que llegan las tramas a los puertos del switch, se registran las direcciones MAC de origen en la tabla de direcciones MAC. Si la dirección MAC tiene una entrada en la tabla, el switch reenvía la trama al puerto correspondiente. Si la dirección MAC no existe en la tabla de direcciones MAC, el switch satura todos los puertos con la trama, excepto el puerto en el cual se la recibió.

El comportamiento de un switch de saturar direcciones MAC para las direcciones desconocidas se puede usar para atacar un switch. Este tipo de ataque se denomina “ataque de desbordamiento de la tabla de direcciones MAC”. En ocasiones, los ataques de desbordamiento de la tabla de direcciones MAC se denominan “ataques de saturación MAC” y “ataques de desbordamiento de la tabla CAM”. En las ilustraciones, se muestra cómo funciona este tipo de ataque.

En la figura 1, el host A envía tráfico al host B. El switch recibe las tramas y busca la dirección MAC de destino en la tabla de direcciones MAC. Si el switch no puede encontrar una MAC de destino en la tabla de direcciones MAC, este copia la trama y satura todos los puertos del switch con esta (la difunde), excepto el puerto en el cual se la recibió.

En la figura 2, el host B recibe la trama y envía una respuesta al host A. A continuación, el switch descubre que la dirección MAC del host B está ubicada en el puerto 2 y registra esa información en la tabla de direcciones MAC.

El host C también recibe la trama que va del host A al host B, pero debido a que la dirección MAC de destino de la trama es el host B, el host C la descarta.

Como se muestra en la figura 3, cualquier trama que envíe el host A (o cualquier otro host) al host B se reenvía al puerto 2 del switch y no se difunde por todos los puertos.

Las tablas de direcciones MAC poseen límite de tamaño. Los ataques de saturación MAC usan esta limitación para sobrecargar al switch con direcciones MAC de origen falsas hasta que la tabla de direcciones MAC del switch esté completa.

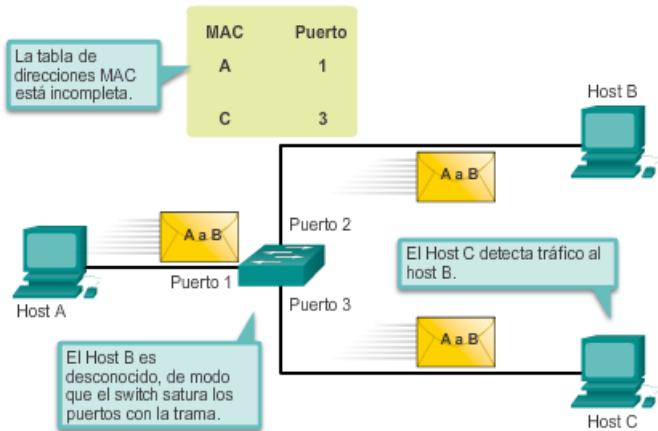
Como se muestra en la figura 4, un atacante en el host C puede enviar tramas al switch con direcciones MAC de origen y destino falsas y generadas aleatoriamente. El switch actualiza la tabla de direcciones MAC con la información de las tramas falsas. Cuando la tabla de direcciones MAC está llena de direcciones MAC falsas, el switch entra en un modo que se conoce como modo “fail-open”. En este modo, el switch transmite todas las tramas a todas las máquinas en la red. Como resultado, el atacante puede ver todas las tramas.

Algunas herramientas de ataques de red pueden generar hasta 155 000 entradas de MAC por minuto en un switch. El tamaño máximo de la tabla de direcciones MAC varía en función del switch.

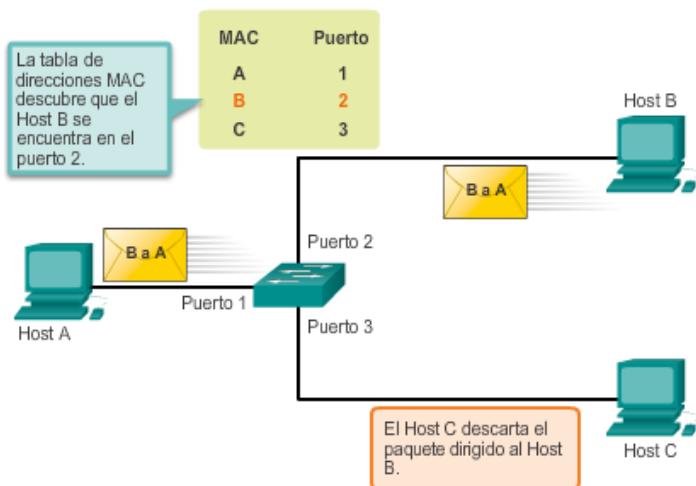
Como se muestra en la figura 5, mientras la tabla de direcciones MAC en el switch esté llena, el switch difunde todas las tramas recibidas por cada puerto. En este ejemplo, las tramas enviadas del host A al host B también se difunden por el puerto 3 del switch, y el atacante en el host C las puede ver.

Una forma de mitigar los ataques de desbordamiento de la tabla de direcciones MAC es configurar la seguridad de puertos.

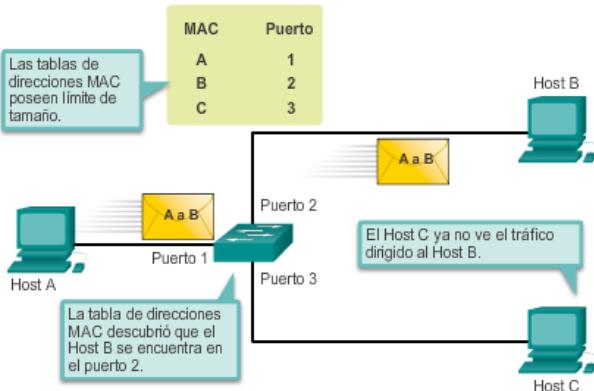
El switch satura los puertos con la trama que tiene una dirección MAC desconocida

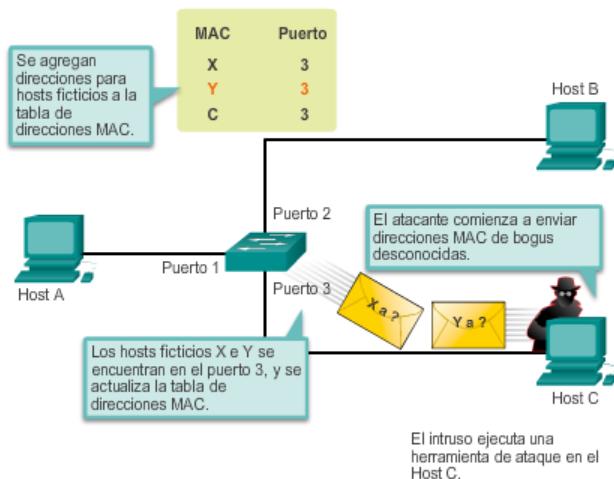
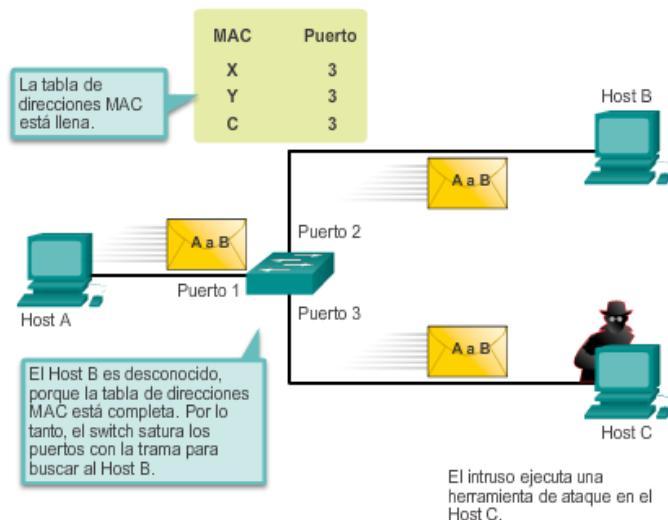


El switch registra la dirección MAC



El switch usa la tabla de direcciones MAC para reenviar el tráfico



Ataque por saturación de direcciones MAC**Ataque por saturación de direcciones MAC**

DHCP es el protocolo que asigna automáticamente una dirección IP válida de un pool de DHCP a un host. En esta industria, el protocolo DHCP se usa hace casi tanto tiempo como TCP/IP como protocolo principal para asignar direcciones IP a los clientes. Se pueden realizar dos tipos de ataques DHCP a una red comutada: los ataques de agotamiento de DHCP y los de suplantación de identidad de DHCP.

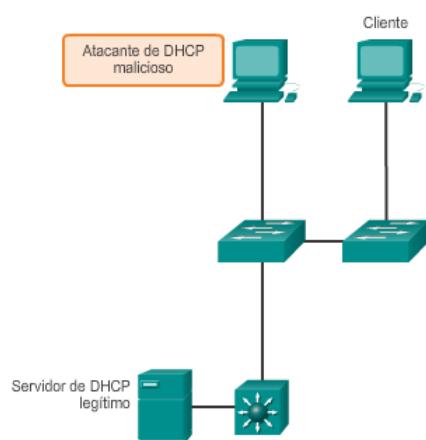
En los ataques de agotamiento de DHCP, un atacante satura el servidor de DHCP con solicitudes de DHCP para utilizar todas las direcciones IP disponibles que el servidor de DHCP puede emitir. Una vez que se emiten estas direcciones IP, el servidor no puede emitir más direcciones; esta situación produce un ataque por denegación de servicio (DoS), ya que los nuevos clientes no pueden obtener acceso a la red. Un ataque DoS es cualquier ataque que se usa para sobrecargar dispositivos y servicios de red específicos con tráfico ilegítimo, lo que impide que el tráfico legítimo llegue a esos recursos.

En los ataques de suplantación de identidad de DHCP, un atacante configura un servidor de DHCP falso en la red para emitir direcciones de DHCP para los clientes. El motivo común de este ataque es obligar a los clientes a que usen servidores de Sistema de nombres de dominios (DNS) o de Servicio de nombres Internet de Windows (WINS) falsos y hacer que los clientes usen al atacante, o una máquina controlada por el atacante, como gateway predeterminado.

El agotamiento de DHCP se suele utilizar antes de un ataque de suplantación de identidad de DHCP para denegar el servicio al servidor de DHCP legítimo, lo que facilita la introducción de un servidor de DHCP falso en la red.

Para mitigar los ataques de DHCP, se usan las características de detección de DHCP y de seguridad de puertos de los switches Cisco Catalyst. Estas características se abordan más adelante en otro tema.

Ataque de suplantación de identidad y de agotamiento de DHCP



El protocolo de descubrimiento de Cisco (CDP, Cisco Discovery Protocol) es un protocolo propiedad de Cisco que puede configurarse en todos los dispositivos de Cisco. CDP detecta otros dispositivos de Cisco conectados directamente, lo que permite que los dispositivos configuren su conexión de forma automática. En algunos casos, esto simplifica la configuración y la conectividad.

De manera predeterminada, la mayoría de los routers y switches Cisco poseen CDP habilitado en todos los puertos. La información de CDP se envía en difusiones periódicas sin cifrar. Esta información se actualiza localmente en la base de datos de CDP de cada dispositivo. Debido a que CDP es un protocolo de capa 2, los routers no propagan los mensajes CDP.

CDP contiene información sobre el dispositivo, como la dirección IP, la versión de software del IOS, la plataforma, las capacidades y la VLAN nativa. Los atacantes pueden usar esta información para encontrar la forma de atacar la red, generalmente mediante ataques por denegación de servicio (DoS).

En la ilustración, se muestra una parte de una captura de Wireshark en la que se muestra el contenido de un paquete CDP. En particular, la versión de software IOS de Cisco descubierta por CDP permite que el atacante determine si existen vulnerabilidades de seguridad específicas para esa versión de IOS. Además, debido a que CDP no se autentica, los atacantes pueden crear paquetes CDP falsos y enviarlos a un dispositivo de Cisco conectado directamente.

Se recomienda inhabilitar el uso de CDP en los dispositivos o los puertos que no necesitan usarlo mediante el comando **no cdp run** del modo de configuración global. CDP se puede inhabilitar por puerto.

Ataques de Telnet

El protocolo Telnet es inseguro, y los atacantes lo pueden usar para acceder de manera remota a un dispositivo de red de Cisco. Existen herramientas que permiten que los atacantes inicien un ataque de decodificación de contraseñas por fuerza bruta contra las líneas vty del switch.

Ataque de contraseña de fuerza bruta

La primera fase de un ataque de contraseña de fuerza bruta comienza con el uso de contraseñas comunes por parte del atacante y de un programa diseñado para intentar establecer una sesión de Telnet mediante todas las palabras del diccionario. Si la contraseña no se descifra en la primera fase, comienza una segunda fase. En la segunda fase del ataque de fuerza bruta, el atacante usa un programa que genera combinaciones de caracteres secuenciales para poder adivinar la contraseña. Si dispone del tiempo suficiente, un ataque de contraseña de fuerza bruta puede decodificar casi todas las contraseñas utilizadas.

Para mitigar los ataques de contraseña de fuerza bruta, use contraseñas seguras y cámbielas con frecuencia. Una contraseña segura debe tener una combinación de mayúsculas y minúsculas, y debe incluir números y símbolos (caracteres especiales). El acceso a las líneas vty también se puede limitar mediante una lista de control de acceso (ACL).

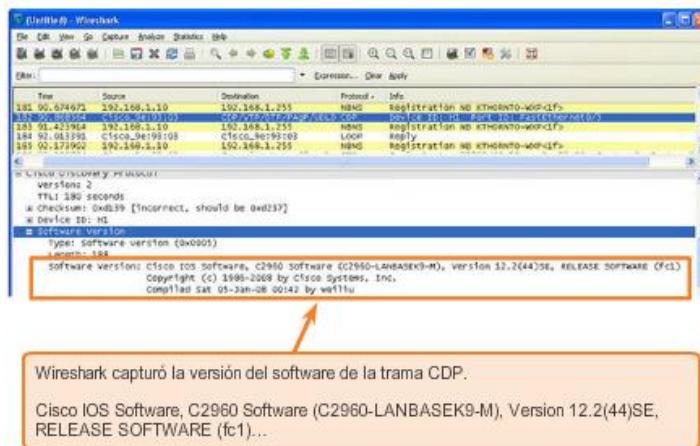
Ataque DoS por Telnet

Telnet también se puede usar para iniciar un ataque DoS. En un ataque DoS por Telnet, el atacante explota un defecto del software del servidor Telnet que se ejecuta en el switch, el cual hace que el servicio de Telnet no esté disponible. Este tipo de ataque impide que un administrador acceda de manera remota a las funciones de administración del switch. Esto se puede combinar con otros ataques directos a la red como parte de un esfuerzo coordinado para impedir que el administrador de red acceda a dispositivos clave durante la infracción.

En general, las vulnerabilidades en el servicio de Telnet que permiten que ocurran los ataques de DoS se enfrentan mediante parches de seguridad incluidos en las revisiones más recientes de IOS de Cisco.

Nota: se recomienda usar SSH en lugar de Telnet para las conexiones de administración remota.

Ataques en CDP



Tipo de ataque de seguridad	Descripción de los ataques de seguridad frecuentes
CDP	Permite que el atacante vea la información acerca de las direcciones IP, de las versiones de software y de la VLAN nativa del entorno para llevar a cabo un ataque DoS.
Inanición DHCP	Satura el servidor de DHCP con solicitudes de DHCP para usar todas las direcciones disponibles; simula un ataque DoS en el switch.
Fuerza bruta	Usa un "diccionario" para buscar contraseñas comunes; intenta iniciar una sesión de Telnet con lo que el "diccionario" sugiere como contraseña.
Saturación de direcciones MAC	Usa direcciones MAC falsas para desbordar la tabla de direcciones MAC.
Detección de DHCP	Permite que un atacante configure un servidor de DHCP falso en la red para emitir direcciones DHCP para los clientes.

2.4.3 Prácticas recomendadas de seguridad

La defensa de la red contra ataques requiere vigilancia y capacitación. Las siguientes son prácticas recomendadas para proteger una red:

- Desarrolle una política de seguridad escrita para la organización.
- Desactive los servicios y puertos que no se utilicen.
- Utilice contraseñas seguras y cámbielas con frecuencia.
- Controle el acceso físico a los dispositivos.
- Evite usar sitios web HTTP estándar inseguros, especialmente para las pantallas de inicio de sesión; en lugar de esto, use HTTPS, que es más seguro.
- Realice copias de respaldo y pruébelas periódicamente.
- Capacite a los empleados sobre los ataques de ingeniería social y desarrolle políticas para validar identidades por teléfono, mediante correo electrónico y personalmente.
- Cifre y proteja con contraseñas los datos confidenciales.

- Implemente hardware y software de seguridad, como firewalls.
- Mantenga el software actualizado mediante la instalación semanal o mensual de parches de seguridad, si es posible.

Estos métodos son solo un punto de partida para la administración de la seguridad. Las organizaciones deben mantenerse alerta en todo momento para defenderse de estas amenazas en constante evolución. Use herramientas de seguridad de red para medir la vulnerabilidad de la red actual.



Las herramientas de seguridad de red ayudan al administrador de red a probar una red para detectar debilidades. Algunas herramientas permiten que el administrador asuma el rol de atacante. Mediante una de estas herramientas, el administrador puede iniciar un ataque contra la red y analizar los resultados para determinar cómo ajustar las políticas de seguridad a fin de mitigar esos tipos de ataques. Las auditorías de seguridad y los pruebas de penetración son dos funciones básicas que llevan a cabo las herramientas de seguridad de red.

El administrador puede iniciar manualmente las técnicas de prueba de seguridad de red. Otras pruebas están automatizadas en gran medida. Sin importar el tipo de prueba, el personal que configura y lleva a cabo las pruebas de seguridad debe tener un amplio conocimiento de seguridad y de redes. Esto incluye conocimientos en las siguientes áreas:

- Seguridad de la red
- Firewalls
- Sistemas de prevención de intrusiones
- Sistemas operativos
- Programación
- Protocolos de red (como TCP/IP)

Pruebas de seguridad de red



Las herramientas de seguridad de red permiten que los administradores de red realicen auditorías de seguridad en una red. Una auditoría de seguridad revela el tipo de información que puede recopilar un atacante con un simple monitoreo del tráfico de la red.

Por ejemplo, las herramientas de auditoría de seguridad de red permiten que un administrador sature la tabla de direcciones MAC con direcciones MAC ficticias. A esto le sigue una auditoría de los puertos del switch a medida que este satura con tráfico todos los puertos. Durante la auditoría, las asignaciones de direcciones MAC legítimas vencen y se reemplazan por las asignaciones de direcciones MAC ficticias. Esto determina qué puertos están comprometidos y no están configurados correctamente para evitar este tipo de ataque.

El tiempo es un factor importante para realizar la auditoría de manera correcta. Los diferentes switches admiten distintas cantidades de direcciones MAC en sus tablas MAC. Puede resultar difícil determinar el número ideal de direcciones MAC suplantadas que se deben enviar al switch. Los administradores de red también deben enfrentar el período de vencimiento de la tabla de direcciones MAC. Si las direcciones MAC suplantadas comienzan a vencerse en el momento en que se realiza la auditoría de red, las direcciones MAC válidas comienzan a completar la tabla de direcciones MAC, lo que limita la cantidad de datos que pueden monitorearse con una herramienta de auditoría de red.

Las herramientas de seguridad de red también se pueden usar para realizar pruebas de penetración en la red. La prueba de penetración es un ataque simulado contra la red para determinar qué tan vulnerable sería en un ataque real. Esto permite que un administrador de red identifique debilidades en la configuración de los dispositivos de red y realice cambios para que los dispositivos sean más resistentes a los ataques. Los administradores pueden llevar a cabo una gran cantidad de ataques, y la mayoría de los conjuntos de herramientas vienen acompañados por documentación completa que detalla la sintaxis necesaria para ejecutar el ataque deseado.

Debido a que las pruebas de penetración pueden tener efectos adversos en la red, se llevan a cabo bajo condiciones muy controladas, respetando los procedimientos registrados que se detallan en una política de seguridad de red completa. Lo ideal es una red sin conexión que imite la red de producción real y funcione como banco de pruebas. El personal de redes puede usar la red del banco de pruebas para realizar pruebas de penetración en la red.

Auditoría de seguridad de red



Deshabilitar puertos en desuso

Un método simple que muchos administradores usan para contribuir a la seguridad de la red ante accesos no autorizados es inhabilitar todos los puertos del switch que no se utilizan. Por ejemplo, si un switch Catalyst 2960 tiene 24 puertos y hay tres conexiones Fast Ethernet en uso, es aconsejable inhabilitar los 21 puertos que no se utilizan. Navegue hasta todos los puertos que no se utilizan y emita el comando **shutdown** de Cisco IOS. Si más adelante se debe reactivar un puerto, este se puede habilitar con el comando **no shutdown**. La figura muestra el resultado parcial para esta configuración.

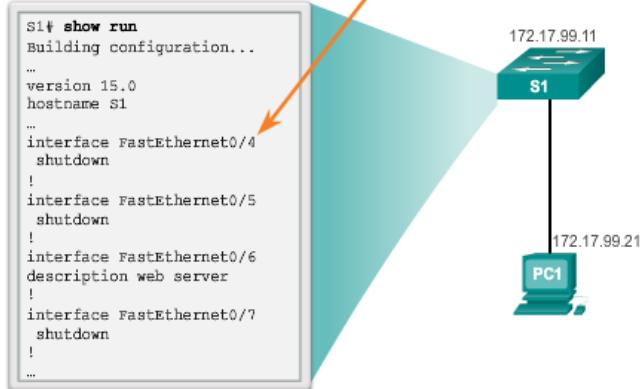
Realizar cambios de configuración a varios puertos de un switch es sencillo. Si se debe configurar un rango de puertos, use el comando **interface range**.

Switch(config)# **interface range** escriba el módulo/primer-número – último-número

El proceso de habilitación e inhabilitación de puertos puede llevar mucho tiempo, pero mejora la seguridad de la red y vale la pena el esfuerzo.

Deshabilitar puertos en desuso

Inhabilite los puertos sin utilizar con el comando **shutdown**.



El snooping DHCP es una función que determina cuáles son los puertos de switch que pueden responder a solicitudes de DHCP. Los puertos se identifican como confiables o no confiables. Los puertos confiables pueden recibir todos los mensajes de DHCP, incluidos los paquetes de oferta de DHCP y de acuse de recibo de DHCP; los puertos no confiables solo pueden recibir solicitudes. Los puertos confiables de los hosts se alojan en el servidor de DHCP o pueden ser un enlace hacia dicho servidor. Si un dispositivo no autorizado en un puerto no confiable intenta enviar un paquete de oferta de DHCP a la red, el puerto se desactiva. Esta función puede unirse con las opciones de DHCP donde la información del switch, como el ID de puerto o la solicitud de DHCP pueden insertarse en el paquete de solicitudes de DHCP.

Como se muestra en las figuras 1 y 2, los puertos no confiables son aquellos que no están configurados explícitamente como confiables. Se construye una tabla enlazada de DHCP para los puertos no confiables. Cada entrada contiene una dirección MAC cliente, una dirección IP, un tiempo de arrendamiento, un número de VLAN y una ID de puerto registrados como clientes que realizan solicitudes de DHCP. Se utiliza entonces la tabla para filtrar el tráfico de DHCP subsiguiente. Desde la perspectiva de la detección de DHCP, los puertos de acceso no confiables no deben enviar mensajes de servidor de DHCP.

Estos pasos describen la forma en que se configura la detección de DHCP en un switch Catalyst 2960:

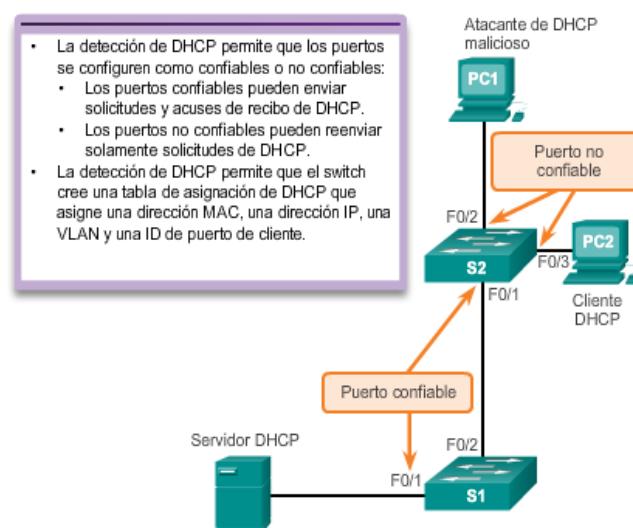
Paso 1. Habilite la detección de DHCP mediante el comando **ip dhcp snooping** del modo de configuración global.

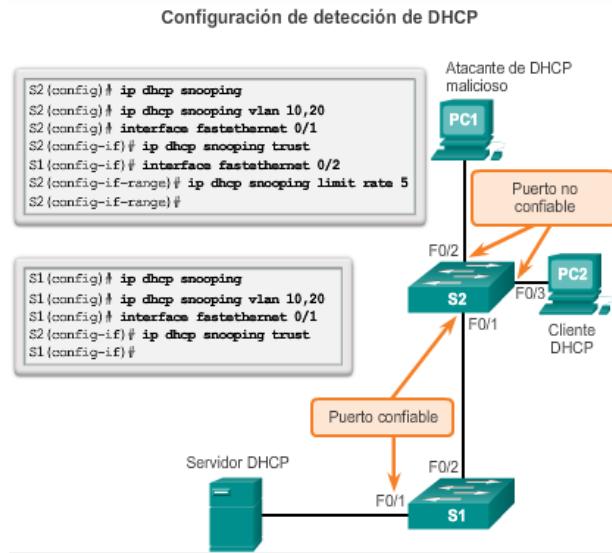
Paso 2. Habilite la detección de DHCP para VLAN específicas mediante el comando **ip dhcp snooping vlan número**.

Paso 3. Defina los puertos como confiables en el nivel de la interfaz mediante la identificación de los puertos confiables con el comando **ip dhcp snooping trust**.

Paso 4. (Optativo) Limite la velocidad a la que un atacante puede enviar solicitudes de DHCP falsas de manera continua a través de puertos no confiables al servidor de DHCP mediante el comando **ip dhcp snooping limit rate velocidad**.

Operación de detección de DHCP





Seguridad del puerto

Se deben proteger todos los puertos (interfaces) del switch antes de implementar el dispositivo para la producción. Una forma de proteger los puertos es mediante la implementación de una característica denominada “seguridad de puertos”. La seguridad de puerto limita la cantidad de direcciones MAC válidas permitidas en el puerto. Se permite el acceso a las direcciones MAC de los dispositivos legítimos, mientras que otras direcciones MAC se rechazan.

La seguridad de puertos se puede configurar para permitir una o más direcciones MAC. Si la cantidad de direcciones MAC permitidas en el puerto se limita a una, solo el dispositivo con esa dirección MAC específica puede conectarse correctamente al puerto.

Si se configura un puerto como seguro y se alcanza la cantidad máxima de direcciones MAC, cualquier intento adicional de conexión de las direcciones MAC desconocidas genera una violación de seguridad. En la figura 1, se resumen estos puntos.

Tipos de direcciones MAC seguras

Existen varias maneras de configurar la seguridad de puerto. El tipo de dirección segura se basa en la configuración e incluye lo siguiente:

- **Direcciones MAC seguras estáticas:** son direcciones MAC que se configuran manualmente en un puerto mediante el comando **switchport port-security mac-address dirección-mac** del modo de configuración de interfaz. Las direcciones MAC configuradas de esta forma se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución del switch.
- **Direcciones MAC seguras dinámicas:** son direcciones MAC detectadas dinámicamente y se almacenan solamente en la tabla de direcciones. Las direcciones MAC configuradas de esta manera se eliminan cuando el switch se reinicia.
- **Direcciones MAC seguras persistentes:** son direcciones MAC que pueden detectarse de forma dinámica o configurarse de forma manual, y que después se almacenan en la tabla de direcciones y se agregan a la configuración en ejecución.

Direcciones MAC seguras persistentes

Para configurar una interfaz a fin de convertir las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes y agregarlas a la configuración en ejecución, debe habilitar el aprendizaje por persistencia. El aprendizaje por persistencia se habilita en una interfaz mediante el comando **switchport port-security mac-address sticky** del modo de configuración de interfaz.

Cuando se introduce este comando, el switch convierte todas las direcciones MAC detectadas dinámicamente en direcciones MAC seguras persistentes, incluso las que se detectaron dinámicamente antes de que se habilitara el aprendizaje por persistencia. Todas las direcciones MAC seguras persistentes se agregan a la tabla de direcciones y a la configuración en ejecución.

Las direcciones MAC seguras persistentes también se pueden definir manualmente. Cuando se configuran direcciones MAC seguras persistentes mediante el comando **switchport port-security mac-address sticky dirección-mac** del modo de configuración de interfaz, todas las direcciones especificadas se agregan a la tabla de direcciones y a la configuración en ejecución.

Si se guardan las direcciones MAC seguras persistentes en el archivo de configuración de inicio, cuando el switch se reinicia o la interfaz se desactiva, la interfaz no necesita volver a aprender las direcciones. Si no se guardan las direcciones seguras persistentes, estas se pierden.

Si se inhabilita el aprendizaje por persistencia mediante el comando **no switchport port-security mac-address sticky** del modo de configuración de interfaz, las direcciones MAC seguras persistentes siguen formando parte de la tabla de direcciones, pero se eliminan de la configuración en ejecución.

En la figura 2, se muestran las características de las direcciones MAC seguras persistentes.

Observe que la característica de seguridad de puertos no funciona hasta que se habilita la seguridad de puertos en la interfaz mediante el comando **switchport port-security**.



Direcciones seguras persistentes

- Las direcciones MAC seguras persistentes descubiertas de forma dinámica se almacenan en el archivo running-config.
- Se eliminan del archivo running-config si se inhabilita la seguridad de puertos.
- Se pierden cuando se reinicia el switch (se apaga y se enciende).
- Si se guardan las direcciones MAC seguras persistentes en el archivo startup-config, se vuelven permanentes, y el switch las conserva después de un reinicio.
- Si se inhabilita el aprendizaje por persistencia, las direcciones MAC persistentes se convierten en direcciones dinámicas seguras y se las elimina del archivo running-config.

Existe una violación de seguridad cuando se produce cualquiera de estas situaciones:

- Se agregó la cantidad máxima de direcciones MAC seguras a la tabla de direcciones para esa interfaz, y una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz.
- Una dirección aprendida o configurada en una interfaz segura puede verse en otra interfaz segura de la misma VLAN.

Se puede configurar una interfaz para uno de tres modos de violación, con la acción específica que se debe realizar si se produce una violación. La figura muestra los tipos de tráficos de datos que se envían cuando se configura en el puerto uno de los siguientes modos de violación de seguridad.

- **Protect (Proteger):** cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. No hay ninguna notificación de que se produjo una violación de seguridad.
- **Restrict (Restringir):** cuando la cantidad de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas se descartan hasta que se elimine una cantidad suficiente de direcciones MAC seguras o se aumente la cantidad máxima de direcciones permitidas. En este modo, hay una notificación de que se produjo una violación de seguridad.
- **Shutdown (Desactivar):** en este modo de violación (predeterminado), una violación de seguridad de puerto produce que la interfaz se inhabilite de inmediato por errores y que se apague el LED del puerto. Aumenta el contador de violaciones. Cuando hay un puerto seguro en estado inhabilitado por errores, se lo puede sacar de dicho estado mediante la introducción de los comandos **shutdown** y **no shutdown** del modo de configuración de interfaz.

Para cambiar el modo de violación en un puerto de switch, use el comando del modo de configuración de interfaz **switchport port-security violation {protect| restrict | shutdown}**.

Modos de violación de seguridad

La violación a la seguridad ocurre en estas situaciones:

- Una estación cuya dirección MAC no figura en la tabla de direcciones intenta acceder a la interfaz cuando la tabla está completa.
- Una dirección se utiliza en dos interfaces seguras en la misma VLAN.

Los modos de violación de seguridad incluyen los siguientes: Protect, Restrict y Shutdown.

Modos de violación de seguridad					
Modo de violación	Envía tráfico	Envía mensaje de syslog	Muestra mensaje de error	Incrementa el contador de violaciones	Desactiva el puerto
Protect	No	No	No	No	No
Restrict	No	Sí	No	Sí	No
Shutdown	No	No	No	Sí	Sí

En la figura 1, se resume la configuración predeterminada de seguridad de puerto en un switch Cisco Catalyst.

En la figura 2, se muestran los comandos de CLI de Cisco IOS necesarios para configurar la seguridad de puertos en el puerto Fast Ethernet F0/18 del switch S1. Observe que el ejemplo no especifica un modo de violación. En este ejemplo, el modo de violación es shutdown, el modo predeterminado.

En la figura 3, se muestra cómo habilitar las direcciones MAC seguras persistentes para la seguridad de puertos en el puerto Fast Ethernet 0/19 del switch S1. Como se mencionó anteriormente, la cantidad máxima de direcciones MAC seguras se puede configurar de forma manual. En este ejemplo, la sintaxis del comando de Cisco IOS se utiliza para establecer en 10 la cantidad máxima de direcciones MAC para el puerto 0/19. De manera predeterminada, el modo de violación se establece en shutdown.

Opciones predeterminadas de seguridad de puerto

Característica	Configuración predeterminada
Seguridad del puerto	Inhabilitada en un puerto.
Número máximo de direcciones MAC seguras	1
Modo de violación	Shutdown. El puerto se desactiva cuando se supera la cantidad máxima de direcciones MAC seguras.
Aprendizaje de direcciones sin modificación	Disabled

Verificar la seguridad de puerto

Después de configurar la seguridad de puertos en un switch, revise cada interfaz para verificar que la seguridad de puertos y las direcciones MAC estáticas se configuraron correctamente.

Verificar los parámetros de seguridad de puerto

Para mostrar la configuración de seguridad de puertos para el switch o la interfaz especificada, use el comando **show port-security [interface ID-de-interfaz]**. El resultado de la configuración de la seguridad del puerto dinámico se muestra en la figura 1. De manera predeterminada, se permite una dirección MAC en este puerto.

El resultado que se muestra en la figura 2 muestra los valores de la configuración de seguridad del puerto persistente. La cantidad máxima de direcciones se estableció en 10, como se configuró.

Nota: la dirección MAC se identifica como sticky MAC (MAC persistente).

Las direcciones MAC persistentes se agregan a la tabla de direcciones MAC y a la configuración en ejecución. Como se muestra en la figura 3, la dirección MAC persistente de la PC2 se agregó a la configuración en ejecución para S1.

Verificar las direcciones MAC seguras

Para mostrar todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz específica con la información de vencimiento para cada una, use el comando **show port-security address**.

Como se muestra en la figura 4, las direcciones MAC seguras se indican junto con los tipos.

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	-

Verificación de dirección MAC: configuración dinámica

S1# show port-security interface fastethernet 0/18	S1# show port-security interface fastethernet 0/19
Port Security : Enabled	Port Security : Enabled
Port Status : Secure-up	Port Status : Secure-up
Violation Mode : Shutdown	Violation Mode : Shutdown
Aging Time : 0 mins	Aging Time : 0 mins
Aging Type : Absolute	Aging Type : Absolute
Securestatic Address Aging : Disabled	Securestatic Address Aging : Disabled
Maximum MAC Addresses : 1	Maximum MAC Addresses : 10
Total MAC Addresses : 1	Total MAC Addresses : 1
Configured MAC Addresses : 0	Configured MAC Addresses : 0
Sticky MAC Addresses : 0	Sticky MAC Addresses : 1
Last Source Address:vlan : 0025.83e6.4b01:1	Last Source Address:vlan : 0025.83e6.4b02:1
Security violation Count : 0	Security violation Count : 0
S1# show run begin FastEthernet 0/19	
interface FastEthernet 0/19	
switchport mode access	
switchport port-security maximum 10	
switchport port-security	
switchport port-security mac-address sticky	
switchport port-security mac-address sticky 0025.83e6.4b02	

Cuando se configura un puerto con seguridad de puertos, una violación puede provocar que el puerto se inhabilite por errores. Cuando un puerto se inhabilita por errores, se desactiva

eficazmente, y no se envía ni se recibe tráfico en ese puerto. En la consola (figura 1), se muestra una serie de mensajes relacionados con la seguridad del puerto.

Nota: el estado del enlace y del protocolo del puerto cambia a down (inactivo).

El LED del puerto cambia a color naranja. El comando **show interfaces** identifica el estado del puerto como **err-disabled** (figura 2). El resultado del comando **show port-security interface** ahora muestra el estado del puerto como **secure-shutdown**. Debido a que el modo de violación de seguridad de puertos está establecido en shutdown, el puerto que experimenta la violación de seguridad pasa al estado de inhabilitación por errores.

El administrador debe determinar la causa de la violación de seguridad antes de volver a habilitar el puerto. Si hay un dispositivo no autorizado conectado a un puerto seguro, el puerto no se debe volver a habilitar hasta que se elimine la amenaza de seguridad. Para volver a habilitar el puerto, use el comando **shutdown** del modo de configuración de interfaz (figura 3). Luego, use el

Mensajes de violación de seguridad de puertos	Estado del puerto
<pre>Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in err-disable state Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 00c.292b.4c75 on port FastEthernet0/18. Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state to down Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down</pre>	<pre>S1# show interface fa0/18 status Port Name Status vlan Duplex Speed Type Fa0/18 err-disabled 1 auto auto 10/100BaseTX S1# show port-security interface fastethernet 0/18 Port Security : Enabled Port Status : Secure-shutdown Violation Mode : Shutdown Aging Time : 0 mins Aging Type : Absolute Securestatic Address Aging : Disabled Maximum MAC Addresses : 1 Total MAC Addresses : 0 Configured MAC Addresses : 0 Sticky MAC Addresses : 0 Last Source Address:vlan : 000c.292b.4c75:1 Security Violation Count : 1</pre>

comando **no shutdown** del modo de configuración de interfaz para que el puerto funcione.

Cómo volver a habilitar un puerto inhabilitado por errores
<pre>S1(config)# interface FastEthernet 0/18 S1(config-if)# shutdown Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down S1(config-if)# no shutdown Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to up Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, changed state to up</pre>

Es importante tener la hora correcta dentro de las redes. Se requieren marcas de tiempo correctas para hacer un seguimiento preciso de los eventos de red, como las violaciones de seguridad. Además, la sincronización de relojes es fundamental para la interpretación correcta de los eventos dentro de los archivos de datos syslog, así como para los certificados digitales.

El protocolo NTP se usa para sincronizar los relojes de los sistemas de computación de las redes de datos conmutadas por paquetes de latencia variable. NTP permite que los dispositivos de red sincronicen la configuración de la hora con un servidor NTP. Un grupo de clientes NTP que obtienen información de fecha y hora de un único origen tiene una configuración de tiempo más coherente.

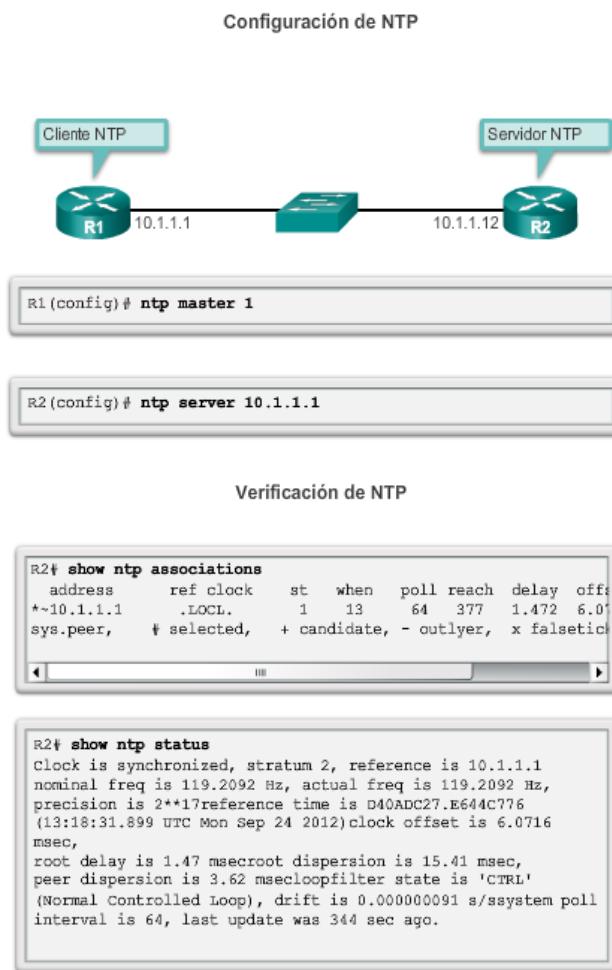
Un método seguro para proporcionar sincronización a la red es que los administradores implementen sus propios relojes maestros de red privada, sincronizados en UTC, mediante satélite o radio. Sin embargo, si los administradores de red no desean implementar sus propios relojes maestros debido al costo o a otros motivos, existen otros orígenes de reloj disponibles en Internet. NTP puede obtener la hora correcta de un origen de hora interno o externo, incluidos los siguientes:

- Reloj maestro local
- Reloj maestro en Internet
- GPS o reloj atómico

Los dispositivos de red se pueden configurar como servidor NTP o cliente NTP. Para permitir que un servidor horario NTP sincronice el reloj del software, use el comando **ntp server dirección-/P** del modo de configuración global. En la figura 1, se muestra un ejemplo de configuración. El router R2 está configurado como cliente NTP, mientras que el router R1 funciona como servidor NTP autoritativo.

Para configurar un dispositivo con un reloj maestro NTP con el que los peers se puedan sincronizar, use el comando **ntp master [capa]** del modo de configuración global. El valor de capa es un número que va de 1 a 15 e indica el número de capa NTP que informa el sistema. Si el sistema está configurado como reloj maestro NTP y no se especifica ningún número de capa, se establece la capa 8 de manera predeterminada. Si el reloj maestro NTP no llega a ningún reloj con un número de capa más bajo, el sistema informa que está sincronizado en el número de capa configurado, y otros sistemas estarán dispuestos a sincronizarse con él mediante NTP.

En la figura 2, se muestra la verificación de NTP. Para mostrar el estado de las asociaciones NTP, use el comando **show ntp associations** del modo EXEC privilegiado. Este comando indica la dirección IP de cualquier dispositivo peer sincronizado a este peer, los peers configurados de forma estática y el número de capa. El comando **show ntp status** del modo EXEC de usuario se puede utilizar para mostrar información como el estado de la sincronización de NTP, el peer con el que el dispositivo está sincronizado y las capas NTP en las que funciona el dispositivo.



2.5 Resumen

Cuando se enciende un switch LAN Cisco por primera vez, realiza la siguiente secuencia de arranque:

1. Primero, el switch carga un programa de autodiagnóstico al encender (POST) almacenado en la memoria ROM. El POST verifica el subsistema de la CPU. Este comprueba la CPU, la memoria DRAM y la parte del dispositivo flash que integra el sistema de archivos flash.
2. A continuación, el switch carga el software del cargador de arranque. El cargador de arranque es un pequeño programa almacenado en la memoria ROM que se ejecuta inmediatamente después de que el POST se completa correctamente.
3. El cargador de arranque lleva a cabo la inicialización de la CPU de bajo nivel. Inicializa los registros de la CPU, que controlan dónde está asignada la memoria física, la cantidad de memoria y su velocidad.
4. El cargador de arranque inicia el sistema de archivos flash en la placa del sistema.
5. Por último, el cargador de arranque ubica y carga en la memoria una imagen del software del sistema operativo IOS predeterminado y le cede el control del switch al IOS.

La variable de entorno BOOT determina el archivo de Cisco IOS específico que se carga. Una vez que se carga Cisco IOS, utiliza los comandos que encuentra en el archivo startup-config para inicializar y configurar las interfaces. Si faltan los archivos de Cisco IOS o estos están dañados, se puede usar el programa del cargador de arranque para volver a cargarlo o para recuperarse del problema.

Una serie de LED en el panel frontal muestra el estado de funcionamiento del switch. Estos LED indican, por ejemplo, el estado de los puertos, el modo dúplex y la velocidad.

Se configura una dirección IP en la SVI de la VLAN de administración para permitir la configuración remota del dispositivo. Se debe configurar un gateway predeterminado que pertenezca a la VLAN de administración en el switch mediante el comando **ip default-gateway**. Si el gateway predeterminado no se configura correctamente, no es posible la administración remota. Se recomienda usar Shell seguro (SSH) para proporcionar una conexión de administración segura (cifrada) a un dispositivo remoto, a fin de evitar la detección de nombres de usuario y contraseñas sin cifrar, lo cual es posible cuando se usan protocolos como Telnet.

Una de las ventajas de los switches es que permiten la comunicación full-duplex entre los dispositivos, lo que duplica la velocidad de comunicación de forma eficaz. Si bien es posible especificar la configuración de dúplex y de velocidad de una interfaz de switch, se recomienda permitir que el switch configure estos parámetros automáticamente para evitar errores.

La seguridad de puertos del switch es un requisito para evitar los ataques como la saturación de direcciones MAC y la suplantación de identidad de DHCP. Los puertos de switch se deben configurar para permitir que ingresen solo las tramas con direcciones MAC de origen específicas. Se deben rechazar las direcciones MAC de origen desconocidas, y se debe desactivar el puerto para evitar otros ataques.

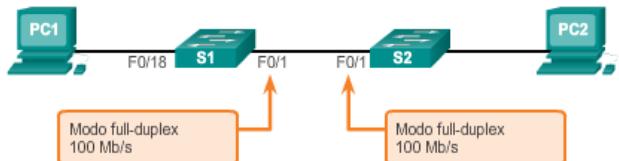
La seguridad de puertos es solo uno de los métodos de defensa contra los riesgos que puede sufrir la red. Existen 10 prácticas recomendadas que representan los métodos más seguros para una red:

- Desarrolle una política de seguridad escrita para la organización.
- Desactive los servicios y puertos que no se utilicen.
- Utilice contraseñas seguras y cámbielas con frecuencia.
- Controle el acceso físico a los dispositivos.
- Evite usar sitios web HTTP estándar inseguros, especialmente para las pantallas de inicio de sesión. En lugar de esto, use HTTPS, que es más seguro.
- Realice copias de respaldo y pruébelas periódicamente.
- Capacite a los empleados sobre los ataques de ingeniería social y desarrolle políticas para validar identidades por teléfono, mediante correo electrónico y personalmente.
- Cifre los datos confidenciales y protéjalos con una contraseña segura.

- Implemente hardware y software de seguridad, como firewalls.
 - Mantenga el software IOS actualizado mediante la instalación semanal o mensual de parches de seguridad, si es posible.

Estos métodos son solo un punto de partida para la administración de la seguridad. Las organizaciones deben mantenerse alerta en todo momento para defenderse de estas amenazas en constante evolución.

Configurar dúplex y velocidad



Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	S1# configure terminal
Ingrese el modo de configuración de interfaz.	S1(config)# interface FastEthernet 0/1
Configura el modo dúplex de la interfaz.	S1(config-if)# duplex full
Configura la velocidad de la interfaz.	S1(config-if)# speed 100
Vuelve al modo EXEC privilegiado.	S1(config-if)# end
Guarda la configuración en ejecución en la configuración de inicio.	S1# copy running-config startup-config

3 VLAN

3.1 Introducción

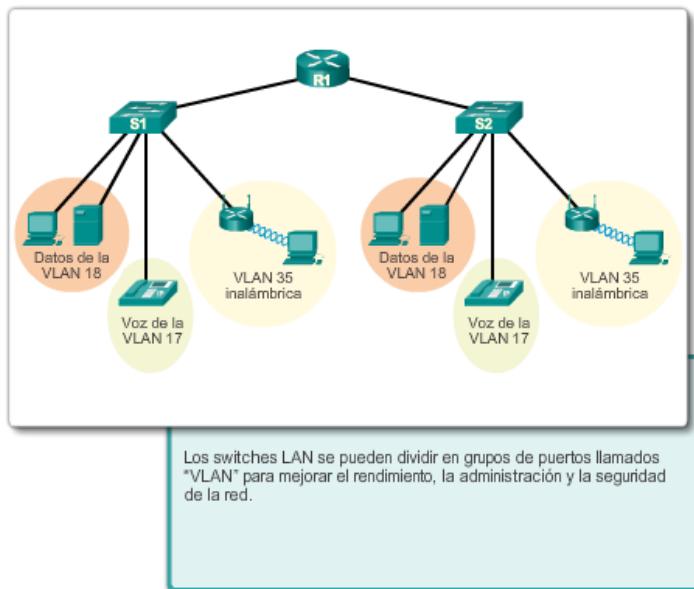
El rendimiento de la red es un factor importante en la productividad de una organización. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños. Por una cuestión de diseño, los routers bloquean el tráfico de difusión en una interfaz. Sin embargo, los routers generalmente tienen una cantidad limitada de interfaces LAN. La función principal de un router es trasladar información entre las redes, no proporcionar acceso a la red a las terminales.

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización. Si bien las VLAN se utilizan principalmente dentro de las redes de área local comutadas, las implementaciones modernas de las VLAN les permiten abarcar redes MAN y WAN.

En este capítulo, se describe cómo configurar y administrar VLAN y enlaces troncales de VLAN, así como resolver problemas relacionados. También se analizan cuestiones y estrategias de seguridad relacionadas con las VLAN y los enlaces troncales, así como las prácticas recomendadas para el diseño de VLAN.

Después de completar este capítulo, podrá hacer lo siguiente:

- Explicar la finalidad de las VLAN en una red comutada.
- Analizar cómo un switch reenvía tramas según la configuración de VLAN en un entorno comutado múltiple.
- Configurar un puerto de switch que se asignará a una VLAN según los requisitos.
- Configurar un puerto de enlace troncal en un switch LAN.
- Configurar el protocolo de enlace troncal dinámico (DTP).
- Solucionar problemas de configuración de VLAN y de enlaces troncales en una red comutada.
- Configurar las características de seguridad para mitigar los ataques en un entorno segmentado por VLAN.
- Explicar las prácticas recomendadas de seguridad para un entorno segmentado por VLAN.



3.2 Segmentación de VLAN

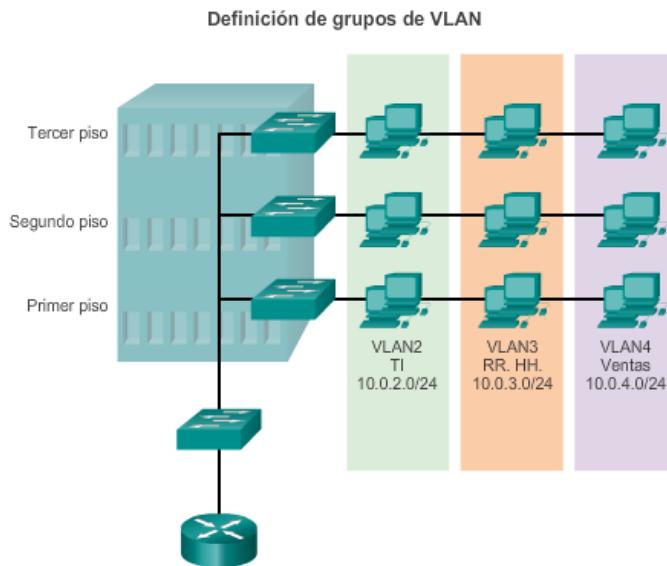
3.2.1

Dentro de un entorno de internetwork comutada, las VLAN proporcionan la segmentación y la flexibilidad organizativa. Las VLAN proporcionan una manera de agrupar dispositivos dentro de una LAN. Un grupo de dispositivos dentro de una VLAN se comunican como si estuvieran conectados al mismo cable. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas.

Las VLAN permiten que el administrador divida las redes en segmentos según factores como la función, el equipo del proyecto o la aplicación, sin tener en cuenta la ubicación física del usuario o del dispositivo. Los dispositivos dentro de una VLAN funcionan como si estuvieran en su propia red independiente, aunque comparten una misma infraestructura con otras VLAN. Cualquier puerto de switch puede pertenecer a una VLAN, y los paquetes de unidifusión, difusión y multidifusión se reenvían y saturan solo las estaciones terminales dentro de la VLAN donde se originan los paquetes. Cada VLAN se considera una red lógica independiente, y los paquetes destinados a las estaciones que no pertenecen a la VLAN se deben reenviar a través de un dispositivo que admite el routing.

Una VLAN crea un dominio de difusión lógico que puede abarcar varios segmentos LAN físicos. Las VLAN mejoran el rendimiento de la red mediante la división de grandes dominios de difusión en otros más pequeños. Si un dispositivo en una VLAN envía una trama de Ethernet de difusión, todos los dispositivos en la VLAN reciben la trama, pero los dispositivos en otras VLAN no la reciben.

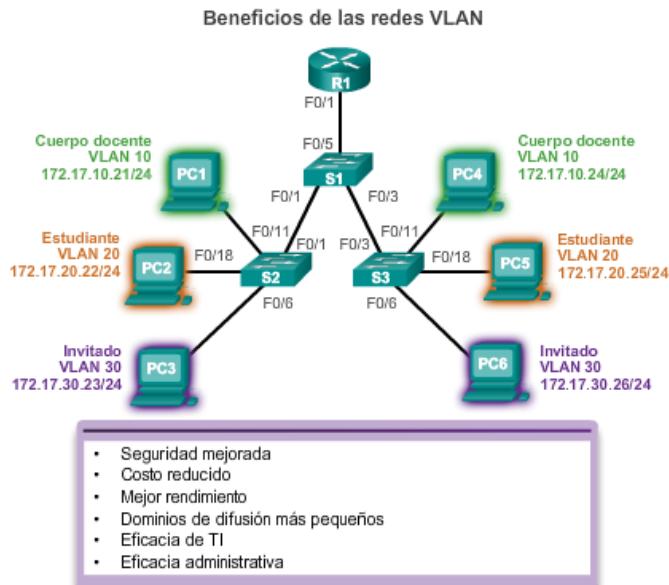
Las VLAN habilitan la implementación de las políticas de acceso y de seguridad según grupos específicos de usuarios. Cada puerto de switch se puede asignar a una sola VLAN (a excepción de un puerto conectado a un teléfono IP o a otro switch).



La productividad de los usuarios y la adaptabilidad de la red son importantes para el crecimiento y el éxito de las empresas. Las redes VLAN facilitan el diseño de una red para dar soporte a los objetivos de una organización. Los principales beneficios de utilizar las VLAN son los siguientes:

- **Seguridad:** los grupos que tienen datos sensibles se separan del resto de la red, lo que disminuye las posibilidades de que ocurran violaciones de información confidencial. Como se muestra en la ilustración, las computadoras del cuerpo docente están en la VLAN 10 y separadas por completo del tráfico de datos de los estudiantes y los Invitados.
- **Reducción de costos:** el ahorro de costos se debe a la poca necesidad de actualizaciones de red costosas y al uso más eficaz de los enlaces y del ancho de banda existentes.
- **Mejor rendimiento:** la división de las redes planas de capa 2 en varios grupos de trabajo lógicos (dominios de difusión) reduce el tráfico innecesario en la red y mejora el rendimiento.
- **Dominios de difusión reducidos:** la división de una red en redes VLAN reduce la cantidad de dispositivos en el dominio de difusión. Como se muestra en la ilustración, existen seis computadoras en esta red, pero hay tres dominios de difusión: Cuerpo docente, Estudiantes e Invitados.
- **Mayor eficiencia del personal de TI:** las VLAN facilitan el manejo de la red debido a que los usuarios con requerimientos similares de red comparten la misma VLAN. Cuando se dispone de un switch nuevo, se implementan todas las políticas y los procedimientos que ya se configuraron para la VLAN específica cuando se asignan los puertos. También es fácil para el personal de TI identificar la función de una VLAN proporcionándole un nombre. En la ilustración, para facilitar la identificación, se denominó "Cuerpo Docente" a la VLAN 10, "Estudiantes" a la VLAN 20 e "Invitados" a la VLAN 30.
- **Administración más simple de aplicaciones y proyectos:** las VLAN agregan dispositivos de red y usuarios para admitir los requisitos geográficos o comerciales. Al tener características diferentes, se facilita la administración de un proyecto o el trabajo con una aplicación especializada; un ejemplo de este tipo de aplicación es una plataforma de desarrollo de aprendizaje por medios electrónicos para el cuerpo docente.

Cada VLAN en una red commutada corresponde a una red IP; por lo tanto, al diseñar la VLAN, se debe tener en cuenta la implementación de un esquema de direccionamiento de red jerárquico. El direccionamiento jerárquico de la red significa que los números de red IP se aplican a los segmentos de red o a las VLAN de manera ordenada, lo que permite que la red se tome en cuenta como conjunto. Los bloques de direcciones de red contiguas se reservan para los dispositivos en un área específica de la red y se configuran en estos, como se muestra en la ilustración.



Existen diferentes tipos de redes VLAN, los cuales se utilizan en las redes modernas. Algunos tipos de VLAN se definen según las clases de tráfico. Otros tipos de VLAN se definen según la función específica que cumplen.

VLAN de datos

Una VLAN de datos es una VLAN configurada para transportar tráfico generado por usuarios. Una VLAN que transporta tráfico de administración o de voz no sería una VLAN de datos. Es una práctica común separar el tráfico de voz y de administración del tráfico de datos. A veces a una VLAN de datos se la denomina VLAN de usuario. Las VLAN de datos se usan para dividir la red en grupos de usuarios o dispositivos.

VLAN predeterminada

Todos los puertos de switch se vuelven parte de la VLAN predeterminada después del arranque inicial de un switch que carga la configuración predeterminada. Los puertos de switch que participan en la VLAN predeterminada forman parte del mismo dominio de difusión. Esto admite cualquier dispositivo conectado a cualquier puerto de switch para comunicarse con otros dispositivos en otros puertos de switch. La VLAN predeterminada para los switches Cisco es la VLAN 1. En la ilustración, se emitió el comando **show vlan brief** en un switch que ejecuta la configuración predeterminada. Observe que todos los puertos se asignan a la VLAN 1 de manera predeterminada.

La VLAN 1 tiene todas las características de cualquier VLAN, excepto que no se le puede cambiar el nombre ni se puede eliminar. Todo el tráfico de control de capa 2 se asocia a la VLAN 1 de manera predeterminada.

VLAN nativa

Una VLAN nativa está asignada a un puerto troncal 802.1Q. Los puertos de enlace troncal son los enlaces entre switches que admiten la transmisión de tráfico asociado a más de una VLAN. Los puertos de enlace troncal 802.1Q admiten el tráfico proveniente de muchas VLAN (tráfico con etiquetas), así como el tráfico que no proviene de una VLAN (tráfico sin etiquetar). El tráfico con etiquetas hace referencia al tráfico que tiene una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original, que especifica la VLAN a la que pertenece la trama. El puerto de enlace troncal 802.1Q coloca el tráfico sin etiquetar en la VLAN nativa, que es la VLAN 1 de manera predeterminada.

Las VLAN nativas se definen en la especificación IEEE 802.1Q a fin de mantener la compatibilidad con el tráfico sin etiquetar de modelos anteriores común a las situaciones de LAN antiguas. Una VLAN nativa funciona como identificador común en extremos opuestos de un enlace troncal.

Se recomienda configurar la VLAN nativa como VLAN sin utilizar, independiente de la VLAN 1 y de otras VLAN. De hecho, es común utilizar una VLAN fija para que funcione como VLAN nativa para todos los puertos de enlace troncal en el dominio comutado.

VLAN de administración

Una VLAN de administración es cualquier VLAN que se configura para acceder a las capacidades de administración de un switch. La VLAN 1 es la VLAN de administración de manera predeterminada. Para crear la VLAN de administración, se asigna una dirección IP y una máscara de subred a la interfaz virtual de switch (SVI) de esa VLAN, lo que permite que el switch se administre mediante HTTP, Telnet, SSH o SNMP. Dado que en la configuración de fábrica de un switch Cisco la VLAN 1 se establece como VLAN predeterminada, la VLAN 1 no es una elección adecuada para la VLAN de administración.

En el pasado, la VLAN de administración para los switches 2960 era la única SVI activa. En las versiones 15.x de IOS de Cisco para los switches de la serie Catalyst 2960, es posible tener más de una SVI activa. Con IOS de Cisco 15.x, se debe registrar la SVI activa específica asignada para la administración remota. Si bien, en teoría, un switch puede tener más de una VLAN de administración, esto aumenta la exposición a los ataques de red.

En la ilustración, actualmente todos los puertos están asignados a la VLAN 1 predeterminada. No hay ninguna VLAN nativa asignada explícitamente ni otras VLAN activas; por lo tanto, la VLAN nativa de la red que se diseñó es la VLAN de administración. Esto se considera un riesgo de seguridad.

VLAN 1			
VLAN Name	Status	Ports	
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2	
1002 fddi-default	act/unsup		
1003 token-ring-default	act/unsup		
1004 fddinet-default	act/unsup		
1005 trnet-default	act/unsup		

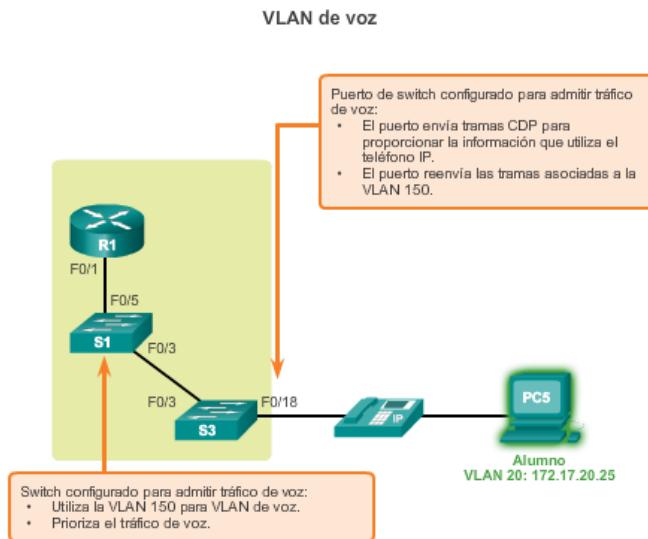
- De manera predeterminada, todos los puertos están asignados a la VLAN 1 para reenviar datos.
- De manera predeterminada, la VLAN nativa es la VLAN 1.
- De manera predeterminada, la VLAN de administración es la VLAN 1.
- No se puede cambiar el nombre ni eliminar la VLAN 1.

Se necesita una VLAN separada para admitir la tecnología de voz sobre IP (VoIP). El tráfico de VoIP requiere:

- Ancho de banda garantizado para asegurar la calidad de la voz
- Prioridad de la transmisión sobre los tipos de tráfico de la red
- Capacidad para ser enrutado en áreas congestionadas de la red
- Una demora inferior a 150 ms a través de la red

Para cumplir estos requerimientos, se debe diseñar la red completa para que admita VoIP. Los detalles sobre cómo configurar una red para que admita VoIP exceden el ámbito de este curso, pero es útil resumir cómo funciona una VLAN de voz entre un switch, un teléfono IP Cisco y una computadora.

En la figura, la VLAN 150 se diseña para enviar tráfico de voz. La computadora del estudiante PC5 está conectada al teléfono IP de Cisco y el teléfono está conectado al switch S3. La PC5 está en la VLAN 20 que se utiliza para los datos de los estudiantes.



3.2.2 Redes VLAN en un entorno commutado múltiple

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red que lleva más de una VLAN. Un enlace troncal de VLAN amplía las VLAN a través de toda la red. Cisco admite IEEE 802.1Q para coordinar enlaces troncales en las interfaces Fast Ethernet, Gigabit Ethernet y 10-Gigabit Ethernet.

Las VLAN no serían muy útiles sin los enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que se propague todo el tráfico de VLAN entre los switches, de modo que los dispositivos que están en la misma VLAN pero conectados a distintos switches se puedan comunicar sin la intervención de un router.

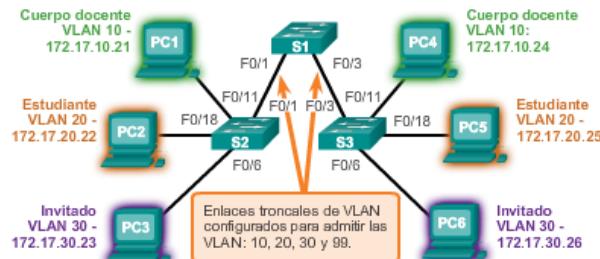
Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para varias VLAN entre switches y routers. También se puede utilizar un enlace troncal entre un dispositivo de red y un servidor u otro dispositivo que cuente con una NIC con capacidad 802.1Q. En los switches Cisco Catalyst, se admiten todas las VLAN en un puerto de enlace troncal de manera predeterminada.

En la ilustración, los enlaces entre los switches S1 y S2, y S1 y S3 se configuraron para transmitir el tráfico proveniente de las VLAN 10, 20, 30 y 99 a través de la red. Esta red no podría funcionar sin los enlaces troncales de VLAN.

Enlaces troncales de la VLAN

VLAN 10 de cuerpo docente/personal:
172.17.10.0/24
VLAN 20 de estudiantes: 172.17.20.0/24
VLAN 30 de invitados: 172.17.30.0/24
VLAN 99 de administración y nativa:
172.17.99.0/24

Las interfaces F0/1 a 5 son interfaces de enlace troncal 802.1Q con una VLAN nativa 99.
Las interfaces F0/11 a 17 están en la VLAN 10.
Las interfaces F0/18 a 24 están en la VLAN 20.
Las interfaces F0/6 a 10 están en la VLAN 30.

**Redes sin VLAN**

En condiciones normales de funcionamiento, cuando un switch recibe una trama de difusión en uno de sus puertos, reenvía la trama por todos los demás puertos, excepto el puerto por donde recibió la difusión. En la animación de la figura 1, se configuró toda la red en la misma subred (172.17.40.0/24), y no se configuró ninguna VLAN. Como consecuencia, cuando la computadora del cuerpo docente (PC1) envía una trama de difusión, el switch S2 envía dicha trama de difusión por todos sus puertos. Finalmente, toda la red recibe la difusión porque la red es un dominio de difusión.

Red con VLAN

Como se muestra en la animación de la figura 2, la red se segmentó mediante dos VLAN. Los dispositivos del cuerpo docente se asignaron a la VLAN 10, y los dispositivos de los estudiantes se asignaron a la VLAN 20. Cuando se envía una trama de difusión desde la computadora del cuerpo docente, la PC1, al switch S2, el switch reenvía esa trama de difusión solo a los puertos de switch configurados para admitir la VLAN 10.

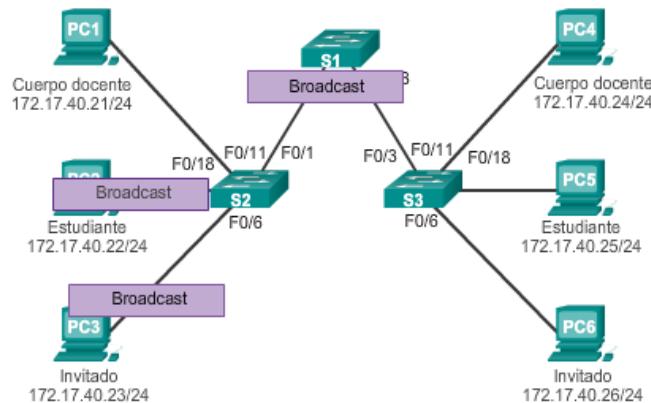
Los puertos que componen la conexión entre los switches S2 y S1 (puertos F0/1), y entre el S1 y el S3 (puertos F0/3) son enlaces troncales y se configuraron para admitir todas las VLAN en la red.

Cuando el S1 recibe la trama de difusión en el puerto F0/1, reenvía la trama de difusión por el único puerto configurado para admitir la VLAN 10, que es el puerto F0/3. Cuando el S3 recibe la trama de difusión en el puerto F0/3, reenvía la trama de difusión por el único puerto configurado para admitir la VLAN 10, que es el puerto F0/11. La trama de difusión llega a la única otra computadora de la red configurada en la VLAN 10, que es la computadora PC4 del cuerpo docente.

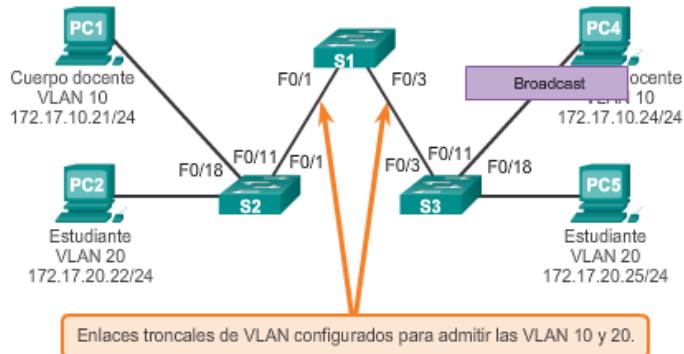
Cuando se implementan las VLAN en un switch, la transmisión del tráfico de unidifusión, multidifusión y difusión desde un host en una VLAN en particular se limita a los dispositivos presentes en esa VLAN.

Sin segmentación de VLAN

La PC1 envía una difusión de capa 2 local. Los switches reenvían la trama del broadcast a todos los puertos disponibles.

**Con segmentación de VLAN**

La PC1 envía una difusión de capa 2 local. Los switches reenvían la trama de la difusión solamente a los puertos configurados para VLAN 10.



Los switches de la serie Catalyst 2960 son dispositivos de capa 2. Estos utilizan la información del encabezado de la trama de Ethernet para reenviar paquetes. No poseen tablas de routing. El encabezado de las tramas de Ethernet estándar no contiene información sobre la VLAN a la que pertenece la trama; por lo tanto, cuando las tramas de Ethernet se colocan en un enlace troncal, se debe agregar la información sobre las VLAN a las que pertenecen. Este proceso, denominado "etiquetado", se logra mediante el uso del encabezado IEEE 802.1Q, especificado en el estándar IEEE 802.1Q. El encabezado 802.1Q incluye una etiqueta de 4 bytes insertada en el encabezado de la trama de Ethernet original que especifica la VLAN a la que pertenece la trama.

Cuando el switch recibe una trama en un puerto configurado en modo de acceso y asignado a una VLAN, el switch coloca una etiqueta VLAN en el encabezado de la trama, vuelve a calcular la FCS y envía la trama etiquetada por un puerto de enlace troncal.

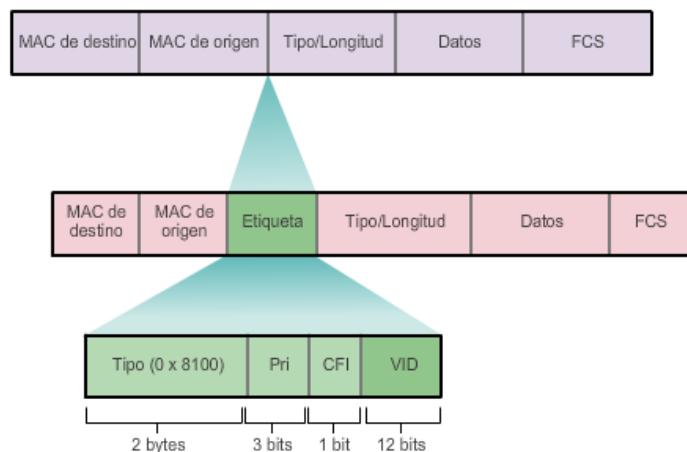
Detalles del campo de etiqueta de la VLAN

El campo de etiqueta de la VLAN consta de un campo de tipo, un campo de prioridad, un campo de identificador de formato canónico y un campo de ID de la VLAN:

- **Tipo:** es un valor de 2 bytes denominado “ID de protocolo de etiqueta” (TPID). Para Ethernet, este valor se establece en 0x8100 hexadecimal.
- **Prioridad de usuario:** es un valor de 3 bits que admite la implementación de nivel o de servicio.
- **Identificador de formato canónico (CFI):** es un identificador de 1 bit que habilita las tramas Token Ring que se van a transportar a través de los enlaces Ethernet.
- **ID de VLAN (VID):** es un número de identificación de VLAN de 12 bits que admite hasta 4096 ID de VLAN.

Una vez que el switch introduce los campos Tipo y de información de control de etiquetas, vuelve a calcular los valores de la FCS e inserta la nueva FCS en la trama.

Campos en una trama Ethernet 802.1Q



Tramas etiquetadas en la VLAN nativa

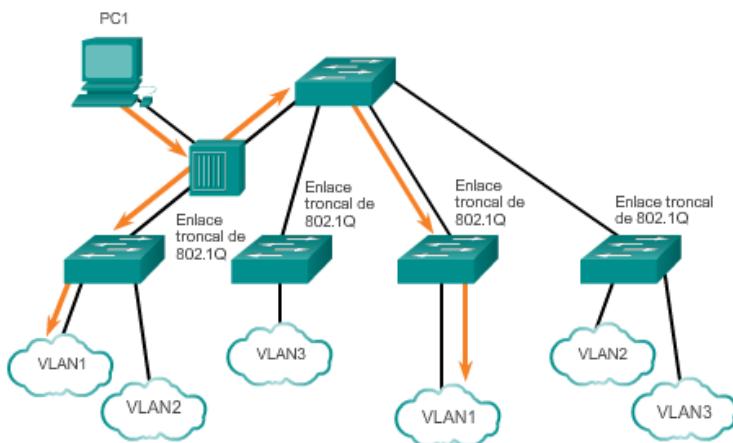
Algunos dispositivos que admiten enlaces troncales agregan una etiqueta VLAN al tráfico de las VLAN nativas. El tráfico de control que se envía por la VLAN nativa no se debe etiquetar. Si un puerto de enlace troncal 802.1Q recibe una trama etiquetada con la misma ID de VLAN que la VLAN nativa, descarta la trama. Por consiguiente, al configurar un puerto de un switch Cisco, configure los dispositivos de modo que no envíen tramas etiquetadas por la VLAN nativa. Los dispositivos de otros proveedores que admiten tramas etiquetadas en la VLAN nativa incluyen: teléfonos IP, servidores, routers y switches que no pertenecen a Cisco.

Tramas sin etiquetar en la VLAN nativa

Cuando un puerto de enlace troncal de un switch Cisco recibe tramas sin etiquetar (poco usuales en las redes bien diseñadas), envía esas tramas a la VLAN nativa. Si no hay dispositivos asociados a la VLAN nativa (lo que no es poco usual) y no existen otros puertos de enlace troncal (lo que no es poco usual), se descarta la trama. La VLAN nativa predeterminada es la VLAN 1. Al configurar un puerto de enlace troncal 802.1Q, se asigna el valor de la ID de VLAN nativa a la ID de VLAN de puerto (PVID) predeterminada. Todo el tráfico sin etiquetar entrante o saliente del puerto 802.1Q se reenvía según el valor de la PVID. Por ejemplo, si se configura la VLAN 99 como VLAN nativa, la PVID es 99, y todo el tráfico sin etiquetar se reenvía a la VLAN 99. Si no se volvió a configurar la VLAN nativa, el valor de la PVID se establece en VLAN 1.

En la ilustración, la PC1 está conectada a un enlace troncal 802.1Q mediante un hub. La PC1 envía el tráfico sin etiquetar que los switches asocian a la VLAN nativa configurada en los puertos de enlace troncal y que reenvían según corresponda. El tráfico etiquetado del enlace troncal que recibe la PC1 se descarta. Esta situación refleja un diseño de red deficiente por varios motivos: utiliza un hub, tiene un host conectado a un enlace troncal y esto implica que los switches tengan puertos de acceso asignados a la VLAN nativa. Sin embargo, ilustra la motivación de la especificación IEEE 802.1Q para que las VLAN nativas sean un medio de manejo de entornos antiguos.

VLAN nativa en el enlace troncal 802.1Q



Recuerde que, para admitir VoIP, se requiere una VLAN de voz separada.

Un puerto de acceso que se usa para conectar un teléfono IP de Cisco se puede configurar para usar dos VLAN separadas: una VLAN para el tráfico de voz y otra VLAN para el tráfico de datos desde un dispositivo conectado al teléfono. El enlace entre el switch y el teléfono IP funciona como un enlace troncal para transportar tanto el tráfico de la VLAN de voz como el tráfico de la VLAN de datos.

El teléfono IP Cisco contiene un switch integrado 10/100 de tres puertos. Los puertos proporcionan conexiones dedicadas para estos dispositivos:

- El puerto 1 se conecta al switch o a otro dispositivo VoIP.

- El puerto 2 es una interfaz interna 10/100 que envía el tráfico del teléfono IP.
 - El puerto 3 (puerto de acceso) se conecta a una PC u otro dispositivo.

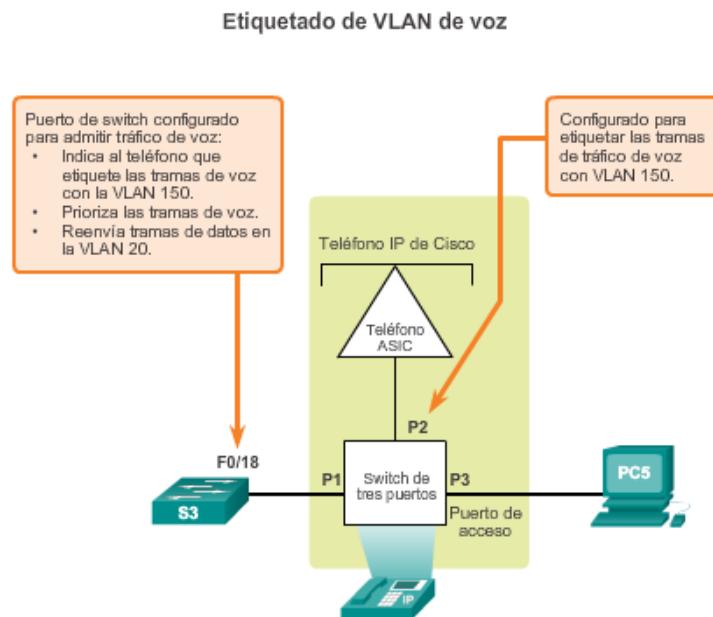
En el switch, el acceso está configurado para enviar paquetes del protocolo de descubrimiento de Cisco (CDP) que instruyen a un teléfono IP conectado para que envíe el tráfico de voz al switch en una de tres formas posibles, según el tipo de tráfico:

- En una VLAN de voz con una etiqueta de valor de prioridad de clase de servicio (CoS) de capa 2.
 - En una VLAN de acceso con una etiqueta de valor de prioridad de CoS de capa 2.
 - En una VLAN de acceso sin etiqueta (sin valor de prioridad de CoS de capa 2).

En la figura 1, la computadora del estudiante PC5 está conectada a un teléfono IP de Cisco, y el teléfono está conectado al switch S3. La VLAN 150 está diseñada para transportar tráfico de voz, mientras que la PC5 está en la VLAN 20, que se usa para los datos de los estudiantes.

Ejemplo de configuración

En la figura 2, se muestra un resultado de ejemplo. El análisis de los comandos de voz de IOS de Cisco exceden el ámbito de este curso, pero las áreas resaltadas en el resultado de ejemplo muestran que la interfaz F0/18 se configuró con una VLAN configurada para datos (VLAN 20) y una VLAN configurada para voz (VLAN 150).



Ejemplo de configuración

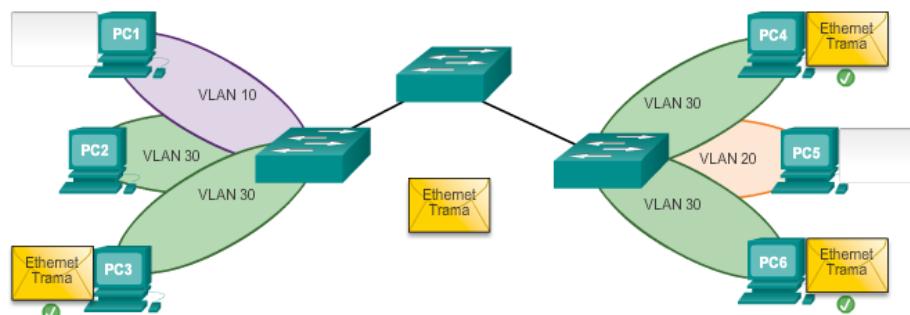
```

S1# sh interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
voice VLAN: 150 (voice)

<resultado omitido>

```

Situación 2: PC 2 envía una difusión. ¿Cuáles son las computadoras que reciben una copia de la trama de difusión?



3.3 Implementaciones de VLAN

3.3.1 Asignación de red VLAN

Los distintos switches Cisco Catalyst admiten diversas cantidades de VLAN. La cantidad de VLAN que admiten es suficiente para satisfacer las necesidades de la mayoría de las organizaciones. Por ejemplo, los switches de las series Catalyst 2960 y 3560 admiten más de 4000 VLAN. Las VLAN de rango normal en estos switches se numeran del 1 al 1005, y las VLAN de rango extendido se numeran del 1006 al 4094. En la ilustración, se muestran las VLAN disponibles en un switch Catalyst 2960 que ejecuta IOS de Cisco, versión 15.x.

VLAN de rango normal

- Se utiliza en redes de pequeños y medianos negocios y empresas.
- Se identifica mediante un ID de VLAN entre 1 y 1005.
- Los ID de 1002 a 1005 se reservan para las VLAN Token Ring y FDDI.
- Los ID 1 y 1002 a 1005 se crean automáticamente y no se pueden eliminar.
- Las configuraciones se almacenan en un archivo de base de datos de VLAN, denominado `vlan.dat`. El archivo `vlan.dat` se encuentra en la memoria flash del switch.
- El protocolo de enlace troncal de VLAN (VTP), que permite administrar la configuración de VLAN entre los switches, solo puede descubrir y almacenar redes VLAN de rango normal.

VLAN de rango extendido

- Posibilita a los proveedores de servicios que amplíen sus infraestructuras a una cantidad de clientes mayor. Algunas empresas globales podrían ser lo suficientemente grandes como para necesitar los ID de las VLAN de rango extendido.
- Se identifican mediante un ID de VLAN entre 1006 y 4094.
- Las configuraciones no se escriben en el archivo `vlan.dat`.
- Admiten menos características de VLAN que las VLAN de rango normal.
- Se guardan en el archivo de configuración en ejecución de manera predeterminada.
- VTP no aprende las VLAN de rango extendido.

Nota: la cantidad máxima de VLAN disponibles en los switches Catalyst es 4096, ya que el campo ID de VLAN tiene 12 bits en el encabezado IEEE 802.1Q.

VLAN de rango normal

switch# show vlan brief			
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdininet-default	act/unsup	
1005	trnet-default	act/unsup	

Al configurar redes VLAN de rango normal, los detalles de configuración se almacenan en la memoria flash del switch en un archivo denominado `vlan.dat`. La memoria flash es persistente y no requiere el comando **copy running-config startup-config**. Sin embargo, debido a que en los switches Cisco se suelen configurar otros detalles al mismo tiempo que se crean las VLAN, es aconsejable guardar los cambios a la configuración en ejecución en la configuración de inicio.

En la figura 1, se muestra la sintaxis del comando de IOS de Cisco que se utiliza para agregar una VLAN a un switch y asignarle un nombre. Se recomienda asignarle un nombre a cada VLAN en la configuración de un switch.

En la figura 2, se muestra cómo se configura la VLAN para estudiantes (VLAN 20) en el switch S1. En el ejemplo de topología, la computadora del estudiante (PC2) todavía no se asoció a ninguna VLAN, pero tiene la dirección IP 172.17.20.22.

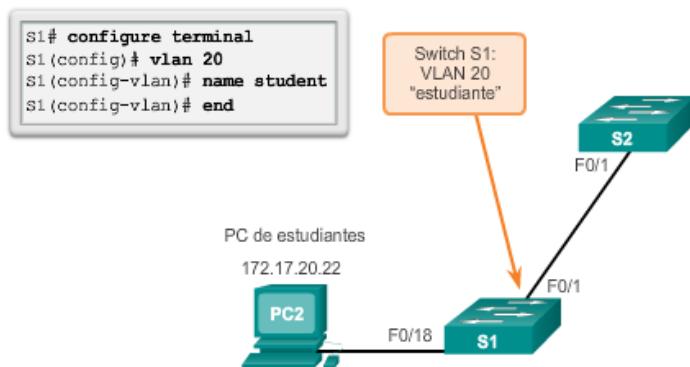
Utilice el verificador de sintaxis de la figura 3 para crear una VLAN y utilice el comando **show vlan brief** para mostrar el contenido del archivo `vlan.dat`.

Además de introducir una única ID de VLAN, se puede introducir una serie de ID de VLAN separadas por comas o un rango de ID de VLAN separado por guiones con el comando **vlan id-vlan**. Por ejemplo, utilice el siguiente comando para crear las VLAN 100, 102, 105, 106 y 107:

```
S1(config)# vlan 100,102,105-107
```

Creación de una VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	s1# configure terminal
Cree una VLAN con un número de ID válido.	s1(config)#vlan id-vlan
Especifique un nombre único para identificar la VLAN.	s1(config-vlan)#name nombre-vlan
Vuelva al modo EXEC privilegiado.	s1(config-vlan)#end



Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. Un puerto de acceso puede pertenecer a una sola VLAN por vez; una excepción a esta regla es un puerto conectado a un teléfono IP, en cuyo caso, hay dos VLAN asociadas al puerto: una para voz y otra para datos.

En la figura 1, se muestra la sintaxis para definir un puerto como puerto de acceso y asignarlo a una VLAN. El comando **switchport mode access** es optativo, pero se aconseja como práctica recomendada de seguridad. Con este comando, la interfaz cambia al modo de acceso permanente.

Nota: utilice el comando **interface range** para configurar varias interfaces simultáneamente.

En el ejemplo de la figura 2, la VLAN 20 se asigna al puerto F0/18 del switch S1; por lo tanto, la computadora de estudiantes (PC2) está en la VLAN 20. Cuando se configura la VLAN 20 en otros switches, el administrador de red sabe que debe configurar las otras computadoras de estudiantes para que estén en la misma subred que la PC2 (172.17.20.0/24).

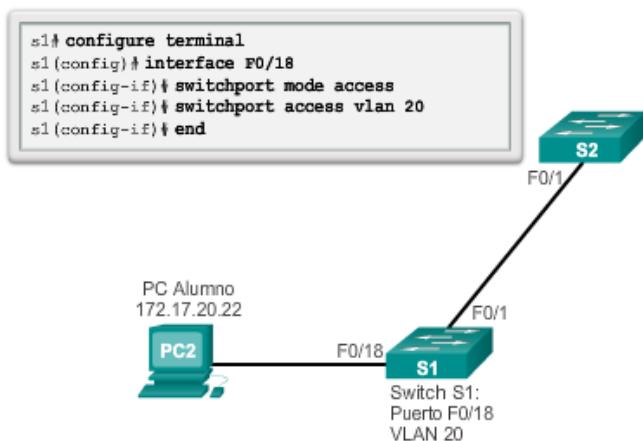
Utilice el verificador de sintaxis de la figura 3 para asignar una VLAN y utilice el comando **show vlan brief** para mostrar el contenido del archivo **vlan.dat**.

El comando **switchport access vlan** fuerza la creación de una VLAN si es que aún no existe en el switch. Por ejemplo, la VLAN 30 no está presente en el resultado del comando **show vlan brief** del switch. Si se introduce el comando **switchport access vlan 30** en cualquier interfaz sin configuración previa, el switch muestra lo siguiente:

```
% Access VLAN does not exist. Creating vlan 30
```

Asignación de puertos a las VLAN

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	s1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	s1(config)# interface id_iface
Establezca el puerto en modo de acceso.	s1(config-if)# switchport mode access
Asigne el puerto a una VLAN.	s1(config-if)# switchport access vlan id_vlan
Vuelva al modo EXEC privilegiado.	s1(config-if)# end



Existen varias maneras de cambiar la pertenencia de puertos de una VLAN. En la figura 1, se muestra la sintaxis para cambiar la pertenencia de un puerto de switch de la VLAN 1 con el comando **no switchport access vlan** del modo de configuración de interfaz.

La interfaz F0/18 se asignó anteriormente a la VLAN 20. Se introduce el comando **no switchport access vlan** para la interfaz F0/18. Examine el resultado del comando **show vlan brief** que le sigue inmediatamente, como se muestra en la figura 2. El comando **show vlan brief** muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. El comando **show vlan brief** muestra una línea para cada VLAN. El resultado para cada VLAN incluye el nombre, el estado y los puertos de switch de la VLAN.

La VLAN 20 sigue activa, aunque no tenga puertos asignados. En la figura 3, se muestra que el resultado del comando **show interfaces f0/18 switchport** verifica que la VLAN de acceso para la interfaz F0/18 se haya restablecido a la VLAN 1.

La pertenencia de VLAN de un puerto se puede cambiar fácilmente. No es necesario eliminar primero un puerto de una VLAN para cambiar su pertenencia de VLAN. Cuando se vuelve a asignar la pertenencia de VLAN de un puerto de acceso a otra VLAN existente, la nueva pertenencia de VLAN simplemente reemplaza la pertenencia de VLAN anterior. En la figura 4, el puerto F0/11 se asignó a la VLAN 20.

Utilice el verificador de sintaxis de la figura 5 para cambiar la pertenencia de puertos de una VLAN.

Eliminación de la asignación de VLAN

Comandos de IOS de un switch Cisco

Ingrese al modo de configuración global.	s1# configure terminal
Elimine la asignación de la VLAN del puerto.	s1(config-if)# no switchport access vlan
Vuelva al modo EXEC privilegiado.	s1(config-if)# end

Ejemplo de configuración

```

S1(config)# int F0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name          Status    Ports
---- --
1     default       active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                           Gi0/1, Gi0/2
20    student        active
1002 fddi-default   act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default   act/unsup
S1#

```

Verificación

```

S1# sh interfaces F0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)

<resultado omitido>

```

Asignación de un puerto a una VLAN

```

S1# config t
S1(config)# int F0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name          Status      Ports
--- -----
1    default        active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/12, Fa0/13
                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                           Fa0/22, Fa0/23, Fa0/24, Gi0/1
                           Gi0/2
20   student        active     F0/11
1002 fddi-default   act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default   act/unsup
S1#

```

En la ilustración, se utiliza el comando **no vlan id-vlan** del modo de configuración global para eliminar la VLAN 20 del switch. El switch S1 tenía una configuración mínima con todos los puertos en la VLAN 1 y una VLAN 20 sin usar en la base de datos de VLAN. El comando **show vlan brief** verifica que la VLAN 20 ya no esté presente en el archivo **vlan.dat** después de utilizar el comando **no vlan 20**.

Precaución: antes de eliminar una VLAN, asegúrese de reasignar primero todos los puertos miembro de una VLAN a otra. Los puertos que no se trasladan a una VLAN activa no se podrán comunicar con otros hosts una vez que se elimine la VLAN y hasta que se asignen a una VLAN activa.

Alternativamente, se puede eliminar el archivo **vlan.dat** completo con el comando **delete flash:vlan.dat** del modo EXEC privilegiado. Se puede utilizar la versión abreviada del comando (**delete vlan.dat**) si no se trasladó el archivo **vlan.dat** de su ubicación predeterminada. Después de emitir este comando y de volver a cargar el switch, las VLAN configuradas anteriormente ya no están presentes. Esto vuelve al switch a la condición predeterminada de fábrica con respecto a la configuración de VLAN.

Nota: para los switches Catalyst, el comando **erase startup-config** debe acompañar al comando **delete vlan.dat** antes de la recarga para restaurar el switch a la condición predeterminada de fábrica.

Eliminación de una VLAN

```

S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

VLAN Name          Status      Ports
----- -----
1    default        active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/12, Fa0/13
                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                           Fa0/22, Fa0/23, Fa0/24, Gi0/1
                           Gi0/2
1002 fddi-default   act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default  act/unsup
S1#

```

Una vez que se configura una VLAN, se puede validar la configuración con los comandos **show** de IOS de Cisco.

En la figura 1, se muestran las opciones de los comandos **show vlan** y **show interfaces**.

En el ejemplo de la figura 2, el comando **show vlan name student** produce un resultado que no se interpreta fácilmente. Es preferible usar el comando **show vlan brief**. El comando **show vlan summary** muestra el conteo de todas las VLAN configuradas. El resultado de la figura 2 muestra siete VLAN.

El comando **show interfaces vlanid-vlan** muestra detalles que exceden el ámbito de este curso. La información importante aparece en la segunda línea de la figura 3, que indica que la VLAN 20 está activa.

Utilice el verificador de sintaxis de la figura 4 para mostrar la información de VLAN y de puertos del switch, así como para verificar el modo y las asignaciones de VLAN.

Comando `show vlan`

Sintaxis del comando de CLI IOS de Cisco

<code>show vlan [brief id id-vlan name nombre-vlan summary].</code>	
Mostrar una línea para cada VLAN con el nombre, estado y los puertos de la misma.	<code>brief</code>
Mostrar información sobre una sola VLAN identificada por su número de ID. Para la vlan-id, el intervalo es de 1 a 4094.	<code>id id de la VLAN</code>
Mostrar información sobre una sola VLAN identificada por su nombre. El nombre de la VLAN es una cadena ASCII de 1 a 32 caracteres.	<code>name nombre de la VLAN</code>
Mostrar el resumen de información de la VLAN.	<code>resumen</code>

Comando `show interfaces`

<code>show interfaces [id-interfaz vlan id-vlan] switchport</code>	
Las interfaces válidas incluyen puertos físicos (incluidos tipo, módulo y número de puerto) y canales de puerto. El intervalo de canales de puerto es de 1 a 6.	<code>id de la interfaz</code>
Identificación de VLAN. El intervalo es de 1 a 4094.	<code>vlan id de la VLAN</code>
Mostrar el estado de administración y operación de un puerto de comutación, incluidas las configuraciones de bloqueo y protección del puerto.	<code>switchport</code>

Uso del comando `show vlan`

```
S1# show vlan name student
VLAN Name                               Status    Ports
---- -----
20  student                             active   Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ----- ----- ----- ----- ----- ----- -----
20  enet 100020 1500  -     -     -     -     0     0

Remote SPAN VLAN
-----
Disabled

Primary Secondary Type          Ports
----- ----- -----
S1# show vlan summary
Number of existing VLANs           : 7
Number of existing VTP VLANs      : 7
Number of existing extended VLANs : 0

S1#
```

Uso del comando `show interfaces vlan`

```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARP, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output
drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 IP multicast)
  0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
```

3.3.2 Enlaces troncales de la VLAN

Un enlace troncal de VLAN es un enlace de capa 2 del modelo OSI entre dos switches que transporta el tráfico para todas las VLAN (a menos que se restrinja la lista de VLAN permitidas de manera manual o dinámica). Para habilitar los enlaces troncales, configure los puertos en cualquier extremo del enlace físico con conjuntos de comandos paralelos.

Para configurar un puerto de switch en un extremo de un enlace troncal, utilice el comando **switchport mode trunk**. Con este comando, la interfaz cambia al modo de enlace troncal permanente. El puerto establece una negociación de protocolo de enlace troncal dinámico (DTP) para convertir el enlace en un enlace troncal, incluso si la interfaz conectada a este no acepta el cambio. El protocolo DTP se describe en el tema siguiente. En este curso, el comando **switchport mode trunk** es el único método que se implementa para la configuración de enlaces troncales.

En la figura 1, se muestra la sintaxis del comando de IOS de Cisco para especificar una VLAN nativa (distinta de la VLAN 1).

Utilice el comando **switchport trunk allowed vlan *lista-vlan*** de IOS de Cisco para especificar la lista de VLAN que se permiten en el enlace troncal.

En la figura 2, las VLAN 10, 20 y 30 admiten las computadoras de Cuerpo docente, Estudiante e Invitado (PC1, PC2 y PC3). La VLAN nativa también se debe cambiar de la VLAN 1 a otra VLAN, como la VLAN 99. De manera predeterminada, se permiten todas las VLAN a lo largo de un enlace troncal. Para limitar las VLAN permitidas, se puede usar el comando **switchport trunk allowed vlan**.

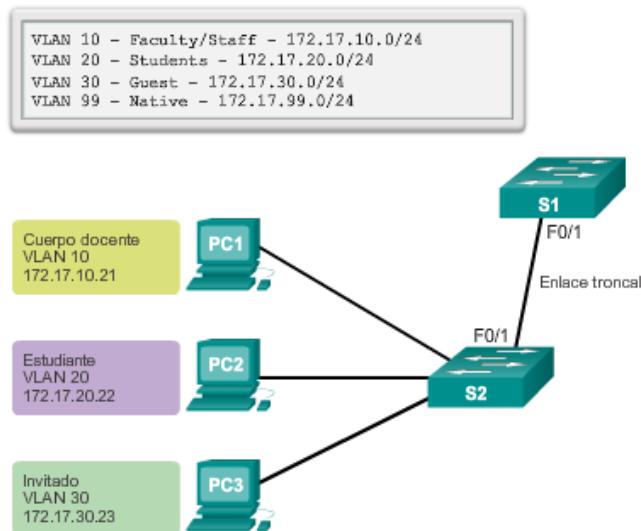
En la figura 3, el puerto F0/1 en el switch S1 está configurado como puerto de enlace troncal, asigna la VLAN nativa a la VLAN 99 y especifica el enlace troncal para que solo reenvíe tráfico para las VLAN 10, 20, 30 y 99.

Nota: esta configuración supone el uso de los switches Cisco Catalyst 2960 que utilizan de manera automática la encapsulación 802.1Q en los enlaces troncales. Es posible que otros switches requieran la configuración manual de la encapsulación. Siempre configure ambos extremos de un enlace troncal con la misma VLAN nativa. Si la configuración de enlace troncal 802.1Q no es la misma en ambos extremos, el software IOS de Cisco registra errores.

Configuración de enlaces troncales

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# interface id_iface
Haga que el enlace sea un enlace troncal.	S1(config-if)# switchport mode trunk
Especifique una VLAN nativa para enlaces troncales 802.1Q sin etiquetar.	S1(config-if)# switchport trunk native vlan id_vlan
Especifique la lista de VLAN que se permitirán en el enlace troncal.	S1(config-if)# switchport trunk allowed vlan <i>lista-vlan</i>
Vuelva al modo EXEC privilegiado.	S1(config-if)# end

Topología de ejemplo



Ejemplo de configuración

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

En la figura 1, se muestran los comandos para eliminar las VLAN permitidas y restablecer la VLAN nativa del enlace troncal. Cuando se restablece al estado predeterminado, el enlace troncal permite todas las VLAN y utiliza la VLAN 1 como VLAN nativa.

En la figura 2, se muestran los comandos utilizados para restablecer todas las características de enlace troncal de una interfaz troncal a la configuración predeterminada. El comando **show interfaces f0/1 switchport** revela que el enlace troncal se volvió a configurar en un estado predeterminado.

En la figura 3, el resultado de ejemplo muestra los comandos utilizados para eliminar la característica de enlace troncal del puerto F0/1 del switch S1. El comando **show interfaces f0/1 switchport** revela que la interfaz F0/1 ahora está en modo de acceso estático.

Restablecimiento de valores configurados en enlaces troncales

Comandos de IOS de un switch Cisco	
Ingrese al modo de configuración global.	S1# configure terminal
Ingrese al modo de configuración de interfaz para la SVI.	S1(config)# interface id_intefaz
Establezca el enlace troncal para permitir todas las VLAN.	S1(config-if)# no switchport trunk allowed vlan
Restablezca la VLAN nativa al valor predeterminado.	S1(config-if)# no switchport trunk native vlan
Vuelva al modo EXEC privilegiado.	S1(config-if)# end

Ejemplo de restablecimiento de enlace troncal

```

S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>

```

Restablecimiento del puerto al modo de acceso

```

S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>

```

En la figura 1, se muestra la configuración del puerto F0/1 del switch S1. La configuración se verifica con el comando **show interfaces ID-interfaz switchport**.

En el área superior resaltada, se muestra que el modo administrativo del puerto F0/1 se estableció en **trunk**. El puerto está en modo de enlace troncal. En la siguiente área resaltada, se verifica que la VLAN nativa es la VLAN 99. Más abajo en el resultado, en el área inferior resaltada, se muestra que todas las VLAN están habilitadas en el enlace troncal.

Utilice el verificador de sintaxis de la figura 2 para configurar un enlace troncal que admita todas las VLAN en la interfaz F0/1 con la VLAN 99 como VLAN nativa. Verifique la configuración de enlace troncal con el comando **show interfaces f0/1 switchport**.

Verificación de la configuración de enlace troncal

```

S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<resultado omitido>

```

3.3.3 Protocolo de enlace troncal dinámico

Las interfaces troncales Ethernet admiten diferentes modos de enlace troncal. Una interfaz se puede establecer como troncal o no troncal, o esta puede negociar el enlace troncal con la interfaz vecina. La negociación de enlaces troncales entre dispositivos de red la maneja el protocolo de enlace troncal dinámico (DTP), que solo funciona de punto a punto.

DTP es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560. Los switches de otros proveedores no admiten el DTP. DTP maneja la negociación de enlaces troncales solo si el puerto del switch vecino está configurado en un modo de enlace troncal que admite DTP.

Precaución: algunos dispositivos de internetworking pueden reenviar tramas DTP de manera incorrecta, lo que puede causar errores de configuración. Para evitar esto, desactive DTP en las interfaces de los switches Cisco conectadas a dispositivos que no admiten DTP.

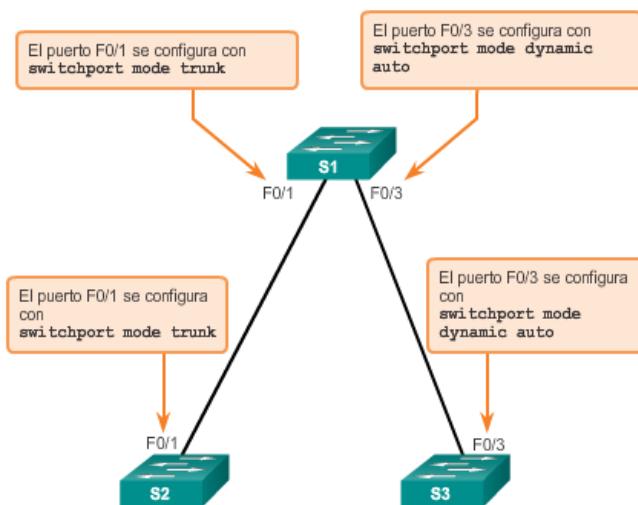
La configuración predeterminada de DTP para los switches Cisco Catalyst 2960 y 3560 es **dynamic auto** (dinámico automático), como se muestra en la figura 1, en la interfaz F0/3 de los switches S1 y S3.

Para habilitar los enlaces troncales desde un switch Cisco hacia un dispositivo que no admite DTP, utilice los comandos **switchport mode trunk** y **switchport nonegotiate** del modo de configuración de interfaz. Esto hace que la interfaz se convierta en un enlace troncal, pero sin que genere tramas DTP.

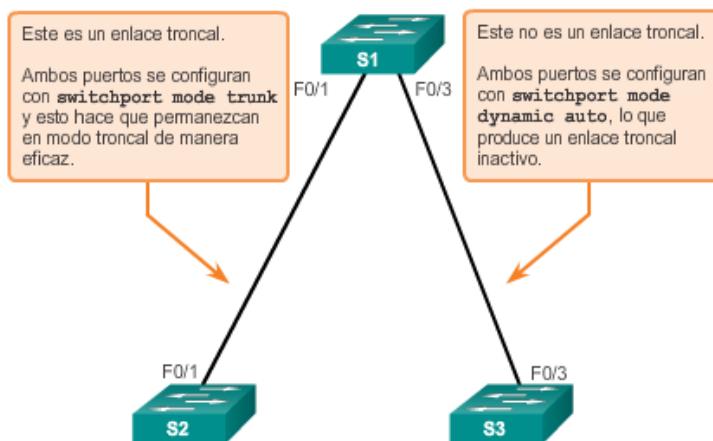
En la figura 2, el enlace entre los switches S1 y S2 se convierte en un enlace troncal porque los puertos F0/1 de los switches S1 y S2 se configuraron para omitir todos los anuncios de DTP, así como para aparecer y permanecer en modo de puerto de enlace troncal. Los puertos F0/3 de los switches S1 y S3 se establecieron en modo dinámico automático, de modo que el resultado de la negociación es el estado de modo de acceso. Esto genera un enlace troncal inactivo. Al configurar un puerto para que esté en modo de enlace troncal mediante el comando **switchport mode trunk**,

no existe ambigüedad sobre el estado en que se encuentra el enlace troncal: este se encuentra siempre activo. Con esta configuración, es fácil recordar en qué estado están los puertos de enlace troncal: si se supone que el puerto es un enlace troncal, el modo se establece en enlace troncal.

Configuración inicial de DTP



Resultados de la interacción de DTP



Las interfaces Ethernet de los switches de las series Catalyst 2960 y Catalyst 3560 admiten diversos modos de enlace troncal con la ayuda de DTP:

- **switchport mode access:** coloca la interfaz (puerto de acceso) en modo de enlace no troncal permanente y negocia para convertir el enlace en uno no troncal. La interfaz se convierte en una interfaz no troncal, independientemente de si la interfaz vecina es una interfaz troncal.
- **switchport mode dynamic auto:** hace que la interfaz pueda convertir el enlace en un enlace troncal. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo de enlace troncal o deseado. El modo de switchport predeterminado para todas las interfaces Ethernet es **dynamic auto**.

- **switchport mode dynamic desirable:** hace que la interfaz intente convertir el enlace en un enlace troncal de manera activa. La interfaz se convierte en una interfaz troncal si la interfaz vecina se establece en modo de enlace troncal, deseado o automático. Este es el modo de switchport predeterminado en los switches antiguos, como los switches de las series Catalyst 2950 y 3550.
- **switchport mode trunk:** coloca la interfaz en modo de enlace troncal permanente y negocia para convertir el enlace en un enlace troncal. La interfaz se convierte en una interfaz de enlace troncal, incluso si la interfaz vecina no es una interfaz de enlace troncal.
- **switchport nonegotiate:** evita que la interfaz genere tramas DTP. Puede utilizar este comando solo cuando el modo de switchport de la interfaz es **access** o **trunk**. Para establecer un enlace troncal, debe configurar manualmente la interfaz vecina como interfaz troncal.

En la figura 1, se muestran los resultados de las opciones de configuración de DTP en extremos opuestos de un enlace troncal conectado a los puertos de un switch Catalyst 2960.

Configure los enlaces troncales estáticamente siempre que sea posible. El modo de DTP predeterminado depende de la versión del software IOS de Cisco y de la plataforma. Para determinar el modo de DTP actual, emita el comando **show dtp interface**, como se muestra en la figura 2.

Utilice el verificador de sintaxis de la figura 3 para determinar el modo de DTP en la interfaz F0/1.

Nota: por lo general, se recomienda que la interfaz se establezca en **trunk ynonegotiate** cuando se requiere un enlace troncal. Se debe inhabilitar DTP en los enlaces cuando no se deben usar enlaces troncales.

Modos de interfaz negociados de DTP

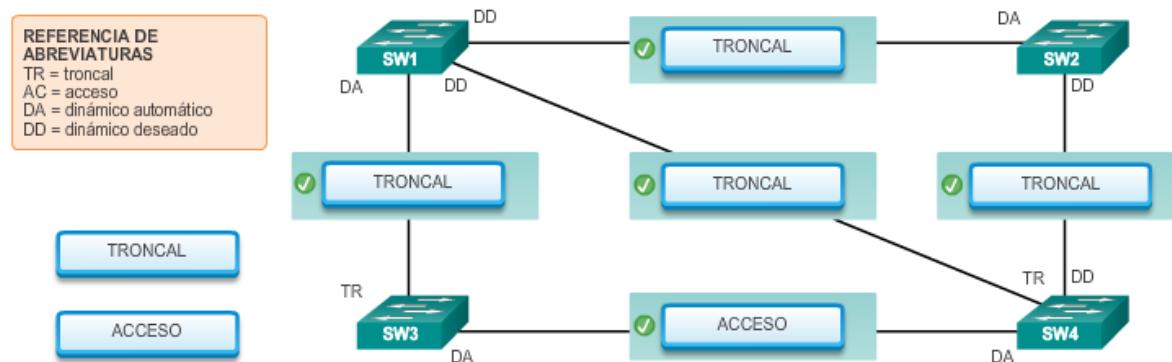
	Dinámico automático	Dinámico deseado	Enlace troncal	Acceso
Dinámico automático	Acceso	Enlace troncal	Enlace troncal	Acceso
Dinámico deseado	Enlace troncal	Enlace troncal	Enlace troncal	Acceso
Enlace troncal	Enlace troncal	Enlace troncal	Enlace troncal	Conectividad limitada
Acceso	Acceso	Acceso	Conectividad limitada	Acceso

Verificación del modo de DTP

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS:                                         TRUNK/ON/TRUNK
TOT/TAT/TNT:                                         802.1Q/802.1Q/802.1Q
Neighbor address 1:                                  0CD996D23F81
Neighbor address 2:                                  000000000000
Hello timer expiration (sec/state):                12/RUNNING
Access timer expiration (sec/state):                never/STOPPED
Negotiation timer expiration (sec/state):          never/STOPPED
Multidrop timer expiration (sec/state):            never/STOPPED
FSM state:                                           S6:TRUNK
# times multi & trunk:                            0
Enabled:                                            yes
In STP:                                             no

<resultado omitido>
```

Actividad: predecir el comportamiento del protocolo de enlace troncal dinámico (DTP)
 ¿Cuáles son las combinaciones de modo de DTP entre dos switches que se convertirán en enlaces troncales y cuáles son las que se convertirán en enlaces de acceso? Arrastre cada una de las etiquetas de enlace hacia los campos proporcionados en la topología. No utilizará todas las etiquetas.



3.3.4 Resolución de problemas de VLAN y enlaces troncales

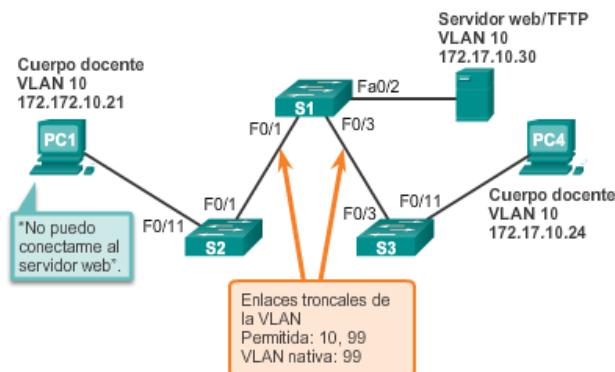
Cada VLAN debe corresponder a una subred IP única. Si dos dispositivos en la misma VLAN tienen direcciones de subred diferentes, no se pueden comunicar. Este es un problema frecuente y se resuelve fácilmente mediante la identificación de la configuración incorrecta y el cambio de la dirección de la subred por una dirección correcta.

En la figura 1, la PC1 no se puede conectar al servidor Web/TFTP que se muestra.

La verificación de las opciones de configuración IP de la PC1, que se muestra en la figura 2, revela el error más frecuente en la configuración de redes VLAN: una dirección IP mal configurada. La PC1 se configuró con la dirección IP 172.172.10.21, pero debería haberse configurado con la dirección 172.17.10.21.

El cuadro de diálogo de la configuración de Fast Ethernet de la PC1 muestra la dirección IP actualizada, 172.17.10.21. En la figura 3, el resultado que se muestra en la parte inferior indica que la PC1 recuperó la conectividad al servidor Web/TFTP que se encuentra en la dirección IP 172.17.10.30.

Problema de IP dentro de la VLAN

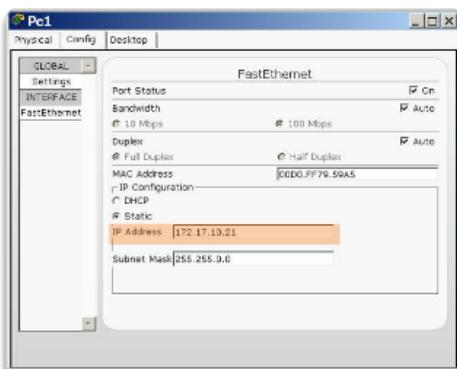


Problema: dirección IP incorrecta

Resultado de la PC1

```
PC1> ipconfig
IP Address.....: 172.17.10.21
Subnet Mask.....: 255.255.0.0
Default Gateway...: 0.0.0.0
PC1>
```

Solución: cambiar la dirección IP de la computadora



Resultado de la Computadora PC1

```
PC1> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: Bytes=32 Time=147ms TTL=128
```

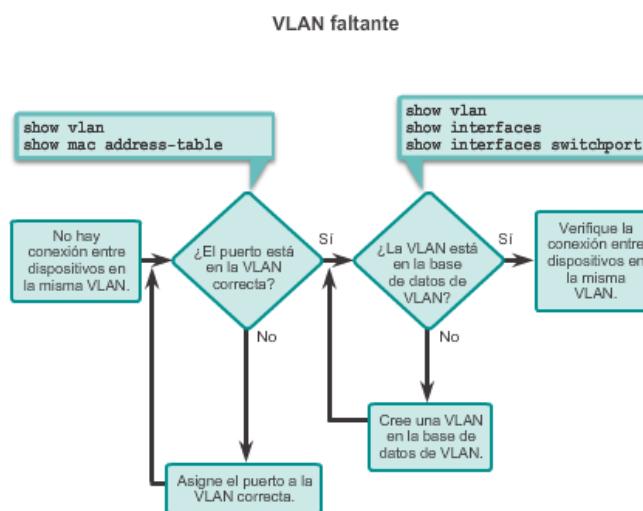
Si todavía no hay conexión entre los dispositivos en una VLAN pero se descartaron los problemas de direccionamiento IP, consulte el diagrama de flujo de la figura 1 para llevar a cabo la resolución de problemas:

Paso 1. Utilice el comando **show vlan** para verificar si el puerto pertenece a la VLAN esperada. Si el puerto se asignó a una VLAN incorrecta, utilice el comando **switchport access vlan** para corregir la pertenencia de VLAN. Utilice el comando **show mac address-table** para revisar qué direcciones se obtuvieron en un puerto determinado del switch y a qué VLAN se asignó ese puerto.

Paso 2. Si se elimina la VLAN a la que se asignó el puerto, el puerto pasa a estar inactivo. Utilice los comandos **show vlan** o **show interfaces switchport**.

Para ver la tabla de direcciones MAC, utilice el comando **show mac-address-table**. En el ejemplo de la figura 2, se muestran las direcciones MAC que se obtuvieron en la interfaz F0/1. Se puede observar que en la interfaz F0/1 de la VLAN 10 se obtuvo la dirección MAC 000c.296a.a21c. Si este no es el número de VLAN previsto, cambie la pertenencia de puerto de VLAN con el comando **switchport access vlan**.

Cada puerto de un switch pertenece a una VLAN. Si se elimina la VLAN a la que pertenece el puerto, este pasa a estar inactivo. Ninguno de los puertos que pertenecen a la VLAN que se eliminó puede comunicarse con el resto de la red. Utilice el comando **show interface f0/1 switchport** para verificar si el puerto está inactivo. Si el puerto está inactivo, no funciona hasta que se cree la VLAN con el comando **vlan id_vlan**.



VLAN faltante

```
S1# show mac address-table interface FastEthernet 0/1
Mac Address Table
-----
Vlan      Mac Address           Type      Ports
-----  -----
10        000c.296a.a21c       DYNAMIC   Fa0/1
10        000f.34f9.9181       DYNAMIC   Fa0/1
Total Mac Addresses for this criterion: 2
```



```
S1# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Una de las tareas frecuentes de los administradores de red es resolver problemas de formación de enlaces troncales o de enlaces que se comportan incorrectamente como enlaces troncales. En ocasiones, un puerto de switch se puede comportar como puerto de enlace troncal, incluso si no se configuró como tal. Por ejemplo, un puerto de acceso puede aceptar tramas de redes VLAN distintas de la VLAN a la cual se asignó. Esto se conoce como “filtración de VLAN”.

En la figura 1, se muestra un diagrama de flujo de las pautas generales de resolución de problemas de enlaces troncales.

Para resolver problemas de enlaces troncales que no se forman o de filtración de VLAN, proceda de la siguiente manera:

Paso 1. Utilice el comando **show interfaces trunk** para verificar si hay coincidencia entre la VLAN nativa local y peer. Si la VLAN nativa no coincide en ambos extremos, hay una filtración de VLAN.

Paso 2. Utilice el comando **show interfaces trunk** para verificar si se estableció un enlace troncal entre los switches. Configure estéticamente los enlaces troncales siempre que sea posible. Los puertos de los switches Cisco Catalyst utilizan DTP de manera predeterminada e intentan negociar un enlace troncal.

Para mostrar el estado del enlace troncal, la VLAN nativa utilizada en ese enlace troncal y verificar el establecimiento del enlace troncal, utilice el comando **show interfaces trunk**. En el ejemplo de la figura 2, se muestra que la VLAN nativa en un extremo del enlace troncal se cambió a la VLAN 2. Si un extremo del enlace troncal se configura como VLAN 99 nativa y el otro extremo como VLAN 2 nativa, las tramas que se envían desde la VLAN 99 en un extremo se reciben en la VLAN 2 en el otro extremo. La VLAN 99 se filtra en el segmento VLAN 2.

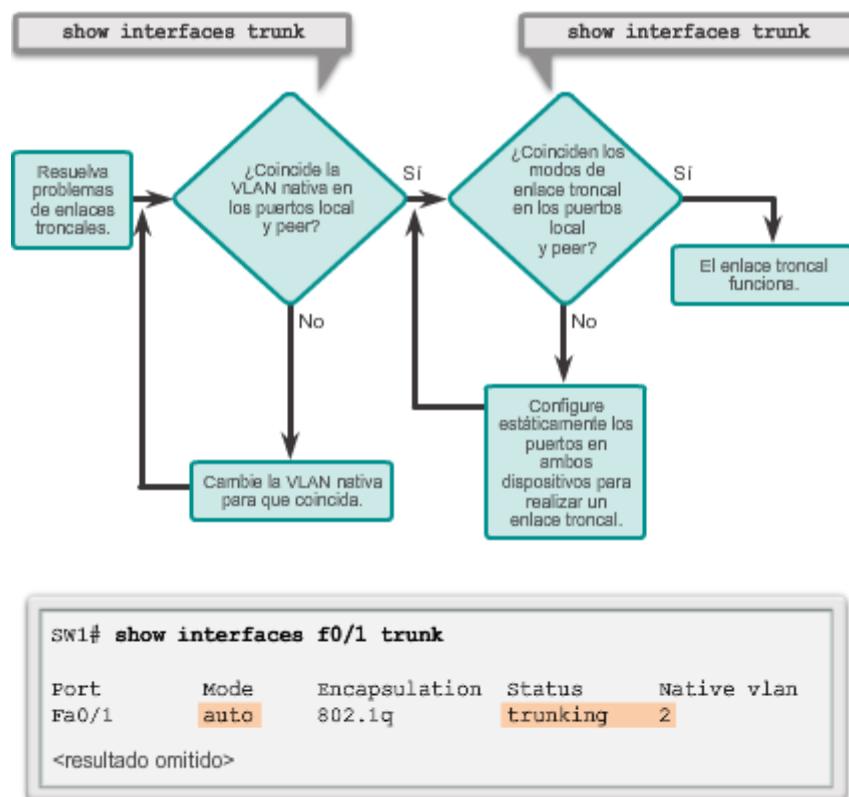
CDP muestra un aviso de incompatibilidad de VLAN nativa en un enlace troncal con este mensaje:

*Mar 1 06:45:26.232: %CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (2), with S2 FastEthernet0/1 (99).

Si existe una incompatibilidad de VLAN nativa, se producen problemas de conectividad en la red. El tráfico de datos para las VLAN distintas de las dos VLAN nativas configuradas se propaga correctamente a través del enlace troncal, pero los datos relacionados con cualquiera de las VLAN nativas no se propagan correctamente a través del enlace troncal.

Como se muestra en la figura 2, los problemas de incompatibilidad de la VLAN nativa no impiden que se forme el enlace troncal. Para resolver una incompatibilidad de VLAN nativa, configure la VLAN nativa para que sea la misma VLAN en ambos lados del enlace.

Resolución de problemas de enlaces troncales



En general, los problemas de enlaces troncales se deben a una configuración incorrecta. Al configurar las VLAN y los enlaces troncales en una infraestructura comutada, los errores de configuración más frecuentes son los siguientes:

- **Incompatibilidad de VLAN nativa:** los puertos de enlace troncal se configuraron con VLAN nativas diferentes. Este error de configuración genera notificaciones de consola y provoca que el tráfico de control y administración se dirija erróneamente. Esto representa un riesgo de seguridad.
- **Incompatibilidades de modo de enlace troncal:** un puerto de enlace troncal está configurado en un modo que no es compatible para enlaces troncales en el puerto peer correspondiente. Estos errores de configuración hacen que el vínculo de enlace troncal deje de funcionar.

- **VLAN permitidas en enlaces troncales:** no se actualizó la lista de VLAN permitidas en un enlace troncal con los requisitos de enlace troncal de VLAN actuales. En este caso, se envía tráfico inesperado o ningún tráfico al enlace troncal.

Si se detecta un problema con un enlace troncal y se desconoce la causa, comience la resolución de problemas con un examen de los enlaces troncales para determinar si hay una incompatibilidad de VLAN nativa. Si esa no es la causa, verifique si hay una incompatibilidad de modo de enlace troncal y, por último, revise la lista de VLAN permitidas en el enlace troncal. En las dos páginas siguientes, se analiza cómo solucionar problemas frecuentes de los enlaces troncales.

Problemas comunes con enlaces troncales

Problema	Resultado	Ejemplo
Faltas de concordancia de la VLAN nativa	Presenta un riesgo a la seguridad y crea resultados no deseados.	Por ejemplo, un puerto se define como VLAN 99 y el otro como VLAN 100.
Faltas de concordancia del modo de enlace troncal	Causa pérdida de la conectividad de la red.	Por ejemplo, un puerto está configurado como modo de enlace troncal "desactivado" y el otro, como modo de enlace troncal "activado".
VLAN permitidas en enlaces troncales	Causa que se envíe tráfico no deseado o que no se envíe tráfico a través del enlace troncal.	La lista de las VLAN permitidas no admite los requisitos de enlace troncal de VLAN actuales.

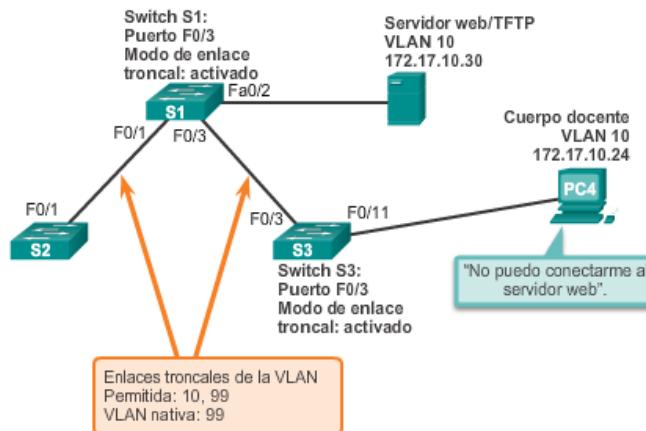
Por lo general, los enlaces troncales se configuran estáticamente con el comando **switchport mode trunk**. Los puertos de enlace troncal de los switches Cisco Catalyst utilizan DTP para negociar el estado del enlace. Cuando un puerto en un enlace troncal se configura con un modo de enlace troncal que no es compatible con el puerto de enlace troncal vecino, no se puede formar un enlace troncal entre los dos switches.

En la situación que se describe en la figura 1, la PC4 no puede conectarse al servidor web interno. La topología indica una configuración válida. ¿Por qué hay un problema?

Verifique el estado de los puertos de enlace troncal del switch S1 con el comando **show interfaces trunk**. El resultado que se muestra en la figura 2 indica que la interfaz Fa0/3 del switch S1 actualmente no es un enlace troncal. Si se examina la interfaz F0/3, se descubre que el puerto del switch está en modo dinámico automático. Si se examinan los enlaces troncales del switch S3, se descubre que no hay puertos de enlace troncal activos. Si se sigue examinando, se descubre que la interfaz Fa0/3 también está en modo dinámico automático. Esto explica la inactividad del enlace troncal.

Para resolver el problema, vuelva a configurar el modo de enlace troncal de los puertos F0/3 de los switches S1 y S3, como se muestra en la figura 3. Despues del cambio de configuración, el resultado del comando **show interfaces** indica que el puerto del switch S1 ahora está en modo de enlace troncal. El resultado de la PC4 indica que esta recuperó la conectividad al servidor Web/TFTP que se encuentra en la dirección IP 172.17.10.30.

Topología de la situación



Modos de DTP no compatibles

Resultado del switch S1

```
S1# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 99
Port Vlans allowed on trunk
Fa0/1 10,99
Port Vlans allowed and active in management domain
Fa0/1 10,99
Port Vlans in spanning tree forwarding state and not pruned
Fa0/1 10,99
S1# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
```

Resultado del switch S3

```
S3# show interfaces trunk
S3#
S3# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: dynamic auto
...
```

Resultado del switch S1

```
S1# config terminal
S1(config)# interface f0/3
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
```

Resultado del switch S3

```
S3# config terminal
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
S3# show interfaces f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
...
S3# show interfaces trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/3    on        802.1q         trunking   99
Port      Vlans allowed on trunk
Fa0/3    10,99
Port      Vlans allowed and active in management domain
Fa0/3    10,99
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/3    10,99
S3#
```

Resultado de la computadora PC4

```
PC4> ping 172.17.10.30
Pinging 172.17.10.30 with 32 bytes of data:
Reply from 172.17.10.30: bytes=32 time=147ms TTL=128
...
```

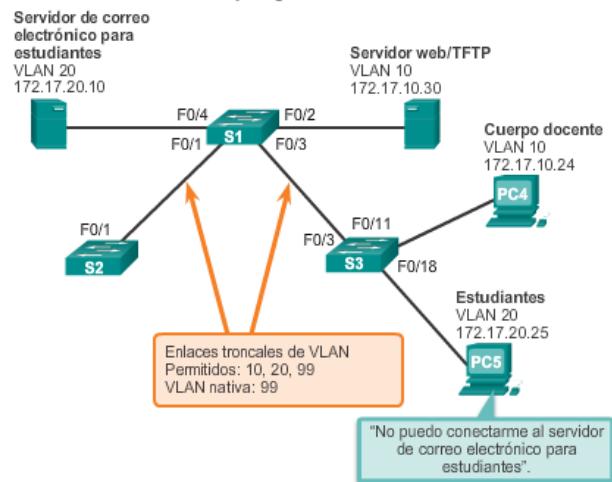
Para que el tráfico de una VLAN se transmita a través de un enlace troncal, debe estar permitido en dicho enlace. Para hacerlo, utilice el comando **switchport trunk allowed vlan id-vlan**.

En la figura 1, se agregaron la VLAN 20 (Estudiantes) y la PC5 a la red. La documentación se ha actualizado para mostrar que las VLAN permitidas en el enlace troncal son las 10, 20 y 99. En esta situación, la PC5 no puede conectarse al servidor de correo electrónico para estudiantes.

Verifique los puertos de enlace troncal del switch S1 con el comando **show interfaces trunk**, como se muestra en la figura 2. El comando revela que la interfaz F0/3 del switch S3 se configuró correctamente para permitir las VLAN 10, 20 y 99. Si se examina la interfaz F0/3 del switch S1, se descubre que las interfaces F0/1 y F0/3 permiten solo las VLAN 10 y 99. Alguien actualizó el registro pero olvidó volver a configurar los puertos del switch S1.

Vuelva a configurar los puertos F0/1 y F0/3 del switch S1 con el comando **switchport trunk allowed vlan 10,20,99**, como se muestra en la figura 3. El resultado muestra que ya se agregaron las VLAN 10, 20 y 99 a los puertos F0/1 y F0/3 del switch S1. El comando **show interfaces trunk** es una excelente herramienta para revelar problemas frecuentes de enlace troncal. La PC5 recuperó la conectividad al servidor de correo electrónico para estudiantes que se encuentra en la dirección IP 172.17.20.10.

Topología de la situación



VLAN faltantes

Resultado del switch S3

```
s3# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/3 on 802.1q trunking 99
Port vlans allowed on trunk
Fa0/3 10,20,99
Port vlans allowed and active in management domain
Fa0/3 10,20,99
Port vlans in spanning tree forwarding state and not
pruned
Fa0/3 10,20,99
```

Resultado del switch S1

```
s1# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 99
Fa0/3 on 802.1q trunking 99
Port vlans allowed on trunk
Fa0/1 10,99
Fa0/3 10,99
...
S1#
```

Lista de VLAN corregida

Resultado del switch S1

```
s1# config terminal
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# interface f0/3
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1# show interfaces trunk
Port Mode Encapsulation Status Native vlan
Fa0/1 on 802.1q trunking 99
Fa0/3 on 802.1q trunking 99
Port vlans allowed on trunk
Fa0/1 10,20,99
Fa0/3 10,20,99
...
```

Resultado de la computadora PC5

```
PC5> ping 172.17.20.10
Pinging 172.17.20.10 with 32 bytes of data:
Reply from 172.17.20.10: bytes=32 time=147ms TTL=128
...
```

3.4 Seguridad y diseño de redes VLAN

3.4.1 Ataques a redes VLAN

Existen diferentes tipos de ataques a VLAN en las redes comutadas modernas. La arquitectura VLAN simplifica el mantenimiento de la red y mejora el rendimiento, pero también posibilita el uso indebido. Es importante comprender la metodología general detrás de estos ataques y los métodos principales para mitigarlos.

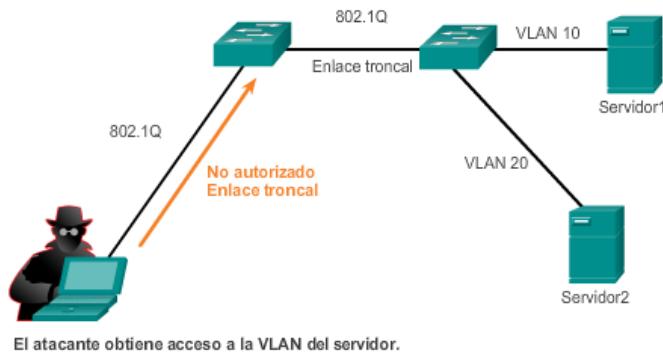
Los saltos de VLAN permiten que una VLAN pueda ver el tráfico de otra VLAN. La suplantación de identidad de switch es un tipo de ataque con salto de VLAN que funciona mediante el aprovechamiento de un puerto de enlace troncal mal configurado. De manera predeterminada, los puertos de enlace troncal tienen acceso a todas las VLAN y pasan el tráfico para varias VLAN a través del mismo enlace físico, generalmente entre switches.

Haga clic en el botón Play (Reproducir) de la ilustración para ver una animación del ataque de suplantación de identidad de switch.

En un ataque de suplantación de identidad de switch básico, el atacante aprovecha el hecho de que la configuración predeterminada del puerto del switch sea dinámica automática. El atacante de la red configura un sistema para suplantar su propia identidad y hacerse pasar por un switch. Esta suplantación de identidad requiere que el atacante de la red pueda emular mensajes 802.1Q y DTP. Al hacerle creer al switch que otro switch intenta crear un enlace troncal, el atacante puede acceder a todas las VLAN permitidas en el puerto de enlace troncal.

La mejor manera de prevenir un ataque de suplantación de identidad de switch básico es inhabilitar los enlaces troncales en todos los puertos, excepto en los que específicamente requieren enlaces troncales. En los puertos de enlace troncal requeridos, inhabilite DTP y habilite los enlaces troncales manualmente.

Ataque de suplantación de identidad de switch



Otro tipo de ataque VLAN es el ataque con salto de VLAN de etiquetado doble (o de encapsulado doble). Este tipo de ataque aprovecha la forma en que funciona el hardware en la mayoría de los switches. La mayoría de los switches realizan solo un nivel de desencapsulación 802.1Q, lo que permite que un atacante incorpore una etiqueta 802.1Q oculta en la trama. Esta etiqueta permite que la trama se reenvíe a una VLAN que la etiqueta 802.1Q original no especificó. Una característica importante del ataque con salto de VLAN de encapsulado doble es que funciona

incluso si se inhabilitan los puertos de enlace troncal, ya que, generalmente, un host envía una trama por un segmento que no es un enlace troncal.

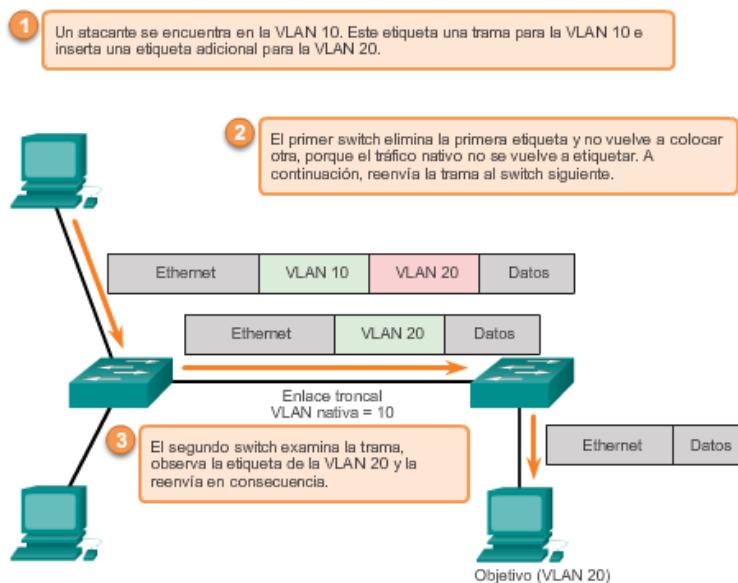
Los ataques con salto de VLAN de etiquetado doble implican los siguientes tres pasos:

1. El atacante envía una trama 802.1Q con doble etiqueta al switch. El encabezado externo tiene la etiqueta VLAN del atacante, que es la misma que la VLAN nativa del puerto de enlace troncal. Se supone que el switch procesa la trama que recibe del atacante como si estuviera en un puerto de enlace troncal o un puerto con una VLAN de voz (un switch no debe recibir una trama de Ethernet etiquetada en un puerto de acceso). A los fines de este ejemplo, suponga que la VLAN nativa es la VLAN 10. La etiqueta interna es la VLAN víctima; en este caso, la VLAN 20.
2. La trama llega al switch, que observa la primera etiqueta 802.1Q de 4 bytes. El switch observa que la trama está destinada a la VLAN 10, que es la VLAN nativa. El switch reenvía el paquete por todos los puertos de la VLAN 10 después de eliminar la etiqueta de VLAN 10. En el puerto de enlace troncal, se elimina la etiqueta de VLAN 10, y no se vuelve a etiquetar el paquete porque esta forma parte de la VLAN nativa. En este punto, la etiqueta de VLAN 20 sigue intacta, y el primer switch no la inspeccionó.
3. El segundo switch observa solo la etiqueta 802.1Q interna que envió el atacante y ve que la trama está destinada a la VLAN 20, el objetivo. El segundo switch envía la trama al puerto víctima o lo satura, según si existe una entrada en la tabla de direcciones MAC para el host víctima.

Este tipo de ataque es unidireccional y solo funciona cuando el atacante se conecta a un puerto que reside en la misma VLAN que la VLAN nativa del puerto de enlace troncal. Frustrar este tipo de ataque no es tan fácil como detener ataques de salto de VLAN básicos.

El mejor método para mitigar los ataques de etiquetado doble es asegurar que la VLAN nativa de los puertos de enlace troncal sea distinta de la VLAN de cualquier puerto de usuario. De hecho, se considera una práctica recomendada de seguridad la utilización de una VLAN fija distinta de todas las VLAN de usuario como VLAN nativa para todos los enlaces troncales 802.1Q en la red comunitada.

Ataque de etiquetado doble



Algunas aplicaciones requieren que no se reenvíe tráfico en la capa 2 entre los puertos del mismo switch, de modo que un vecino no vea el tráfico generado por otro vecino. En ese entorno, el uso de la característica de perímetro de VLAN privada (PVLAN), también conocida como “puertos protegidos”, asegura que no se intercambie tráfico de unidifusión, difusión o multidifusión entre estos puertos del switch (figura 1).

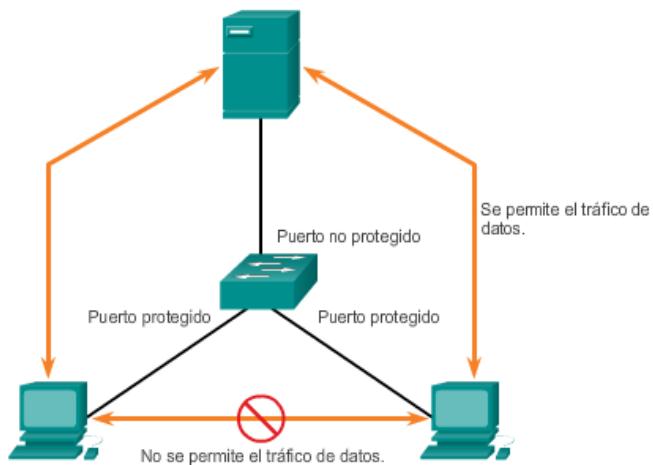
Las características de la función de perímetro de PVLAN son las siguientes:

- Los puertos protegidos no reenvían tráfico (de unidifusión, difusión o multidifusión) a ningún otro puerto que también sea un puerto protegido, excepto el tráfico de control. El tráfico de datos no se puede reenviar entre los puertos protegidos en la capa 2.
- El comportamiento de reenvío entre un puerto protegido y un puerto no protegido continúa normalmente.
- Los puertos protegidos se deben configurar manualmente.

Para configurar la característica de perímetro de PVLAN, introduzca el comando **switchport protected** en el modo de configuración de interfaz (figura 2). Para inhabilitar los puertos protegidos, utilice el comando **no switchport protected** del modo de configuración de interfaz. Para verificar la configuración de la característica de perímetro de PVLAN, utilice el comando **show interfaces id-interfaz switchport** del modo de configuración global.

Utilice el verificador de sintaxis de la figura 3 para configurar la característica de perímetro de PVLAN en la interfaz G0/1 y verificar la configuración.

Perímetro de PVLAN



Perímetro de PVLAN

```

S1(config)# interface g0/1
S1(config-if)# switchport protected
S1(config-if)# end
S1# show interfaces g0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: on
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<resultado omitido>

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
  
```

- ✓ Perímetro de PVLAN
Un usuario ataca a otras computadoras de usuario en el entorno de una cafetería. Las computadoras de usuario aún necesitan obtener acceso a Internet y al servidor de impresión.
- ✓ Ataque con salto de VLAN
Deshabilita el DTP en todos los puertos y asigna a estos últimos de manera estática como puerto de acceso o puerto de enlace troncal.
- ✓ Ataque de Double-Tagging
Asegura que la VLAN nativa de los puertos troncales sea diferente de las VLAN del puerto de acceso.

3.5 Prácticas recomendadas de diseño para las VLAN

Los switches Cisco tienen una configuración de fábrica en la cual las VLAN predeterminadas se preconfiguran para admitir diversos tipos de medios y protocolos. La VLAN Ethernet predeterminada es la VLAN 1. Por seguridad, se recomienda configurar todos los puertos de todos los switches para que se asocien a VLAN distintas de la VLAN 1. Generalmente, esto se logra configurando todos los puertos sin utilizar en una VLAN de agujero negro que no se use para nada en la red. Todos los puertos utilizados se asocian a VLAN independientes de la VLAN 1 y de la VLAN de agujero negro. También se recomienda desactivar los puertos de switch sin utilizar para evitar el acceso no autorizado.

Una buena práctica de seguridad es separar el tráfico de administración y de datos de usuario. La VLAN de administración, que es la VLAN 1 de manera predeterminada, se debe cambiar a una VLAN diferente e independiente. Para comunicarse de manera remota con un switch Cisco con fines de administración, el switch debe tener una dirección IP configurada en la VLAN de administración. Los usuarios en otras VLAN no pueden establecer sesiones de acceso remoto al switch, a menos que se los enrute a la VLAN de administración, lo que proporciona una capa de seguridad adicional. Además, se debe configurar el switch para que solo acepte sesiones SSH cifradas para la administración remota.

Todo el tráfico de control se envía por la VLAN 1. Por lo tanto, cuando se cambia la VLAN nativa a una opción distinta de la VLAN 1, todo el tráfico de control se etiqueta en los enlaces troncales de VLAN IEEE 802.1Q (se etiqueta con la ID de VLAN 1). Por seguridad, se recomienda cambiar la VLAN nativa a una VLAN distinta de la VLAN 1. La VLAN nativa también debe ser distinta de todas las VLAN de usuarios. Asegúrese de que la VLAN nativa para un enlace troncal 802.1Q sea la misma en ambos extremos del enlace troncal.

DTP ofrece cuatro modos de puerto de switch: acceso, enlace troncal, dinámico automático y dinámico deseado. Una pauta general es inhabilitar la autonegociación. Una práctica recomendada de seguridad de puertos es no utilizar los modos de puerto de switch dinámico automático o dinámico deseado.

Por último, el tráfico de voz tiene requisitos de QoS estrictos. Si las computadoras y los teléfonos IP de los usuarios están en la misma VLAN, cada uno intenta usar el ancho de banda disponible sin tener en cuenta al otro dispositivo. Para evitar este conflicto, es aconsejable utilizar VLAN separadas para la telefonía IP y para el tráfico de datos.

3.6 Resumen

En este capítulo, se presentaron las redes VLAN. Las VLAN se basan en conexiones lógicas, en lugar de conexiones físicas. Las VLAN son un mecanismo para permitir que los administradores de red creen dominios de difusión lógicos que puedan extenderse a través de un único switch o varios switches, independientemente de la cercanía física. Esta función es útil para reducir el tamaño de los dominios de difusión o para permitir la agrupación lógica de grupos o usuarios sin la necesidad de que estén ubicados físicamente en el mismo lugar.

Existen varios tipos de VLAN:

- VLAN predeterminada

- VLAN de administración
- VLAN nativa
- VLAN de datos/de usuarios
- VLAN de agujero negro
- VLAN de voz

En los switches Cisco, la VLAN 1 es la VLAN Ethernet predeterminada, la VLAN nativa predeterminada y la VLAN de administración predeterminada. Las prácticas recomendadas sugieren que la VLAN nativa y la de administración se cambien a una VLAN distinta, y que los puertos de switch sin utilizar se trasladen a una VLAN de “agujero negro” para mayor seguridad.

El comando **switchport access vlan** se utiliza para crear una VLAN en un switch. Después de crear una VLAN, el siguiente paso es asignar puertos a la VLAN. El comando **show vlan brief** muestra el tipo de asignación y pertenencia de VLAN para todos los puertos de switch. Cada VLAN debe corresponder a una subred IP única.

Utilice el comando **show vlan** para verificar si el puerto pertenece a la VLAN esperada. Si el puerto se asignó a una VLAN incorrecta, utilice el comando **switchport access vlan** para corregir la pertenencia de VLAN. Utilice el comando **show mac address-table** para revisar qué direcciones se obtuvieron en un puerto determinado del switch y a qué VLAN se asignó ese puerto.

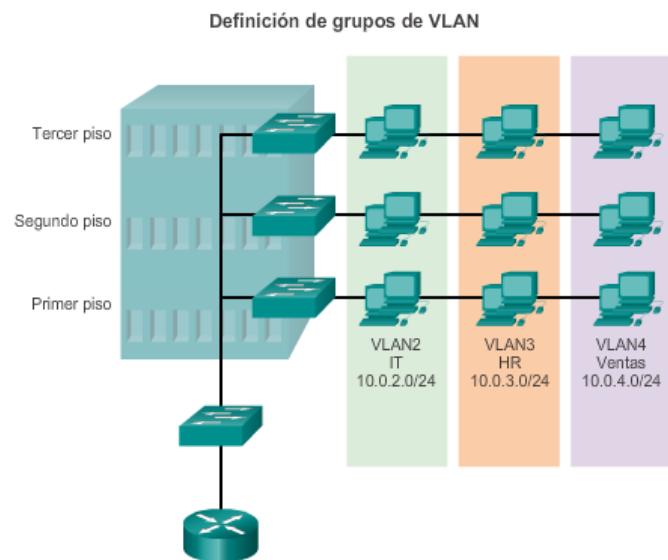
Un puerto de un switch es un puerto de acceso o un puerto de enlace troncal. Los puertos de acceso transportan el tráfico de una VLAN específica asignada al puerto. Un puerto de enlace troncal pertenece a todas las VLAN de manera predeterminada; por lo tanto, transporta el tráfico para todas las VLAN.

Los enlaces troncales de VLAN facilitan la comunicación entre switches mediante el transporte de tráfico relacionado con varias VLAN. El etiquetado de tramas IEEE 802.1Q permite diferenciar tramas de Ethernet asociadas a distintas VLAN a medida que atraviesan enlaces troncales en común. Para habilitar los enlaces troncales, utilice el comando **switchport mode trunk**. Utilice el comando **show interfaces trunk** para verificar si se estableció un enlace troncal entre los switches.

La negociación de enlaces troncales entre dispositivos de red la maneja el protocolo de enlace troncal dinámico (DTP), que solo funciona de punto a punto. DTP es un protocolo exclusivo de Cisco que se habilita de manera automática en los switches de las series Catalyst 2960 y Catalyst 3560.

Para volver un switch a su condición predeterminada de fábrica con una VLAN predeterminada, use el comando **delete flash:vlan.dat** y **erase startup-config**.

En este capítulo, también se analizó la configuración y la verificación de redes VLAN y de enlaces troncales, así como la resolución de problemas relacionados mediante la CLI de IOS de Cisco, y se exploraron las consideraciones básicas de seguridad y de diseño en el contexto de las redes VLAN.



4 Conceptos de routing

4.1 Introducción

Las redes permiten que las personas se comuniquen, colaboren e interactúen de muchas maneras. Las redes se utilizan para acceder a páginas web, hablar mediante teléfonos IP, participar en videoconferencias, competir en juegos interactivos, realizar compras en Internet, completar trabajos de cursos en línea, y más.

Los switches Ethernet funcionan en la capa de enlace de datos, la capa 2, y se utilizan para reenviar tramas de Ethernet entre dispositivos dentro de una misma red.

Sin embargo, cuando las direcciones IP de origen y destino están en distintas redes, la trama de Ethernet se debe enviar a un router.

Los routers conectan una red a otra red. El router es responsable de la entrega de paquetes a través de distintas redes. El destino de un paquete IP puede ser un servidor web en otro país o un servidor de correo electrónico en la red de área local.

El router usa su tabla de routing para encontrar la mejor ruta para reenviar un paquete. Es responsabilidad de los routers entregar esos paquetes a su debido tiempo. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers de reenviar paquetes de la manera más eficiente posible.

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Con frecuencia, se utiliza para conectar una red local a Internet.

En este capítulo, también se responde a la pregunta “¿Qué hace un router con los paquetes que recibe de una red y que están destinados a otra red?”. Se examinan los detalles de la tabla de routing, incluidas las rutas conectadas, estáticas y dinámicas.

Debido a que los routers pueden enrutar paquetes entre redes, los dispositivos que están en redes distintas se pueden comunicar. En este capítulo, se presentará el router, su función en las redes, sus principales componentes de hardware y software, y el proceso de routing. Se proporcionarán ejercicios que demuestran cómo acceder al router, cómo configurar los parámetros básicos del router y cómo verificar la configuración.

Después de completar este capítulo, podrá hacer lo siguiente:

- Describir las funciones y las características principales de un router.
- Conectar dispositivos para una red enrutada pequeña.
- Configurar parámetros básicos en un router mediante la CLI para crear una ruta entre dos redes conectadas directamente.
- Verificar la conectividad entre dos redes que están conectadas directamente a un router.
- Explicar el proceso de encapsulación y desencapsulación que utilizan los routers para el switching de paquetes entre interfaces.
- Explicar la función de determinación de rutas de un router.
- Explicar las entradas de la tabla de routing de las redes conectadas directamente.
- Explicar la forma en que un router crea una tabla de routing de redes conectadas directamente.
- Explicar la forma en que un router crea una tabla de routing mediante rutas estáticas.
- Explicar la forma en que un router crea una tabla de routing mediante un protocolo de routing dinámico.



```
#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 N1 external type 1, N2 - OSPF N2 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 - 000, P - periodic downloaded static route, H - NHRP, 1 - LISP
      + - replicated route, # - next hop override

Gateway of last resort is not set

R1#
```

El routing ayuda a crear tablas de routing, que proporcionan una gran cantidad de información sobre las rutas a otras redes.

4.2 Configuración inicial de un router

4.2.1 Funciones de un router

Las redes tuvieron un impacto considerable en nuestras vidas. Estas cambiaron la forma en que vivimos, trabajamos y jugamos.

Las redes nos permiten comunicarnos, colaborar e interactuar como nunca antes. Utilizamos la red de distintas formas, entre ellas las aplicaciones web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación y más.

Como se muestra en la ilustración, existen muchas características clave relacionadas con las estructuras y el rendimiento a las cuales nos referimos cuando hablamos de redes:

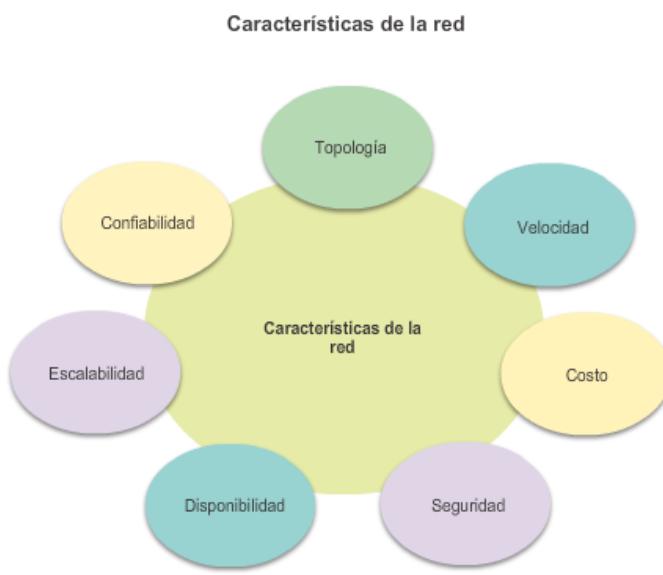
- **Topología:** existen topologías físicas y lógicas. La topología física es la disposición de los cables, los dispositivos de red y los sistemas finales. Esta describe la forma en que los

dispositivos de red se interconectan con los hilos y cables. La topología lógica es la ruta por la cual se transfieren los datos en una red. Describe cómo aparecen conectados los dispositivos de red a los usuarios de la red.

- **Velocidad:** la velocidad mide la velocidad de datos de un enlace dado en la red en bits por segundo (b/s).
- **Costo:** el costo indica el gasto general de la adquisición de componentes de red, así como de la instalación y el mantenimiento de la red.
- **Seguridad:** la seguridad indica el nivel de protección de la red, incluida la información que se transmite a través de esta. El tema de la seguridad es importante, y las técnicas y las prácticas están en constante evolución. Siempre tenga en cuenta la seguridad cuando se tomen medidas que afecten la red.
- **Disponibilidad:** la disponibilidad mide la probabilidad de que la red esté disponible para ser utilizada cuando resulte necesario.
- **Escalabilidad:** la escalabilidad indica la facilidad con la que la red puede admitir más usuarios y requisitos de transmisión de datos. Si un diseño de red está optimizado para cumplir solo con los requisitos actuales, puede resultar muy difícil y costoso satisfacer nuevas necesidades cuando la red crezca.
- **Confiabilidad:** la confiabilidad indica la fiabilidad de los componentes que crean la red, como los routers, los switches, las computadoras y los servidores. A menudo, la confiabilidad se mide como la probabilidad de fallas o como el tiempo medio entre fallas (MTBF).

Estas características y atributos proporcionan un medio para comparar distintas soluciones de redes.

Nota: si bien el término “velocidad” se utiliza comúnmente para referirse al ancho de banda de red, no es del todo preciso. La velocidad propiamente dicha a la que se transmiten los bits no varía en el mismo medio. La diferencia en el ancho de banda se debe a la cantidad de bits transmitidos por segundo, no a la velocidad a la que se trasladan a través del medio cableado o inalámbrico.



¿Cómo es que se logra acceder a la información deseada en pocos segundos haciendo clic en un enlace en un navegador web? Si bien existen muchos dispositivos y tecnologías que trabajan juntos de forma colaborativa para lograr esto, el dispositivo principal es el router. En pocas palabras, un router conecta una red con otra red.

La comunicación entre redes no sería posible sin un router que determine la mejor ruta hacia el destino y que reenvíe el tráfico al router siguiente en esa ruta. El router es responsable del routing del tráfico entre redes.

En la animación de la ilustración, el diagrama de la topología de la red consta de dos hosts, dos switches y un router de servicios integrados (ISR) Cisco 1841.

Cuando un paquete llega a una interfaz del router, este utiliza la tabla de routing para determinar cómo llegar a la red de destino. El destino de un paquete IP puede ser un servidor web en otro país o un servidor de correo electrónico en la red de área local. Es responsabilidad de los routers entregar esos paquetes de forma eficaz. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers de reenviar paquetes de la manera más eficiente posible.



Para que la mayoría de los dispositivos con capacidad de red funcionen (es decir, las computadoras, las tablet PC y los smartphones), estos requieren los siguientes componentes, como se muestra en la figura 1:

- Unidad central de procesamiento (CPU)
- Sistema operativo (OS)
- Memoria y almacenamiento (RAM, ROM, NVRAM, flash, disco duro)

Básicamente, los routers son computadoras especializadas. Estos requieren una CPU y una memoria para almacenar datos de forma temporal y permanente a fin de ejecutar las instrucciones del sistema operativo, como la inicialización del sistema, las funciones de routing y de switching.

Nota: los dispositivos de Cisco utilizan el sistema operativo Internetwork (IOS) de Cisco como software de sistema.

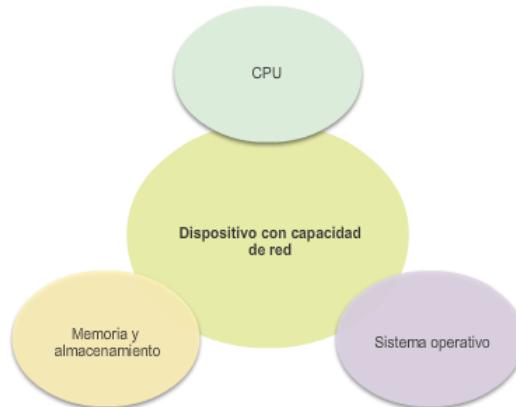
En la tabla de la figura 2, se resumen los tipos de memoria de router, la volatilidad, y se proporcionan ejemplos de lo que se almacena en cada una.

Los routers almacenan datos mediante lo siguiente:

- **Memoria de acceso aleatorio (RAM):** proporciona almacenamiento temporal para una variedad de aplicaciones y procesos, entre ellos, el IOS en ejecución, el archivo de configuración en ejecución, las diversas tablas (es decir, la tabla de routing IP, la tabla ARP de Ethernet) y los búferes para el procesamiento de paquetes. Se dice que la RAM es volátil porque pierde su contenido cuando se apaga el dispositivo.
- **Memoria de solo lectura (ROM):** proporciona almacenamiento permanente para las instrucciones de arranque, el software de diagnóstico básico y un IOS limitado en caso de que el router no pueda cargar el IOS con todas las funciones. La ROM consiste en un firmware y se dice que es no volátil, debido a que no pierde el contenido cuando se apaga el dispositivo.
- **Memoria de acceso aleatorio no volátil (NVRAM):** proporciona almacenamiento permanente para el archivo de configuración de inicio (startup-config). La NVRAM es no volátil y no pierde el contenido cuando se apaga el dispositivo.
- **Flash:** proporciona almacenamiento permanente para el IOS y otros archivos relacionados con el sistema. El IOS se copia de la memoria flash a la RAM durante el proceso de arranque. La memoria flash es no volátil y no pierde el contenido cuando se apaga el dispositivo.

A diferencia de las computadoras, los routers no tienen adaptadores de video o de tarjeta de sonido. En cambio, los routers cuentan con tarjetas de interfaz de red y puertos especializados para interconectar los dispositivos a otras redes. En la figura 3, se identifican algunos de estos puertos e interfaces.

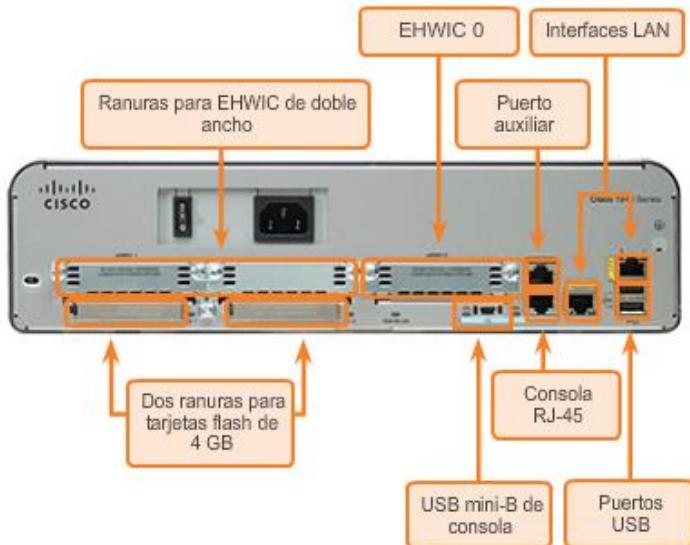
Componentes de un dispositivo con capacidad de red



Memoria del router

Memoria	Volátil/no volátil	Almacena
RAM	Volátil	<ul style="list-style-type: none"> • IOS en ejecución • Archivo de configuración en ejecución • Enrutamiento de IP y tablas ARP • Buffer de paquetes
ROM	No volátil	<ul style="list-style-type: none"> • Instrucciones de arranque • Software básico de diagnóstico • IOS limitado
NVRAM	No volátil	<ul style="list-style-type: none"> • Archivo de configuración de inicio
Flash	No volátil	<ul style="list-style-type: none"> • IOS (Sistema operativo de internetworking) • Otros archivos de sistema

Panel trasero de un router



La mayoría de los usuarios desconocen la presencia de varios routers en su propia red o en Internet. Los usuarios esperan poder acceder a páginas web, enviar correo electrónico y descargar música, sin importar si el servidor al que acceden está en su propia red o en otra. Los profesionales de redes saben que es el router el que se encarga del reenvío de paquetes de una red a otra, desde el origen inicial hasta el destino final.

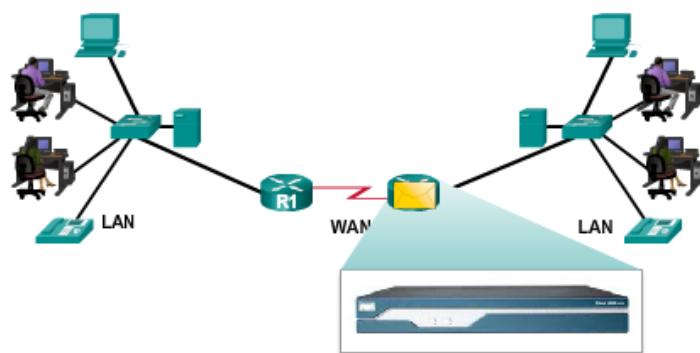
Un router conecta varias redes, lo que significa que posee varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz debe usar para reenviar el paquete hacia el destino. La interfaz que usa el router para reenviar el paquete puede ser el destino final o una red conectada a otro router que se usa para llegar a la red de destino.

En la animación de la figura 1, se observa que el R1 y el R2 son responsables de recibir el paquete en una red y reenviarlo desde otra red hacia la red de destino.

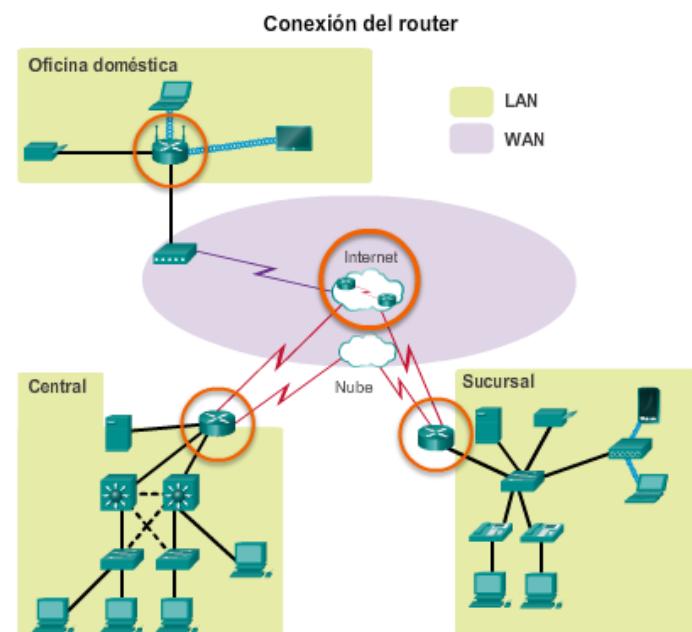
Generalmente, cada red a la que se conecta un router requiere una interfaz separada. Estas interfaces se usan para conectar una combinación de redes de área local (LAN) y redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como computadoras, impresoras y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

Observe que cada sitio de la figura 2 requiere el uso de un router para interconectarse a otros sitios. Incluso la oficina doméstica requiere un router. En esta topología, el router ubicado en la oficina doméstica es un dispositivo especializado que lleva a cabo varios servicios para la red doméstica.

Conexión por medio de routers



Los routers dirigen paquetes hacia el destino adecuado. Los routers conectan diferentes medios.



Las funciones principales de un router son las siguientes:

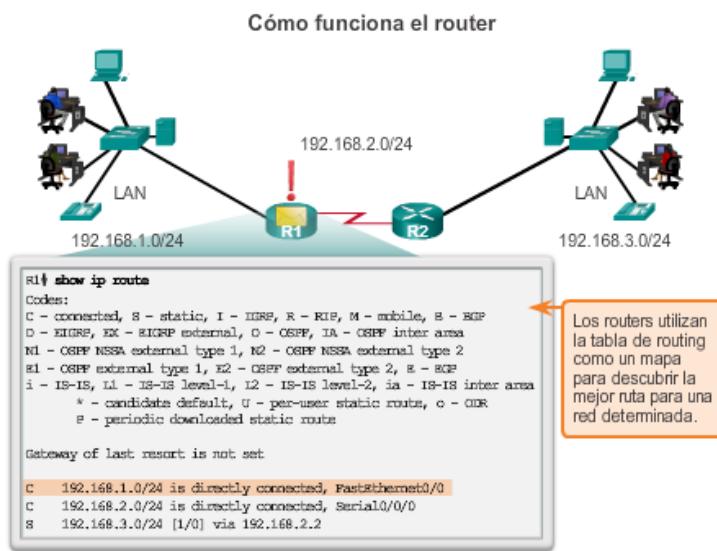
- Determinar la mejor ruta para enviar paquetes.
- Reenviar paquetes a su destino.

El router usa su tabla de routing para encontrar la mejor ruta para reenviar un paquete. Cuando el router recibe un paquete, analiza la dirección de destino del paquete y usa la tabla de routing para buscar la mejor ruta hacia esa red. La tabla de routing también incluye la interfaz que se debe usar para reenviar los paquetes a cada red conocida. Cuando se encuentra una coincidencia, el router encapsula el paquete en la trama de enlace de datos de la interfaz de salida, y el paquete se reenvía hacia el destino.

Un router puede recibir un paquete encapsulado en un tipo de trama de enlace de datos y reenviarlo por una interfaz que usa otro tipo de trama de enlace de datos. Por ejemplo, un router puede recibir un paquete en una interfaz Ethernet, pero debe reenviarlo por una interfaz configurada con el protocolo punto a punto (PPP). La encapsulación de enlace de datos depende del tipo de interfaz en el router y del tipo de medio al que se conecta. Las distintas tecnologías de enlace de datos a las que se puede conectar un router incluyen Ethernet, PPP, Frame Relay, DSL, tecnología de cable y tecnología inalámbrica (802.11, Bluetooth).

En la animación de la ilustración, se sigue un paquete desde la computadora de origen hasta la computadora de destino. Debe observarse que el router es responsable de encontrar la red de destino en su tabla de enrutamiento y reenviar el paquete hacia su destino. En este ejemplo, el router R1 recibe el paquete encapsulado en una trama de Ethernet. Despues de desencapsular el paquete, el R1 usa la dirección IP de destino del paquete para buscar una dirección de red que coincide en su tabla de routing. Luego de encontrar una dirección de red de destino en la tabla de enrutamiento, R1 encapsula el paquete dentro de una trama PPP y reenvía el paquete a R2. El R2 realiza un proceso similar.

Nota: los routers usan rutas estáticas y protocolos de routing dinámico para descubrir redes remotas y crear sus tablas de routing.



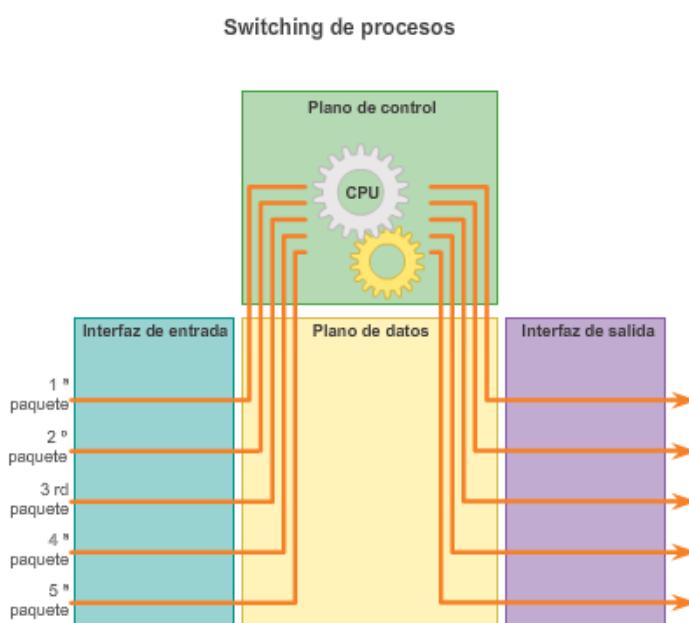
Los routers admiten tres mecanismos de reenvío de paquetes:

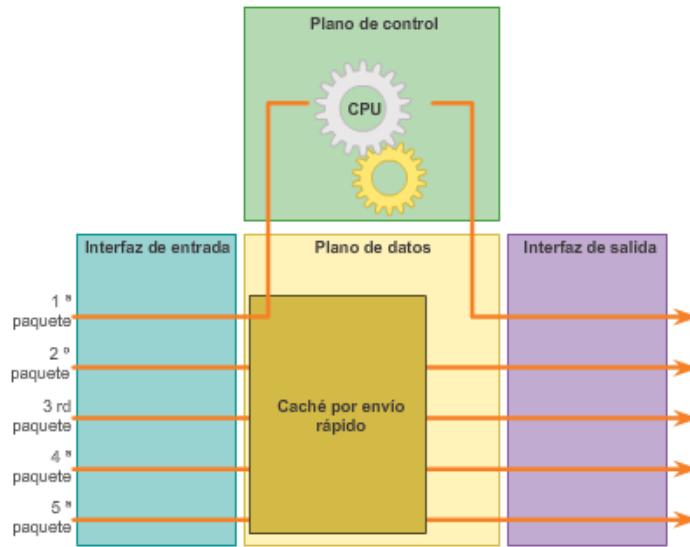
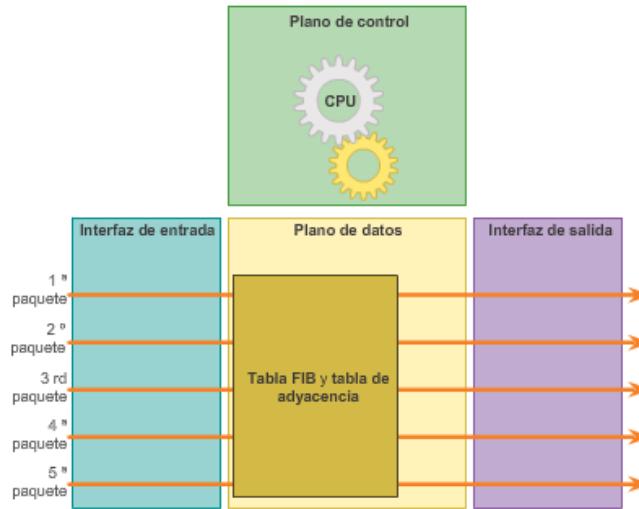
- **Switching de procesos:** es un mecanismo de reenvío de paquetes más antiguo que todavía está disponible para los routers Cisco. Cuando un paquete llega a una interfaz, se reenvía al plano de control, donde la CPU hace coincidir la dirección de destino con una entrada de la tabla de routing y, a continuación, determina la interfaz de salida y reenvía el paquete. Es importante comprender que el router hace esto con cada paquete, incluso si el destino es el mismo para un flujo de paquetes. Este mecanismo de switching de procesos es muy lento y rara vez se implementa en las redes modernas.
- **Switching rápido:** este es un mecanismo frecuente de reenvío de paquetes que usa una memoria caché de switching rápido para almacenar la información de siguiente salto. Cuando un paquete llega a una interfaz, se reenvía al plano de control, donde la CPU busca una coincidencia en la caché de switching rápido. Si no encuentra ninguna, se aplica el switching de procesos al paquete, y este se reenvía a la interfaz de salida. La información de flujo del paquete también se almacena en la caché de switching rápido. Si otro paquete con el mismo destino llega a una interfaz, se vuelve a utilizar la información de siguiente salto de la caché sin intervención de la CPU.
- **Cisco Express Forwarding (CEF):** CEF es el mecanismo de reenvío de paquetes más reciente y más utilizado del IOS de Cisco. Al igual que el switching rápido, CEF arma una base de información de reenvío (FIB) y una tabla de adyacencia. Sin embargo, las entradas de la tabla no se activan por los paquetes como en el switching rápido, sino que se activan por los cambios, como cuando se modifica un elemento en la topología de la red. Por lo tanto, cuando se converge una red, la FIB y las tablas de adyacencia contienen toda la información que el router debe tener en cuenta al reenviar un paquete. La FIB contiene búsquedas inversas calculadas previamente, información de siguiente salto para las rutas, incluida la información de interfaz y de capa 2. Cisco Express Forwarding es el mecanismo de reenvío más rápido y la opción más utilizada en los routers Cisco.

En las figuras 1 a 3, se muestran las diferencias entre los tres mecanismos de reenvío de paquetes. Suponga que hay un flujo de tráfico que consta de cinco paquetes que van hacia el mismo destino. Como se muestra en la figura 1, con el switching de procesos, la CPU debe procesar cada paquete en forma individual. Compare esto con el switching rápido, el cual se muestra en la figura 2. Con el switching rápido, observe que el switching de procesos se aplica solo al primer paquete de un flujo, el cual se agrega a la caché de switching rápido. Los cuatro paquetes siguientes se procesan rápidamente según la información de la caché de switching rápido. Por último, en la figura 3, se observa que CEF crea la FIB y las tablas de adyacencia una vez que se converge la red. Los cinco paquetes se procesan rápidamente en el plano de datos.

Una analogía frecuente que se usa para describir los tres mecanismos de reenvío de paquetes es la siguiente:

- El switching de procesos resuelve un problema realizando todos los cálculos matemáticos, incluso si los problemas son idénticos.
 - El switching rápido resuelve un problema realizando todos los cálculos matemáticos una vez y recuerda la respuesta para los problemas posteriores idénticos.
 - CEF soluciona todos los problemas posibles antes de tiempo en una hoja de cálculo.

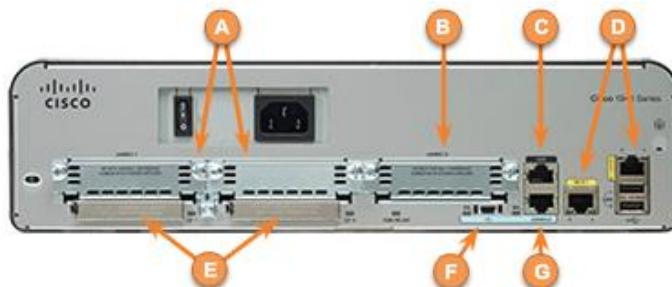


Switching rápido**Envío express de Cisco**

Tipo de memoria	Características del tipo de memoria
NVRAM	Configuración de inicio
Flash	Archivos de IOS y del sistema
ROM	Instrucciones de diagnóstico y de arranque
RAM	Configuración en ejecución

Actividad (parte 2): identificar los componentes del router

Identifique los puertos y las ranuras en este router Cisco serie 1941. Una el nombre de puerto o de ranura con la letra correspondiente a la ubicación apropiada en el panel trasero. Arrastre las letras de las ubicaciones hacia los campos correspondientes.



Nombre de puerto o de ranura del panel trasero	Ubicación en el panel posterior
Interfaces LAN	D
Puerto USB mini-B de consola	F
Puerto auxiliar	C
Cuatro ranuras para tarjetas flash de 4 GB	E
Ranuras para EHWIC de doble ancho	A
Puerto de consola RJ-45	G
Ranura EHWIC 0	B

Verificar
Resta

4.2.2 Conexión de los Dispositivos

Por lo general, los dispositivos de red y los usuarios finales se conectan a una red mediante una conexión Ethernet por cable o una conexión inalámbrica. Consulte la ilustración para ver un ejemplo de topología de referencia. Las LAN que se muestran en la ilustración sirven como ejemplo de cómo los usuarios y los dispositivos de red pueden conectarse a las redes.

Los dispositivos de la oficina doméstica pueden conectarse de la siguiente manera:

- Las computadoras portátiles y las tablet PC se conectan de forma inalámbrica a un router doméstico.

- Una impresora de red se conecta mediante un cable Ethernet al puerto de switch en el router doméstico.
- El router doméstico se conecta al cable módem del proveedor de servicios mediante un cable Ethernet.
- El cable módem se conecta a la red del proveedor de servicios de Internet (ISP).

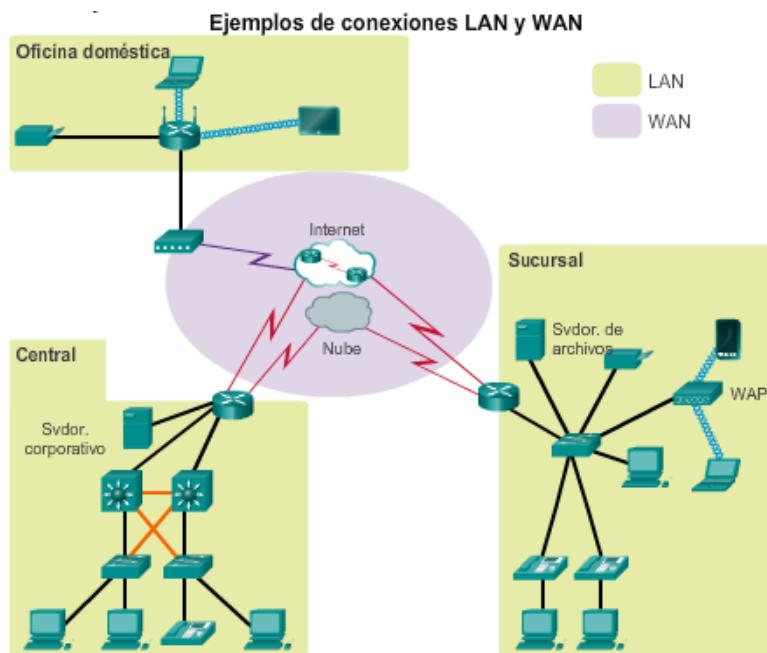
Los dispositivos de Sucursal se conectan de la siguiente manera:

- Los recursos corporativos (es decir, los servidores de archivos y las impresoras) se conectan a los switches de capa 2 mediante cables Ethernet.
- Las computadoras de escritorio y los teléfonos de voz sobre IP (VoIP) se conectan a los switches de capa 2 mediante cables Ethernet.
- Las computadoras portátiles y los smartphones se conectan de forma inalámbrica a los puntos de acceso inalámbrico (WAP).
- Los WAP se conectan a los switches mediante cables Ethernet.
- Los switches de capa 2 se conectan a una interfaz Ethernet en el router perimetral mediante cables Ethernet. Un router perimetral es un dispositivo que se encuentra en el perímetro o el límite de una red y crea rutas entre esa red y otra red, por ejemplo, entre una LAN y una WAN.
- El router perimetral se conecta al proveedor de servicios (SP) de una WAN.
- El router perimetral también se conecta a un ISP para propósitos de respaldo.

Los dispositivos del sitio Central se conectan de la siguiente manera:

- Las computadoras de escritorio y los teléfonos VoIP se conectan a los switches de capa 2 mediante cables Ethernet.
- Los switches de capa 2 se conectan de forma redundante a los switches multicapa de capa 3 con cables Ethernet de fibra óptica (conexiones anaranjadas).
- Los switches multicapa de capa 3 se conectan a una interfaz Ethernet en el router perimetral mediante cables Ethernet.
- El servidor del sitio web corporativo se conecta a la interfaz del router perimetral mediante un cable Ethernet.
- El router perimetral se conecta al SP de una WAN.
- El router perimetral también se conecta a un ISP para propósitos de respaldo.

En las LAN de los sitios Sucursal y Central, los hosts se conectan a la infraestructura de red de forma directa o indirecta (a través de WAP) mediante un switch de capa 2.



Para habilitar el acceso a la red, se deben configurar los dispositivos con la información de dirección IP para identificar los elementos correspondientes, entre ellos:

- **Dirección IP:** identifica un host único en una red local.
- **Máscara de subred:** identifica con qué subred de la red se puede comunicar el host.
- **Gateway predeterminado:** identifica el router al que se debe enviar un paquete cuando el destino no está en la misma subred de la red local.

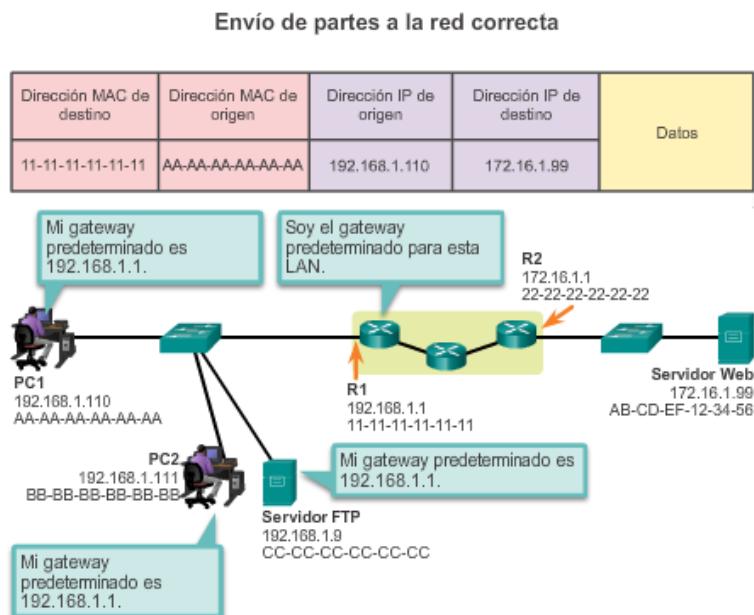
Cuando un host envía un paquete a un dispositivo que está en la misma red IP, el paquete tan solo se reenvía por la interfaz del host al dispositivo de destino.

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Con frecuencia, se utiliza para conectar una red local a Internet.

Por lo general, el gateway predeterminado es la dirección de la interfaz en el router que se conecta a la red local. El router mantiene entradas de la tabla de routing de todas las redes conectadas, así como entradas de redes remotas, y determina la mejor ruta para llegar a esos destinos.

Por ejemplo, si la PC1 envía un paquete al Web Server (Servidor web) ubicado en 176.16.1.99, descubrirá que este no está en la red local y, por lo tanto, debe enviar el paquete a la dirección de control de acceso a los medios (MAC) de su gateway predeterminado. La unidad de datos del protocolo (PDU) del paquete que se muestra en la ilustración identifica las direcciones MAC e IP de origen y destino.

Nota: los routers también se suelen configurar con su propio gateway predeterminado. En ocasiones, este se conoce como “gateway de último recurso”.



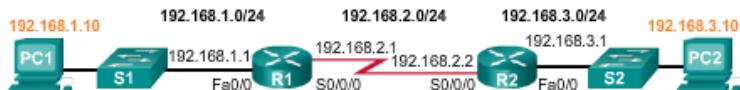
Cuando se diseña una nueva red o se hacen asignaciones en una red existente, es necesario documentar la red. Como mínimo, el registro debe identificar lo siguiente:

- Nombres de los dispositivos
- Interfaces usadas en el diseño
- Direcciones IP y máscaras de subred
- Direcciones de gateway predeterminado

Como se muestra en la ilustración, esta información se captura mediante la creación de dos registros útiles de la red:

- **Diagrama de topología:** proporciona una referencia visual que indica la conectividad física y el direccionamiento lógico de capa 3. A menudo se crea mediante software, por ejemplo, Microsoft Visio.
- **Tabla de direccionamiento:** es una tabla que captura nombres de dispositivos, interfaces, direcciones IPv4, máscaras de subred y direcciones de gateway predeterminado.

Registro del direccionamiento de red



Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

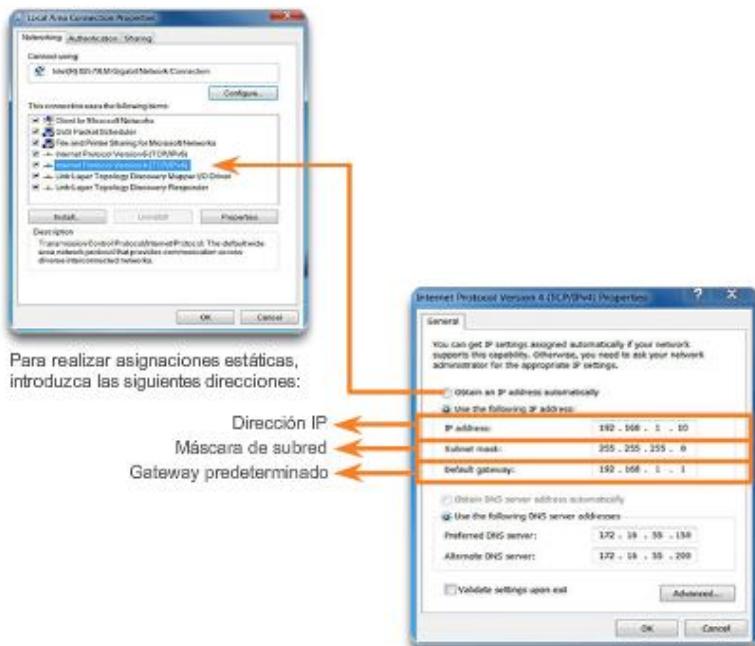
Se puede asignar información de dirección IP a un host de dos formas:

- **Estática:** se asigna la dirección IP, la máscara de subred y el gateway predeterminado correctos al host de forma manual. También se puede configurar la dirección IP del servidor DNS.
- **Dinámica:** un servidor proporciona la información de dirección IP mediante el protocolo de configuración dinámica de host (DHCP). El servidor de DHCP proporciona una dirección IP, una máscara de subred y un gateway predeterminado válidos para las terminales. El servidor también puede proporcionar otra información.

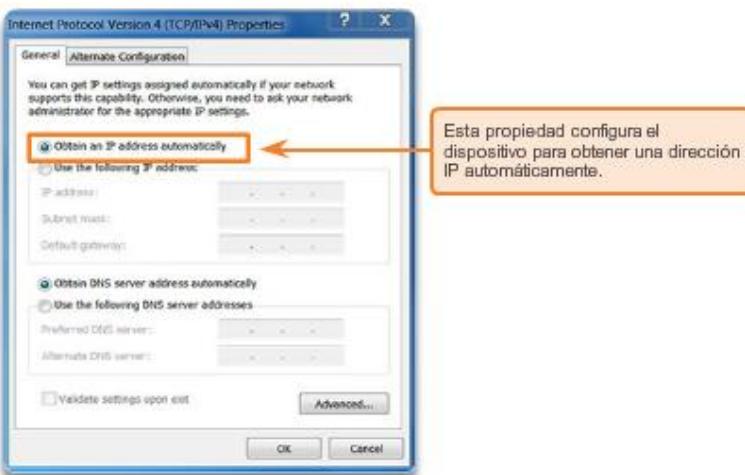
En las figuras 1 y 2, se proporcionan ejemplos de configuración estática y dinámica de direcciones IPv4.

Por lo general, las direcciones asignadas estáticamente se usan para identificar recursos de red específicos, como servidores e impresoras de red. También se pueden usar en redes más pequeñas con pocos hosts. Sin embargo, la mayoría de los dispositivos host adquieren su información de dirección IPv4 accediendo a un servidor de DHCP. En las empresas grandes, se implementan servidores de DHCP dedicados que proporcionan servicios a muchas LAN. En un entorno más pequeño de sucursal u oficina pequeña, un switch Cisco Catalyst o un ISR Cisco pueden proporcionar los servicios de DHCP.

Asignación estática de una dirección IP



Asignación dinámica de una dirección IP



Los equipos host se conectan a una red conectada por cable mediante una interfaz de red y un cable Ethernet RJ-45. La mayoría de las interfaces de red tienen uno o dos indicadores LED de enlace junto a la interfaz. Generalmente, un LED verde indica una conexión correcta, mientras que un LED verde que parpadea indica actividad de red.

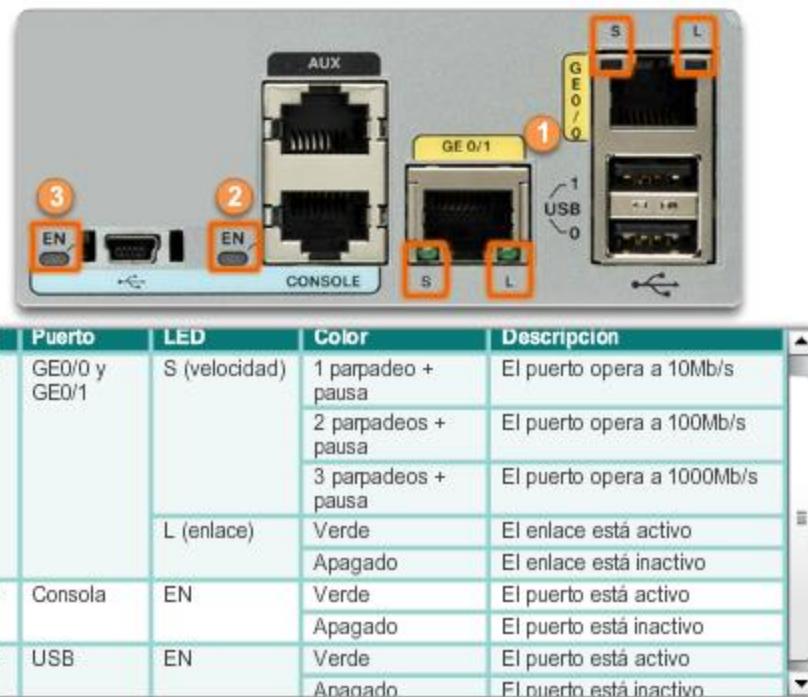
Si la luz de enlace no está encendida, puede existir un problema con el cable de red o con la red propiamente dicha. En el puerto del switch donde termina la conexión también hay un indicador LED encendido. Si un extremo no se enciende o ninguno lo hace, intente con otro cable de red.

Nota: la función de los LED varía entre los fabricantes de computadoras.

De manera similar, los dispositivos de infraestructura de red suelen utilizar varios indicadores LED para proporcionar una vista rápida del estado. Por ejemplo, un switch Cisco Catalyst 2960 tiene varios LED de estado para ayudar a controlar la actividad y el rendimiento del sistema. En general, estos LED están encendidos de color verde cuando el switch funciona normalmente y de color ámbar cuando funciona mal.

Los ISR Cisco utilizan distintos indicadores LED para proporcionar la información de estado. En la ilustración, se muestra un router Cisco 1941. Los LED del router ayudan al administrador de red a realizar un proceso básico de resolución de problemas. Cada dispositivo tiene un conjunto único de LED. Consulte la documentación específica de los dispositivos para obtener una descripción precisa de los LED.

Indicadores LED de Cisco 1941



En un entorno de producción, generalmente se accede a los dispositivos de infraestructura de manera remota mediante shell seguro (SSH) o el protocolo de transferencia de hipertexto seguro (HTTPS). El acceso a la consola solo es realmente necesario para realizar la configuración inicial de un dispositivo o si el acceso remoto falla.

El acceso a la consola requiere lo siguiente:

- Cable de consola:** un cable de consola RJ-45 a DB-9
- Software de emulación de terminal:** Tera Term, PuTTY, HyperTerminal

El cable se conecta entre el puerto serie del host y el puerto de consola en el dispositivo. La mayoría de las computadoras portátiles y de escritorio ya no cuentan con puertos serie incorporados. Si el host no tiene ningún puerto serie, se puede utilizar el puerto USB para establecer una conexión de consola. Cuando se usa el puerto USB, se requiere un adaptador especial de puerto serie compatible USB a RS-232.

El ISR Cisco G2 admite una conexión serie de consola USB. Para establecer la conectividad, se requiere un USB de tipo A a tipo B (USB mini-B), así como un controlador de dispositivo del sistema operativo. Este controlador de dispositivo se puede descargar en www.cisco.com. Si bien estos routers tienen dos puertos de consola, los puertos solo se pueden usar de a uno por vez. Cuando se conecta un cable al puerto de consola USB, el puerto RJ-45 queda inactivo. Cuando se quita el cable USB del puerto USB, el puerto RJ-45 se activa.

En la tabla de la figura 1, se resumen los requisitos para las conexiones de consola. En la figura 2, se muestran los distintos puertos y cables que se requieren.

Requisitos para las conexiones de consola

Puerto en la computadora	Cable requerido	Puerto en el ISR	Emulación de terminal
Puerto serie	Cable de consola RJ-45 a DB-9	Puerto de consola RJ-45	 Tera Term
USB Puerto tipo A	<ul style="list-style-type: none"> • Adaptador de puerto serie compatible con USB a RS-232 • El adaptador puede requerir un controlador de software. • Cable de consola RJ-45 a DB-9 • USB tipo A a USB tipo B (USB mini-B) • Se requiere un controlador de dispositivo disponible en cisco.com. 	USB tipo B (USB mini-B)	 PuTTY

Puertos y cables

Puerto en la computadora	Cable requerido	Puerto en el ISR	Emulación de terminal
 Puerto serie	 Cable de consola	 CONSOLE Puerto de consola RJ-45	 Tera Term
 USB Puerto tipo A	 Adaptador de puerto serie USB a RS-232  Cable de consola		
	 Cable USB tipo A a USB tipo B	 EN  USB tipo B Puerto de consola (USB mini-B)	 PuTTY

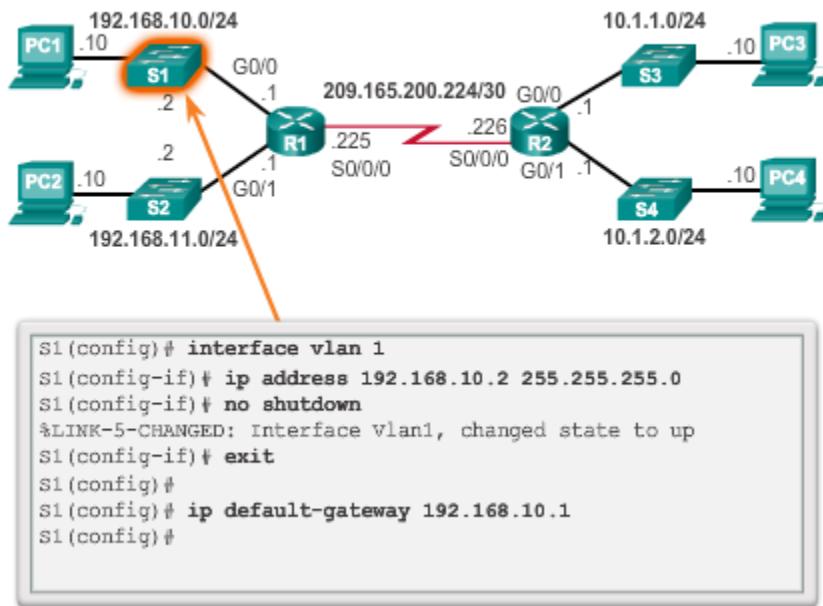
Los dispositivos de infraestructura de red requieren direcciones IP para habilitar la administración remota. Con la dirección IP del dispositivo, el administrador de red puede conectarse al dispositivo de forma remota mediante Telnet, SSH, HTTP o HTTPS.

Los switches no tienen una interfaz dedicada a la que se pueda asignar una dirección IP. En cambio, la información de dirección IP se configura en una interfaz virtual denominada “interfaz virtual comutada” (SVI).

Por ejemplo, en la figura 1, se asigna la dirección IP 192.168.10.2/24 y un gateway predeterminado del router ubicado en 192.168.10.1 a la SVI del switch de capa 2 S1.

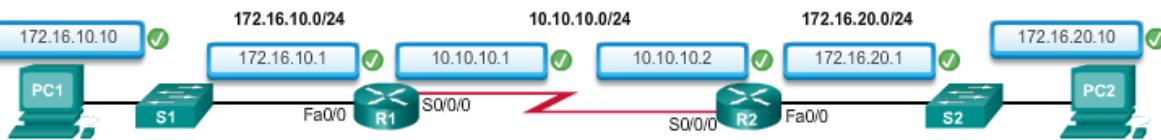
Utilice el verificador de sintaxis de la figura 2 para configurar el switch de capa 2 S2.

Configuración de la interfaz de administración de switches



Actividad: registrar el direccionamiento de red

Del conjunto de direcciones, arrastre una dirección a la tabla y a la topología para asignar una dirección a cada dispositivo.



Dispositivo	Interfaz	Dirección IPv4	Máscara de subred	Gateway predeterminado
R1	Fa0/0	172.16.10.1	255.255.255.0	N/A
	S0/0/0	10.10.10.1	255.255.255.0	N/A
R2	Fa0/0		255.255.255.0	N/A
	S0/0/0		255.255.255.0	N/A
PC1	N/A	172.16.10.10	255.255.255.0	172.16.10.1
PC2	N/A		255.255.255.0	

4.2.3 Configuración básica de un router

Los routers y los switches Cisco tienen muchas similitudes: admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Además, los pasos de configuración inicial son similares para ambos dispositivos.

Al configurar un switch o un router Cisco, primero se deben realizar las siguientes tareas básicas:

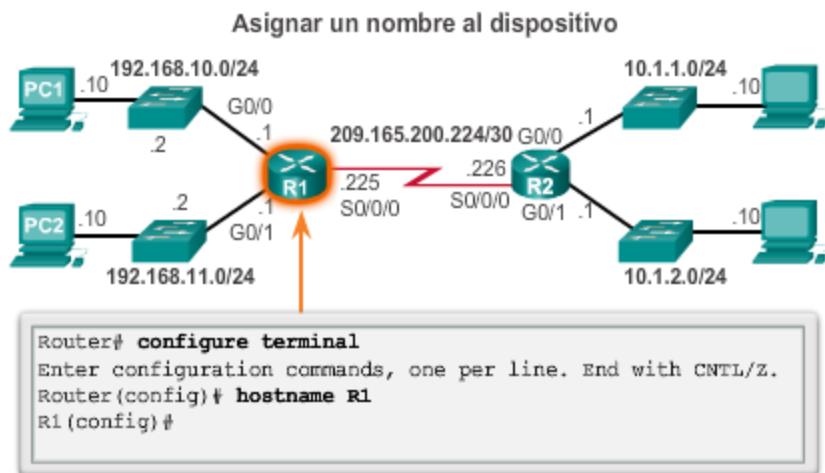
- **Asignar un nombre al dispositivo:** para distinguirlo de otros routers.
- **Proteger el acceso de administración:** para proteger el acceso a EXEC privilegiado, a EXEC de usuario y el acceso por Telnet, y cifrar las contraseñas con el máximo nivel.
- **Configurar un aviso:** para proporcionar notificaciones legales de acceso no autorizado.

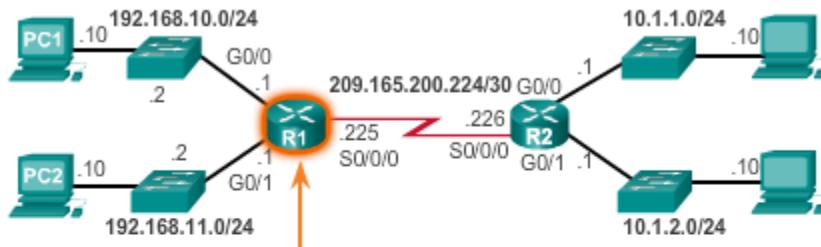
Nota: siempre guarde los cambios en un router y verifique la configuración básica y las operaciones del router.

En las figuras 1 a 4, se proporcionan ejemplos de configuración de parámetros básicos en el router R1:

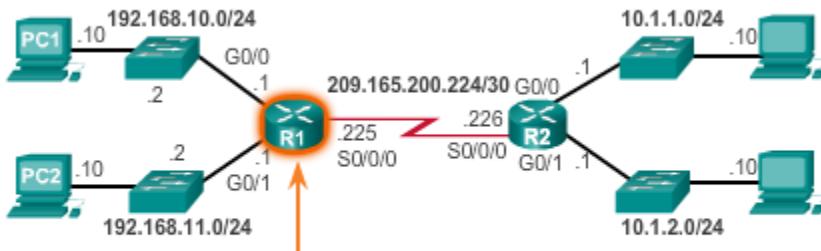
- En la figura 1, se asigna un nombre al dispositivo.
- En la figura 2, se protege el acceso de administración.
- En la figura 3, se configura un aviso.
- En la figura 4, se guarda la configuración.

Utilice el verificador de sintaxis de la figura 5 para configurar el router R2.

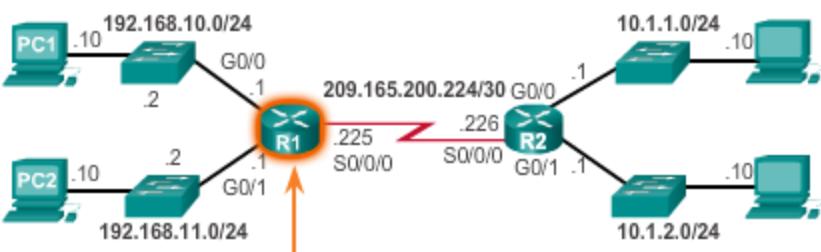


Proteger el acceso administrativo

```
R1(config)# enable secret class
R1(config)#
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)#
R1(config)# service password-encryption
R1(config)#
```

Configurar un aviso

```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

Guardar la configuración

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Una característica que distingue a los switches de los routers es el tipo de interfaces que admite cada uno. Por ejemplo, los switches de capa 2 admiten redes LAN y, por lo tanto, tienen varios puertos FastEthernet o Gigabit Ethernet.

Los routers admiten redes LAN y WAN, y pueden interconectar distintos tipos de redes; por lo tanto, admiten muchos tipos de interfaces. Por ejemplo, los ISR G2 tienen una o dos interfaces Gigabit Ethernet integradas y ranuras para tarjetas de interfaz WAN de alta velocidad (HWIC) para admitir otros tipos de interfaces de red, incluidas las interfaces seriales, DSL y de cable.

Para que una interfaz esté disponible, debe cumplir los siguientes requisitos:

- **Si se utiliza IPv4, se debe configurar la interfaz con una dirección y una máscara de subred:** use el comando de configuración de interfaz **ip address dirección-ip máscara-de-subred**.
- **Activar la interfaz:** las interfaces LAN y WAN no están activadas (**shutdown**) de manera predeterminada. Para habilitar una interfaz, esta se debe activar mediante el comando **no shutdown**. (Esto es similar al encendido de la interfaz). La interfaz también debe estar conectada a otro dispositivo (un hub, un switch u otro router) para que la capa física esté activa.

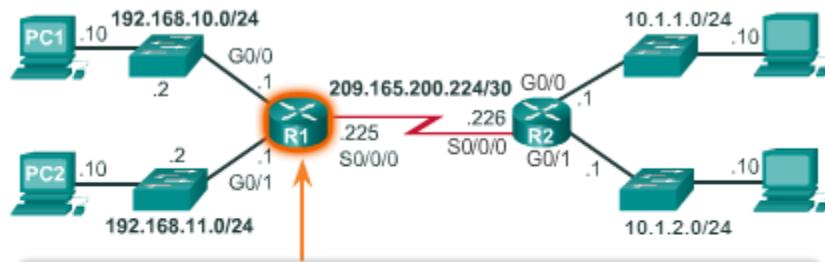
La interfaz también se puede configurar con una breve descripción. Es aconsejable configurar una descripción en cada interfaz. El texto de la descripción tiene un límite de 240 caracteres. En las redes de producción, una descripción puede ser útil para la resolución de problemas, dado que proporciona información con respecto al tipo de red a la que está conectada la interfaz. Si la interfaz se conecta a un ISP o un proveedor de servicios de telefonía móvil, resulta útil introducir la información de contacto y de conexión de dichos terceros.

Según el tipo de interfaz, es posible que se requieran parámetros adicionales. Por ejemplo, en el entorno del laboratorio, la interfaz serial que se conecta al extremo del cable serial rotulado DCE se debe configurar con el comando **clock rate**.

Nota: si se usa el comando **clock rate** por accidente en una interfaz DTE, se genera el mensaje de error %Error: This command applies only to DCE interface (%Error: este comando se aplica únicamente a la interfaz DCE).

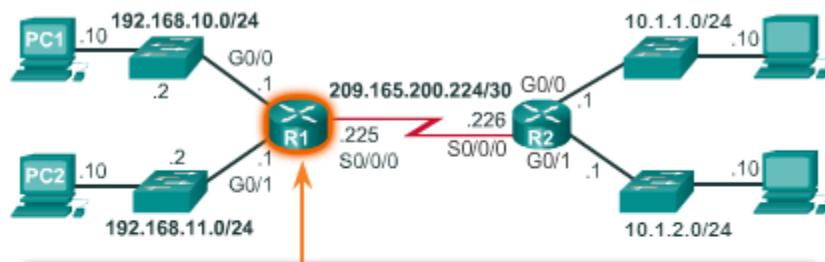
En las figuras 1 a 3, se proporcionan ejemplos de configuración de las interfaces del router R1.

Utilice el verificador de sintaxis de la figura 4 para configurar el router R2.

Configuración de la interfaz G0/0

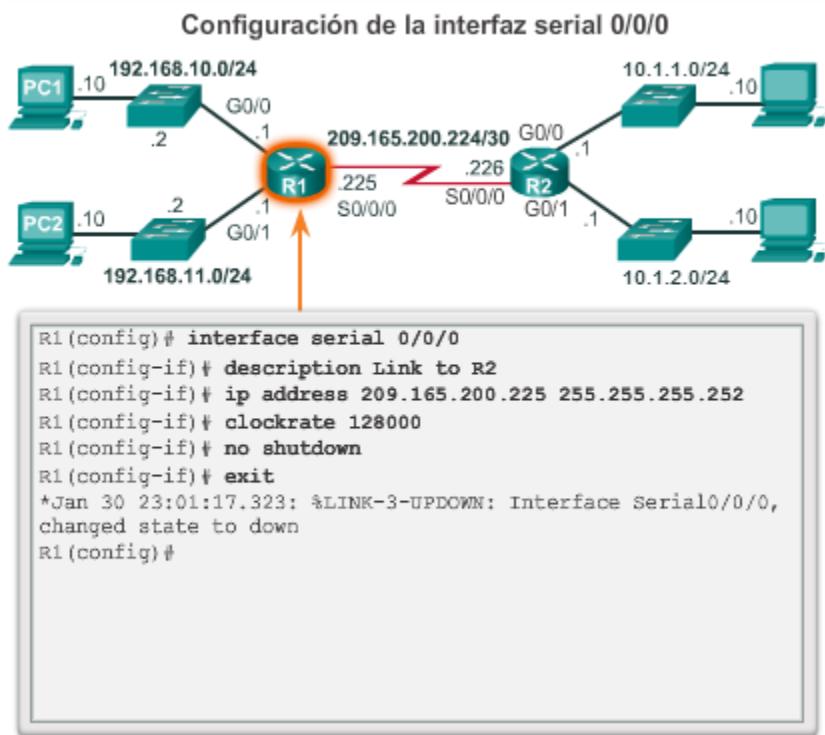
```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Jan 30 22:04:47.551: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
R1(config)#
*Jan 30 22:04:50.899: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Jan 30 22:04:51.899: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#

```

Configuración de la interfaz G0/1

```
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
*Jan 30 22:06:02.543: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to down
R1(config)#
*Jan 30 22:06:05.899: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jan 30 22:06:06.899: %LINEPROTO-5-UPDOWN: Line
protocol on Interface GigabitEthernet0/1, changed state
to up
R1(config)#

```



La configuración de una interfaz IPv6 es similar a la configuración de una interfaz para IPv4. La mayoría de los comandos de configuración y verificación de IPv6 del IOS de Cisco son muy similares a sus equivalentes de IPv4. En muchos casos, la única diferencia es el uso de **ipv6** en lugar de **ip** en los comandos.

Se debe realizar lo siguiente con la interfaz IPv6:

- **Configurar la interfaz con una máscara de subred y una dirección IPv6:** use el comando de configuración de interfaz **ipv6 address dirección-ipv6/longitud-prefijo [link-local | eui-64]**.
- **Activar la interfaz:** la interfaz se debe activar mediante el comando **no shutdown**.

Nota: una interfaz puede generar su propia dirección link-local de IPv6 sin tener una dirección de unidifusión global mediante el comando de configuración de interfaz **ipv6 enable**.

A diferencia de IPv4, las interfaces IPv6 generalmente tienen más de una dirección IPv6. Como mínimo, los dispositivos IPv6 deben tener una dirección link-local de IPv6, pero también es muy probable que tengan una dirección de unidifusión global de IPv6. IPv6 también admite la capacidad de que una interfaz tenga varias direcciones de unidifusión global de IPv6 de la misma subred. Los siguientes comandos se pueden usar para crear, de forma estática, una dirección de unidifusión global o link-local de IPv6:

- **ipv6 address dirección-ipv6/longitud-prefijo :** crea una dirección de unidifusión global de IPv6 según lo especificado.
- **ipv6 address dirección-ipv6/longitud-prefijo eui-64 :** configura una dirección de unidifusión global de IPv6 con un identificador de interfaz (ID) en los 64 bits de bajo orden de la dirección IPv6 mediante el proceso EUI-64.

- **ipv6 address dirección-ipv6/ longitud-prefijo Link-local:** configura una dirección link-local estática en la interfaz que se usa en lugar de la dirección link-local que se configura automáticamente cuando se asigna la dirección de unidifusión global de IPv6 a la interfaz, o cuando se habilita con el comando de interfaz **ipv6 enable**. Recuerde que el comando de interfaz **ipv6 enable** se usa para crear de forma automática una dirección link-local de IPv6, así se haya asignado una dirección de unidifusión global de IPv6 o no.

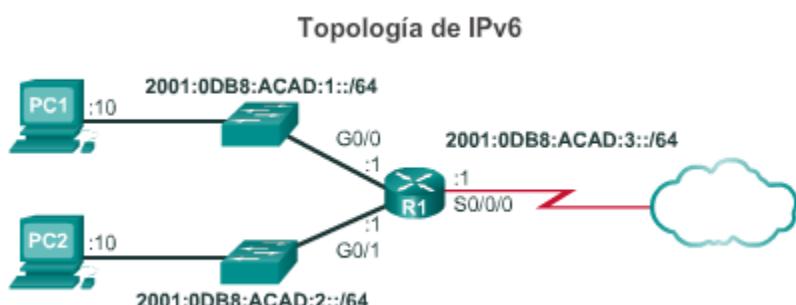
En la topología de ejemplo que se muestra en la figura 1, el R1 se debe configurar para que admita las siguientes direcciones de red IPv6:

- 2001:0DB8:ACAD:0001::/64 o 2001:DB8:ACAD:1::/64
- 2001:0DB8:ACAD:0002::/64 o 2001:DB8:ACAD:2::/64
- 2001:0DB8:ACAD:0003::/64 o 2001:DB8:ACAD:3::/64

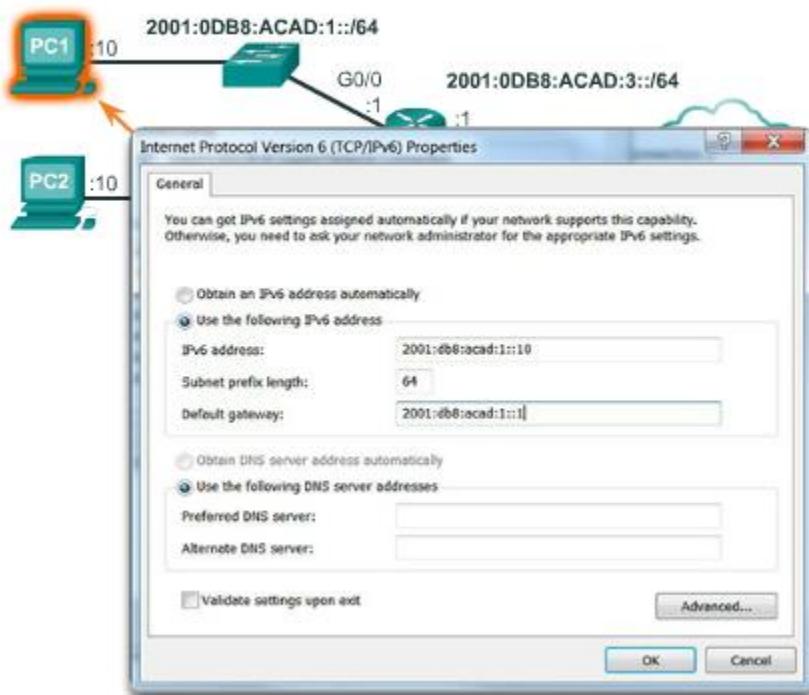
Cuando el router se configura con el comando de configuración global **ipv6 unicast-routing**, el router comienza a enviar mensajes de anuncio de router ICMPv6 por la interfaz. Esto permite que una computadora que está conectada a la interfaz configure una dirección IPv6 y establezca un gateway predeterminado de forma automática, sin necesidad de utilizar los servicios de un servidor de DHCPv6. Por otra parte, una computadora conectada a la red IPv6 puede obtener la dirección IPv6 asignada estáticamente, como se muestra en la figura 2. Observe que la dirección de gateway predeterminado configurada para la PC1 es la dirección de unidifusión global de IPv6 de la interfaz GigabitEthernet 0/0 del R1.

Las interfaces del router en la topología de ejemplo se deben configurar y habilitar como se muestra en las figuras 3 a 5.

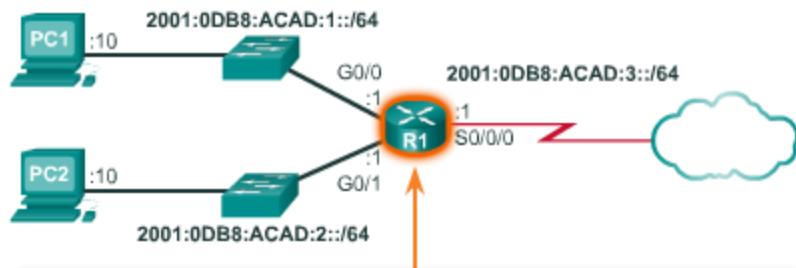
Utilice el verificador de sintaxis de la figura 6 para configurar las direcciones de unidifusión global de IPv6 en el router R2.



Asignación estática de una dirección IPv6 a PC1

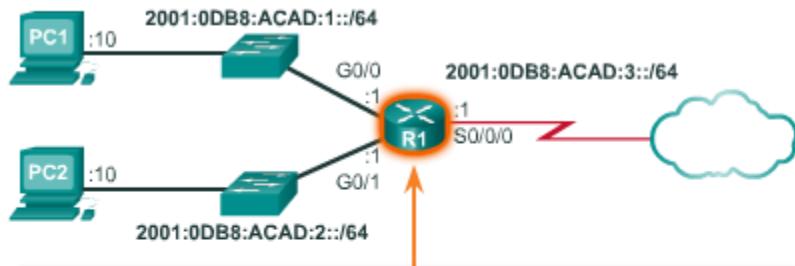


Configuración de la interfaz G0/0 de R1



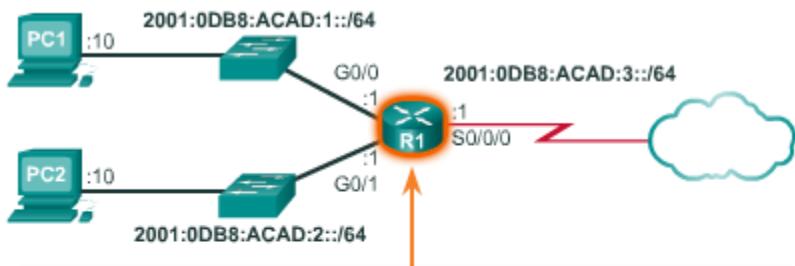
```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#description Link to LAN 1
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Feb 3 21:38:37.279: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
*Feb 3 21:38:40.967: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Feb 3 21:38:41.967: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#

```

Configuración de la interfaz G0/1 de R1

```
R1(config)#interface gigabitethernet 0/1
R1(config-if)#description Link to LAN 2
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Feb 3 21:39:21.867: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to down
*Feb 3 21:39:24.967: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Feb 3 21:39:25.967: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
R1(config)#

```

Configuración de la interfaz serial 0/0/0 de R1

```
R1(config)#interface serial 0/0/0
R1(config-if)#description Link to R2
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#
*Feb 3 21:39:43.307: %LINK-3-UPDOWN: Interface Serial0/0/0,
changed state to down
R1(config-if)#

```

Otra configuración común de los routers Cisco IOS es la habilitación de una interfaz loopback.

La interfaz loopback es una interfaz lógica interna del router. Esta no se asigna a un puerto físico y, por lo tanto, nunca se puede conectar a otro dispositivo. Se la considera una interfaz de software que se coloca automáticamente en estado UP (activo), siempre que el router esté en funcionamiento.

La interfaz loopback es útil para probar y administrar un dispositivo Cisco IOS, ya que asegura que por lo menos una interfaz esté siempre disponible. Por ejemplo, se puede usar con fines de prueba, como la prueba de procesos de routing interno, mediante la emulación de redes detrás del router.

Además, la dirección IPv4 asignada a la interfaz loopback puede ser importante para los procesos en el router que usan una dirección IPv4 de interfaz con motivos de identificación, como el proceso de routing del protocolo OSPF (Open Shortest Path First). Al habilitar una interfaz loopback, el router usa la dirección de la interfaz loopback que está siempre disponible para la identificación, en lugar de una dirección IP asignada a un puerto físico que puede dejar de funcionar.

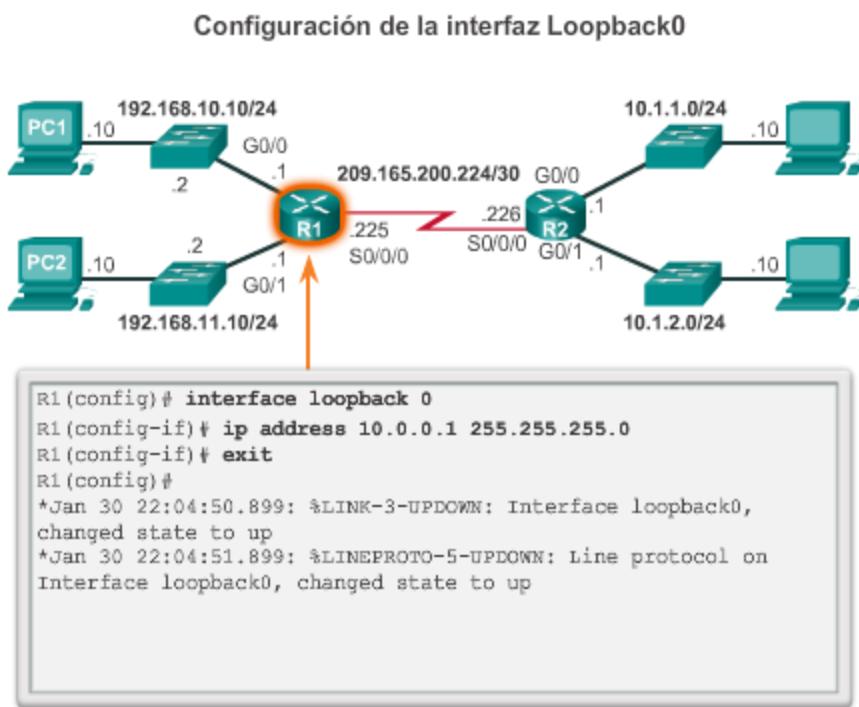
El proceso de habilitación y asignación de una dirección de loopback es simple:

```
Router(config)# interface loopback number
```

```
Router(config-if)# ip address ip-address subnet-mask
```

```
Router(config-if)# exit
```

Se pueden habilitar varias interfaces loopback en un router. La dirección IPv4 para cada interfaz loopback debe ser única y no la debe usar ninguna otra interfaz.



4.2.4 Verificación de la conectividad de redes conectadas directamente

Existen varios comandos **show** que se pueden usar para verificar el funcionamiento y la configuración de una interfaz. Los siguientes tres comandos son particularmente útiles para identificar de forma rápida el estado de una interfaz:

- **show ip interface brief**: muestra un resumen de todas las interfaces, incluso la dirección IPv4 de la interfaz y el estado operativo actual.
- **show ip route**: muestra el contenido de la tabla de enrutamiento IPv4 almacenada en la RAM. En el IOS de Cisco 15, las interfaces activas deben aparecer en la tabla de routing con dos entradas relacionadas identificadas con el código “C” (conectada) o “L” (local). En versiones anteriores de IOS, solo aparece una única entrada con el código “C”.
- **show running-config interface *id-interfaz***: muestra los comandos configurados en la interfaz especificada.

En la figura 1, se muestra el resultado del comando **show ip interface brief**. El resultado muestra que todas las interfaces LAN y el enlace WAN están activos y en funcionamiento, como lo indica el valor “up” en las columnas Status (Estado) y Protocol (Protocolo). Un resultado distinto indicaría un problema con la configuración o el cableado.

Nota: en la figura 1, se muestra la interfaz Embedded-Service-Engine0/0 porque los ISR Cisco G2 tienen CPU de doble núcleo en la placa madre. La interfaz Embedded-Service-Engine0/0 excede el ámbito de este curso.

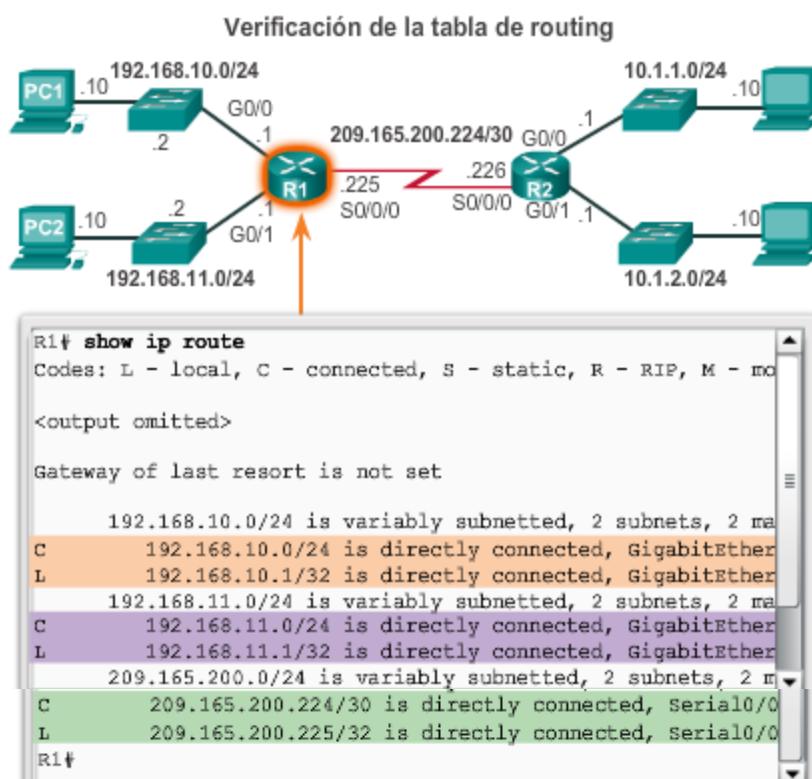
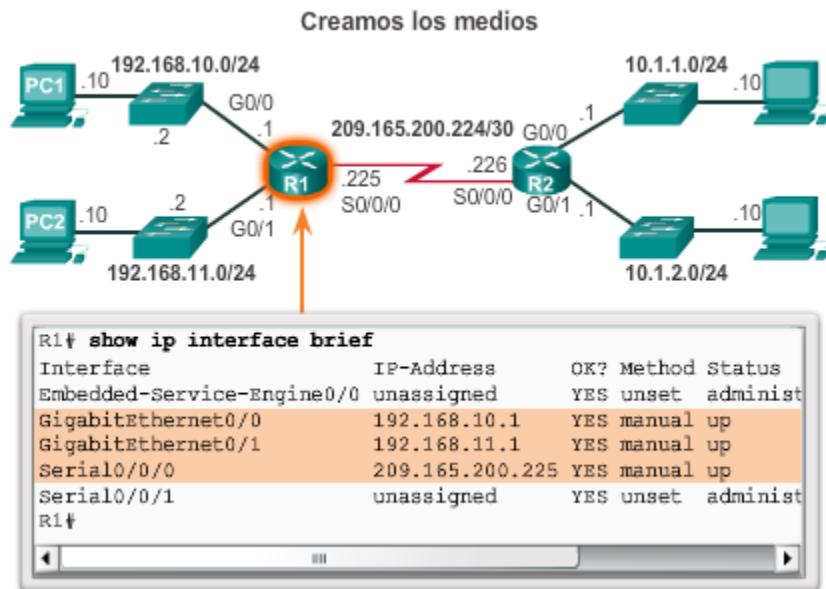
En la figura 2, se muestra el resultado del comando **show ip route**. Observe las tres entradas de redes conectadas directamente y las tres entradas de interfaz de ruta de host local. Una ruta de host local tiene una distancia administrativa de 0. También tiene una máscara /32 para IPv4 y una máscara /128 para IPv6. La ruta de host local es para las rutas en el router que posee la dirección IP. Estas se usan para permitir que el router procese los paquetes destinados a esa dirección IP.

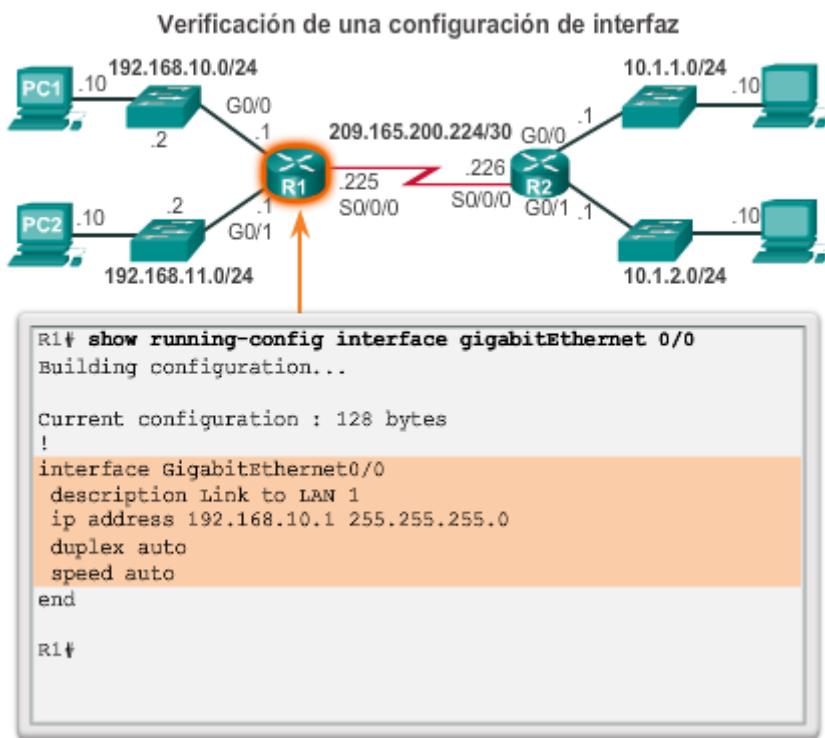
En la figura 3, se muestra el resultado del comando **show running-config interface**. El resultado muestra los comandos configurados actualmente en la interfaz especificada.

Los dos comandos siguientes se usan para recopilar información más detallada sobre la interfaz:

- **show interfaces**: muestra información sobre la interfaz y el conteo de flujo de paquetes de todas las interfaces del dispositivo.
- **show ip interface**: muestra la información relacionada con IPv4 de todas las interfaces de un router.

Utilice el verificador de sintaxis de las figuras 4 y 5 para verificar las interfaces del R1.





Los comandos para verificar la configuración de interfaz IPv6 son similares a los comandos que se usan para IPv4.

El comando **show ipv6 interface brief** de la figura 1 muestra un resumen para cada una de las interfaces. El resultado [up/up] en la misma línea que el nombre de interfaz indica el estado de interfaz de capa 1/capa 2. Esto es lo mismo que las columnas Status (Estado) y Protocol (Protocolo) en el comando IPv4 equivalente.

El resultado muestra dos direcciones IPv6 configuradas por interfaz. Una de las direcciones es la dirección de unidifusión global de IPv6 que se introdujo manualmente. La otra, que comienza con FE80, es la dirección de unidifusión link-local para la interfaz. La dirección link-local se agrega automáticamente a una interfaz cuando se asigna una dirección de unidifusión global. Las interfaces de red IPv6 deben tener una dirección link-local, pero no necesariamente una dirección de unidifusión global.

El resultado del comando **show ipv6 interface gigabitethernet 0/0** que se muestra en la figura 2 indica el estado de interfaz y todas las direcciones IPv6 que pertenecen a la interfaz. Además de la dirección link-local y la dirección de unidifusión global, el resultado incluye las direcciones de multidifusión asignadas a la interfaz, las cuales comienzan con el prefijo FF02.

Como se muestra en la figura 3, el comando **show ipv6 route** se puede utilizar para verificar si las redes IPv6 y las direcciones específicas de la interfaz IPv6 se instalaron en la tabla de routing IPv6. El comando **show ipv6 route** muestra solamente redes IPv6, no redes IPv4.

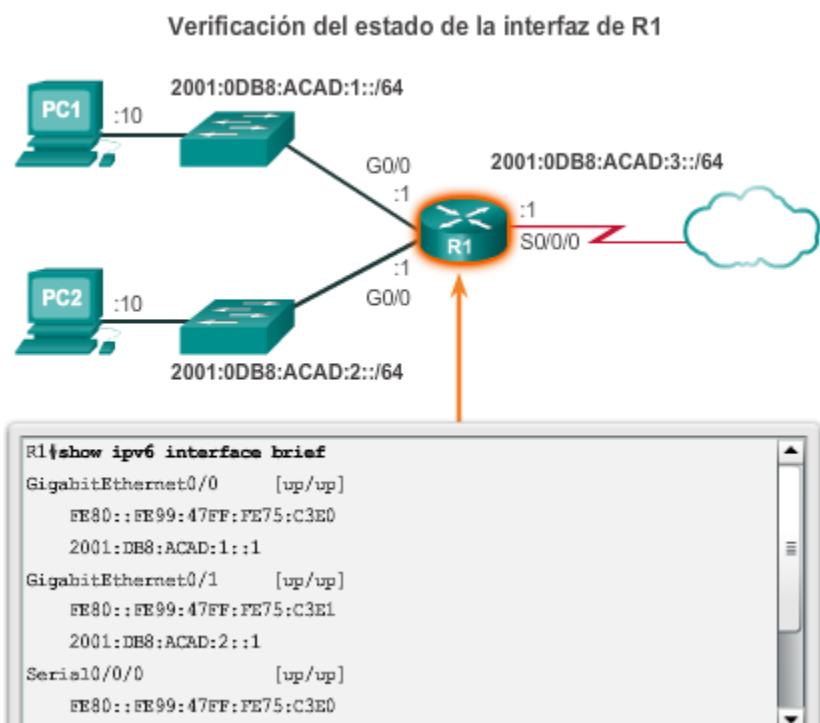
En la tabla de routing, una "C" junto a una ruta indica que se trata de una red conectada directamente. Cuando la interfaz del router se configura con una dirección unicast global y su estado es "up/up", se agrega el prefijo y la duración de prefijo IPv6 a la tabla de enrutamiento IPv6 como una ruta conectada.

La dirección IPv6 unicast global configurada en la interfaz también se instala en la tabla de enrutamiento como una ruta local. La ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente los paquetes cuyo destino es la dirección de la interfaz del router.

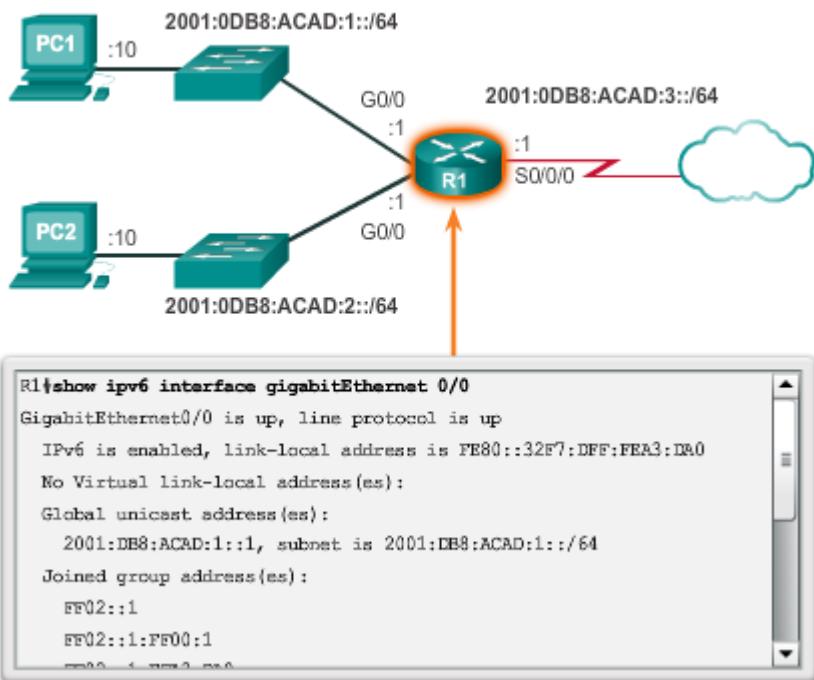
El comando **ping** para IPv6 es idéntico al comando que se utiliza con IPv4, excepto que se utiliza una dirección IPv6. Como se muestra en la figura 4, el comando **ping** se utiliza para verificar la conectividad de capa 3 entre el R1 y la PC1.

Otros comandos de verificación de IPv6 incluyen los siguientes:

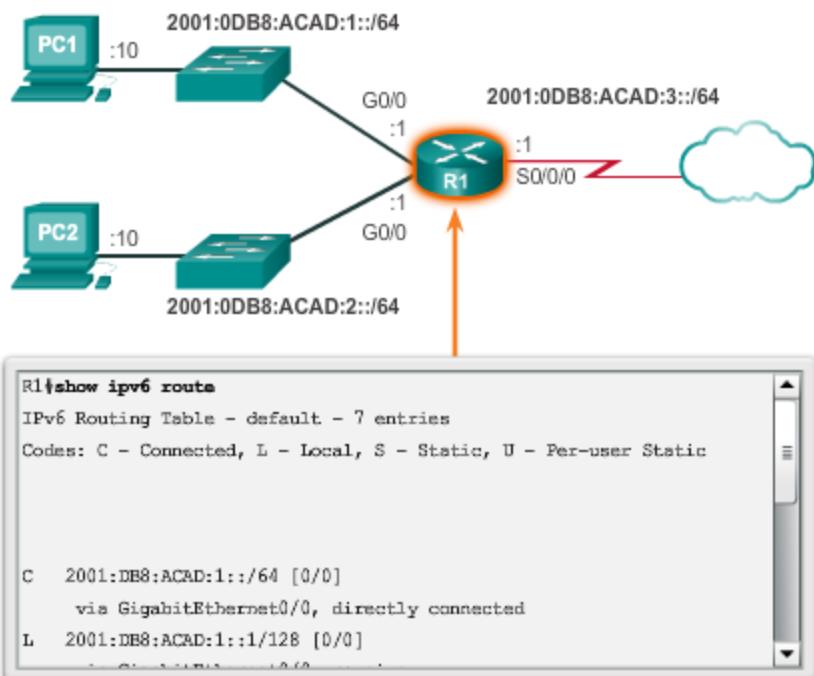
- **show interfaces**
- **show ipv6 routers**

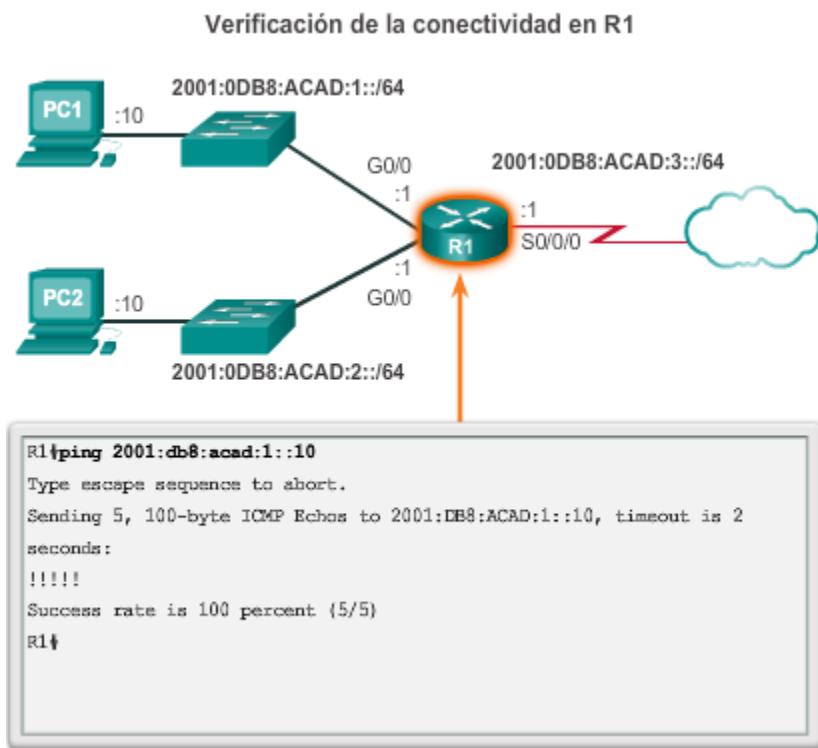


Verificación de la configuración de IPv6 en la G0/0 de R1



Verificación de la tabla de routing IPv6 de R1





Los comandos que generan varias pantallas de resultados se pausan al cabo de 24 líneas de manera predeterminada. Al final del resultado detenido, se muestra el texto --More--. Si presiona **Entrar**, se muestra la siguiente línea, y si presiona la barra espaciadora, se muestra el siguiente grupo de líneas. Utilice el comando **terminal length número** para especificar la cantidad de líneas que se muestran. Un valor 0 (cero) evita que el router haga una pausa entre las pantallas de resultados.

Otra característica muy útil que mejora la experiencia del usuario en la interfaz de línea de comandos (CLI) es el filtrado de los resultados del comando **show**. Los comandos de filtrado se pueden utilizar para mostrar secciones específicas de los resultados. Para habilitar el comando de filtrado, introduzca una barra vertical (|) después del comando **show** y, a continuación, introduzca un parámetro de filtrado y una expresión de filtrado.

Los parámetros de filtrado que se pueden configurar después de la barra vertical incluyen lo siguiente:

- **section**: muestra la sección completa que comienza con la expresión de filtrado.
- **include**: incluye todas las líneas de resultados que coinciden con la expresión de filtrado.
- **exclude**: excluye todas las líneas de resultados que coinciden con la expresión de filtrado.
- **begin**: muestra todas las líneas de resultados desde determinado punto, comenzando por la línea que coincide con la expresión de filtrado.

Nota: los filtros de resultados se pueden utilizar junto con cualquier comando **show**.

En las figuras 1 a 4, se proporcionan ejemplos de los diversos filtros de resultados.

Utilice el verificador de sintaxis de la figura 5 para filtrar los resultados.

Filtrado de comandos show

```
R1# show running-config | section line vty  
line vty 0 4  
password 7 030752180500  
login  
transport input all  
R1#
```

Filtrado de comandos show

```
R1# show ip interface brief  
Interface          IP-Address      OK? Method Status  
Embedded-Service-Engine0/0 unassigned    YES unset  administ  
GigabitEthernet0/0     192.168.10.1    YES manual up  
GigabitEthernet0/1     192.168.11.1    YES manual up  
Serial0/0/0           209.165.200.225 YES manual up  
Serial0/0/1           unassigned       YES unset  administ  
R1#  
R1# show ip interface brief | include up  
GigabitEthernet0/0     192.168.10.1    YES manual up  
GigabitEthernet0/1     192.168.11.1    YES manual up  
Serial0/0/0           209.165.200.225 YES manual up  
R1#
```

```
R1# show ip interface brief  
Interface          IP-Address      OK? Method Status  
Embedded-Service-Engine0/0 unassigned    YES unset  administ  
GigabitEthernet0/0     192.168.10.1    YES manual up  
GigabitEthernet0/1     192.168.11.1    YES manual up  
Serial0/0/0           209.165.200.225 YES manual up  
Serial0/0/1           unassigned       YES unset  administ  
  
R1# show ip interface brief | exclude unassigned  
Interface          IP-Address      OK? Method Status  
GigabitEthernet0/0     192.168.10.1    YES manual up  
GigabitEthernet0/1     192.168.11.1    YES manual up  
Serial0/0/0           209.165.200.225 YES manual up  
  
R1#
```

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

      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/0/0
L        209.165.200.225/32 is directly connected, Serial0/0/0
R1#
```

La característica de historial de comandos es útil, ya que almacena temporalmente la lista de comandos ejecutados que se deben recuperar.

Para recuperar comandos del búfer de historial, presione **Ctrl+P** o la tecla **Flecha arriba**. El resultado de los comandos comienza con el comando más reciente. Repita la secuencia de teclas para recuperar sucesivamente los comandos más antiguos. Para volver a los comandos más recientes en el búfer de historial, presione **Ctrl+N** o la tecla **Flecha abajo**. Repita la secuencia de teclas para recuperar sucesivamente los comandos más recientes.

De manera predeterminada, el historial de comandos está habilitado, y el sistema captura las últimas 10 líneas de comandos en el búfer de historial. Utilice el comando **show history** del modo EXEC privilegiado para mostrar el contenido del búfer.

También es práctico aumentar la cantidad de líneas de comandos que registra el búfer de historial solamente durante la sesión de terminal actual. Utilice el comando **terminal history size** del modo EXEC del usuario para aumentar o reducir el tamaño del búfer.

En la figura 1, se muestra un ejemplo de los comandos **terminal history size** y **show history**.

Utilice el verificador de sintaxis de la figura 2 para practicar los dos comandos del modo EXEC.

Característica de historial de comandos

```
R1# terminal history size 200
R1#
R1# show history
show ip interface brief
show interface g0/0
show ip interface g0/1
show ip route
show ip route 209.165.200.224
show running-config interface s0/0/0
terminal history size 200
show history
R1#
```

4.3 Decisiones de Routing

4.3.1 Switching de paquetes entre redes

Una de las funciones principales de un router es reenviar paquetes hacia su destino. Esto se logra mediante una función de switching, que es el proceso que utiliza un router para aceptar un paquete en una interfaz y reenviarlo por otra interfaz. Una responsabilidad clave de la función de conmutación es la de encapsular los paquetes en el tipo de trama de enlace de datos correcto para el enlace de datos de salida.

Nota: en este contexto, el término “switching” significa literalmente mover paquetes de origen a destino y no se lo debe confundir con la función de un switch de capa 2.

Una vez que el router determinó la interfaz de salida mediante la función de determinación de rutas, el router debe encapsular el paquete en la trama de enlace de datos de la interfaz de salida.

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

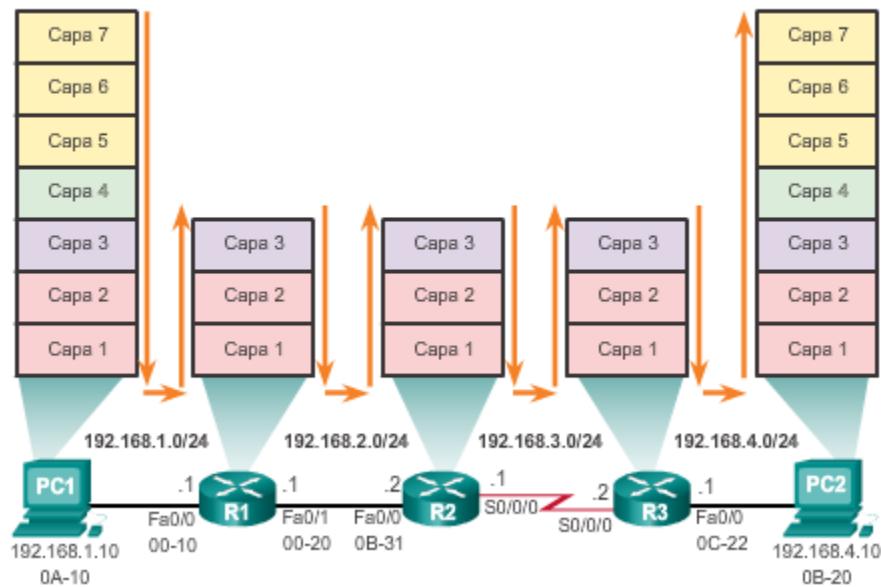
Paso 1. Desencapsula el paquete de capa 3 eliminando el encabezado y el tráiler de la trama de capa 2.

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

Paso 3. Si el router encuentra una ruta hacia el destino, encapsula el paquete de capa 3 en una nueva trama de capa 2 y reenvía la trama por la interfaz de salida.

Como se muestra en la ilustración, los dispositivos tienen direcciones IPv4 de capa 3, y las interfaces Ethernet tienen direcciones de enlace de datos de capa 2. Por ejemplo, la PC1 se configuró con la dirección IPv4 192.168.1.10 y una dirección MAC de ejemplo 0A-10. A medida que un paquete se desplaza desde el dispositivo de origen hacia el dispositivo de destino final, las direcciones IP de capa 3 no se modifican. Sin embargo, las direcciones de enlace de datos de capa 2 cambian en cada salto cuando cada router desencapsula y vuelve a encapsular el paquete en una nueva trama. Es muy probable que el paquete se encapsule en un tipo de trama de capa 2 diferente de la trama en la que se recibió. Por ejemplo, el router puede recibir una trama de Ethernet encapsulada en una interfaz FastEthernet y, a continuación, procesarla para reenviarla por una interfaz serial como trama encapsulada de protocolo punto a punto (PPP).

Encapsulación y desencapsulación de paquetes



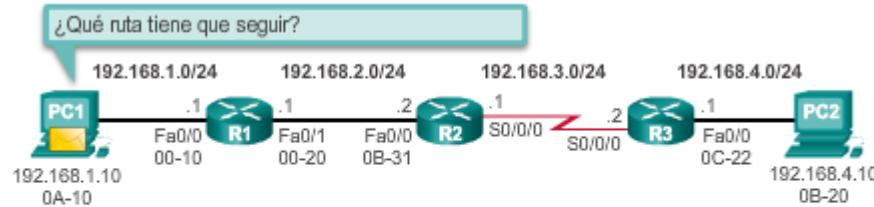
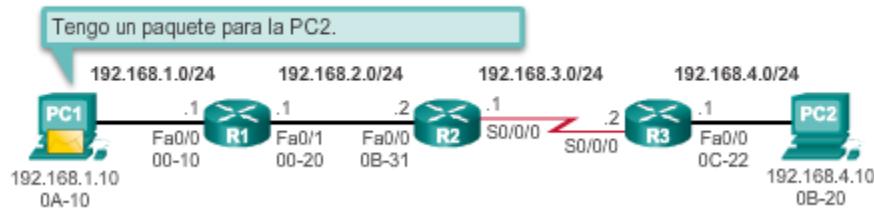
En la animación de la ilustración, la PC1 envía un paquete a la PC2. La PC1 debe determinar si la dirección IPv4 de destino está en la misma red. La PC1 determina su propia subred realizando una operación **AND** en su propia dirección y máscara de subred IPv4. Esto produce la dirección de red a la que pertenece la PC1. A continuación, la PC1 realiza la misma operación **AND** con la dirección IPv4 de destino del paquete y la máscara de subred de la PC1.

Si la dirección de red de destino está en la misma red que la PC1, entonces la PC1 no utiliza el gateway predeterminado. En lugar de esto, la PC1 consulta su caché ARP para obtener la dirección MAC del dispositivo con esa dirección IPv4 de destino. Si la dirección MAC no está en la caché, la PC1 genera una solicitud de ARP para obtener la dirección a fin de completar el paquete y enviarlo al destino. Si la dirección de red de destino está en una red diferente, la PC1 reenvía el paquete a su gateway predeterminado.

Para determinar la dirección MAC del gateway predeterminado, la PC1 busca la dirección IPv4 del gateway predeterminado y la dirección MAC relacionada en su tabla ARP.

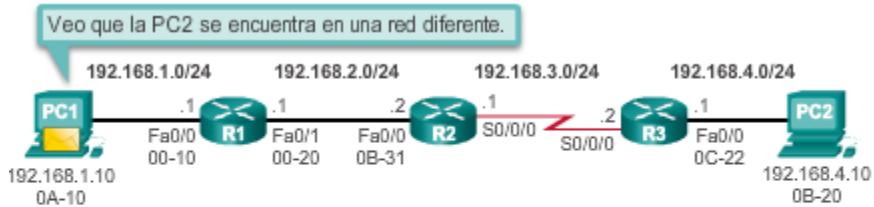
Si no existe ninguna entrada ARP para el gateway predeterminado en la tabla ARP, la PC1 envía una solicitud de ARP. El router R1 envía una respuesta de ARP. Luego, la PC1 puede reenviar el paquete a la dirección MAC del gateway predeterminado, la interfaz Fa0/0 del router R1.

Para los paquetes IPv6, se realiza un proceso similar. En lugar del proceso ARP, la resolución de direcciones IPv6 utiliza los mensajes ICMPv6 de solicitud y de anuncio de vecino. Las asignación de direcciones IPv6 a MAC se guarda en una tabla similar a la caché ARP, denominada "caché de vecinos".

La PC1 envía un paquete a la PC2

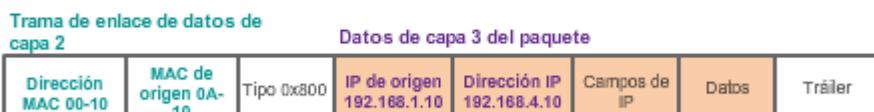
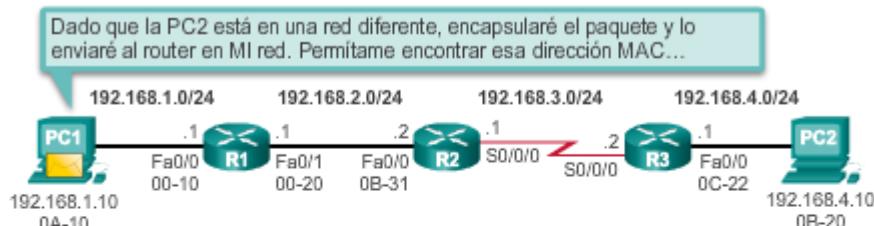
Datos de capa 3 del paquete

IP de origen	Dirección IP	Campos de IP	Datos
192.168.1.10	192.168.4.10		

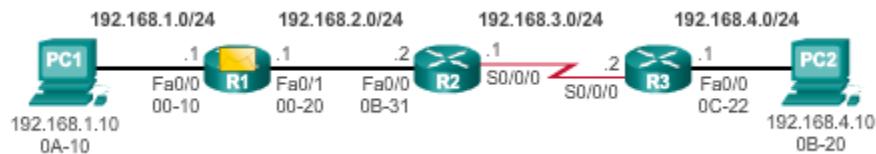


Datos de capa 3 del paquete

IP de origen	Dirección IP	Campos de IP	Datos
192.168.1.10	192.168.4.10		



Caché ARP de la PC1 para R1	
Dirección IP	Dirección MAC
192.168.1.1	00-10



Los siguientes procesos ocurren cuando el R1 recibe la trama de Ethernet de la PC1:

1. El R1 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, FastEthernet 0/0. Por lo tanto, el R1 copia la trama en su búfer.
2. El R1 distingue que el campo tipo de Ethernet es 0x800, lo que significa que la trama de Ethernet contiene un paquete IPv4 en la porción de datos de la trama.
3. El R1 desencapsula la trama de Ethernet.
4. Dado que la dirección IPv4 de destino del paquete no coincide con ninguna de las redes directamente conectadas del R1, este consulta su tabla de routing para enrutar este paquete. El R1 busca una dirección de red en la tabla de routing que incluya la dirección IPv4 de destino del paquete como dirección host dentro de esa red. En este ejemplo la tabla de enrutamiento tiene una ruta para la red 192.168.4.0/24. La dirección IPv4 de destino del paquete es 192.168.4.10, que es una dirección host IPv4 en esa red.

La ruta a la red 192.168.4.0/24 que encuentra el R1 tiene la dirección IPv4 de siguiente salto 192.168.2.2 y una interfaz de salida FastEthernet 0/1. Esto significa que el paquete IPv4 se encapsula en una nueva trama de Ethernet con la dirección MAC de destino de la dirección IPv4 del router de siguiente salto.

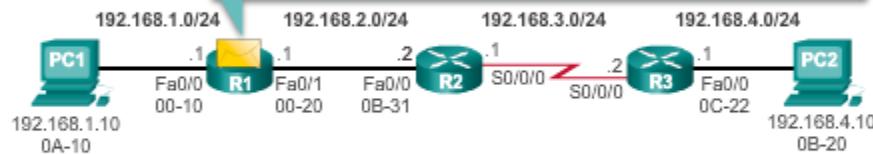
Debido a que la interfaz de salida se encuentra en una red Ethernet, el R1 debe resolver la dirección IPv4 de siguiente salto con una dirección MAC de destino mediante ARP:

1. El R1 busca la dirección IPv4 de siguiente salto 192.168.2.2 en su caché ARP. Si la entrada no aparece en la caché ARP, el R1 envía una solicitud de ARP por la interfaz FastEthernet 0/1, y el R2 envía una respuesta de ARP. A continuación, el R1 actualiza su caché ARP con una entrada para 192.168.2.2 y la dirección MAC asociada.
2. El paquete IPv4 ahora se encapsula en una nueva trama de Ethernet y se reenvía por la interfaz FastEthernet 0/1 del R1.

En la animación de la ilustración, se muestra cómo el R1 reenvía el paquete al R2.

El R1 reenvía el paquete a la PC2

La dirección MAC 0A-10 me envió una trama. Permitame investigar más.

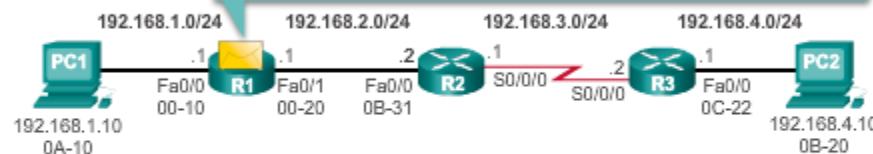


Trama de enlace de datos de capa 2

Datos de capa 3 del paquete

Dirección MAC 00-10	MAC de origen 0A-10	Tipo 0x800	IP de origen 192.168.1.10	Dirección IP 192.168.4.10	Campos de IP	Datos	Tráiler

Por el tipo y la dirección IP de destino, puedo ver que este paquete debe reenviarse.

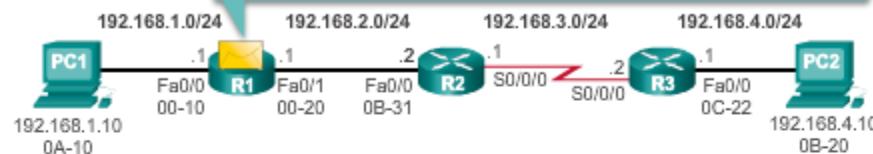


Trama de enlace de datos de capa 2

Datos de capa 3 del paquete

		Tipo 0x800	IP de origen 192.168.1.10	Dirección IP 192.168.4.10	Campos de IP	Datos	Tráiler

Tengo una ruta fuera de mi interfaz Fa0/1 para llegar a la PC2.



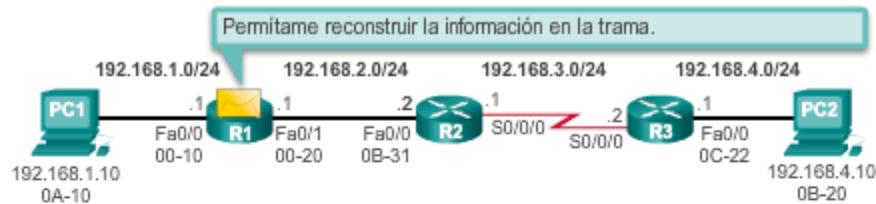
Trama de enlace de datos de capa 2

Datos de capa 3 del paquete

		Tipo 0x800	IP de origen 192.168.1.10	Dirección IP 192.168.4.10	Campos de IP	Datos	Tráiler

Tabla de routing del R1

Red	Saltos	IP del siguiente salto	Interfaz de salida
192.168.1.0/24	0	Dir. Conéctese.	Fa0/0
192.168.2.0/24	0	Dir. Conéctese.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1

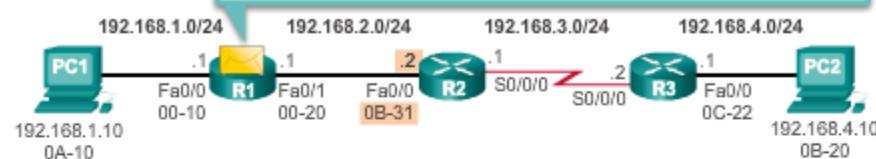


Trama de enlace de datos de capa 2		Datos de capa 3 del paquete					
		Tipo 0x800	IP de origen 192.168.1.10	Dirección IP 192.168.4.10	Campos de IP	Datos	Tráiler

Tabla de routing del R1

Red	Saltos	IP del siguiente salto	Interfaz de salida
192.168.1.0/24	0	Dir. Conéctese.	Fa0/0
192.168.2.0/24	0	Dir. Conéctese.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1

Mi tabla ARP me indica que la PC2 utiliza la dirección MAC 0B-31.



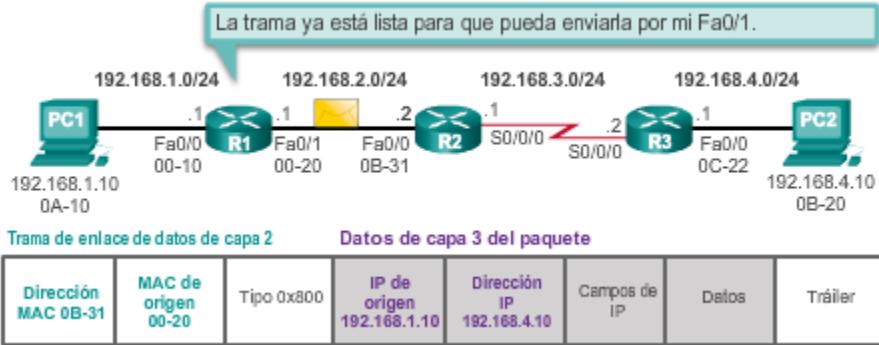
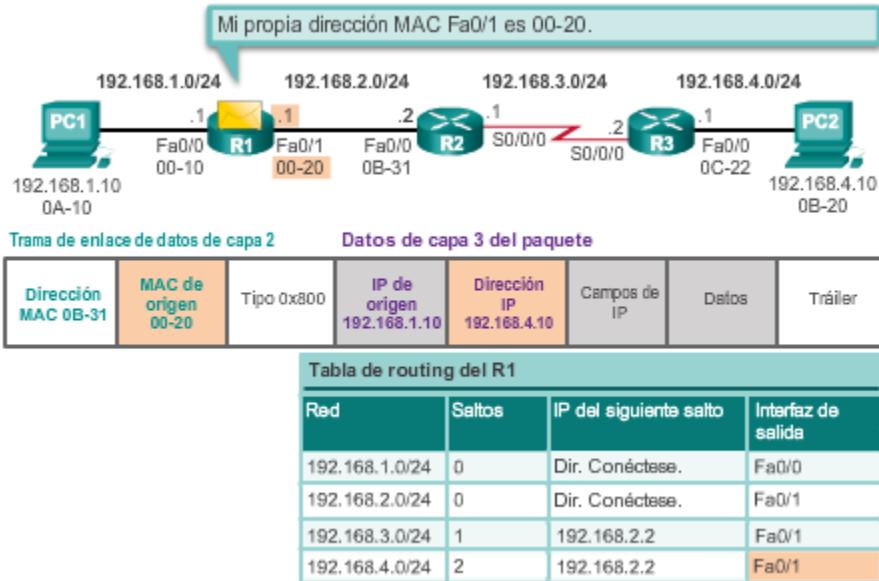
Trama de enlace de datos de capa 2		Datos de capa 3 del paquete					
Dirección MAC 0B-31		Tipo 0x800	IP de origen 192.168.1.10	Dirección IP 192.168.4.10	Campos de IP	Datos	Tráiler

Caché ARP del R1

Dirección IP	Dirección MAC
192.168.2.2	0B-31

Tabla de routing del R1

Red	Saltos	IP del siguiente salto	Interfaz de salida
192.168.1.0/24	0	Dir. Conéctese.	Fa0/0
192.168.2.0/24	0	Dir. Conéctese.	Fa0/1
192.168.3.0/24	1	192.168.2.2	Fa0/1
192.168.4.0/24	2	192.168.2.2	Fa0/1



Los siguientes procesos ocurren cuando el R2 recibe la trama en su interfaz Fa0/0:

- El R2 examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, FastEthernet 0/0. Por lo tanto, el R2 copia la trama en su búfer.
- El R2 distingue que el campo tipo de Ethernet es 0x800, lo que significa que la trama de Ethernet contiene un paquete IPv4 en la porción de datos de la trama.
- El R2 desencapsula la trama de Ethernet.
- Dado que la dirección IPv4 de destino del paquete no coincide con ninguna de las direcciones de interfaz del R2, este consulta su tabla de routing para enrutar este paquete. El R2 busca la dirección IPv4 de destino del paquete en la tabla de routing con el mismo proceso que usó el R1.

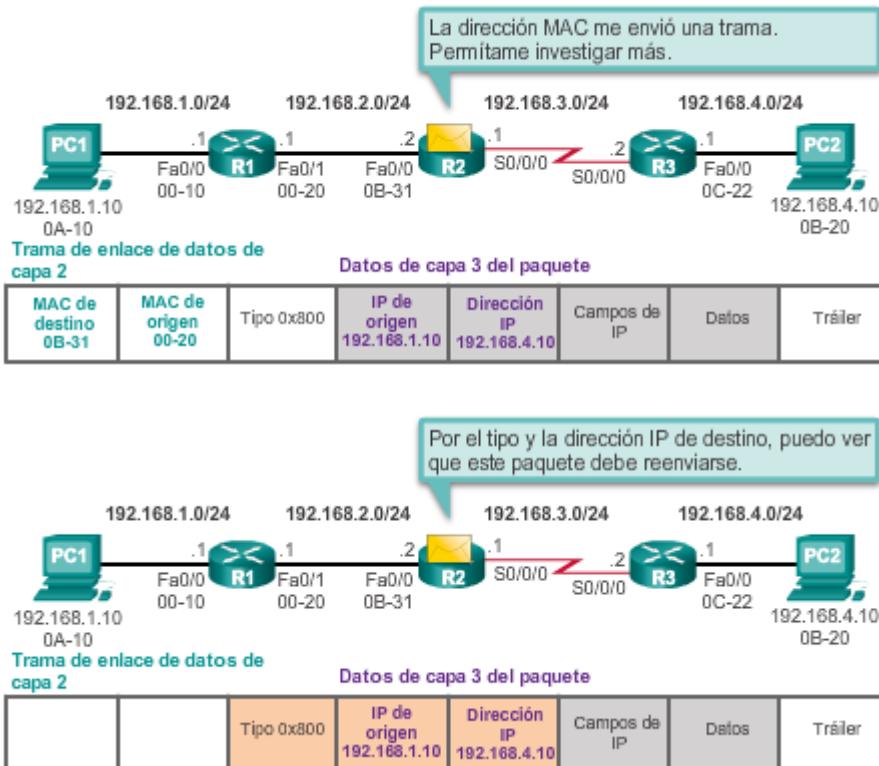
La tabla de routing del R2 tiene una ruta a la red 192.168.4.0/24, con la dirección IPv4 de siguiente salto 192.168.3.2 y la interfaz de salida Serial 0/0/0. Debido a que la interfaz de salida no es una red Ethernet, el R2 no tiene que resolver la dirección IPv4 de siguiente salto con una dirección MAC de destino.

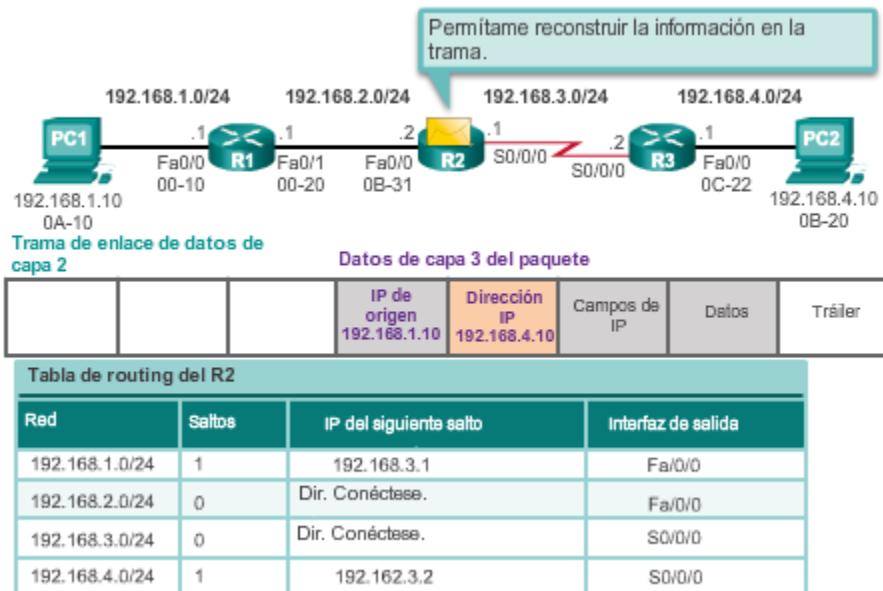
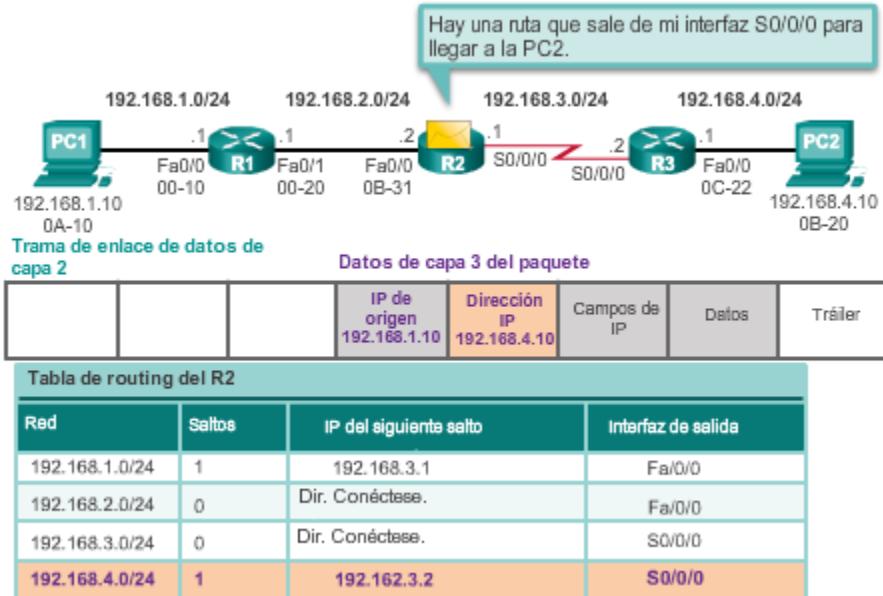
5. El paquete IPv4 ahora se encapsula en una nueva trama de enlace de datos y se envía por la interfaz de salida Serial 0/0/0.

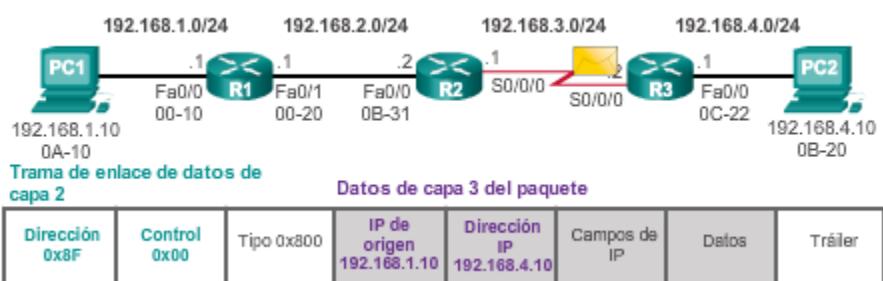
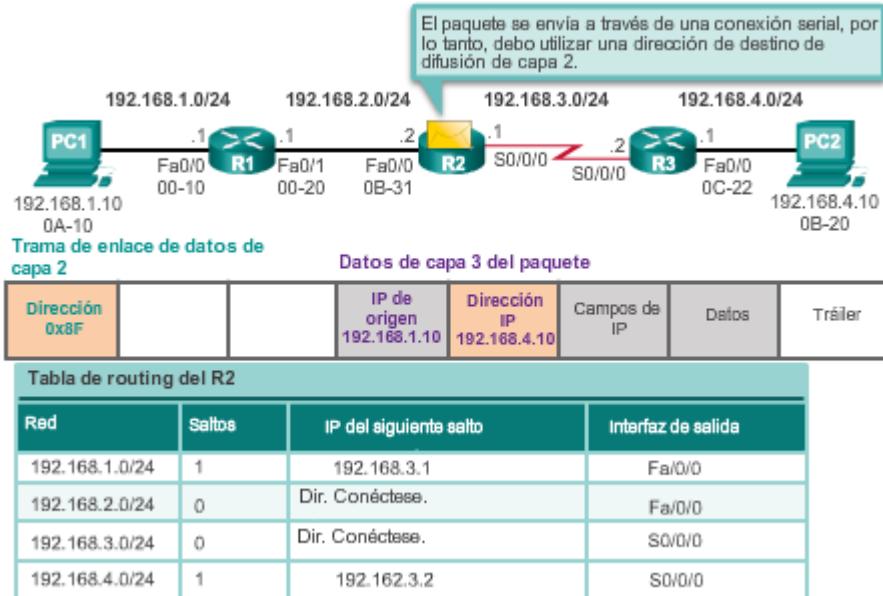
Cuando la interfaz es una conexión serial punto a punto (P2P), el router encapsula el paquete IPv4 en el formato de trama de enlace de datos correspondiente que utiliza la interfaz de salida (HDLC, PPP, etc.). Debido a que no hay direcciones MAC en las interfaces seriales, el R2 establece la dirección de destino de enlace de datos en el equivalente a una difusión.

En la animación de la ilustración, se muestra cómo el R2 reenvía el paquete al R3.

El R2 reenvía el paquete al R3







Los siguientes procesos ocurren cuando la trama llega al R3:

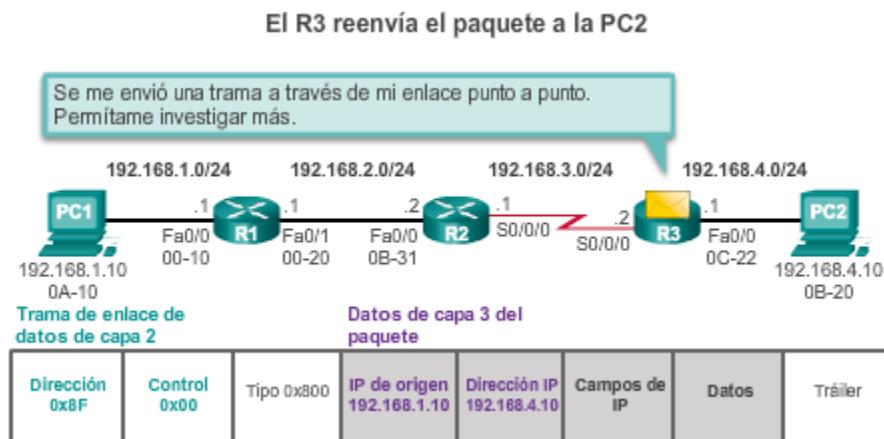
1. El R3 copia la trama PPP de enlace de datos en su búfer.

2. El R3 desencapsula la trama PPP de enlace de datos.
3. El R3 busca la dirección IPv4 de destino del paquete en la tabla de routing. La tabla de routing tiene una ruta a una red conectada directamente en el R3. Esto significa que el paquete puede enviarse directamente al dispositivo de destino y no es necesario enviarlo a otro router.

Dado que la interfaz de salida es una red Ethernet conectada directamente, el R3 debe resolver la dirección IPv4 de destino del paquete con una dirección MAC de destino:

1. El R3 busca la dirección IPv4 de destino del paquete en la caché del protocolo de resolución de direcciones (ARP). Si la entrada no aparece en la caché ARP, el R3 envía una solicitud de ARP por la interfaz FastEthernet 0/0. La PC2 envía a cambio una respuesta ARP con su dirección MAC. A continuación, el R3 actualiza su caché ARP con una entrada para 192.168.4.10 y la dirección MAC que se devolvió en la respuesta de ARP.
2. El paquete IPv4 se encapsula en una nueva trama de enlace de datos de Ethernet y se envía por la interfaz FastEthernet 0/0 del R3.
3. Cuando la PC2 recibe la trama, examina la dirección MAC de destino, que coincide con la dirección MAC de la interfaz receptora, la tarjeta de interfaz de red (NIC) Ethernet. Por lo tanto, la PC2 copia el resto de la trama en su búfer.
4. La PC2 distingue que el campo tipo de Ethernet es 0x800, lo que significa que la trama de Ethernet contiene un paquete IPv4 en la porción de datos de la trama.
5. La PC2 desencapsula la trama de Ethernet y envía el paquete IPv4 al proceso IPv4 de su sistema operativo.

En la animación de la ilustración, se muestra cómo el R3 reenvía el paquete a la PC2.



Por el tipo y la dirección IP de destino, puedo ver que este paquete debe reenviarse.



Hay una ruta que sale de mi interfaz Fa0/0 para llegar a la PC2.



Tabla de routing del R3

Red	Saltos	IP del siguiente salto	Interfaz de salida
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Conéctese.	S0/0/0
192.168.4.0/24	0	Dir. Conéctese.	Fa0/0

Permitame reconstruir la información en la trama.

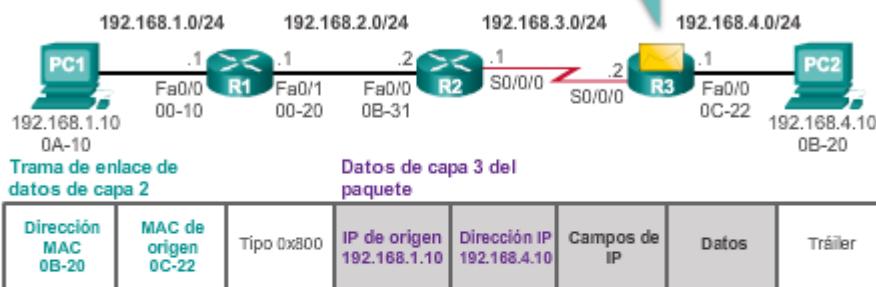
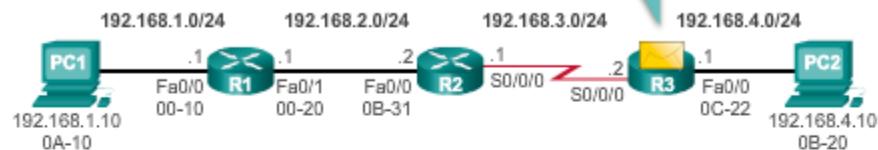


Tabla de routing del R3

Red	Saltos	IP del siguiente salto	Interfaz de salida
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Conéctese.	S0/0/0
192.168.4.0/24	0	Dir. Conéctese.	Fa0/0

Mi tabla ARP me indica que la PC2 utiliza la dirección MAC 0B-20.



Trama de enlace de datos de capa 2

Dirección MAC	MAC de origen	Tipo	IP de origen	Dirección IP	Campos de IP	Datos	Tráiler
0B-20	0C-22	0x800	192.168.1.10	192.168.4.10			

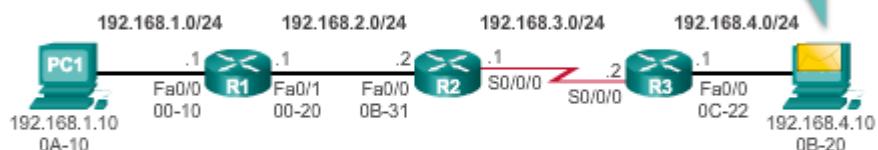
Caché ARP de R3

Dirección IP	Dirección MAC
192.168.4.10	0B-20

Tabla de routing del R3

Réte	Saltos	IP del siguiente salto	Interfaz de salida
192.168.1.0/24	2	192.168.3.1	S0/0/0
192.168.2.0/24	1	192.168.3.1	S0/0/0
192.168.3.0/24	0	Dir. Conéctese.	S0/0/0
192.168.4.0/24	0	Dir. Conéctese.	Fa0/0

Mire: se está enviando una trama a mi dirección MAC; permítame procesarla. Además, el paquete coincide con mi dirección IP, entonces DEBE ser mío.



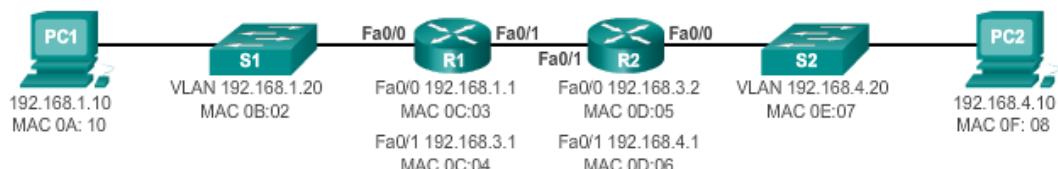
Trama de enlace de datos de capa 2

Dirección MAC	MAC de origen	Tipo	IP de origen	Dirección IP	Campos de IP	Datos	Tráiler
0B-20	0C-22	0x800	192.168.1.10	192.168.4.10			

Actividad

En esta actividad, se le proporciona una trama en blanco para que la arme según la situación. Determine las direcciones MAC de destino y de origen, así como las direcciones IP de origen y de destino, con las que se armaría la trama en forma correcta según lo especificado. Para introducir las respuestas, arrastre las direcciones MAC e IP a los campos correspondientes.

Situación 1: la PC1 envía datos a la PC2; en todos los dispositivos se completó el proceso ARP. En esta trama, indique el comienzo del tráfico de datos para el armado de la trama. No se utilizan todas las respuestas.



Trama de enlace de datos de capa 2

Paquete de datos de capa 3

MAC de destino	MAC de origen	Tipo	IP origen	IP destino	Campos de IP	Datos	Tráiler
0C:03	0A:10	0x800	192.168.1.10	192.168.4.10			

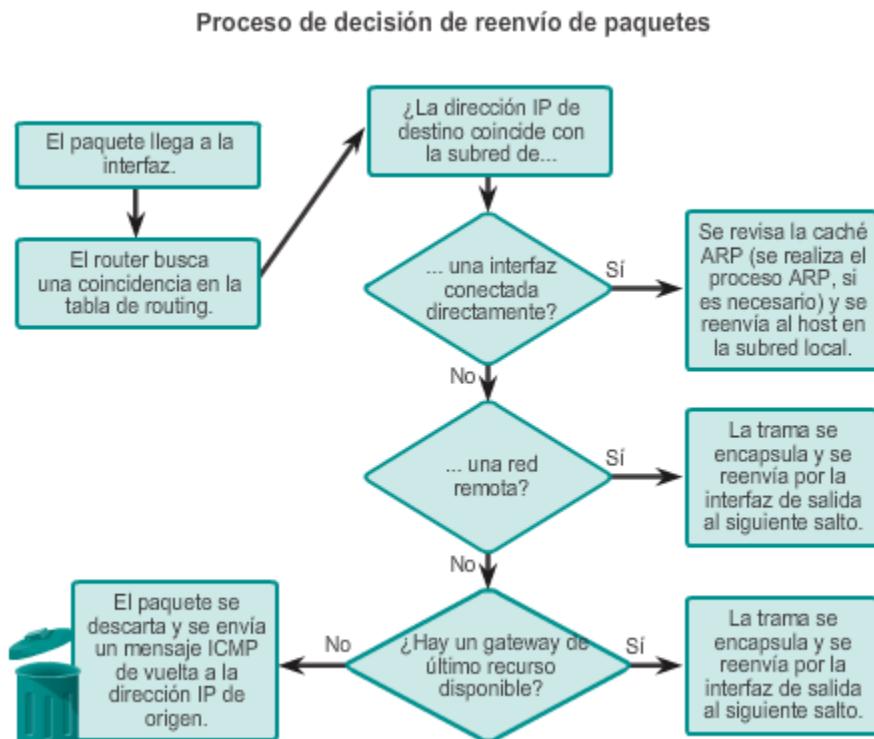
4.3.2 Determinación de ruta

Una de las funciones principales de los routers es determinar la mejor ruta para enviar paquetes. Para determinar la mejor ruta, el router busca en su tabla de routing una dirección de red que coincida con la dirección IP de destino del paquete.

La tabla de routing busca resultados en una de tres determinaciones de ruta:

- **Red conectada directamente:** si la dirección IP de destino del paquete pertenece a un dispositivo en una red que está conectada directamente a una de las interfaces del router, ese paquete se reenvía directamente al dispositivo de destino. Esto significa que la dirección IP de destino del paquete es una dirección host en la misma red que la interfaz del router.
- **Red remota:** si la dirección IP de destino del paquete pertenece a una red remota, el paquete se reenvía a otro router. Sólo se pueden alcanzar las redes remotas mediante el reenvío de paquetes hacia otra red.
- **Ninguna ruta determinada:** si la dirección IP de destino del paquete no pertenece a una red conectada ni remota, el router determina si se dispone de un gateway de último recurso. El gateway de último recurso se establece cuando se configura una ruta predeterminada en un router. Si hay una ruta predeterminada, el paquete se reenvía al gateway de último recurso. Si el router no tiene una ruta predeterminada, el paquete se descarta. Si se descarta el paquete, el router envía un mensaje de ICMP de destino inalcanzable a la dirección IP de origen del paquete.

En el diagrama de flujo lógico de la ilustración, se describe el proceso de decisión de reenvío de paquetes del router.



La determinación de la mejor ruta implica la evaluación de varias rutas hacia la misma red de destino y la selección de la ruta óptima o la más corta para llegar a esa red. Cuando existen varias rutas hacia la misma red, cada ruta utiliza una interfaz de salida diferente en el router para llegar a esa red.

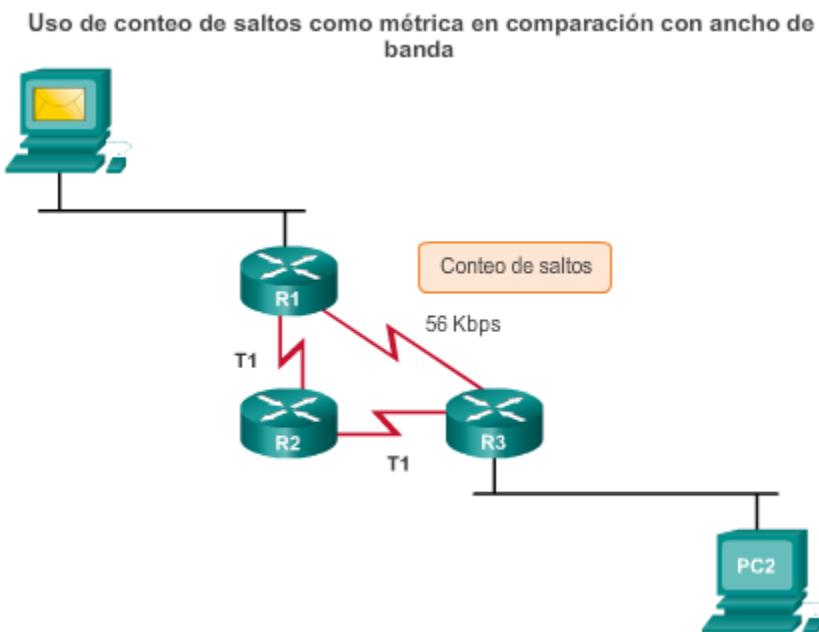
El mejor camino es elegido por un protocolo de enrutamiento en función del valor o la métrica que usa para determinar la distancia para llegar a esa red. Una métrica es un valor cuantitativo que se utiliza para medir la distancia que existe hasta una red determinada. El mejor camino a una red es la ruta con la métrica más baja.

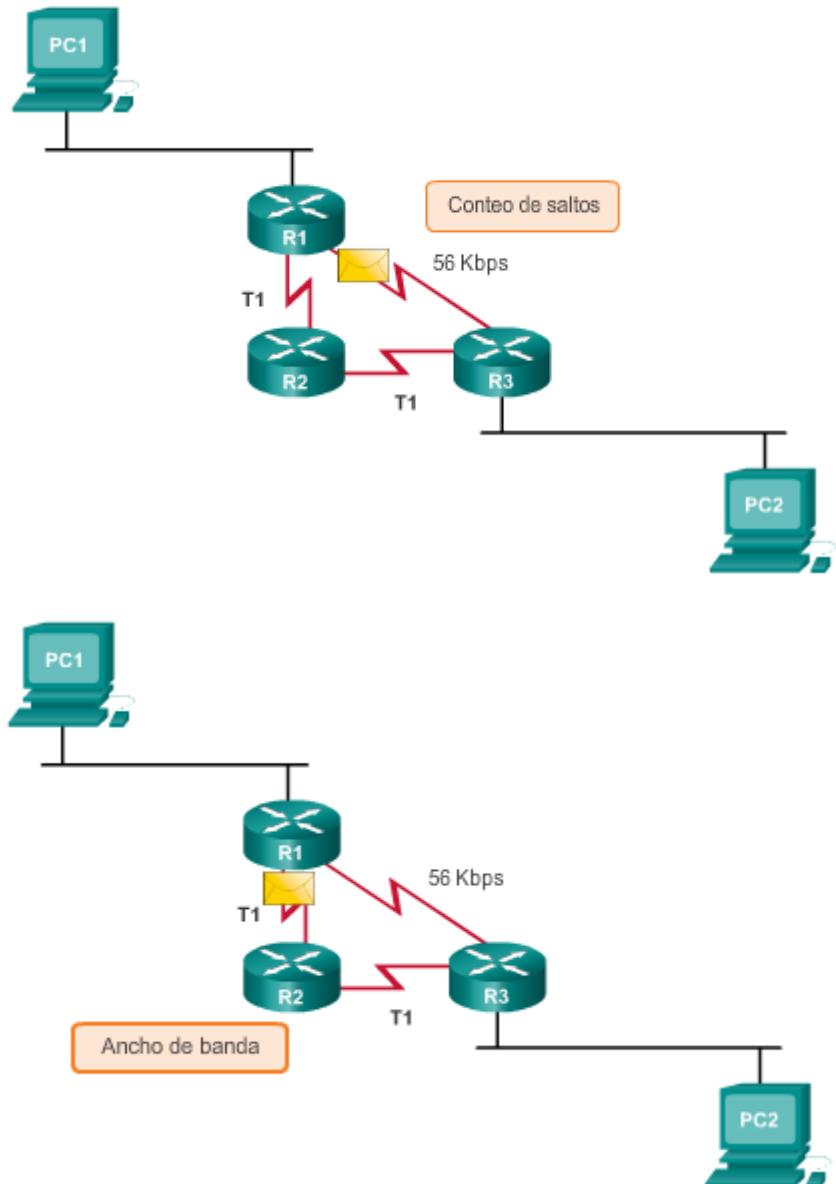
Los protocolos de enrutamiento dinámico generalmente usan sus propias reglas y métricas para construir y actualizar las tablas de enrutamiento. El algoritmo de enrutamiento genera un valor, o una métrica, para cada ruta a través de la red. Las métricas se pueden calcular sobre la base de una sola característica o de varias características de una ruta. Algunos protocolos de enrutamiento pueden basar la elección de la ruta en varias métricas, combinándolas en un único valor métrico.

A continuación, se indican algunos protocolos dinámicos y las métricas que utilizan:

- **Protocolo de información de routing (RIP):** conteo de saltos.
- **Protocolo OSPF (Open Shortest Path First):** el costo de Cisco según el ancho de banda acumulativo de origen a destino.
- **Protocolo de routing de gateway interior mejorado (EIGRP):** ancho de banda, retraso, carga, confiabilidad.

En la animación de la ilustración, se destaca cómo la ruta puede ser diferente según la métrica que se utiliza.





¿Qué sucede si una tabla de routing tiene dos o más rutas con métricas idénticas hacia la misma red de destino?

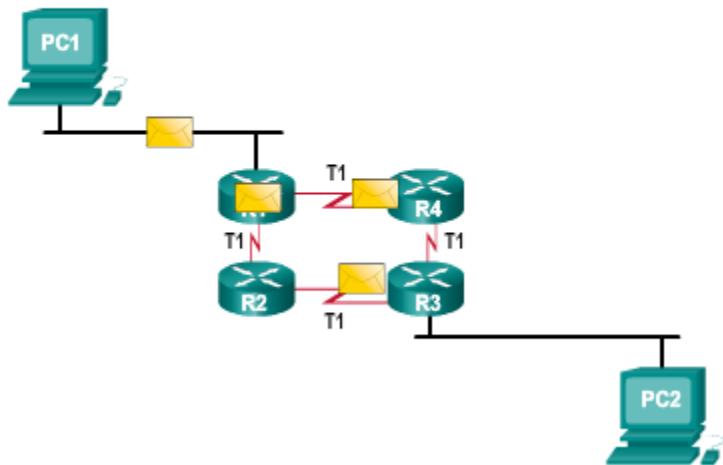
Cuando un router tiene dos o más rutas hacia un destino con métrica del mismo costo, el router reenvía los paquetes usando ambas rutas por igual. Esto se denomina “balanceo de carga de mismo costo”. La tabla de routing contiene la única red de destino pero tiene varias interfaces de salida, una para cada ruta de mismo costo. El router reenvía los paquetes utilizando las distintas interfaces de salida que se indican en la tabla de routing.

Si está configurado correctamente, el balanceo de carga puede aumentar la efectividad y el rendimiento de la red. El balanceo de carga de mismo costo puede configurarse para usar tanto protocolos de enrutamiento dinámico como rutas estáticas.

Nota: solo EIGRP admite el balanceo de carga con distinto costo.

En la animación de la ilustración, se proporciona un ejemplo de balanceo de carga de mismo costo.

Balanceo de carga de mismo costo



Es posible configurar un router con varios protocolos de routing y varias rutas estáticas. Si esto ocurre, la tabla de routing puede tener más de un origen de ruta para la misma red de destino. Por ejemplo, si se configura RIP y EIGRP en un router, ambos protocolos de routing pueden descubrir la misma red de destino. Sin embargo, cada protocolo de routing puede decidir tomar una ruta diferente para llegar al destino según las métricas de ese protocolo de routing. RIP elige una ruta según el conteo de saltos, mientras que EIGRP elige una ruta según la métrica compuesta. ¿Cómo sabe el router qué ruta debe utilizar?

El IOS de Cisco utiliza lo que se conoce como “distancia administrativa” (AD) para determinar la ruta que se debe instalar en la tabla de routing de IP. La AD representa la “confiabilidad” de la ruta: cuanto menor sea la AD, más confiable será el origen de la ruta. Por ejemplo, la AD de una ruta estática es 1, mientras que la AD de una ruta descubierta por EIGRP es 90. El router elige la ruta con la AD más baja entre dos rutas diferentes al mismo destino. Cuando un router puede elegir entre una ruta estática y una ruta EIGRP, la ruta estática tiene prioridad. Asimismo, una ruta conectada directamente con una AD de 0 tiene prioridad sobre una ruta estática con una AD de 1.

En la ilustración, se muestran diferentes protocolos de routing y sus AD asociadas.

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

Situación 1 de reenvío de paquetes**Paso siguiente**

Su router recibió un paquete destinado a una dirección IP en otra red. La dirección IP de destino no está en una red local y no hay coincidencias para ella en su tabla de routing. No hay un gateway de último recurso disponible.

✓ Descartar el paquete y enviar un mensaje ICMP de vuelta a la dirección IP de origen.

Situación 2 de reenvío de paquetes**Paso siguiente**

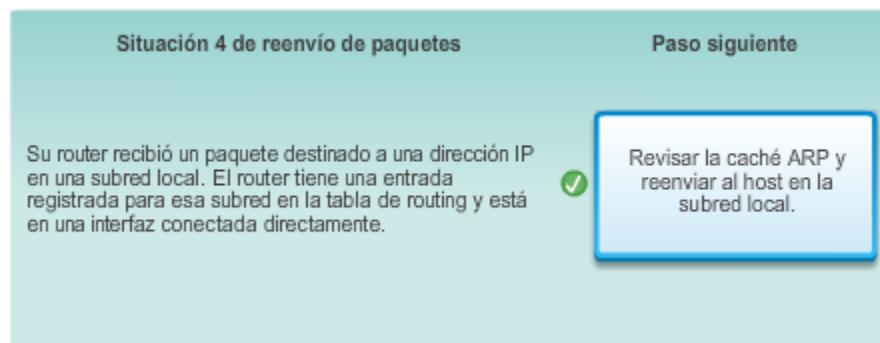
Su router recibió un paquete destinado a una dirección IP en una red remota. El router tiene una entrada para la red remota en la tabla de routing.

✓ Encapsular la trama y reenviarla por la interfaz de salida al siguiente salto.

Situación 3 de reenvío de paquetes**Paso siguiente**

Su router recibió un paquete destinado a una dirección IP en otra red. La dirección IP de destino no está en una red local y no hay coincidencias para ella en la tabla de routing, pero hay un gateway de último recurso.

✓ Encapsular la trama y reenviarla por la interfaz de salida al siguiente salto.



4.4 Funcionamiento del router

4.4.1 Análisis de la tabla de Routing

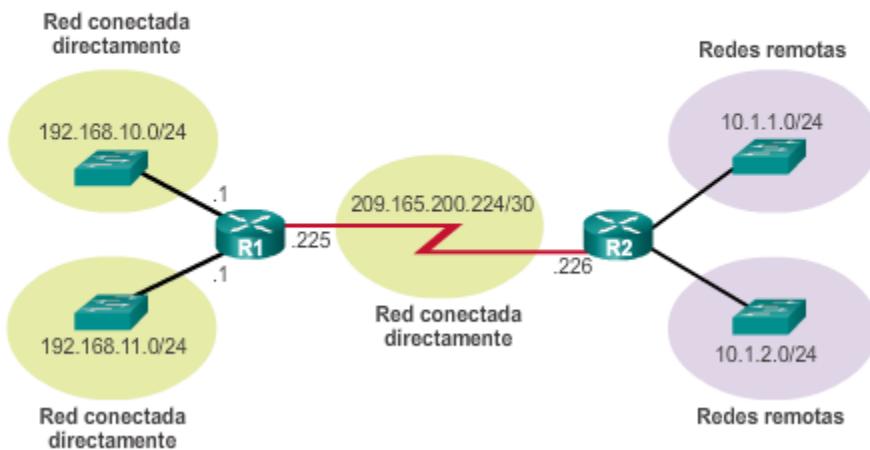
La tabla de enrutamiento de un router almacena información sobre lo siguiente:

- **Rutas conectadas directamente:** estas rutas provienen de las interfaces activas del router. Los routers agregan una ruta conectada directamente cuando se configura una interfaz con una dirección IP y se activa.
- **Rutas remotas:** estas son redes remotas conectadas a otros routers. Las rutas que van a estas redes se pueden configurar de forma estática o dinámica mediante protocolos de routing dinámico.

Concretamente, una tabla de routing es un archivo de datos que se encuentra en la RAM y se utiliza para almacenar información de rutas sobre redes remotas y conectadas directamente. La tabla de routing contiene asociaciones de red o de siguiente salto. Estas asociaciones le indican al router que un destino en particular se puede alcanzar de forma óptima si se envía el paquete hacia un router en particular que representa el siguiente salto en el camino hacia el destino final. La asociación del siguiente salto también puede ser la interfaz de salida hacia el siguiente destino.

En la ilustración, se identifican las redes conectadas directamente y las redes remotas del router R1.

Rutas de redes conectadas directamente y de redes remotas



En los routers Cisco IOS, se puede utilizar el comando **show ip route** para mostrar la tabla de routing IPv4 de un router. Los routers proporcionan información adicional de la ruta, incluso la forma en que se descubrió la ruta, cuánto tiempo estuvo la ruta en la tabla de routing y qué interfaz específica se debe utilizar para llegar a un destino predefinido.

Las entradas en la tabla de routing se pueden agregar como lo siguiente:

- **Interfaces de ruta local:** se agregan cuando la interfaz está configurada y activa. Esta entrada solo se muestra en la versión IOS 15 o más reciente para las rutas IPv4, y en todas las versiones de IOS para las rutas IPv6.
- **Interfaces conectadas directamente:** se agregan a la tabla de routing cuando la interfaz está configurada y activa.
- **Rutas estáticas:** se agregan cuando una ruta se configura manualmente y la interfaz de salida está activa.
- **Protocolo de routing dinámico:** se agrega cuando se implementan protocolos de routing que descubren la red de manera dinámica, como EIGRP u OSPF, y cuando se identifican las redes.

Los orígenes de las entradas de la tabla de routing se identifican con un código. El código identifica la forma en que se descubrió la ruta. Por ejemplo, los códigos frecuentes incluyen lo siguiente:

- **L:** identifica la dirección asignada a la interfaz de un router. Esto permite que el router determine de forma eficaz si recibe un paquete para la interfaz o para reenviar.
- **C:** identifica una red conectada directamente.
- **S:** identifica una ruta estática creada para llegar a una red específica.
- **D:** identifica una red que se descubre de forma dinámica de otro router con EIGRP.
- **O:** indica una red que se descubre de forma dinámica de otro router con el protocolo de routing OSPF.

Nota: otros códigos exceden el ámbito de este capítulo.

En la ilustración, se muestra la tabla de enrutamiento del R1 en una red simple.



```

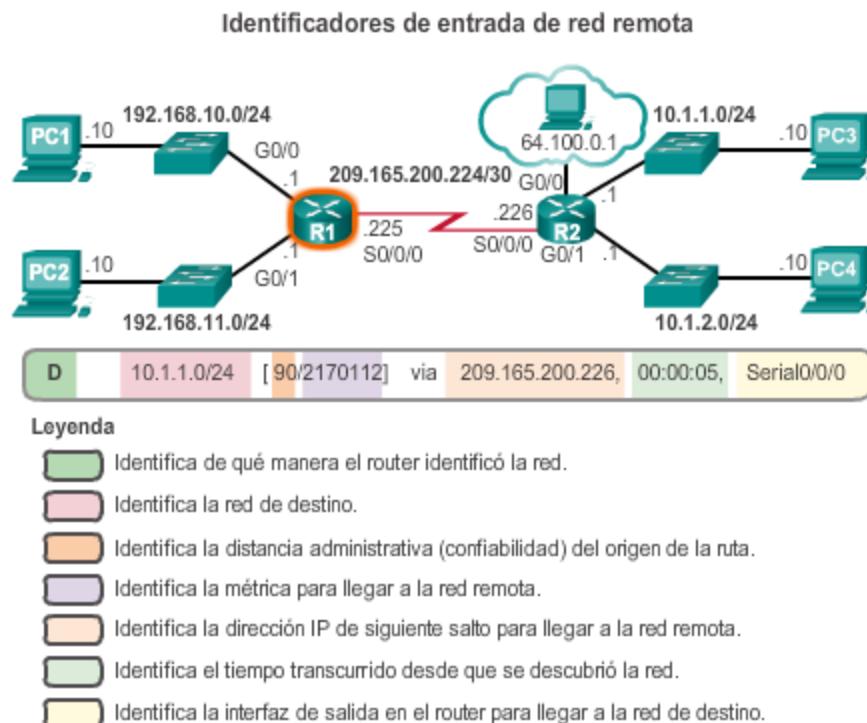
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - EGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
      IS-IS inter areas
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D        10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
          Serial0/0/0
D        10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
          Serial0/0/0
      192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C          192.168.10.0/24 is directly connected, GigabitEthernet0/0
L          192.168.10.1/32 is directly connected, GigabitEthernet0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C          192.168.11.0/24 is directly connected, GigabitEthernet0/1
L          192.168.11.1/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 3 masks
C          209.165.200.224/30 is directly connected, Serial0/0/0
L          209.165.200.225/32 is directly connected, Serial0/0/0
  
```

Como administrador de red, es imprescindible saber cómo interpretar el contenido de una tabla de routing IPv4 e IPv6. En la ilustración, se muestra una entrada de la tabla de routing IPv4 en el R1 para la ruta a la red remota 10.1.1.0.

La entrada indica la siguiente información:

- Origen de la ruta:** identifica el modo en que se descubrió la ruta.
- Red de destino:** identifica la dirección de la red remota.
- Distancia administrativa:** identifica la confiabilidad del origen de la ruta. Los valores más bajos indican el origen de ruta preferido.
- Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.

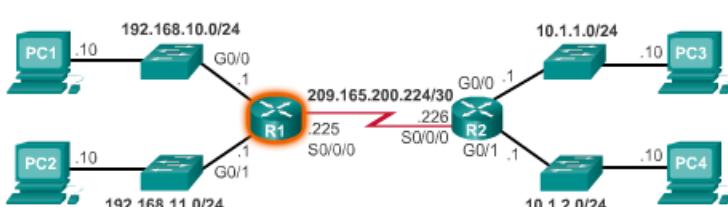
- Siguiente salto:** identifica la dirección IPv4 del router siguiente al que se debe reenviar el paquete.
- Marca de hora de la ruta:** identifica el tiempo que pasó desde que se descubrió la ruta.
- Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.



Actividad

Con la topología que se muestra, cree una entrada en la tabla de routing para el R1 sobre la base de la situación que se presenta a continuación. Para introducir las respuestas, arrástrelas a los campos correspondientes.

Situación: se envían datos de red de la PC1 al host 10.1.1.10. No hay rutas estáticas ni predeterminadas configuradas en el R1 o el R2. El R1 y el R2 utilizan EIGRP como protocolo de routing.



Entrada de la tabla de routing del R1						
✓	✓	✓	✓	✓	✓	✓
D	10.1.1.0/24	90/3072	via	209.165.200.226	00:00:33	S0/0/0

4.4.2 Rutas conectadas directamente

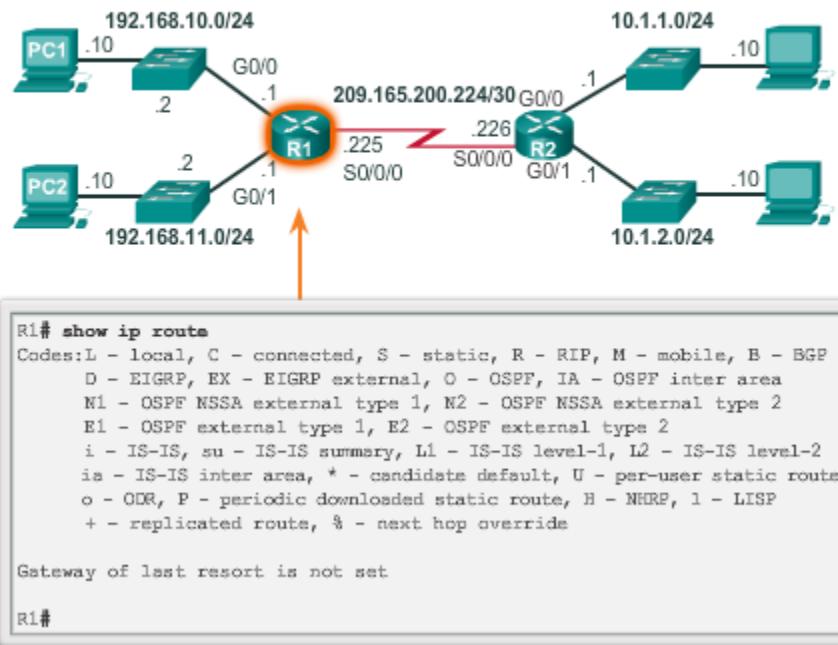
Un router implementado recientemente, sin interfaces configuradas, tiene una tabla de routing vacía, como se muestra en la ilustración.

Antes de que el estado de la interfaz se considere up/up y se agregue a la tabla de routing IPv4, la interfaz debe cumplir con los siguientes requisitos:

- Se le debe asignar una dirección IPv4 o IPv6 válida.
- Se debe activar mediante el comando **no shutdown**.
- Debe recibir una señal portadora de otro dispositivo (router, switch, host, etc.).

Una vez que la interfaz está activa, la red de esa interfaz se incorpora a la tabla de routing como red conectada directamente.

Tabla de routing vacía



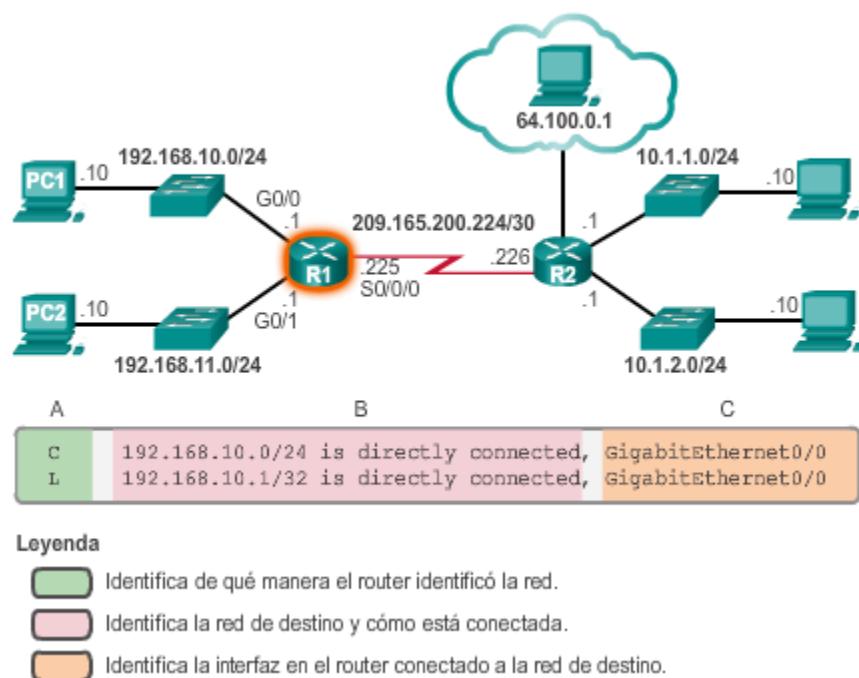
Una interfaz activa, correctamente configurada y conectada directamente, genera dos entradas en la tabla de routing. En la ilustración, se muestran las entradas de la tabla de routing IPv4 en el R1 para la red conectada directamente 192.168.10.0.

La entrada de la tabla de routing para las interfaces conectadas directamente es más simple que las entradas para las redes remotas. Las entradas contienen la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. El código "C" identifica una red conectada directamente. El código "L" identifica la dirección IPv4 asignada a la interfaz del router.
- **Red de destino:** la dirección de la red remota.
- **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

Nota: antes de IOS 15, no se mostraban las entradas de la tabla de routing de ruta local (L) en la tabla de routing IPv4. Las entradas de ruta local (L) siempre formaron parte de la tabla de routing IPv6.

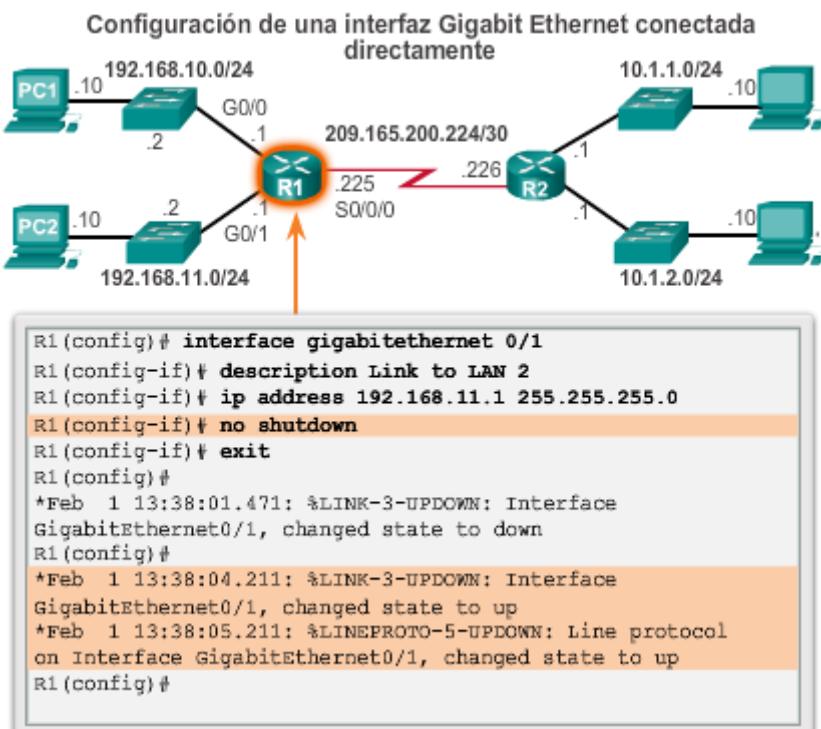
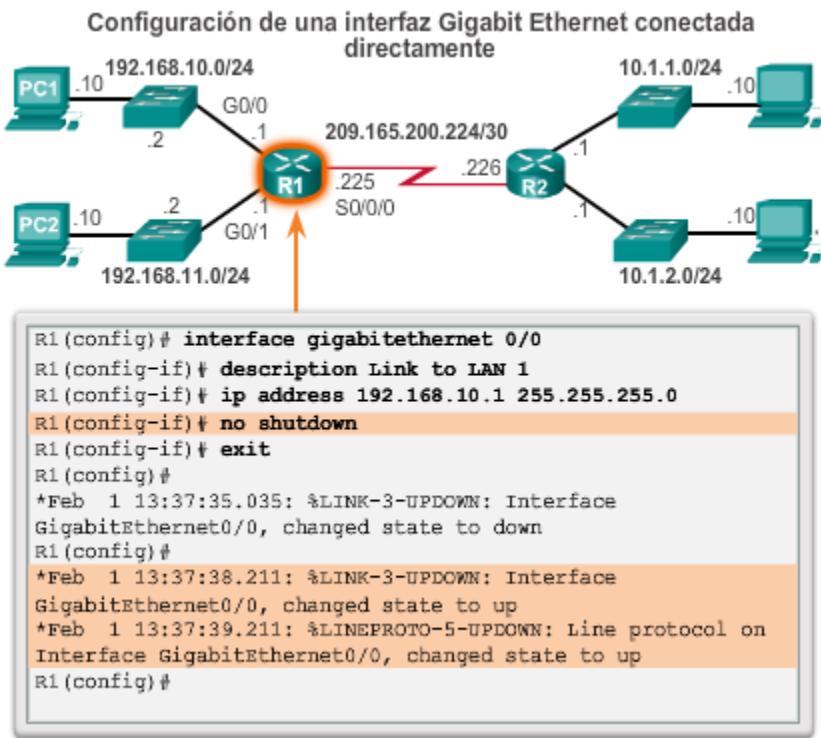
Identificadores de entrada de red conectada directamente

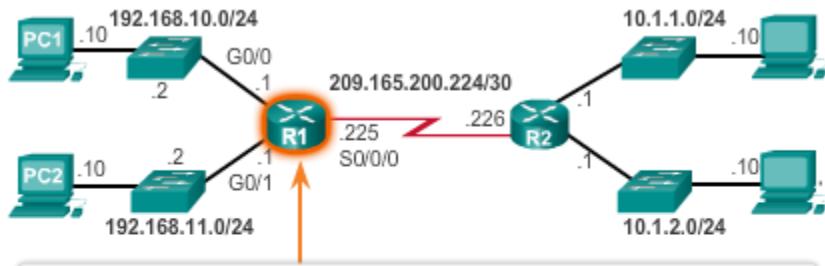


En los ejemplos de las figuras 1 a 3, se muestran los pasos para configurar y activar las interfaces conectadas al R1. Observe los mensajes informativos de capa 1 y 2 que se generan a medida que se activa cada interfaz.

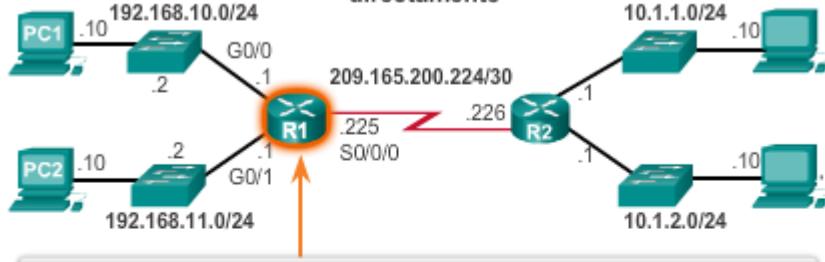
A medida que se agregan interfaces, la tabla de routing agrega automáticamente las entradas conectadas ("C") y locales ("L"). En la figura 4, se proporciona un ejemplo de la tabla de routing con las interfaces del R1 conectadas directamente configuradas y activadas.

Utilice el verificador de sintaxis de la figura 5 para configurar y activar las interfaces conectadas al R2.



Configuración de una interfaz serial conectada directamente

```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Feb 1 13:38:22.723: %LINK-3-UPDOWN: Interface Serial0/0/0,
changed state to up
*Feb 1 13:38:23.723: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/0, changed state to up
R1(config)# exit
```

Verificación de las entradas de la tabla de routing conectada directamente

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

    192.168.10.0/24 is variably subnetted, 2 subnets, 2
    masks
    C      192.168.10.0/24 is directly connected,
    GigabitEthernet0/0
    L      192.168.10.1/32 is directly connected,
    GigabitEthernet0/0
        192.168.11.0/24 is variably subnetted, 2 subnets, 2
    masks
    C      192.168.11.0/24 is directly connected,
    GigabitEthernet0/1
    L      192.168.11.1/32 is directly connected,
    GigabitEthernet0/1
```

En el ejemplo de la figura 1, se muestran los pasos de configuración de las interfaces del R1 conectadas directamente con las direcciones IPv6 indicadas. Observe los mensajes informativos de capa 1 y capa 2 que se generan a medida que se configura y se activa cada interfaz.

Como se muestra en la figura 2, el comando **show ipv6 route** se utiliza para verificar si se instalaron las redes IPv6 y las direcciones específicas de interfaz IPv6 en la tabla de routing IPv6.

Como en IPv4, una “C” junto a una ruta indica que se trata de una red conectada directamente. Una “L” indica la ruta local. En una red IPv6, la ruta local tiene un prefijo /128. La tabla de routing utiliza las rutas locales para procesar eficazmente los paquetes cuya dirección de destino es la interfaz del router.

Observe que también se instaló una ruta a la red FF00::/8. Esta ruta se requiere para el routing de multidifusión.

En la figura 3, se muestra cómo el comando **show ipv6 route** se puede combinar con un destino de red específico para mostrar los detalles de cómo el router descubrió dicha ruta.

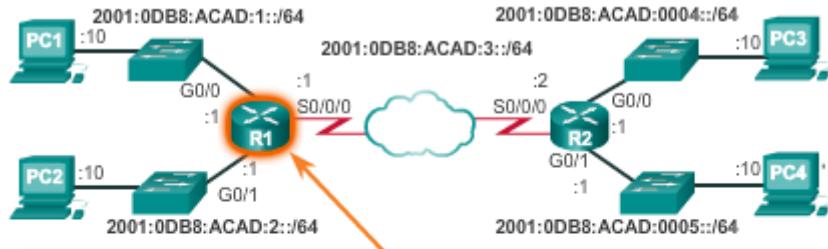
En la figura 4, se muestra cómo se puede verificar la conectividad al R2 mediante el comando **ping**.

En la figura 5, observe qué sucede cuando la interfaz LAN G0/0 del R2 es el objetivo del comando **ping**. Los pings no tienen éxito. Esto se debe a que el R1 no tiene ninguna entrada en la tabla de routing para llegar a la red 2001:DB8:ACAD:4::/64.

El R1 requiere información adicional para llegar a una red remota. Se pueden agregar entradas de ruta de red remota a la tabla de routing mediante los siguientes métodos:

- Enrutamiento estático
- Protocolos de enrutamiento dinámico

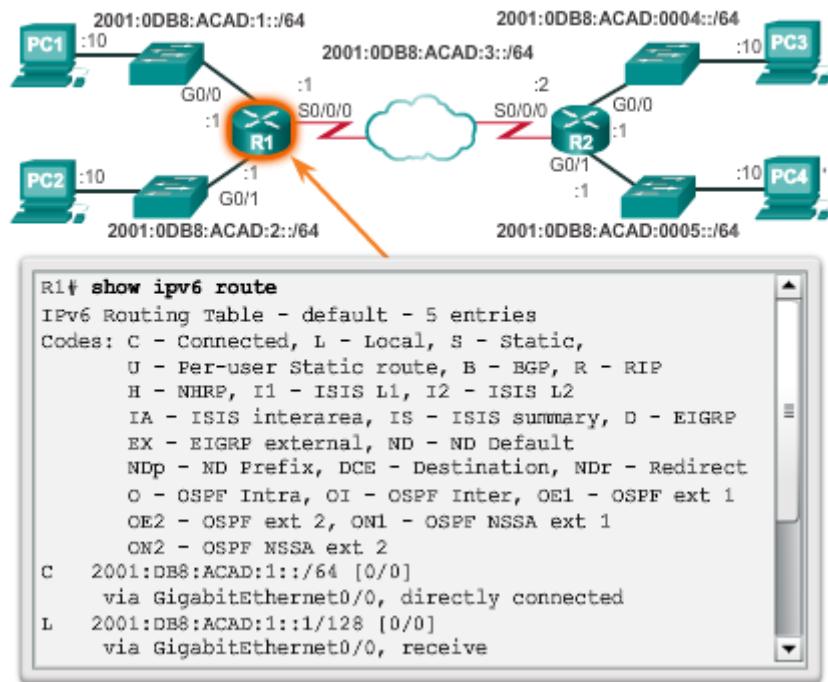
Configuración de las interfaces IPv6 de R1 conectadas directamente



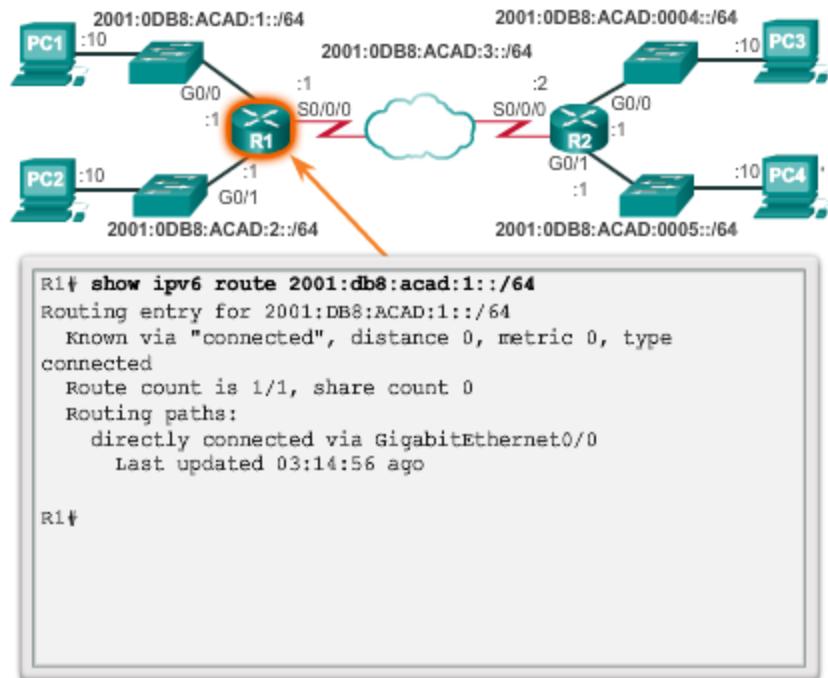
```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# description Link to LAN 1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Feb 3 21:38:37.279: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to down
*Feb 3 21:38:40.967: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
*Feb 3 21:38:41.967: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0, changed state to up
R1(config)#
R1(config)# interface gigabitethernet 0/1
R1(config-if)# description Link to LAN 2
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
*Feb 3 21:39:21.867: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to down
*Feb 3 21:39:24.967: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Feb 3 21:39:25.967: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
R1(config)#
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown
R1(config-if)#
*Feb 3 21:39:43.307: %LINK-3-UPDOWN: Interface
Serial0/0/0, changed state to down
R1(config)#

```

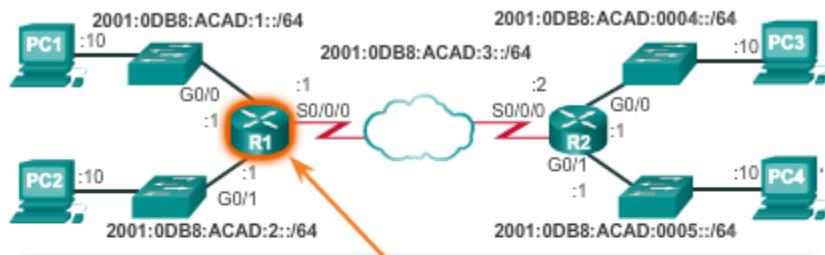
Visualización de la tabla de rutas IPv6



Visualización de una entrada de ruta IPv6

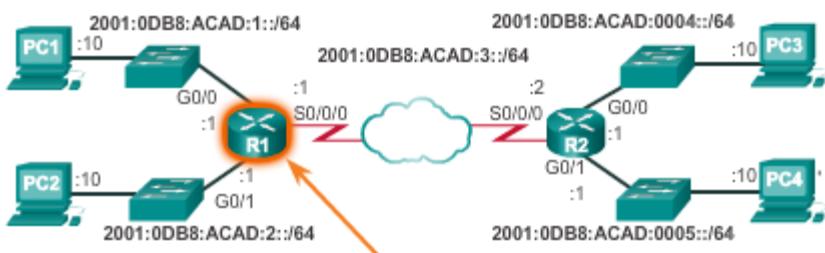


Prueba de conectividad para probar la interfaz S0/0/0 de R2



```
R1# ping 2001:db8:acad:3::2
Type escape sequence to abort.
sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:3::2,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
12/13/16 ms
R1#
```

Prueba de conectividad a la interfaz G0/0 de R2



```
R1# ping 2001:db8:acad:4::1
Type escape sequence to abort.
sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::1,
timeout is 2 seconds:
% No valid route for destination
Success rate is 0 percent (0/1)
R1#
```

4.4.3 Rutas descubiertas est谩ticamente

Despu茅s de configurar las interfaces conectadas directamente y de agregarlas a la tabla de routing, se puede implementar el routing est谩tico o din谩mico.

Las rutas estáticas se configuran de forma manual. Estas definen una ruta explícita entre dos dispositivos de red. A diferencia de los protocolos de routing dinámico, las rutas estáticas no se actualizan automáticamente y se deben reconfigurar de forma manual si se modifica la topología de la red. Los beneficios de utilizar rutas estáticas incluyen la mejora de la seguridad y la eficacia de los recursos. Las rutas estáticas consumen menos ancho de banda que los protocolos de routing dinámico, y no se usa ningún ciclo de CPU para calcular y comunicar las rutas. La principal desventaja de usar rutas estáticas es que no se vuelven a configurar de manera automática si se modifica la topología de la red.

Existen dos tipos de rutas estáticas comunes en la tabla de routing:

- Ruta estática a una red específica
- Ruta estática predeterminada

Las rutas estáticas se pueden configurar para llegar a una red remota específica. Las rutas estáticas IPv4 se configuran con el comando de configuración global **ip route** máscara de red {ip-siguiente-salto | interfaz-salida}. Las rutas estáticas se identifican en la tabla de routing con el código "S".

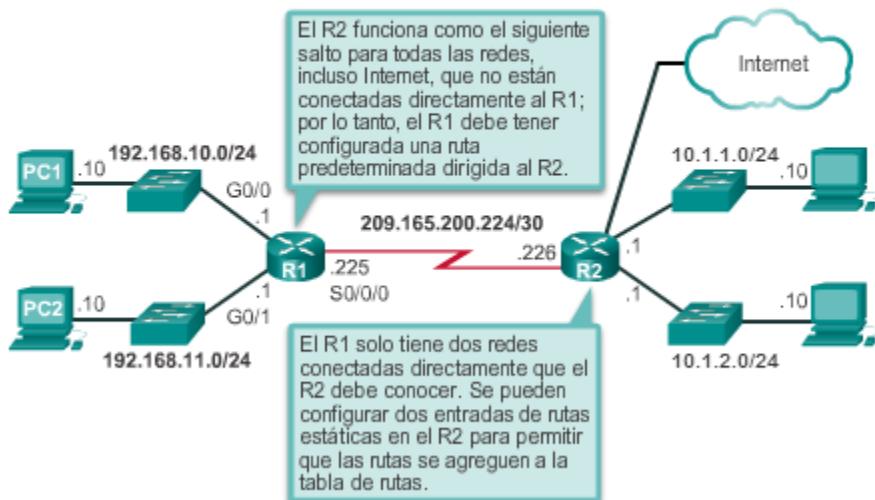
Las rutas estáticas predeterminadas son similares a un gateway predeterminado en un host. Las rutas estáticas predeterminadas especifican el punto de salida que se debe utilizar cuando la tabla de routing no contiene una ruta para la red de destino.

Las rutas estáticas predeterminadas son útiles cuando un router tiene solo un punto de salida a otro router, por ejemplo, cuando el router se conecta a un router central o a un proveedor de servicios.

Para configurar una ruta estática predeterminada IPv4, utilice el comando de configuración global **ip route 0.0.0.0 0.0.0.0 {interfaz-salida | ip-siguiente-salto}**.

En la ilustración, se proporciona una situación simple sobre cómo se pueden aplicar las rutas predeterminadas y estáticas.

Situación de rutas estáticas y predeterminadas



En la figura 1, se muestra la configuración de una ruta estática predeterminada IPv4 en el R1 a la interfaz Serial 0/0/0. Observe que la configuración de la ruta generó una entrada “S*” en la tabla de routing. La “S” significa que el origen de la ruta es una ruta estática, mientras que el asterisco (*) indica que esta ruta es una posible candidata para ser la ruta predeterminada. De hecho, se eligió como ruta predeterminada, como se observa en la línea que dice “Gateway of Last Resort is 0.0.0.0 to network 0.0.0.0.” (El gateway de último recurso es 0.0.0.0 para la red 0.0.0.0).

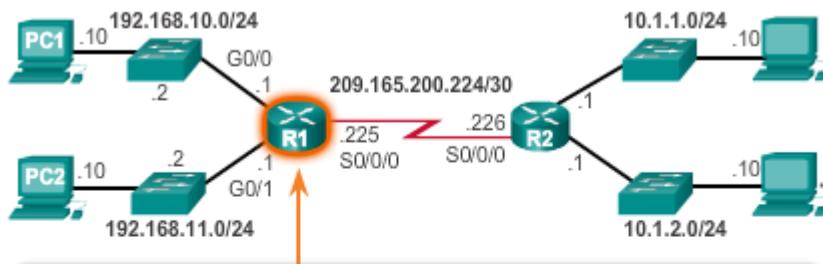
En la figura 2, se muestra la configuración de dos rutas estáticas del R2 para llegar a las dos LAN en el R1. La ruta a 192.168.10.0/24 se configuró con la interfaz de salida, mientras que la ruta a 192.168.11.0/24 se configuró con la dirección IPv4 de siguiente salto. Si bien ambas son aceptables, existen algunas diferencias con respecto a la forma en que funcionan. Por ejemplo, observe que se ven diferentes en la tabla de routing. Observe también que, debido a que estas rutas estáticas estaban dirigidas a redes específicas, el resultado indica que no se estableció el gateway de último recurso.

Nota: las rutas estáticas y las estáticas predeterminadas se explican en detalle en el capítulo siguiente.

Utilice el verificador de sintaxis de la figura 3 para configurar una ruta estática predeterminada en el router R1 que vaya al R2.

Utilice el verificador de sintaxis de la figura 4 para configurar rutas estáticas en el router R2 para llegar a las LAN del R1.

Introducción y verificación de una ruta estática predeterminada

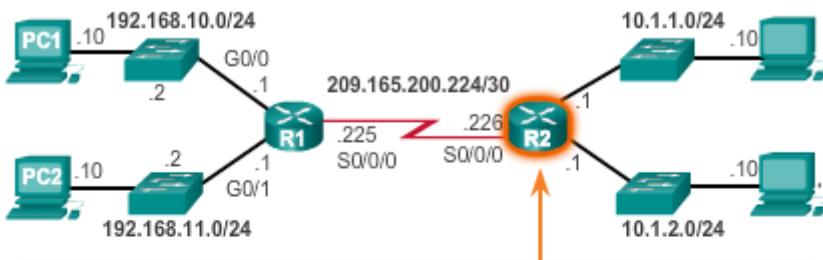


```
R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0
R1(config)# exit
R1#
*Feb 1 10:19:34.483: %SYS-5-CONFIG_I: Configured from console
by console

R1# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

S* 0.0.0.0/0 is directly connected, Serial0/0/0
    192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.10.0/24 is directly connected, GigabitEthernet0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0
    192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.11.0/24 is directly connected, GigabitEthernet0/1
L    192.168.11.1/32 is directly connected, GigabitEthernet0/1
...
```

Introducción y verificación de una ruta estática



```
R2(config)# ip route 192.168.10.0 255.255.255.0 s0/0/0
R2(config)# ip route 192.168.11.0 255.255.255.0 209.165.200.225
R2(config)# exit
R2#
R2# show ip route | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 4 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
S      192.168.10.0/24 is directly connected, Serial0/0/0
S      192.168.11.0/24 [1/0] via 209.165.200.225
    209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C      209.165.200.224/30 is directly connected, Serial0/0/0
...
```

Como en IPv4, IPv6 admite rutas estáticas y estáticas predeterminadas. Estas se usan y se configuran como las rutas estáticas IPv4.

Para configurar una ruta estática predeterminada IPv6, utilice el comando de configuración global **ipv6 route ::/0{dirección-ipv6 | tipo-interfaz número-interfaz}**.

En la figura 1, se muestra la configuración de una ruta estática predeterminada en el R1 a la interfaz Serial 0/0/0.

Observe que, en el resultado que se muestra en la figura 2, la configuración de la ruta estática predeterminada generó una entrada “S” en la tabla de routing. La “S” significa que el origen de la ruta es una ruta estática. A diferencia de las rutas estáticas IPv4, no figura ningún asterisco (*) ni se identifica ningún gateway de último recurso de forma explícita.

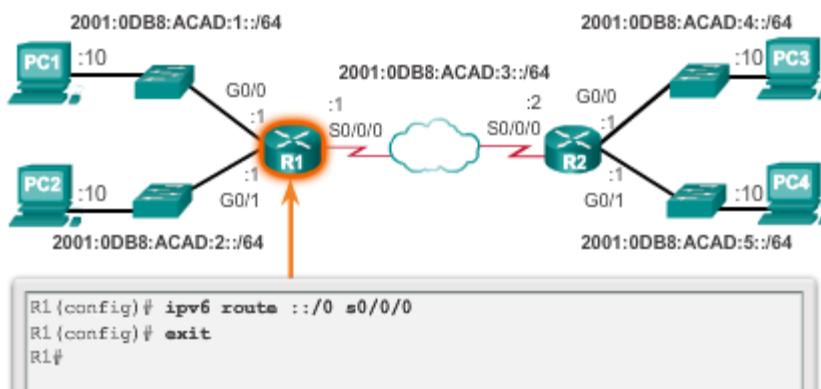
Como en IPv4, las rutas estáticas son rutas configuradas explícitamente para llegar a una red remota específica. Las rutas estáticas IPv6 se configuran con el comando de configuración global **ipv6 route prefijo-ipv6/longitud-prefijo{dirección-ipv6|tipo-interfaz número-interfaz}**.

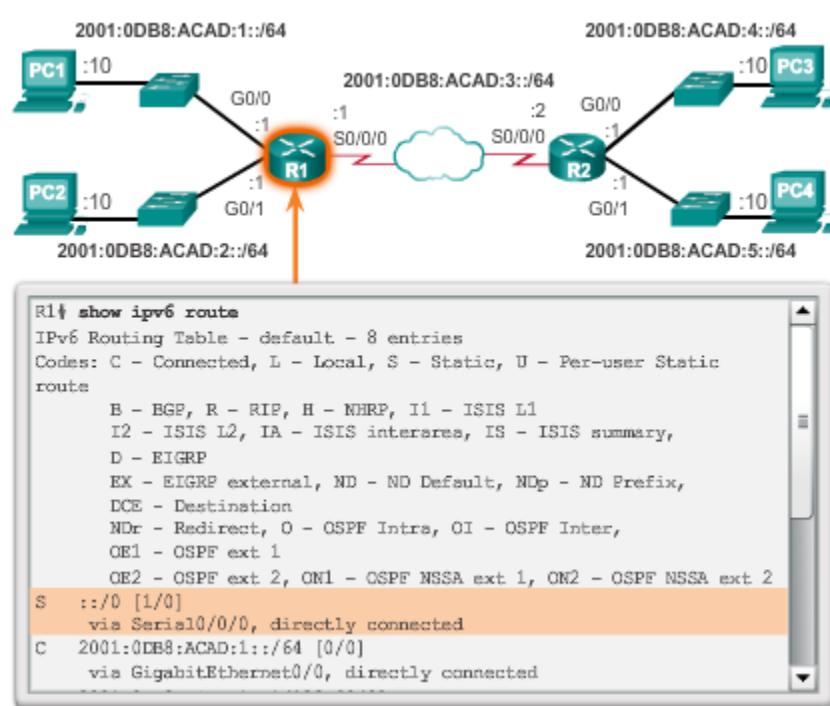
En el ejemplo de la figura 3, se muestra la configuración de dos rutas estáticas del R2 para llegar a las dos LAN en el R1. La ruta a la LAN 2001:0DB8:ACAD:2::/64 se configuró con una interfaz de salida, mientras que la ruta a la LAN 2001:0DB8:ACAD:1::/64 se configuró con la dirección IPv6 de siguiente salto. La dirección IPv6 de siguiente salto puede ser una dirección de unidifusión global o link-local de IPv6.

En la figura 4, se muestra la tabla de routing con las nuevas rutas estáticas instaladas.

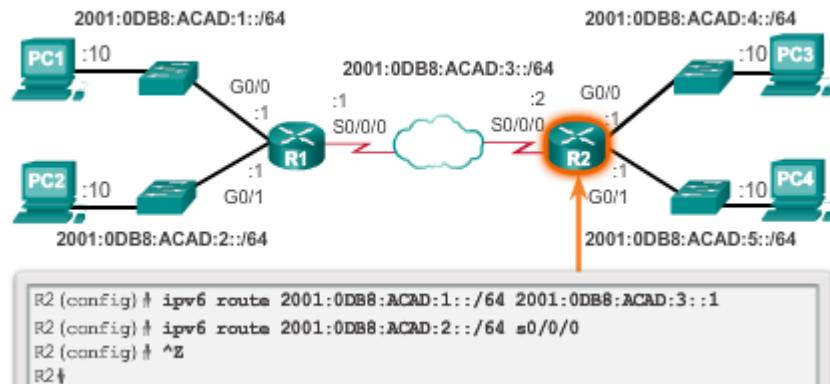
En la figura 5, se confirma la conectividad de red remota del R1 a la LAN 2001:0DB8:ACAD:4::/64 en el R2.

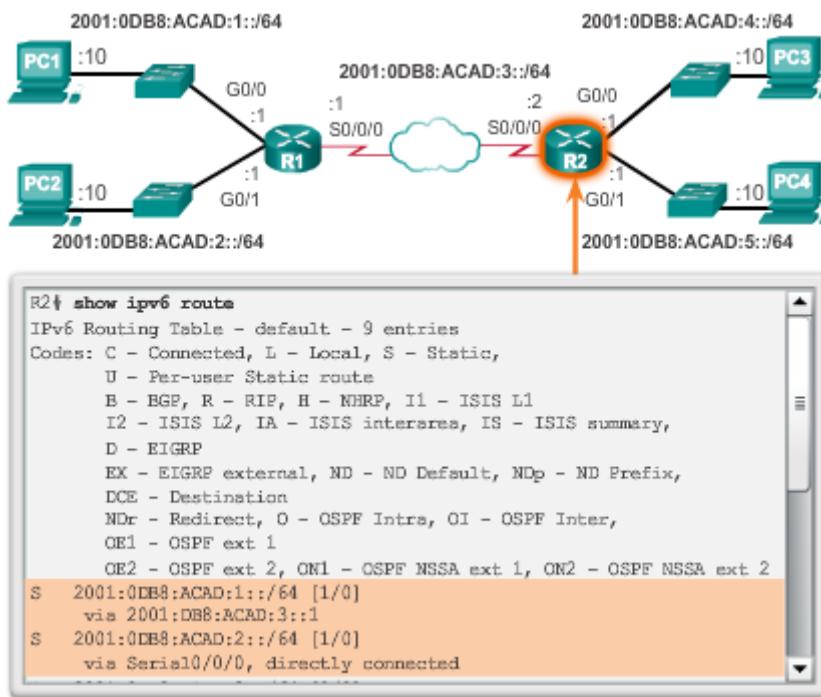
Introducción y verificación de una ruta estática predeterminada IPv6



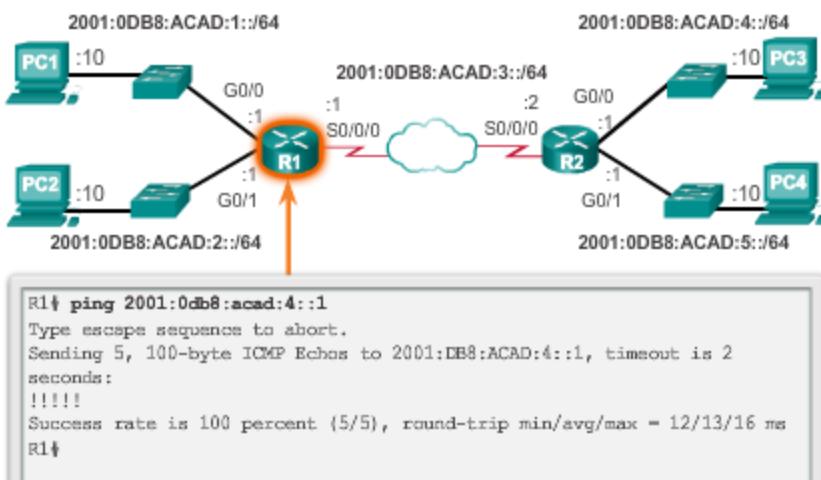


Introducción y verificación de rutas estáticas IPv6





Verificación de conectividad de red remota



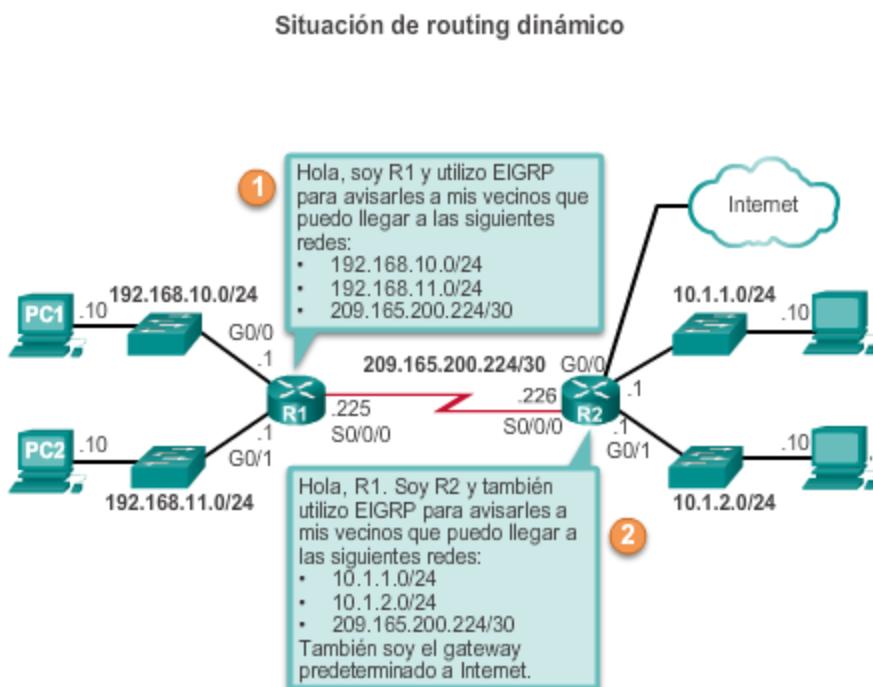
4.4.4 Protocolos de enrutamiento dinámico

Los routers usan protocolos de enrutamiento dinámico para compartir información sobre el estado y la posibilidad de conexión de redes remotas. Los protocolos de routing dinámico realizan diversas actividades, como la detección de redes y el mantenimiento de las tablas de routing.

El descubrimiento de redes es la capacidad de un protocolo de routing de compartir información sobre las redes que conoce con otros routers que también están usando el mismo protocolo de routing. En lugar de depender de las rutas estáticas configuradas manualmente hacia redes remotas en cada router, los protocolos de routing dinámico permiten que los routers descubran estas redes de forma automática a través de otros routers. Estas redes y la mejor ruta hacia cada una se agregan a la tabla de routing del router y se identifican como redes descubiertas por un protocolo de routing dinámico específico.

Durante la detección de redes, los routers intercambian rutas y actualizan sus tablas de routing. Los routers convergen una vez que finalizan el intercambio y actualizan sus tablas de routing. Luego, los routers conservan las redes en sus tablas de routing.

En la ilustración, se proporciona una situación simple sobre cómo dos routers vecinos intercambiarían inicialmente la información de routing. En este mensaje simplificado, el R1 de intercambio se presenta y detalla las redes que puede alcanzar. El R2 responde y proporciona sus redes al R1.



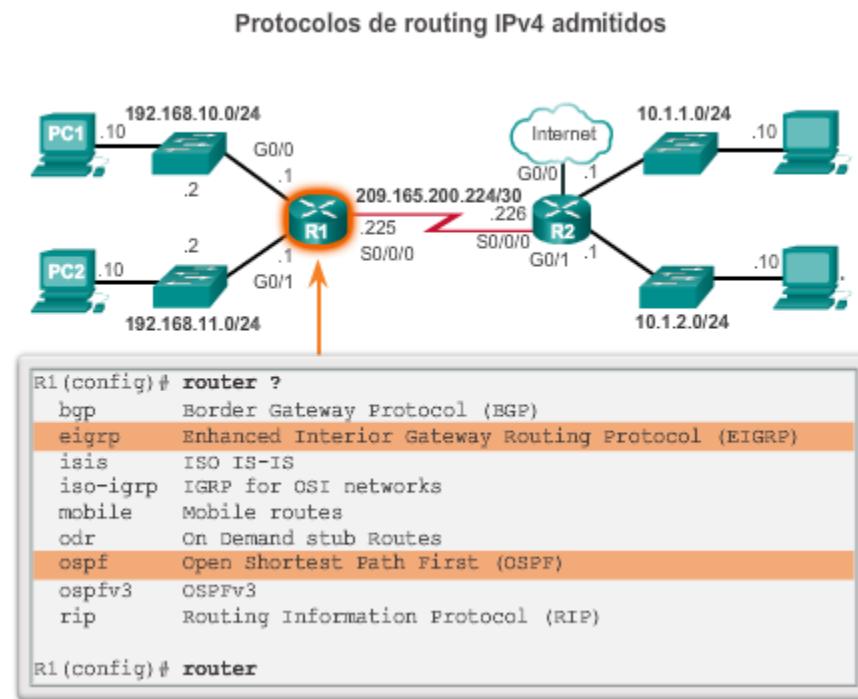
Un router que ejecuta un protocolo de routing dinámico no solo determina la mejor ruta hacia una red, sino que también determina una nueva mejor ruta si la ruta inicial se vuelve inutilizable (o si cambia la topología). Por estos motivos, los protocolos de enrutamiento dinámico representan una ventaja sobre las rutas estáticas. Los routers que usan protocolos de enrutamiento dinámico comparten automáticamente la información de enrutamiento con otros routers y compensan cualquier cambio de topología sin que sea necesaria la participación del administrador de la red.

Los routers ISR Cisco admiten diversos protocolos de routing dinámico IPv4, incluidos los siguientes:

- **EIGRP:** protocolo de routing de gateway interior mejorado
- **OSPF:** Open Shortest Path First
- **IS-IS:** Intermediate System-to-Intermediate System
- **RIP:** protocolo de información de routing

Para determinar qué protocolos de routing admite IOS, use el comando **router ?** en el modo de configuración global, como se muestra en la ilustración.

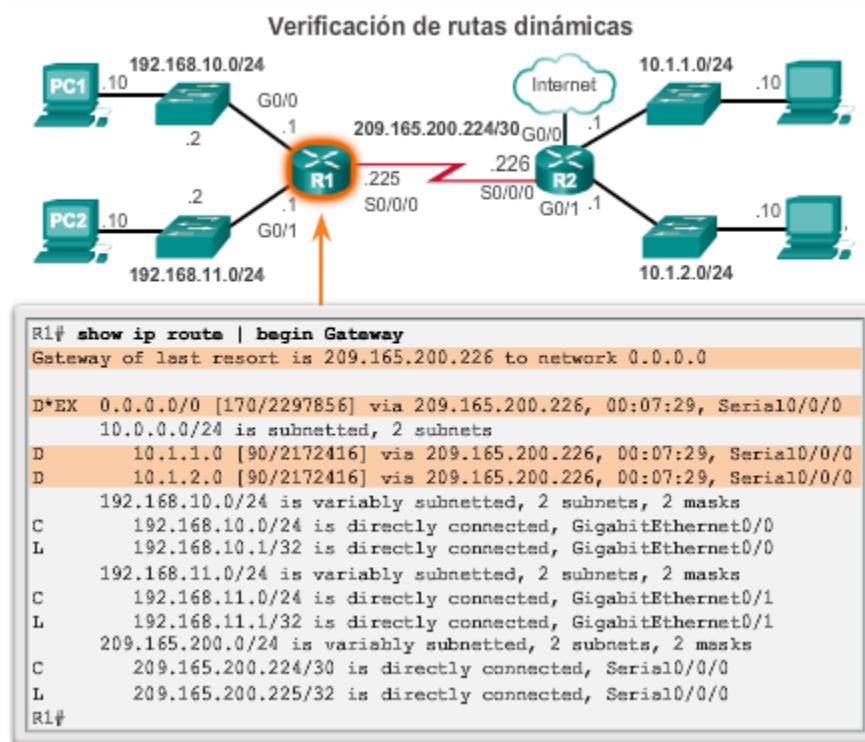
Nota: este curso se centra en EIGRP y OSPF. RIP se analizará solo por motivos de antigüedad; el resto de los protocolos de routing que admite IOS exceden el ámbito de la certificación CCNA.



En este ejemplo de routing dinámico, suponga que el R1 y el R2 se configuraron para admitir el protocolo de routing dinámico EIGRP. Los routers también anuncian las redes conectadas directamente. El R2 anuncia que es el gateway predeterminado a otras redes.

En el resultado de la ilustración, se muestra la tabla de routing del R1 después del intercambio de actualizaciones y la convergencia de los routers. Además de la interfaz conectada y la interfaz link-local, hay tres entradas “D” en la tabla de routing.

- La entrada que comienza con “D*EX” identifica que el origen de esta entrada fue EIGRP (“D”). La ruta es candidata a ser una ruta predeterminada (“*”) y es una ruta externa (“*EX”) reenviada por EIGRP.
- Las otras dos entradas “D” son rutas instaladas en la tabla de routing según la actualización del R2 que anuncia sus LAN.



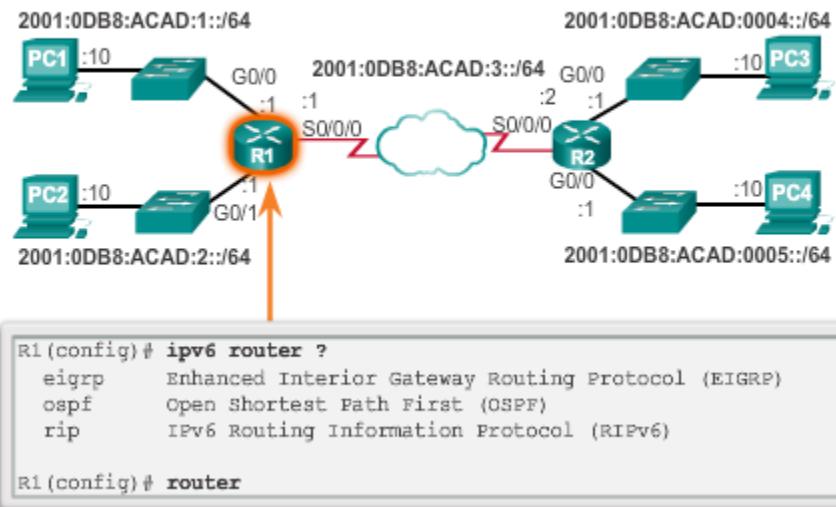
Como se muestra en la ilustración, los routers ISR admiten protocolos de routing dinámico IPv6, incluidos los siguientes:

- RIPng (RIP de última generación)
- OSPFv3
- EIGRP para IPv6

La compatibilidad con los protocolos de routing dinámico IPv6 depende del hardware y la versión del IOS. La mayoría de las modificaciones en los protocolos de routing se hacen para admitir direcciones IPv6 más largas y estructuras de encabezado diferentes.

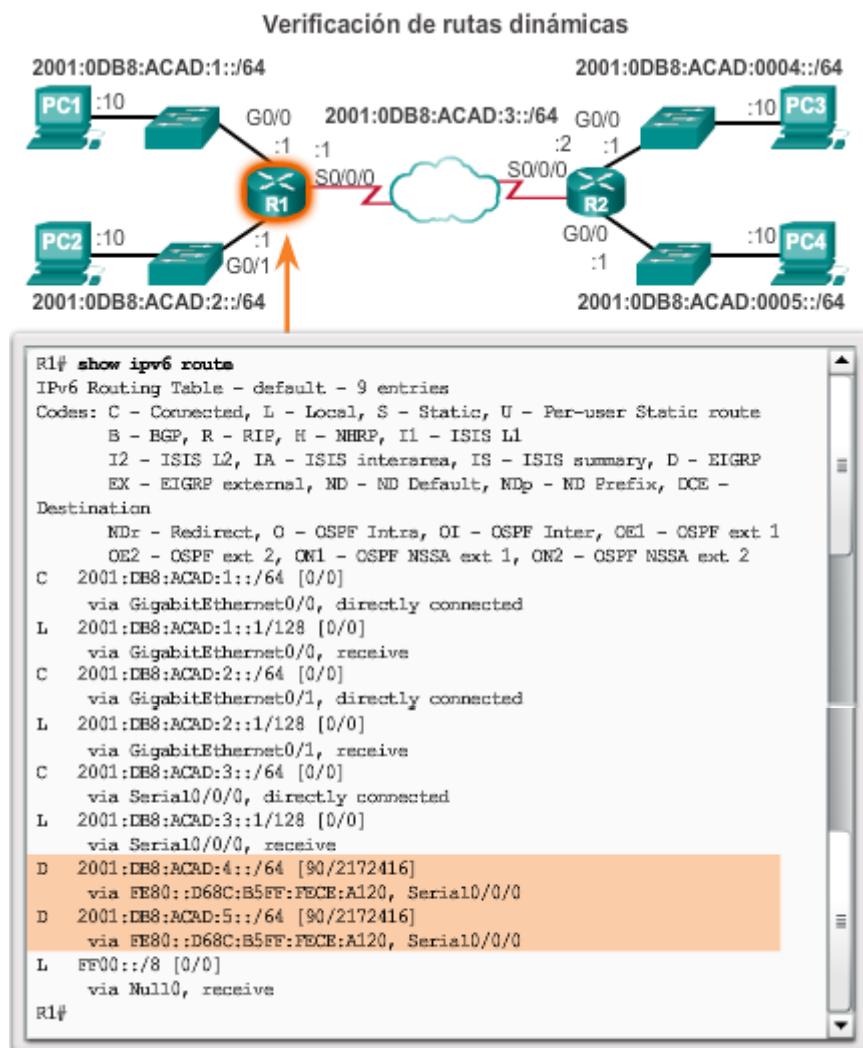
Para habilitar que los routers IPv6 reenvíen tráfico, se debe utilizar el comando de configuración global **ipv6 unicast-routing**.

Protocolos de routing IPv6 admitidos



Los routers R1 y R2 se configuraron con el protocolo de routing dinámico EIGRP para IPv6. (Este es el equivalente a EIGRP para IPv4 en IPv6).

Para ver la tabla de routing en el R1, introduzca el comando **show ipv6 route**, como se muestra en la ilustración. En el resultado de la ilustración, se muestra la tabla de routing del R1 después del intercambio de actualizaciones y la convergencia de los routers. Además de las rutas conectadas y locales, hay dos entradas "D" (rutas EIGRP) en la tabla de routing.



4.5 Resumen

Existen muchas características clave relacionadas con las estructuras y el rendimiento a las cuales nos referimos cuando hablamos de redes: topología, velocidad, costo, seguridad, disponibilidad, escalabilidad y confiabilidad.

Los routers y los switches Cisco tienen muchas similitudes: admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Una característica que distingue a los switches de los routers es el tipo de interfaces que admite cada uno. Una vez que se configuró una interfaz en ambos dispositivos, se deben utilizar los comandos show adecuados para verificar que la interfaz funcione.

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

El IOS de Cisco utiliza lo que se conoce como “distancia administrativa” (AD) para determinar la ruta que se debe instalar en la tabla de routing de IP. La tabla de routing es una lista de redes que conoce el router. La tabla de enrutamiento incluye direcciones de red para sus propias interfaces

que son las redes conectadas directamente, además de direcciones de red para redes remotas. Una red remota es una red a la que se puede llegar únicamente reenviando el paquete a otro router.

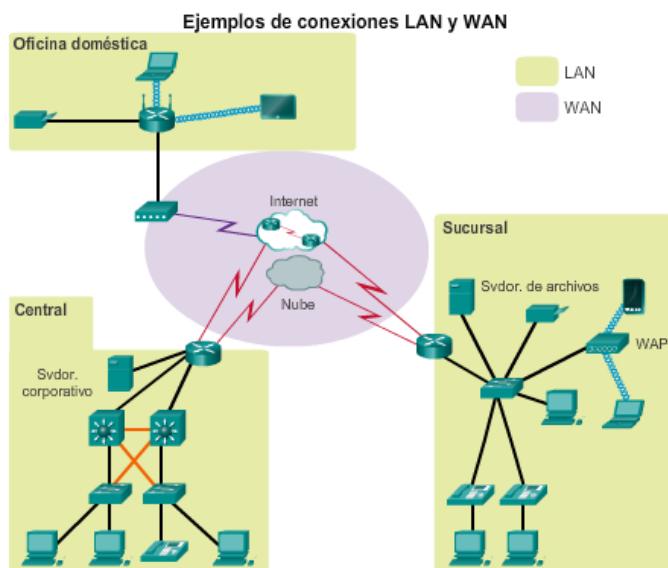
Las redes remotas se agregan a la tabla de routing de dos maneras: por el administrador de red que configura manualmente las rutas estáticas o implementando un protocolo de routing dinámico. Las rutas estáticas no tienen tanta sobrecarga como los protocolos de enrutamiento dinámico; sin embargo, las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

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

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

La tabla de enrutamiento IP de Cisco no es una base de datos plana. La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes.

Los componentes de la tabla de routing IPv6 son muy similares a los de la tabla de routing IPv4. Por ejemplo, se completa con las interfaces conectadas directamente, con las rutas estáticas y con las rutas descubiertas de forma dinámica.



5 Enrutamiento entre VLAN

5.1 Introducción

Hemos visto que el uso de redes VLAN para segmentar una red comutada proporciona mayor rendimiento, seguridad y capacidad de administración. Se utilizan enlaces troncales para transportar información de varias VLAN entre dispositivos. Sin embargo, debido a que estas VLAN segmentan la red, es necesario un proceso de capa 3 para permitir que el tráfico pase de un segmento de red a otro.

Este proceso de routing de capa 3 puede implementarse utilizando un router o una interfaz de switch de capa 3. El uso de un dispositivo de capa 3 proporciona un método para controlar el flujo de tráfico entre segmentos de red, incluidos los segmentos de red creados por las VLAN.

En este capítulo, se analizan los métodos utilizados para la implementación del routing entre VLAN. Se incluye configuraciones para el uso de un router y un switch de capa 3 y también se describen los problemas que se encuentran al implementar routing entre VLAN y técnicas estándar de resolución de problemas.

Después de completar este capítulo, podrá hacer lo siguiente:

- Describir las tres opciones principales para habilitar el routing entre VLAN.
- Configurar routing entre VLAN antiguo.
- Configurar el enrutamiento entre VLAN con router-on-a-stick.
- Solucionar problemas comunes de configuración entre VLAN.
- Solucionar problemas comunes de direccionamiento IP en un entorno de routing entre VLAN.
- Configurar routing entre VLAN mediante switching de capa 3.
- Solucionar problemas de routing entre VLAN en un entorno comutado de capa 3.



El routing entre VLAN ayuda a las redes comutadas de forma local a comunicarse entre sí.

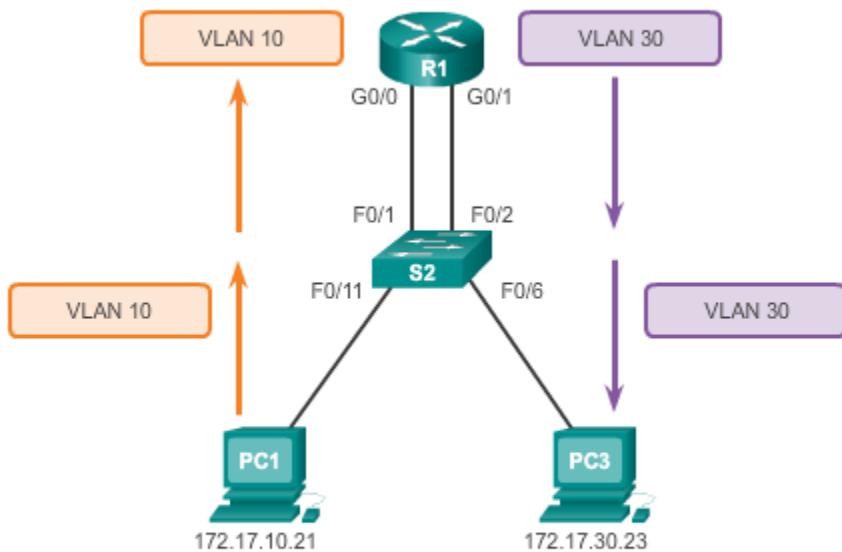
5.2 Configuración del routing entre VLAN

5.2.1 Funcionamiento del routing entre VLAN

Las VLAN se utilizan para segmentar redes comutadas. Un profesional de redes puede configurar switches de capa 2, tales como los de la serie Catalyst 2960, con más de 4000 VLAN. Sin embargo, los switches de capa 2 tienen una funcionalidad muy limitada en cuanto a IPv4 e IPv6, y no pueden realizar las funciones de routing de los routers. Mientras que los switches de capa 2 adquieren cada vez una mayor funcionalidad de IP, como la capacidad de realizar routing estático, no admiten routing dinámico. La gran cantidad de VLAN posibles en estos switches hace que el routing estático sea insuficiente.

Una VLAN es un dominio de difusión, por lo que las computadoras en VLAN separadas no pueden comunicarse sin la intervención de un dispositivo de routing. Se puede usar cualquier dispositivo que admita routing de capa 3, como un router o un switch multicapa, para lograr la funcionalidad de routing necesaria. Independientemente del dispositivo empleado, el proceso de reenvío del tráfico de la red de una VLAN a otra mediante routing se conoce como “routing entre VLAN”.

¿Qué es el enruteamiento entre VLAN?



El enruteamiento entre VLAN basado en routers es un proceso para reenviar el tráfico de la red desde una VLAN a otra mediante un router.

Históricamente, la primera solución para el routing entre VLAN se valía de routers con varias interfaces físicas. Era necesario conectar cada interfaz a una red separada y configurarla para una subred diferente.

En este enfoque antiguo, el routing entre VLAN se realiza mediante la conexión de diferentes interfaces físicas del router a diferentes puertos físicos de switch. Los puertos de switch conectados al router se colocan en modo de acceso, y cada interfaz física se asigna a una VLAN diferente. Cada interfaz del router puede entonces aceptar el tráfico desde la VLAN asociada a la interfaz del switch que se encuentra conectada y el tráfico puede enrutararse a otras VLAN conectadas a otras interfaces.

Nota: la topología utiliza enlaces paralelos para establecer los enlaces troncales entre los switches a fin de obtener agregación de enlaces y redundancia. Sin embargo, los enlaces redundantes hacen que la topología sea más compleja y pueden introducir problemas de conectividad si no se administran de la manera adecuada. Deben implementarse protocolos y técnicas, tales como árbol de expansión y EtherChannel, para administrar los enlaces redundantes. Estas técnicas exceden el ámbito de este capítulo.

Haga clic en el botón Reproducir de la ilustración para ver una animación del routing entre VLAN antiguo.

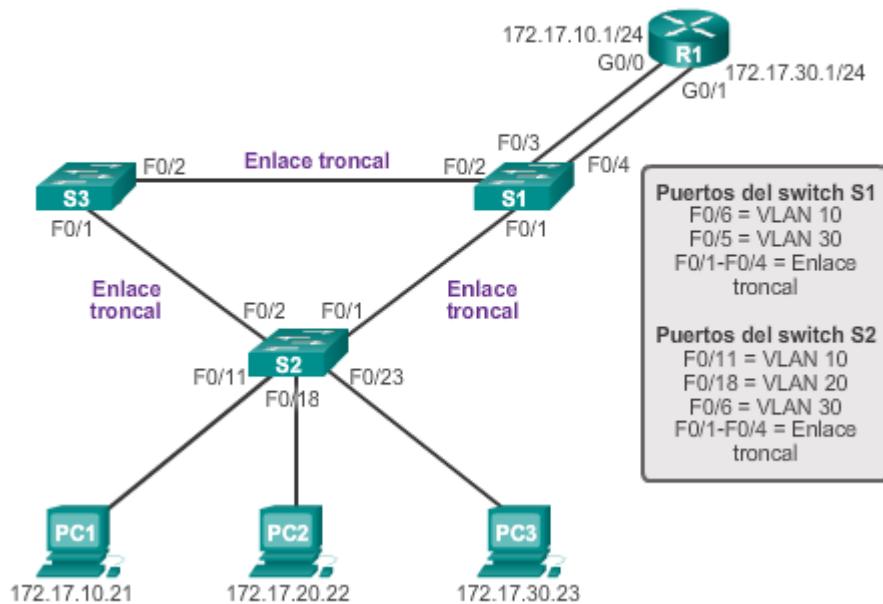
Tal como se observa en la animación:

1. La PC1 en la VLAN 10 se comunica con la PC3 en la VLAN 30 a través del router R1.
2. PC1 y PC3 están en VLAN diferentes y tienen direcciones IP en subredes diferentes.
3. El router R1 tiene una interfaz separada configurada para cada una de las VLAN.
4. La PC1 envía el tráfico de unidifusión destinado a la PC3 al switch S2 en la VLAN 10, desde el cual luego se reenvía por la interfaz troncal al switch S1.
5. Después, el switch S1 reenvía el tráfico de unidifusión al router R1 en la interfaz G0/0.
6. El router enruta el tráfico de unidifusión a través de la interfaz G0/1, que está conectada a la VLAN 30.
7. El router reenvía el tráfico unicast al switch S1 en la VLAN 30.
8. El switch S1 luego reenvía el tráfico de unidifusión al switch S2 a través del enlace troncal activo, tras lo cual el switch S2 puede reenviar el tráfico de unidifusión a la PC3 en la VLAN 30.

En este ejemplo el router se configuró con dos interfaces físicas separadas para interactuar con las distintas VLAN y realizar el enrutamiento.

Nota: este método de routing entre VLAN no es eficaz y, por lo general, ya no se implementa en las redes comutadas. Se muestra en este curso solo con fines explicativos.

Routing entre VLAN antiguo



A diferencia del routing entre VLAN antiguo, que requiere varias interfaces físicas, tanto en el router como en el switch, las implementaciones más comunes y actuales de routing entre VLAN no tienen esos requisitos. En cambio, algunos softwares de router permiten configurar una interfaz del router como enlace troncal, lo que significa que solo es necesaria una interfaz física en el router y en el switch para enrutar paquetes entre varias VLAN.

“Router-on-a-stick” es un tipo de configuración de router en la cual una única interfaz física enruta el tráfico entre varias VLAN en una red. Como puede verse en la ilustración, el router está conectado al switch S1 mediante una única conexión de red física (un enlace troncal).

La interfaz del router se configura para funcionar como enlace troncal y se conecta a un puerto del switch configurado en modo de enlace troncal. Para realizar el routing entre VLAN, el router acepta en la interfaz troncal el tráfico con etiquetas de VLAN proveniente del switch adyacente y luego lo enruta en forma interna entre las VLAN, mediante subinterfaces. El router reenvía el tráfico enrutado con etiquetas de VLAN para la VLAN de destino a través de la misma interfaz física utilizada para recibir el tráfico.

Las subinterfaces son interfaces virtuales basadas en software, asociadas con una única interfaz física. Las subinterfaces se configuran en software en un router, y cada subinterfaz se configura de manera independiente con una dirección IP y una asignación de VLAN. Las subinterfaces se configuran para subredes diferentes que corresponden a su asignación de VLAN para facilitar el routing lógico. Después de que se toma una decisión de routing según la VLAN de destino, las tramas de datos reciben etiquetas de VLAN y se envían de vuelta por la interfaz física.

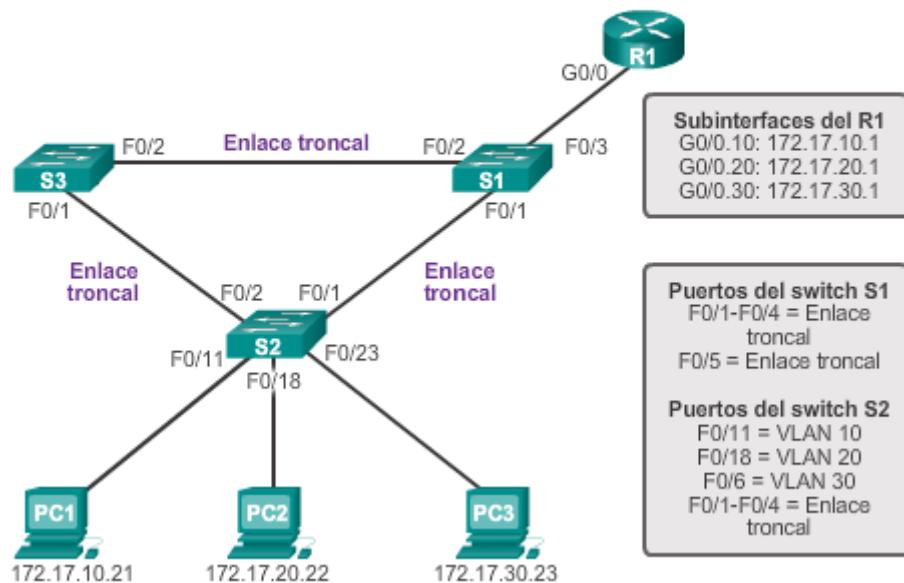
Haga clic en el botón Reproducir de la ilustración para ver una animación de la forma en que un router-on-a-stick desempeña su función de routing.

Tal como se observa en la animación:

1. La PC1 en la VLAN 10 se comunica con la PC3 en la VLAN 30 a través del router R1 mediante una única interfaz física del router.
 2. PC1 envía el tráfico unicast al switch S2.
 3. Luego, el switch S2 etiqueta el tráfico de unidifusión como originado en la VLAN 10 y lo reenvía por el enlace troncal al switch S1.
 4. El switch S1 reenvía el tráfico etiquetado por la otra interfaz troncal en el puerto F0/5 a la interfaz en el router R1.
 5. El router R1 acepta el tráfico de unidifusión etiquetado en la VLAN 10 y lo enruta a la VLAN 30 mediante sus subinterfaces configuradas.
 6. El tráfico de unidifusión se etiqueta con la VLAN 30 mientras se envía por la interfaz del router al switch S1.
 7. El switch S1 reenvía el tráfico unicast etiquetado por el otro enlace troncal al switch S2.
 8. El switch S2 elimina la etiqueta de la VLAN de la trama de unicast y reenvía la trama a PC3 en el puerto F0/6.

Nota: el método de routing entre VLAN de router-on-a-stick no es escalable más allá de las 50 VLAN.

Enrutamiento entre VLAN de un "Router-on-a-Stick"



La implementación de routing entre VLAN de router-on-a-stick requiere solamente una interfaz física en un router y una interfaz en un switch, lo que simplifica el cableado del router. Sin embargo, en otras implementaciones de routing entre VLAN, no se necesita un router dedicado.

Los switches multicapa pueden realizar funciones de capa 2 y de capa 3, lo que remplaza la necesidad de utilizar routers dedicados para realizar tareas de routing básico en una red. Los switches multicapa admiten routing dinámico y routing entre VLAN.

Haga clic en el botón Reproducir de la ilustración para ver una animación de la forma en que se realiza el routing entre VLAN basado en switch.

Tal como se observa en la animación:

1. La PC1 en la VLAN 10 se comunica con la PC3 en la VLAN 30 a través del switch S1 mediante las interfaces VLAN configuradas para cada VLAN.
2. PC1 envía el tráfico unicast al switch S2.
3. El switch S2 etiqueta el tráfico de unidifusión como originado en la VLAN 10 a medida que lo reenvía por el enlace troncal al switch S1.
4. El switch S1 elimina la etiqueta de VLAN y reenvía el tráfico de unidifusión a la interfaz de la VLAN 10.
5. El switch S1 enruta el tráfico de unidifusión a su interfaz de la VLAN 30.
6. El switch S1 luego vuelve a etiquetar el tráfico de unidifusión con la VLAN 30 y lo reenvía por el enlace troncal al switch S2.
7. El switch S2 elimina la etiqueta de la VLAN de la trama de unicast y reenvía la trama a PC3 en el puerto F0/6.

Para habilitar un switch multicapa para que realice funciones de routing, debe tener routing IP habilitado.

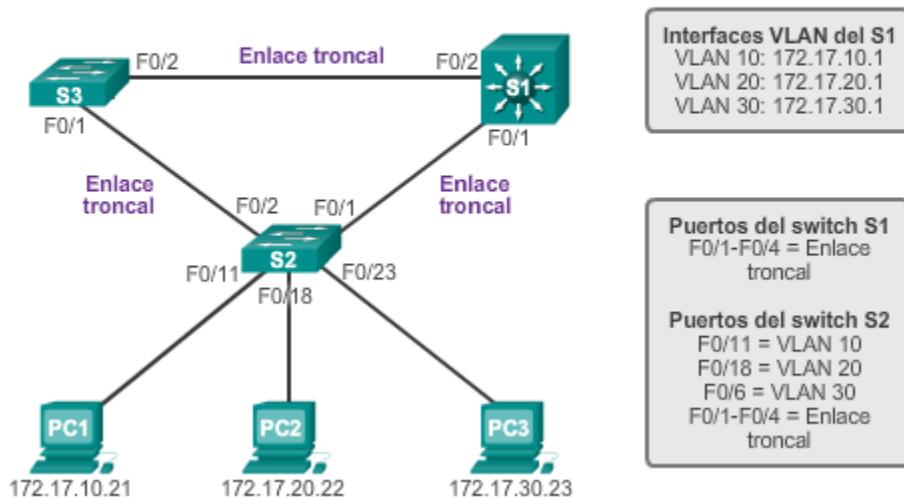
El switching de multicapa es más escalable que cualquier otra implementación de routing entre VLAN. Esto se debe a que los routers tienen una cantidad limitada de puertos disponibles para conectarse a las redes. Además, en el caso de las interfaces que se configuran como una línea troncal, se puede admitir una cantidad limitada de tráfico en la línea al mismo tiempo.

Con un switch multicapa, el tráfico se enruta internamente al dispositivo de switch, lo que significa que los paquetes no se filtran por una única línea troncal para obtener nueva información de etiquetado de VLAN. Sin embargo, un switch multicapa no reemplaza totalmente la funcionalidad de un router. Los routers admiten una cantidad considerable de características adicionales, como la capacidad de implementar mayores controles de seguridad. En cambio, un switch multicapa se puede pensar como un dispositivo de capa 2 actualizado para tener algunas capacidades de routing.

Nota: en este curso, la configuración de routing entre VLAN en un switch se restringe a configurar rutas estáticas en un switch 2960, que es la única funcionalidad de routing admitida en los switches 2960. Los switches 2960 admiten hasta 16 rutas estáticas (entre las que se incluyen las rutas configuradas por el usuario y la ruta predeterminada) y todas las rutas conectadas directamente y las rutas predeterminadas para la interfaz de administración. Los switches 2960 pueden tener una dirección IP asignada a cada interfaz virtual de switch (SVI). En cuanto a switches multicapa

relativamente económicos con todas las características, los switches de la serie Cisco Catalyst 3560 admiten los protocolos de routing EIGRP, OSPF y BGP.

Enrutamiento entre VLAN basado en switch



5.2.2 Configuración de routing entre VLAN antiguo

El routing entre VLAN antiguo requiere que los routers tengan varias interfaces físicas. El router realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz se configura con una dirección IP para la subred asociada con la VLAN específica a la cual está conectada. Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el router mediante la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el router como un gateway para acceder a los dispositivos conectados a las otras VLAN.

El proceso de enrutamiento requiere del dispositivo de origen para determinar si el dispositivo de destino es local o remoto con respecto a la subred local. El dispositivo de origen realiza esta determinación al comparar las direcciones IP de origen y de destino con la máscara de subred. Una vez que se determina que la dirección IP de destino está en una red remota, el dispositivo de origen debe identificar adónde necesita reenviar el paquete para llegar al dispositivo de destino. El dispositivo de origen examina la tabla de enrutamiento local para determinar dónde es necesario enviar los datos. Los dispositivos utilizan sus gateways predeterminados como destino de capa 2 para todo el tráfico que debe abandonar la subred local. El gateway predeterminado es la ruta que el dispositivo utiliza cuando no tiene otra ruta explícitamente definida hacia la red de destino. La dirección IP de la interfaz del router en la subred local actúa como gateway predeterminado para el dispositivo emisor.

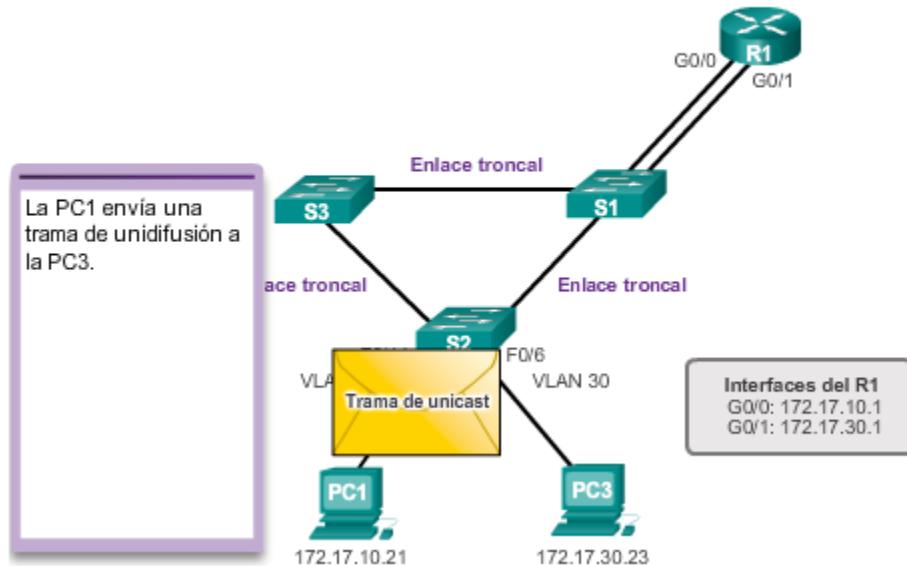
Una vez que el dispositivo de origen determina que el paquete debe viajar a través de la interfaz del router local en la VLAN conectada, envía una solicitud de ARP para determinar la dirección MAC de la interfaz del router local. Una vez que el router envía su respuesta de ARP al dispositivo de origen, este puede utilizar la dirección MAC para finalizar el entramado del paquete antes de enviarlo a la red como tráfico de unidifusión.

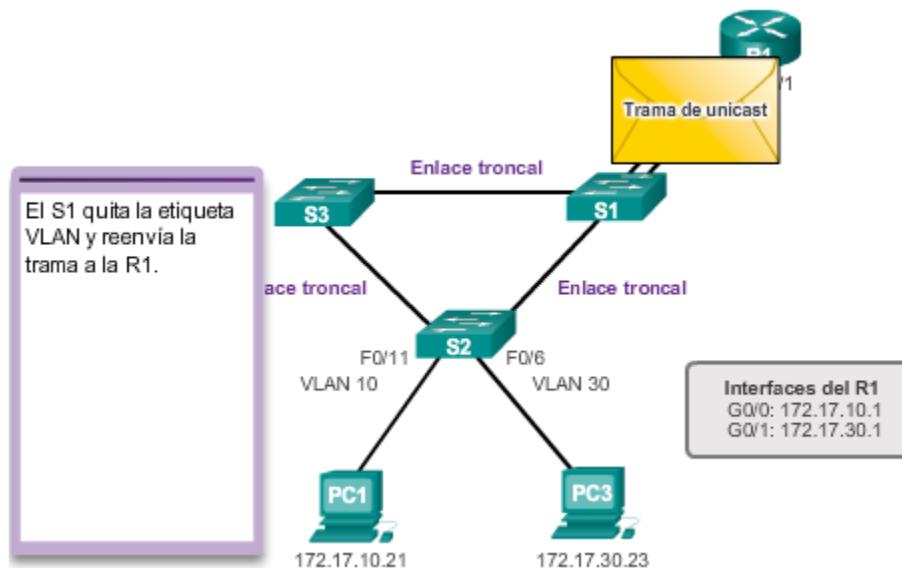
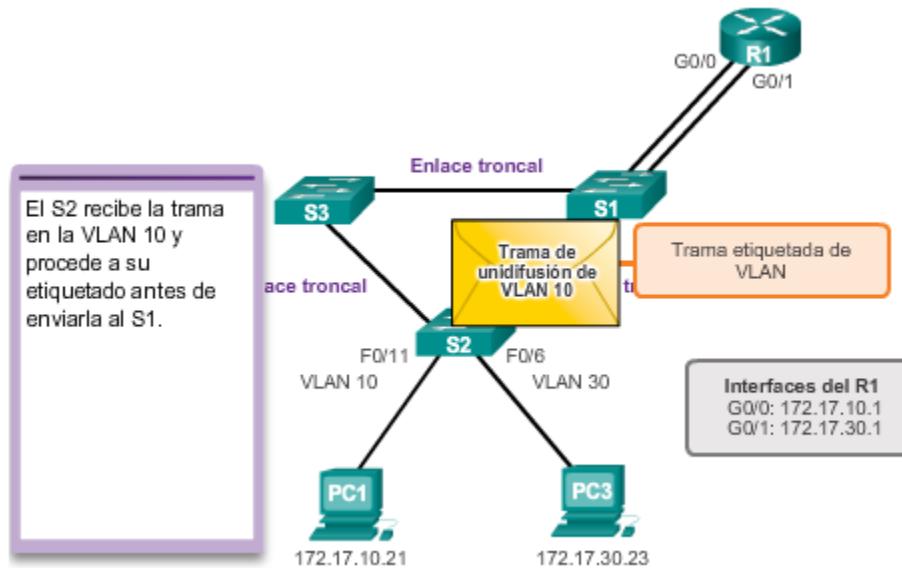
Dado que la trama de Ethernet tiene la dirección MAC de destino de la interfaz del router, el switch sabe exactamente a qué puerto del switch reenviar el tráfico de unidifusión para llegar a la interfaz del router de dicha VLAN. Cuando la trama llega al router, el router elimina la información de la dirección MAC de origen y destino para examinar la dirección IP de destino del paquete. El router compara la dirección de destino con las entradas en la tabla de enrutamiento para determinar dónde es necesario reenviar los datos para alcanzar el destino final. Si el router determina que la red de destino es una red conectada en forma local, como sería el caso del routing entre VLAN, envía una solicitud de ARP por la interfaz conectada físicamente a la VLAN de destino. El dispositivo de destino responde al router con la dirección MAC, la cual luego utiliza el router para entramar el paquete. El router envía el tráfico unicast al switch, que lo reenvía por el puerto donde se encuentra conectado el dispositivo de destino.

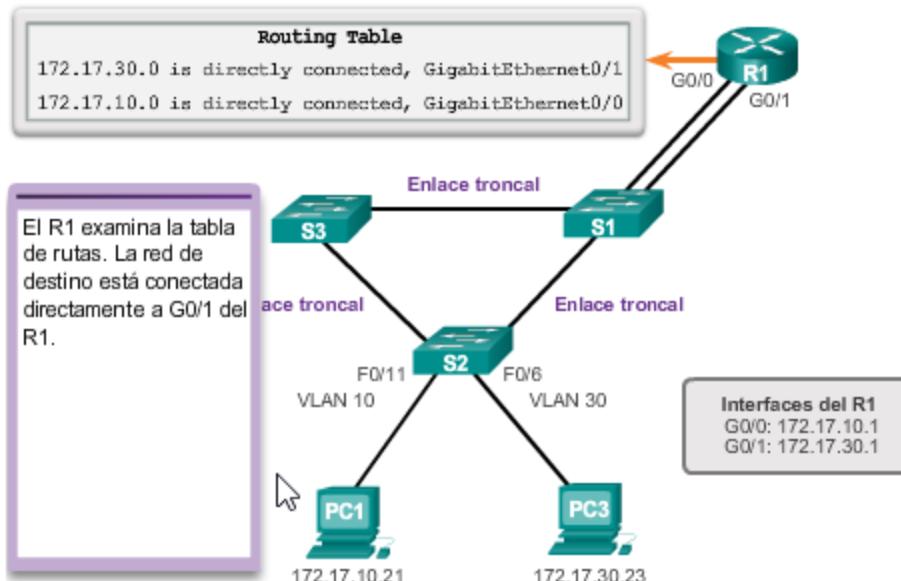
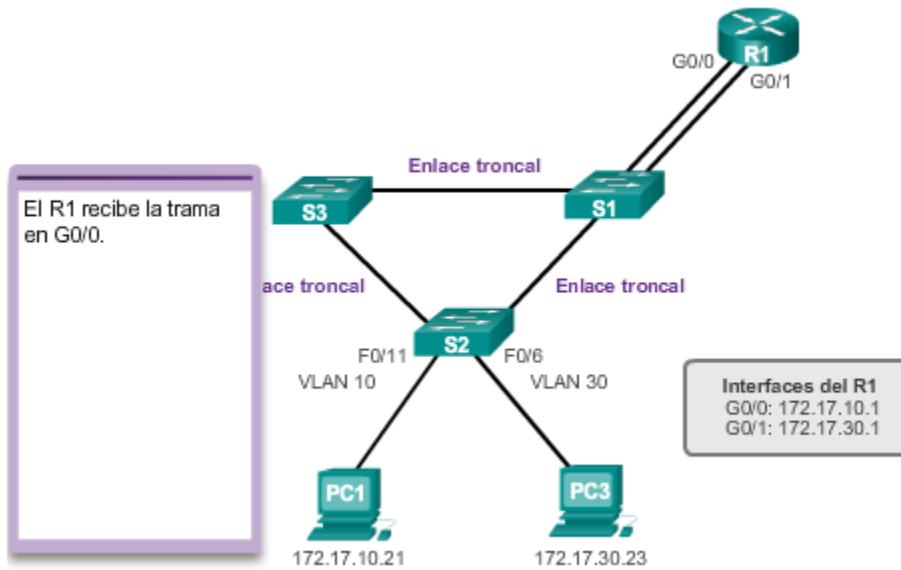
Haga clic en el botón Reproducir de la ilustración para ver cómo se realiza el routing entre VLAN antiguo.

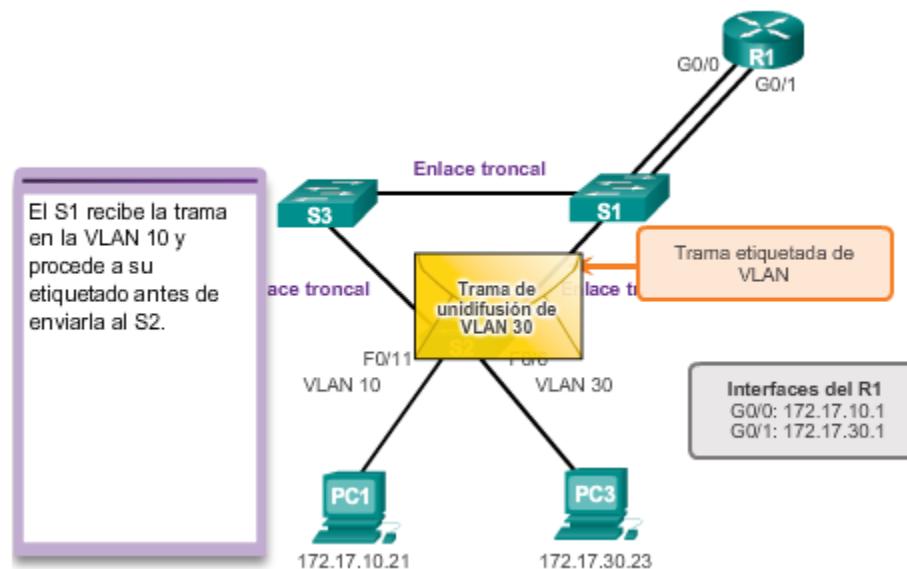
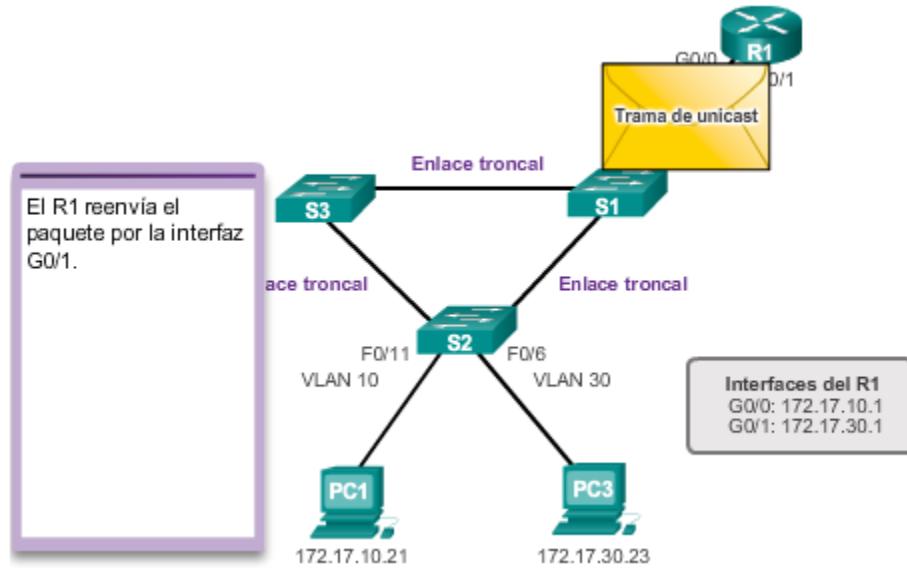
Aunque existen muchos pasos en el proceso de routing entre VLAN, cuando dos dispositivos en diferentes VLAN se comunican a través de un router, el proceso completo tiene lugar en una fracción de segundo.

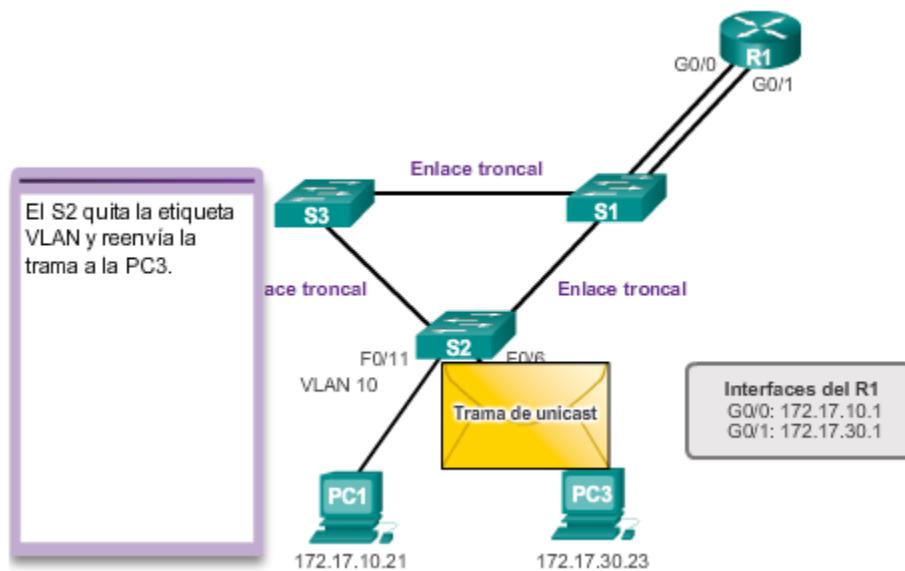
Interfaces del router y enrutamiento entre VLAN











Para configurar el routing entre VLAN antiguo, comience con la configuración del switch.

Como se muestra en la ilustración, el router R1 está conectado a los puertos del switch F0/4 y F0/5, que se configuraron para las VLAN 10 y 30 respectivamente.

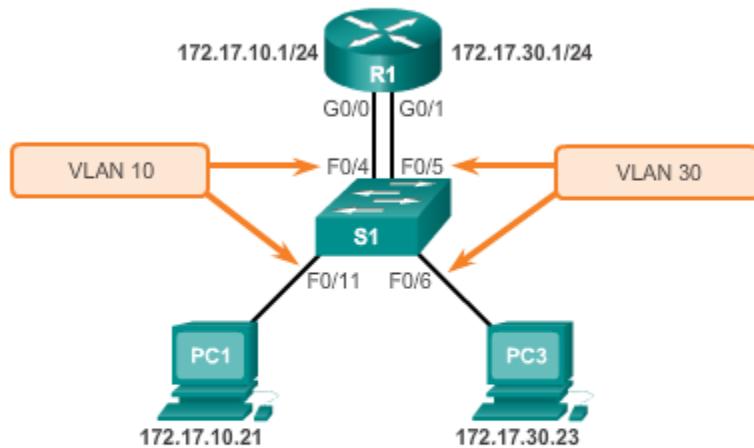
Utilice el comando **vlan id_vlan** del modo de configuración global para crear las VLAN. En este ejemplo las VLAN 10 y 30 se crearon en el switch S1.

Una vez que se crean las VLAN, los puertos de switch se asignan a las VLAN adecuadas. El comando **switchport access vlan id_vlan** se ejecuta desde el modo de configuración de interfaz en el switch para cada interfaz a la cual se conecta el router.

En este ejemplo, las interfaces F0/4 y F0/11 se asignaron a la VLAN 10 con el comando **switchport access vlan 10**. Se utilizó el mismo proceso para asignar la interfaz F0/5 y F0/6 en el switch S1 a la VLAN 30.

Finalmente, para proteger la configuración y no perderla después de una recarga del switch, se ejecuta el comando **copy running-config startup-config** para guardar una copia de seguridad de la configuración en ejecución en la configuración de inicio.

Configuración de routing entre VLAN antiguo



```

S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
*Mar 20 01:22:56.751: %SYS-5-CONFIG_I: Configured from console by
console
S1# copy running-config startup-config
Destination filename [startup-config]?

```

A continuación, se puede configurar el router para que realice routing entre VLAN.

Las interfaces del router se configuran de manera similar a las interfaces de VLAN en los switches. Para configurar una interfaz específica, pase al modo de configuración de interfaz desde el modo de configuración global.

Como se muestra en la figura 1, cada interfaz se configura con una dirección IP mediante el comando **ip address dirección_ip máscara_subred** en el modo de configuración de interfaz.

Como se muestra en el ejemplo, la interfaz G0/0 se configuró con la dirección IP 172.17.10.1 y la máscara de subred 255.255.255.0 mediante el comando **ip address 172.17.10.1 255.255.255.0**.

Las interfaces del router están deshabilitadas de manera predeterminada y es necesario habilitarlas con el comando **no shutdown** antes de utilizarlas. Una vez que se emite el comando del modo de configuración de interfaz **no shutdown**, se muestra una notificación que indica que el estado de la interfaz cambió a activo (up). Esto indica que la interfaz ahora está habilitada.

El proceso se repite para todas las interfaces del router. Es necesario asignar cada interfaz del router a una subred única para que se produzca el routing. En este ejemplo, la otra interfaz del router, G0/1, se configuró para utilizar la dirección IP 172.17.30.1, que se encuentra en una subred diferente que la interfaz G0/0.

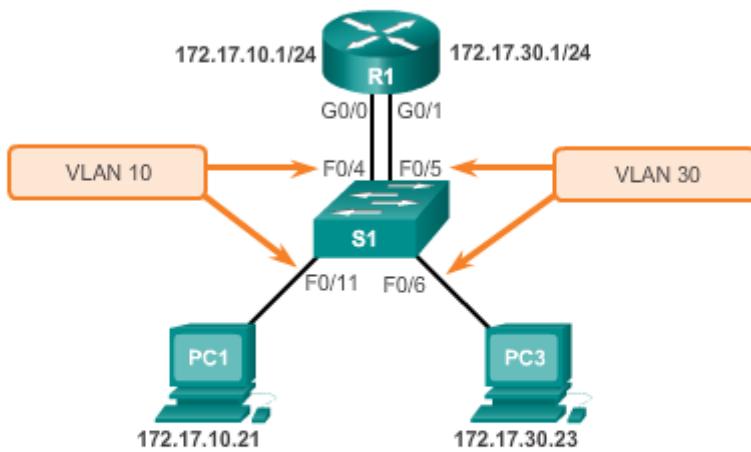
Una vez que se asignan las direcciones IP a las interfaces físicas y que las interfaces se habilitan, el router es capaz de llevar a cabo routing entre VLAN.

Examine la tabla de routing con el comando **show ip route**.

En la figura 2, hay dos rutas visibles en la tabla de routing. Una ruta es la subred 172.17.10.0, que está conectada a la interfaz local G0/0. La otra ruta es la subred 172.17.30.0, que está conectada a la interfaz local G0/1. El router utiliza la tabla de enrutamiento para determinar dónde enviar el tráfico que recibe. Por ejemplo: si el router recibe un paquete en la interfaz G0/0 destinado a la subred 172.17.30.0, el router identificará que debe enviar el paquete por la interfaz G0/1 para que llegue a los hosts en la subred 172.17.30.0.

Observe la letra **C** a la izquierda de cada una de las entradas de ruta para las VLAN. Esta letra indica que la ruta es local para una interfaz conectada, que también está identificada en la entrada de ruta. Según el resultado de este ejemplo, si el tráfico estuviera destinado a la subred 172.17.30.0, el router debería reenviar el tráfico por la interfaz G0/1.

Configuración de routing entre VLAN antiguo



```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
```

5.2.3 Configurar un enrutamiento router-on-a-stick entre VLAN

El routing entre VLAN antiguo con interfaces físicas tiene una limitación importante. Los routers tienen una cantidad limitada de interfaces físicas para conectarse a diferentes VLAN. A medida que aumenta la cantidad de VLAN en una red, el hecho de tener una interfaz física del router por VLAN

agota rápidamente la capacidad de interfaces físicas de un router. Una alternativa en redes más grandes es utilizar subinterfaces y enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que una única interfaz física del router enrute el tráfico de varias VLAN. Esta técnica se denomina “router-on-a-stick” y utiliza subinterfaces virtuales en el router para superar las limitaciones de interfaces físicas del hardware.

Las subinterfaces son interfaces virtuales basadas en software asignadas a interfaces físicas. Cada subinterfaz se configura de forma independiente con su propia dirección IP y máscara de subred. Esto permite que una única interfaz física forme parte de varias redes lógicas de manera simultánea.

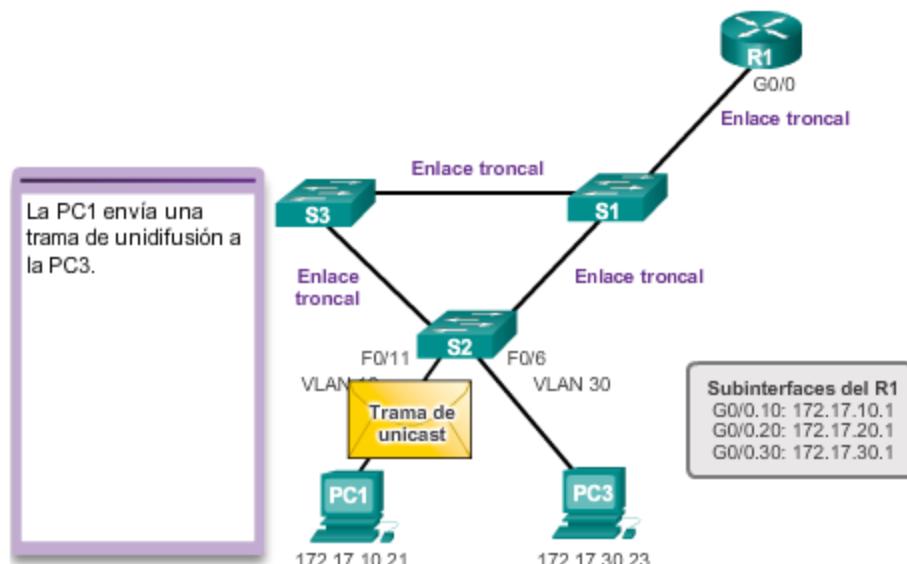
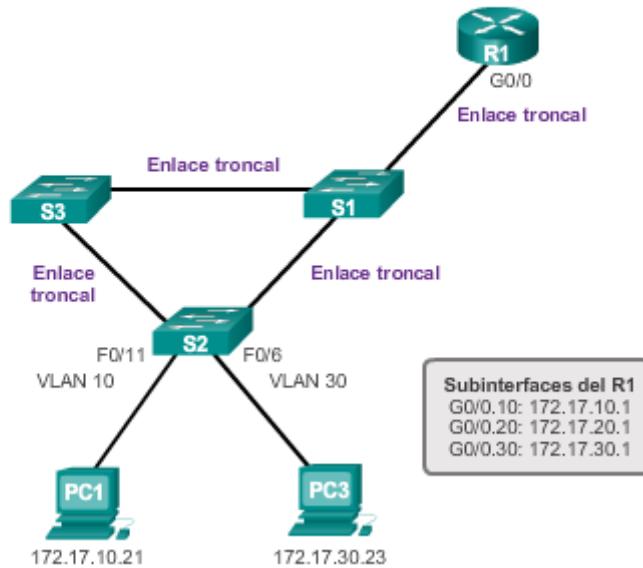
Al configurar el enrutamiento inter VLAN mediante el modelo router-on-a-stick, la interfaz física del router debe estar conectada al enlace troncal en el switch adyacente. En el router, se crean subinterfaces para cada VLAN única en la red. A cada subinterfaz se le asigna una dirección IP específica para su subred/VLAN y también se configura para etiquetar las tramas para esa VLAN. De esa manera, el router puede mantener separado el tráfico de cada subinterfaz a medida que atraviesa el enlace troncal hacia el switch.

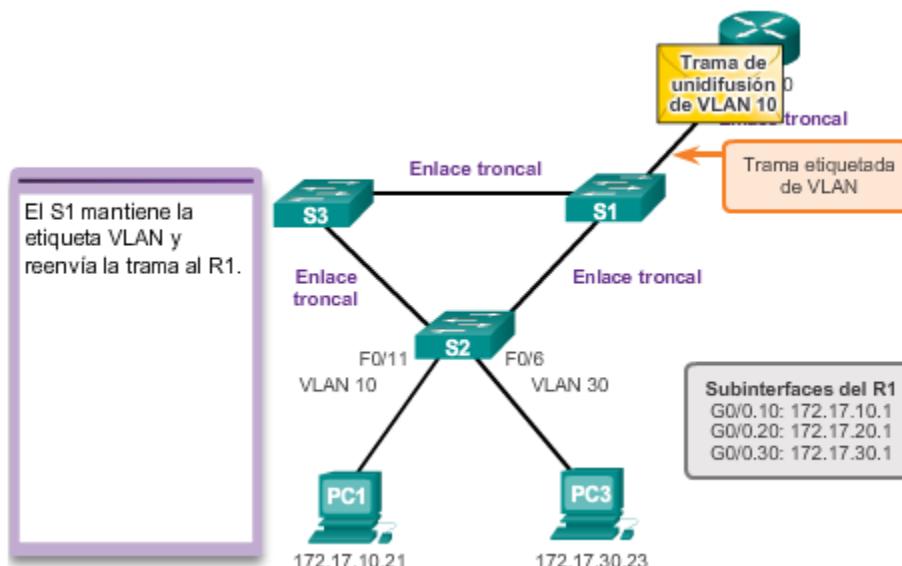
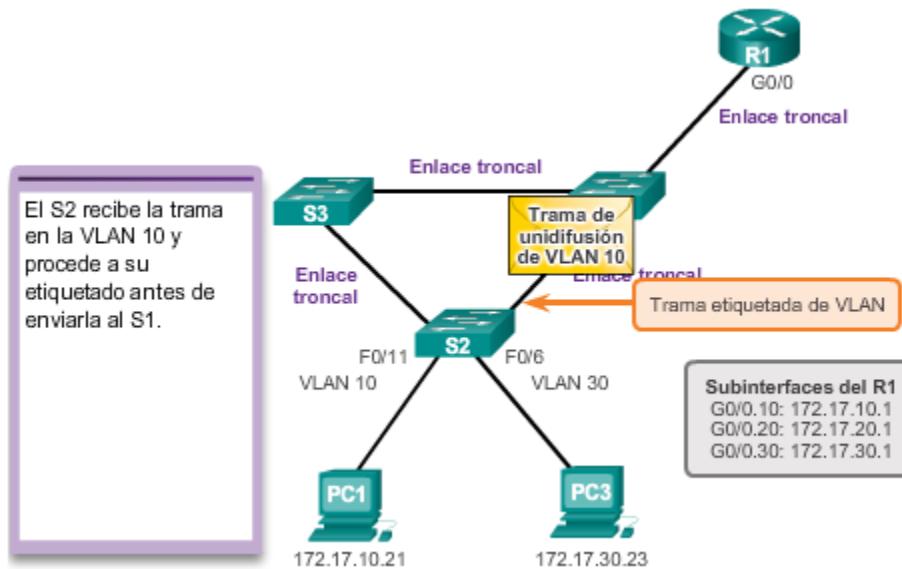
En términos de funcionamiento, utilizar el modelo router-on-a-stick es lo mismo que utilizar el modelo de routing entre VLAN antiguo, pero en lugar de utilizar las interfaces físicas para realizar el routing, se utilizan las subinterfaces de una única interfaz física.

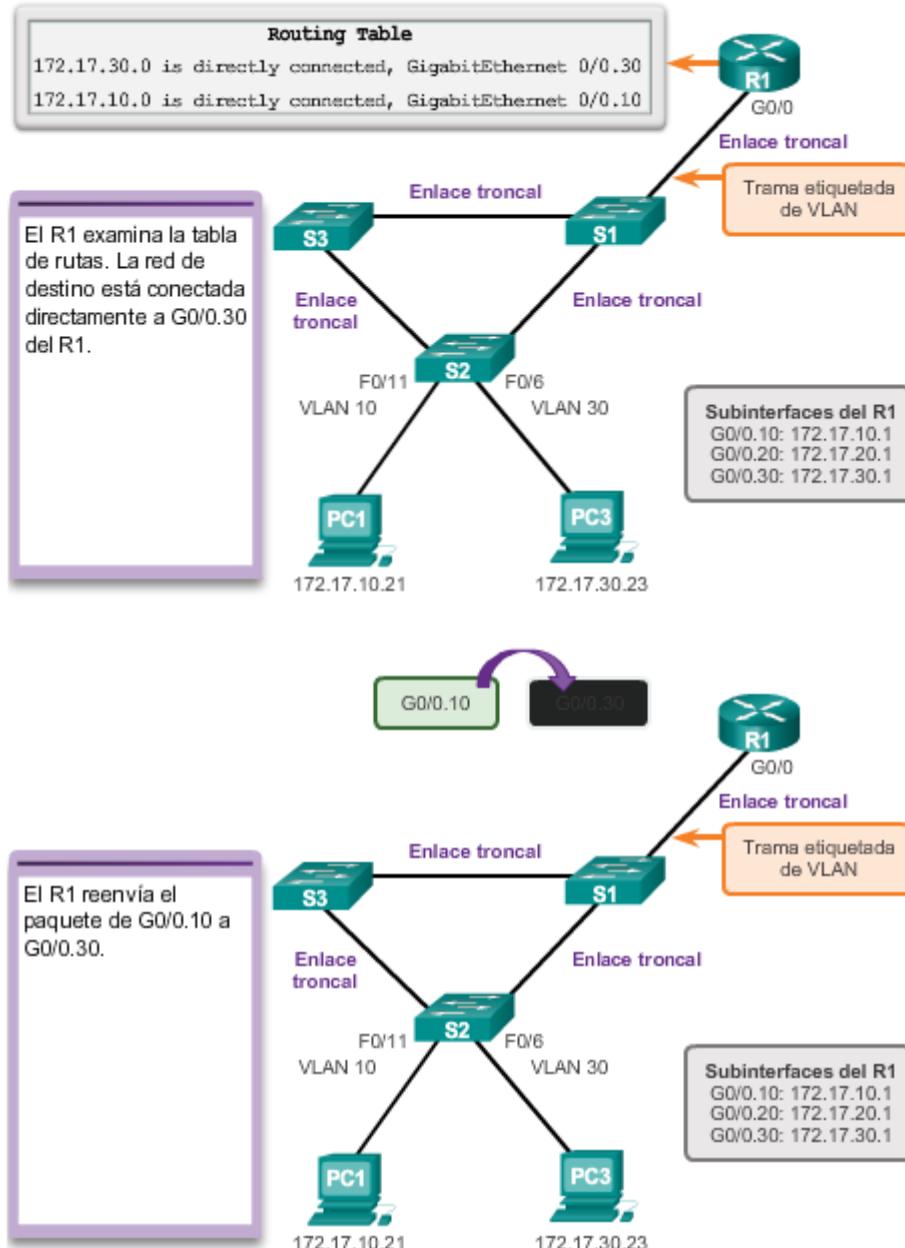
En la figura, PC1 desea comunicarse con PC3. La PC1 se encuentra en la VLAN 10, y la PC3, en la VLAN 30. Para que la PC1 se comunique con la PC3, la PC1 necesita enrutar sus datos a través del router R1, por medio de subinterfaces.

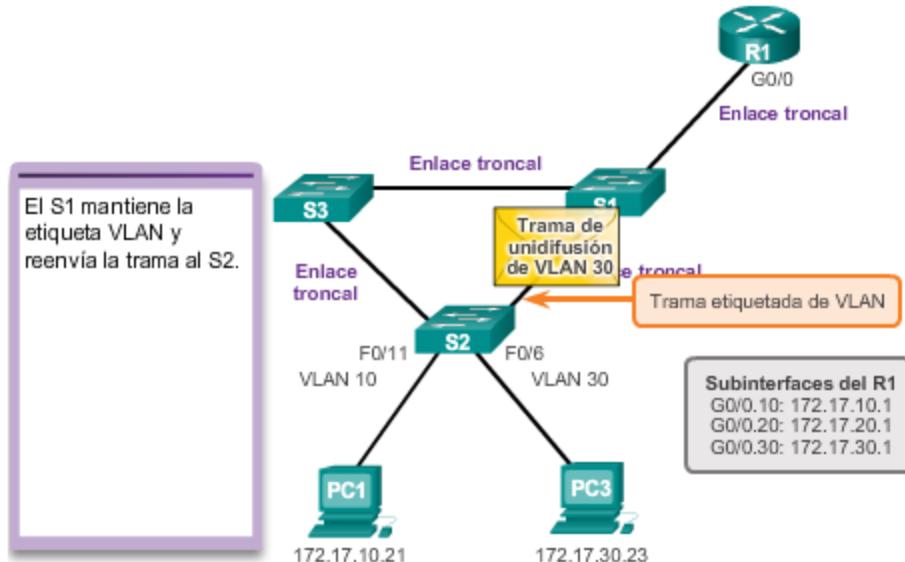
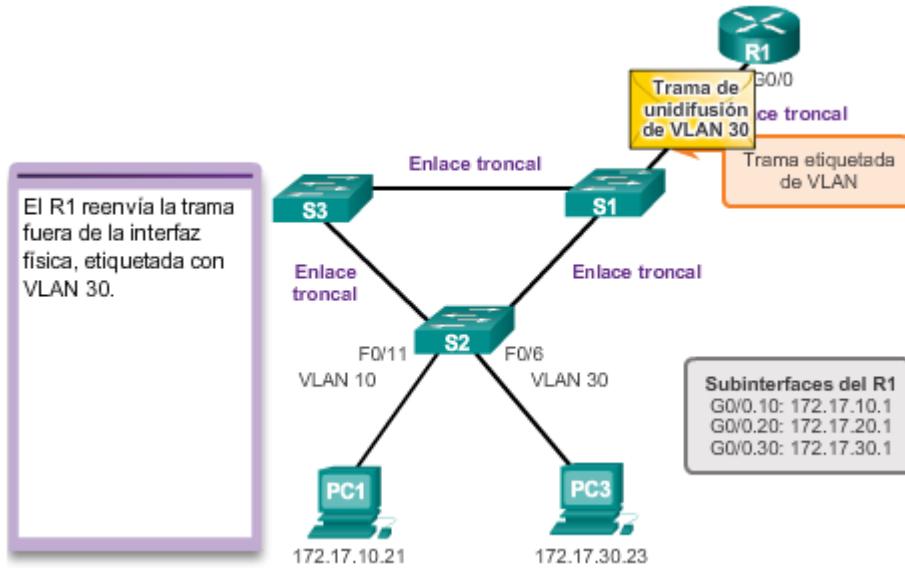
Haga clic en el botón Reproducir que se muestra en la figura para ver cómo se utilizan las subinterfaces para enrutar entre las VLAN. Cuando se detenga la animación, lea el texto a la izquierda de la topología. Haga clic en Reproducir nuevamente para seguir viendo la animación.

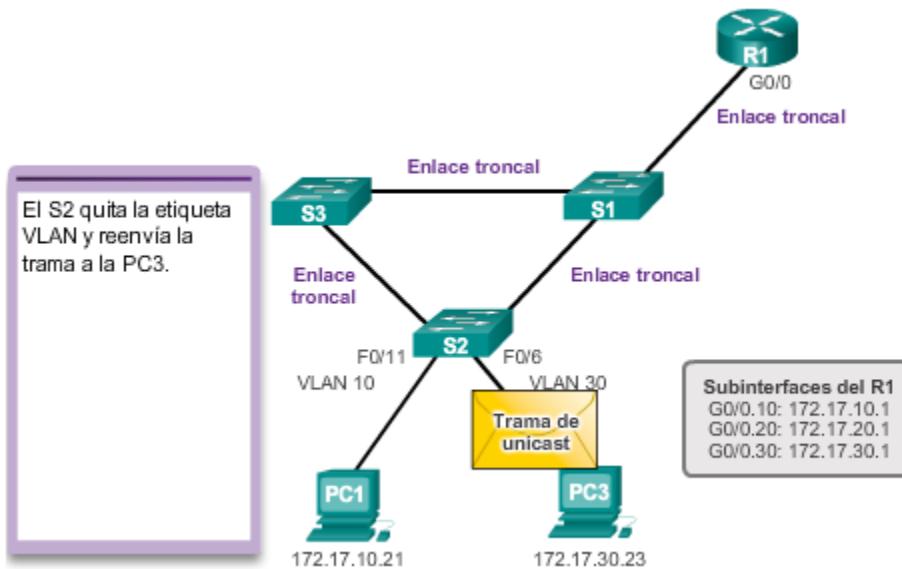
El uso de los enlaces troncales y las subinterfaces disminuye la cantidad de puertos de switch y de router que se utilizan. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de la subinterfaz del router puede ampliarse hasta un número mucho más alto de VLAN que una configuración con una interfaz física por diseño de VLAN.

Subinterfaces del router y enruteamiento entre VLAN









Para habilitar el routing entre VLAN utilizando el método router-on-a stick, comience por habilitar el enlace troncal en el puerto del switch que está conectado al router.

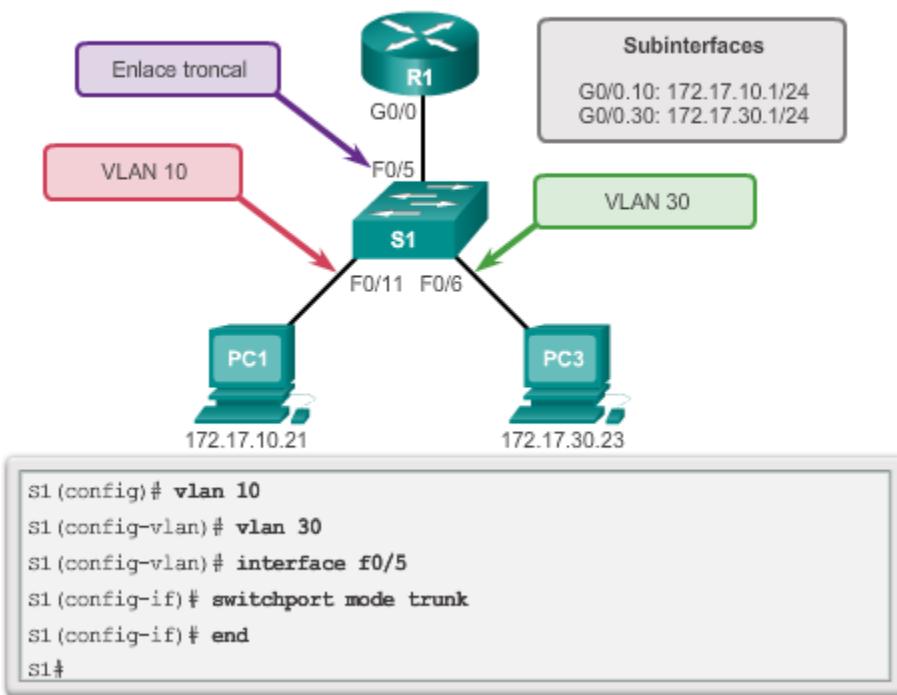
En la ilustración, el router R1 se conecta al switch S1 en el puerto de enlace troncal F0/5. Las VLAN 10 y 30 se agregaron al switch S1.

Debido a que el puerto del switch F0/5 está configurado como puerto de enlace troncal, no necesita asignarse a ninguna VLAN. Para configurar el puerto del switch F0/5 como un puerto de enlace troncal, ejecute el comando **switchport mode trunken** el modo de configuración de la interfaz para el puerto F0/5.

Nota: el router no admite el protocolo de enlace troncal dinámico (DTP), que es utilizado por los switches, por lo que no pueden usarse los siguientes comandos:**switchport mode dynamic auto o switchport mode dynamic desirable**.

Ahora se puede configurar el router para que realice routing entre VLAN.

Configuración del enruteamiento entre VLAN del router-on-a-stick



Cuando se utiliza una configuración de router-on-a-stick, la configuración del router es diferente en comparación con el routing entre VLAN antiguo. En la ilustración se muestra que hay varias subinterfaces configuradas.

Cada subinterfaz se crea con el comando **interface id_interface id_subinterfaz** en el modo de configuración global. La sintaxis para la subinterfaz es la interfaz física, en este caso **g0/0**, seguida de un punto y un número de subinterfaz. El número de subinterfaz es configurable, pero en general refleja el número de VLAN. En este ejemplo, las subinterfaces utilizan los números **10** y **30** como números de subinterfaz para que sea más fácil recordar las VLAN con las que están asociadas. La subinterfaz GigabitEthernet0/0.10 se crea con el comando **interface g0/0.10** del modo de configuración global.

Antes de asignar una dirección IP a una subinterfaz, es necesario configurar la subinterfaz para que funcione en una VLAN específica mediante el comando **encapsulation dot1q VLAN_id**. En este ejemplo, la subinterfaz G0/0.10 se asignó a la VLAN 10.

Nota: hay una opción de palabra clave **native** que se puede agregar a este comando para establecer la VLAN nativa IEEE 802.1Q. En este ejemplo, la opción de palabra clave **native** se excluyó para dejar el valor predeterminado de VLAN nativa a la VLAN 1.

A continuación, asigne la dirección IP para la subinterfaz mediante el comando **ip address dirección_ip máscara_subred** en el modo de configuración de subinterfaz. En este ejemplo, la subinterfaz G0/0.10 se asignó a la dirección IP 172.17.10.1 mediante el comando **ip address 172.17.10.1 255.255.255.0**.

Este proceso se repite para todas las subinterfaces del router necesarias para el enruteamiento entre las VLAN configuradas en la red. Es necesario asignar una dirección IP a cada subinterfaz

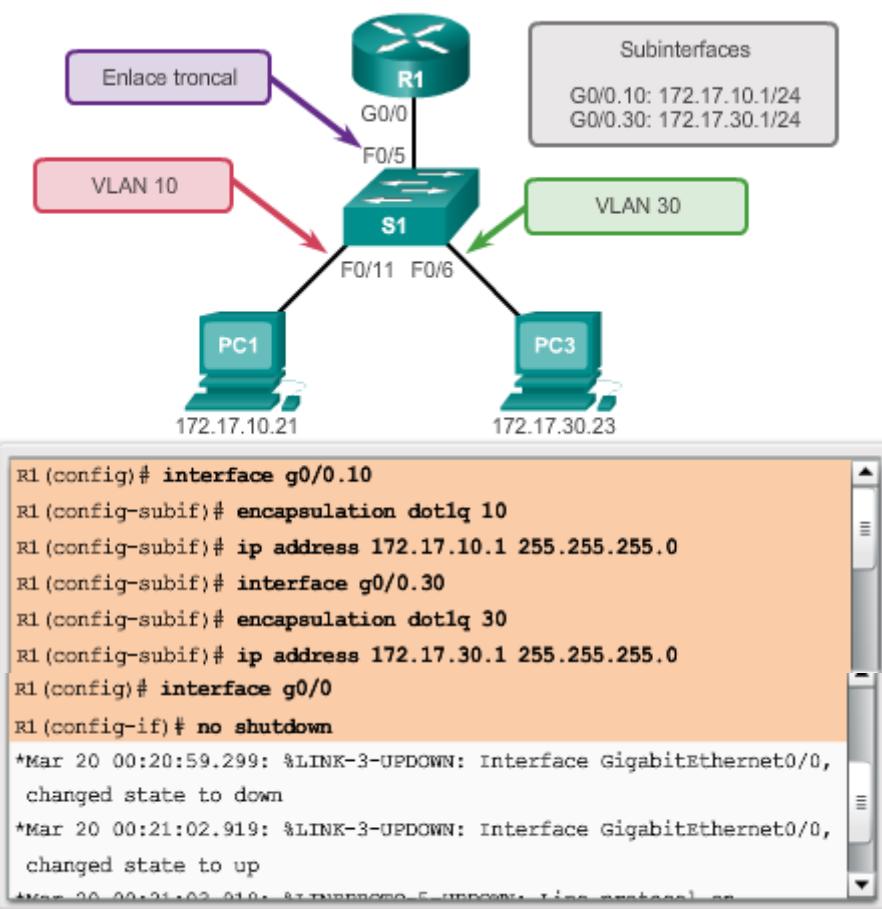
del router en una subred única para que se produzca el routing. En este ejemplo, se configuró la otra subinterfaz del router (G0/0.30) con la dirección IP 172.17.30.1, que está en una subred diferente que la subinterfaz G0/0.10.

Una vez que se configuran las subinterfaces, es necesario habilitarlas.

A diferencia de las interfaces físicas, las subinterfaces no se habilitan con el comando **no shutdown** en el nivel del modo de configuración de subinterfaz del software IOS de Cisco. Introducir el comando **no shutdown** en el nivel de subinterfaz no tiene ningún efecto. En cambio, cuando se habilita la interfaz física con el comando **no shutdown**, todas las subinterfaces configuradas se habilitan. De manera similar, si la interfaz física está deshabilitada, todas las subinterfaces están deshabilitadas. En este ejemplo, en el modo de configuración de interfaz se introduce el comando **no shutdown** para la interfaz G0/0, lo que, a su vez, habilita todas las subinterfaces configuradas.

Las subinterfaces individuales pueden desactivarse administrativamente con el comando **shutdown**.

Configuración del enruteamiento entre VLAN del router-on-a-stick



Los routers Cisco están configurados de manera predeterminada para enrutar el tráfico entre subinterfaces locales. Por lo tanto, no es necesario que esté habilitado el enruteamiento.

En la figura 1, el comando **show vlans** muestra información sobre las subinterfaces VLAN del IOS de Cisco. El resultado muestra las dos subinterfaces VLAN, GigabitEthernet0/0.10 y GigabitEthernet0/0.30.

A continuación, examine la tabla de routing con el comando **show ip route**(figura 2). En el ejemplo, las rutas definidas en la tabla de routing indican que están asociadas a subinterfaces específicas, en lugar de interfaces físicas separadas. Hay dos rutas en la tabla de routing: una ruta va a la subred 172.17.10.0, que está conectada a la subinterfaz local G0/0.10; la otra ruta va a la subred 172.17.30.0, que está conectada a la subinterfaz local G0/0.30. El router utiliza la tabla de enrutamiento para determinar dónde enviar el tráfico que recibe. Por ejemplo, si el router recibe un paquete en la subinterfaz G0/0.10 destinado a la subred 172.17.30.0, identificará que debe enviar el paquete por la subinterfaz G0/0.30 para que llegue a los hosts en la subred 172.17.30.0.

En la figura 3, utilice el verificador de sintaxis para configurar y verificar router-on-a-stick en el R1.

```
R1# show vlans
<resultado omitido>
Virtual LAN ID: 10 (IEEE 802.1Q Encapsulation)
  VLAN Trunk Interface: GigabitEthernet0/0.10
    Protocols Configured: Address: Received: Transmitted:
      IP           172.17.10.1     11        18
<resultado omitido>
Virtual LAN ID: 30 (IEEE 802.1Q Encapsulation)
  VLAN Trunk Interface: GigabitEthernet0/0.30
    Protocols Configured: Address: Received: Transmitted:
      IP           172.17.30.1     11         8
<resultado omitido>
```

Tabla de routing de router-on-a-stick

```
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 - LISPs
      + - replicated route, % - next hop override

Gateway of last resort is not set

      172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C    172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L    172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C    172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L    172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

Después de configurar el router y el switch para llevar a cabo routing entre VLAN, el siguiente paso es verificar la conectividad de host a host. El acceso a los dispositivos en las VLAN remotas puede probarse con el comando **ping**.

En el ejemplo que se muestra en la ilustración, se inician los comandos **ping y tracert** desde la PC1 hasta la dirección de destino de la PC3.

Prueba de ping

El comando **ping** envía una solicitud de eco ICMP a la dirección de destino. Cuando un host recibe una solicitud de eco del ICMP, éste responde con una respuesta de eco del ICMP para confirmar que recibió dicha solicitud. El comando **ping** calcula el tiempo transcurrido, para lo cual utiliza la diferencia de tiempo entre el momento en que se envió la solicitud de eco y el momento en que se recibió la respuesta de eco. El tiempo transcurrido se utiliza para determinar la latencia de la conexión. Al recibir una respuesta con éxito, confirma que existe una ruta entre el dispositivo emisor y el dispositivo receptor.

Prueba de tracert

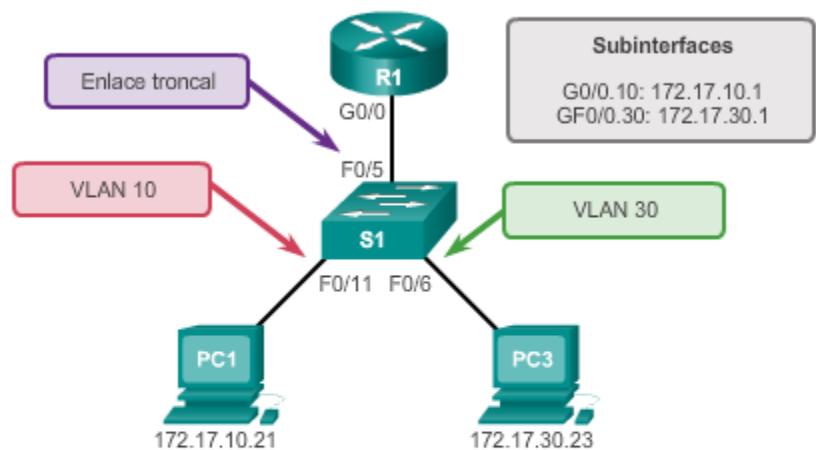
Tracert es una utilidad práctica usada para confirmar la ruta enrutada tomada entre dos dispositivos. En los sistemas UNIX, la utilidad se especifica como **traceroute**. Tracert también utiliza el ICMP para determinar la ruta tomada, pero utiliza las solicitudes de eco del ICMP con valores de tiempo de vida específicos definidos en la trama.

El valor de tiempo de vida determina con exactitud la cantidad de saltos del router que el eco del ICMP puede alcanzar. La primera solicitud de eco del ICMP se envía con un valor de tiempo de vida configurado para expirar en el primer router en la ruta hacia el dispositivo de destino.

Cuando se excede el tiempo de espera de la solicitud de eco ICMP en la primera ruta, se reenvía un mensaje ICMP desde el router hasta el dispositivo de origen. El dispositivo registra la respuesta desde el router y procede a enviar otra solicitud de eco del ICMP, pero esta vez con un valor de tiempo de vida mayor. Esto permite a la solicitud de eco del ICMP atravesar el primer router y llegar al segundo dispositivo en la ruta hacia el destino final. El proceso se repite de manera recursiva hasta que, finalmente, se envía la solicitud de eco ICMP hacia el dispositivo de destino final. Una vez que la utilidad **tracert** termina de ejecutarse, se muestra una lista de las interfaces de entrada del router alcanzadas por la solicitud de eco ICMP en camino al destino.

En el ejemplo, la utilidad **ping** pudo enviar una solicitud de eco ICMP a la dirección IP de la PC3. Además, la utilidad **tracert** confirma que el camino a la PC3 es a través de la dirección IP de la subinterfaz 172.17.10.1 del router R1.

Configuración del enruteamiento entre VLAN del router-on-a-stick



```
PC1> ping 172.17.30.23
Pinging 172.17.30.23 with 32 bytes of data:
Reply from 172.17.30.23: bytes=32 time=17ms TTL=127
Reply from 172.17.30.23: bytes=32 time=15ms TTL=127
Reply from 172.17.30.23: bytes=32 time=18ms TTL=127
Reply from 172.17.30.23: bytes=32 time=19ms TTL=127

Ping statistics for 172.17.30.23:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 15ms, Maximum = 19ms, Average = 17ms

PC1> tracert 172.17.30.23
Tracing route to 172.17.30.23 over a maximum of 30 hops:
  1  9 ms       7 ms       9 ms      172.17.10.1
  2  16 ms      15 ms      16 ms     172.17.30.23

Trace complete.
```

5.3 Resolución de problemas de routing entre VLAN

5.3.1 Problemas de configuración entre VLAN

Hay varias configuraciones de switch incorrectas comunes que puede producirse al configurar el routing entre varias VLAN.

Al utilizar el modelo de routing antiguo para routing entre VLAN, asegúrese de que los puertos del switch que se conectan a las interfaces del router estén configurados en las VLAN correctas. Si un puerto de switch no está configurado para la VLAN adecuada, los dispositivos configurados en esa VLAN no se pueden conectar a la interfaz del router, por lo que dichos dispositivos no pueden enviar datos a las demás VLAN.

Como se puede ver en la topología de la figura 1, la PC1 y la interfaz G0/0 del router R1 están configuradas en la misma subred lógica, como lo indica su asignación de dirección IP. Sin embargo, el puerto de switch F0/4 que se conecta a la interfaz G0/0 del router R1 no está configurado y permanece en la VLAN predeterminada. Dado que el router R1 está en una VLAN diferente que PC1, no pueden comunicarse.

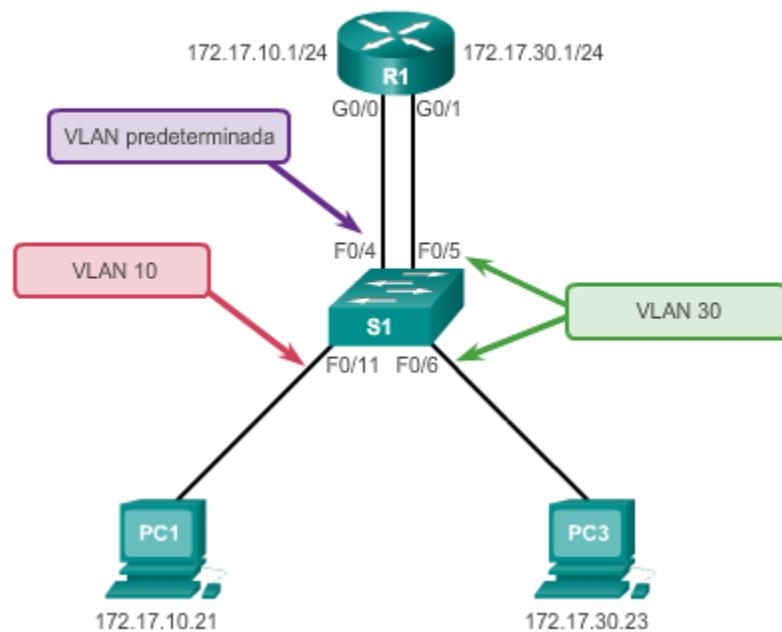
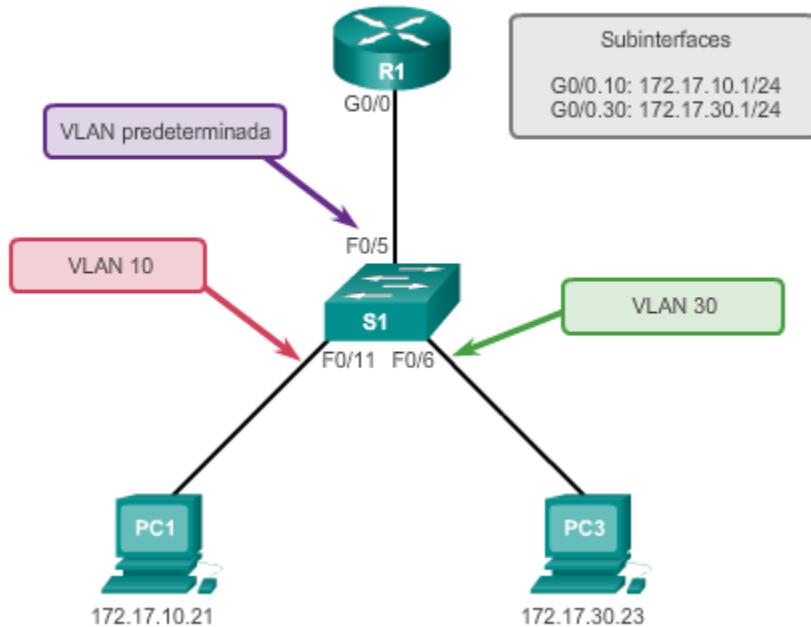
Para corregir este problema, ejecute el comando **switchport access vlan 10** en el modo de configuración de interfaz para el puerto de switch F0/4 en el switch S1. Cuando el puerto del switch se configura para la VLAN correcta, la PC1 puede comunicarse con la interfaz G0/0 del router R1, que le permite acceder a las otras VLAN conectadas al router R1.

La topología de la figura 2 muestra el modelo de routing router-on-a-stick. Sin embargo, la interfaz F0/5 en el switch S1 no está configurada como enlace troncal y queda en la VLAN predeterminada para el puerto. Como resultado, el router no puede realizar enrutamiento entre las VLAN, porque cada una de las subinterfaces configuradas no puede enviar ni recibir el tráfico con etiquetas de VLAN.

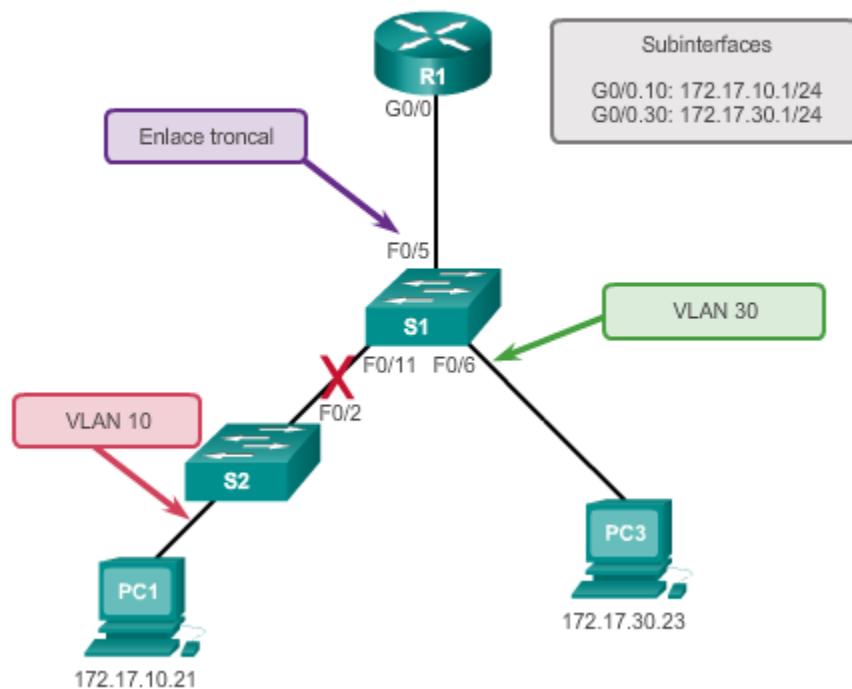
Para corregir este problema, emita el comando **switchport mode trunk** en el modo de configuración de interfaz para el puerto del switch F0/5 en el switch S1. Esto convierte a la interfaz en un puerto de enlace troncal, lo que permite que se establezca un enlace troncal entre el R1 y el S1. Una vez que el enlace troncal se establece correctamente, los dispositivos conectados a cada una de las VLAN pueden comunicarse con la subinterfaz asignada a su VLAN, lo que permite el routing entre VLAN.

En la topología de la figura 3 se muestra que el enlace troncal entre el S1 y S2 está inactivo. Dado que no hay una conexión o ruta redundante entre los dispositivos, ninguno de los dispositivos conectados al S2 puede llegar al router R1. Como resultado, ninguno de los dispositivos conectados al S2 puede realizar enrutamiento a otras VLAN a través del R1.

Para reducir el riesgo de una falla en el enlace entre switches que interrumpe el routing entre VLAN, se deben tener en cuenta enlaces redundantes y rutas alternativas en el diseño de red.

Problemas de configuración del switch**Problemas de configuración del switch**

Problemas de configuración del switch



Cuando sospeche que hay un problema con una configuración del switch, utilice los distintos comandos de verificación para examinar la configuración e identificar el problema.

En el resultado de pantalla de la figura 1, se muestran los resultados de los comandos **show interfaces id-interfaz switchport**. Supongamos que ejecutó estos comandos porque sospecha que la VLAN 10 no se asignó al puerto F0/4 en el switch S1. En el área superior resaltada se muestra que el puerto F0/4 en el switch S1 está en modo de acceso, pero no se muestra que se haya asignado directamente a la VLAN 10. En el área inferior resaltada se confirma que el puerto F0/4 todavía está establecido en la VLAN predeterminada. Los comandos **show running-config** y **show interface id-interfaz switchport** son útiles para identificar problemas de asignación de VLAN y de configuración de puertos.

En la figura 2 se muestra que la comunicación entre el router R1 y el switch S1 se interrumpió después de modificar la configuración de un dispositivo. Se supone que el enlace entre el router y el switch es un enlace troncal. En el resultado de pantalla, se muestran los resultados de los comandos **show interface id_interfaz switchport** y **show running-config**. El área superior resaltada confirma que el puerto F0/4 en el switch S1 está en el modo de acceso, no en el modo de enlace troncal. El área inferior resaltada también confirma que el puerto F0/4 se configuró para el modo de acceso.

Comandos IOS del switch

```
S1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<resultado omitido>
S1#
```

```
S1# show interfaces f0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
<resultado omitido>
S1#
S1# show run
Building configuration...

<resultado omitido>
!
interface FastEthernet0/4
switchport mode access
!

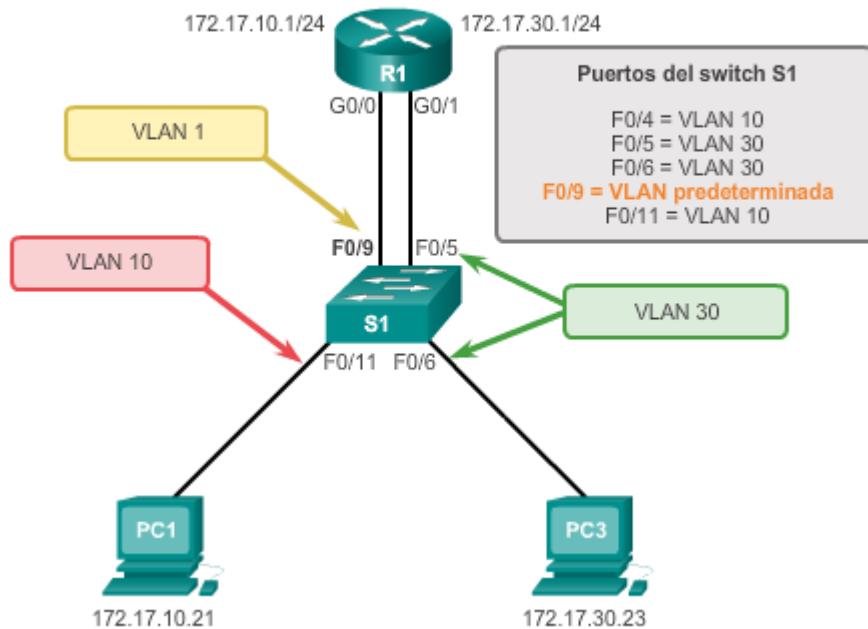
<resultado omitido>
S1#
```

Al habilitar el routing entre VLAN en un router, uno de los errores de configuración más comunes es conectar la interfaz física del router al puerto de switch incorrecto. Esto ubica la interfaz del router en la VLAN incorrecta y evita que alcance otros dispositivos dentro de la misma subred.

Como se muestra en la ilustración, la interfaz G0/0 del router R1 está conectada al puerto F0/9 del switch S1. El puerto de switch F0/9 está configurado para la VLAN predeterminada, no para la VLAN 10. Esto evita que la PC1 pueda comunicarse con la interfaz del router. Por lo tanto, no puede realizar enrutamiento hacia la VLAN 30.

Para corregir este problema, conecte físicamente la interfaz G0/0 del router R1 al puerto F0/4 del switch S1. Esto ubica la interfaz del router en la VLAN correcta y permite el routing entre VLAN. Alternativamente, cambie la asignación de VLAN del puerto de switch F0/9 a la VLAN 10. Esto también permite que la PC1 se comunique con la interfaz G0/0 del router R1.

Problemas de configuración del router



Con configuraciones de router-on-a-stick, un problema común es asignar una ID de VLAN incorrecta a la subinterfaz.

Como se muestra en la figura 1, el router R1 se configuró con la VLAN incorrecta en la subinterfaz G0/0.10, lo que evita que los dispositivos configurados en la VLAN 10 se comuniquen con la subinterfaz G0/0.10. Esto, a la vez, evita que dichos dispositivos puedan enviar datos a otras VLAN en la red.

El uso de los comandos **show interfaces** y **show running-config** puede ser útil para la resolución de problemas de este tipo, tal como se muestra en la ilustración.

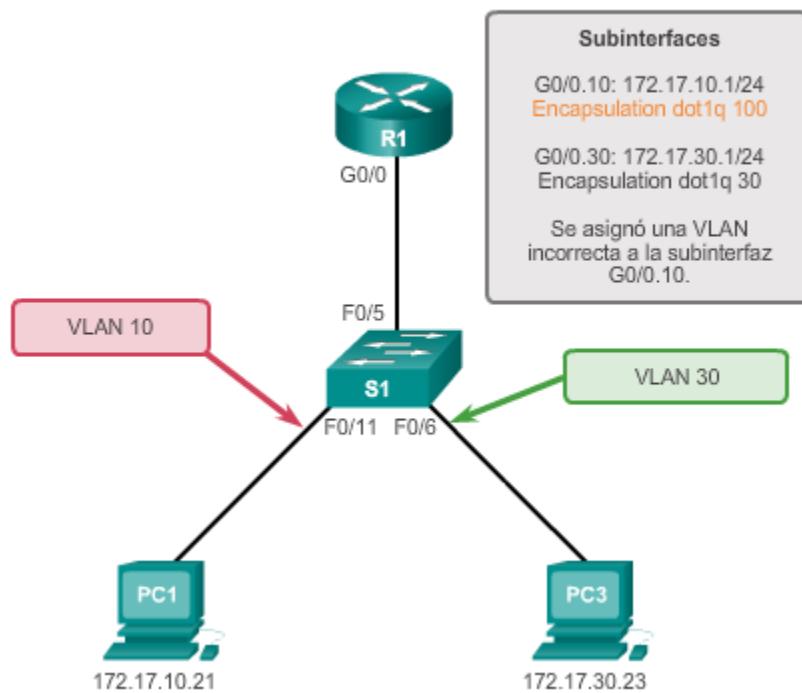
El comando **show interfaces** genera muchos resultados, lo que a veces dificulta encontrar el problema, tal como se muestra en la figura 2. Sin embargo, en la sección superior resaltada muestra que la subinterfaz G0/0.10 en el router R1 utiliza la VLAN 100.

El comando **show running-config** confirma que la subinterfaz G0/0.10 en el router R1 se configuró para permitir el acceso al tráfico de la VLAN 100 y no al de la VLAN 10.

Para corregir este problema, configure la subinterfaz G0/0.10 para que esté en la VLAN correcta mediante el comando **encapsulation dot1q 10** en el modo de configuración de subinterfaz. Una vez asignada la subinterfaz a la VLAN correcta, los dispositivos en esa VLAN pueden acceder a ella, y el router puede realizar routing entre VLAN.

Con la correcta verificación, los problemas de configuración del router se resuelven rápidamente, lo que permite que el routing entre VLAN funcione de forma adecuada.

Problemas de configuración del router



Verificar la configuración del router

```
R1# show interface
<resultado omitido>
GigabitEthernet0/0.10 is up, line protocol is down (disabled)
  Encapsulation 802.1Q virtual Lan,vlan ID 100
    ARP type :ARPA, ARP Timeout 04:00:00,
    Last clearing of "show interface" counters never
<resultado omitido>
R1#
R1# show run
Building configuration...
Current configuration : 505 bytes
<resultado omitido>
!
interface GigabitEthernet0/0.10
  encapsulation dot1q 100
  ip address 172.17.10.1 255.255.255.0
!
interface GigabitEthernet0/0.30
```

5.3.2 Problemas de direccionamiento IP

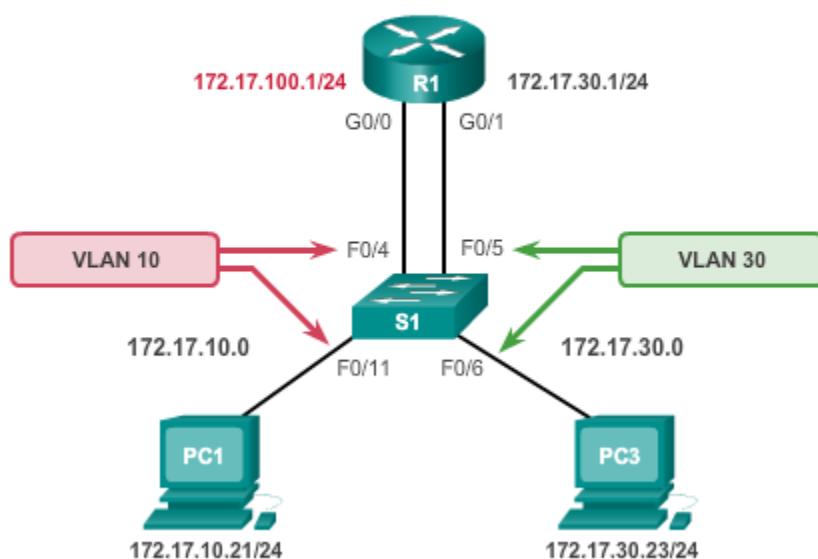
Las VLAN corresponden a subredes únicas en la red. Para que el routing entre VLAN funcione, es necesario conectar un router a todas las VLAN, ya sea por medio de interfaces físicas separadas o subinterfaces. A cada interfaz o subinterfaz se le debe asignar una dirección IP que corresponda a

la subred a la cual está conectada. Esto permite que los dispositivos en la VLAN se comuniquen con la interfaz del router y habilita el routing del tráfico a otras VLAN conectadas al router.

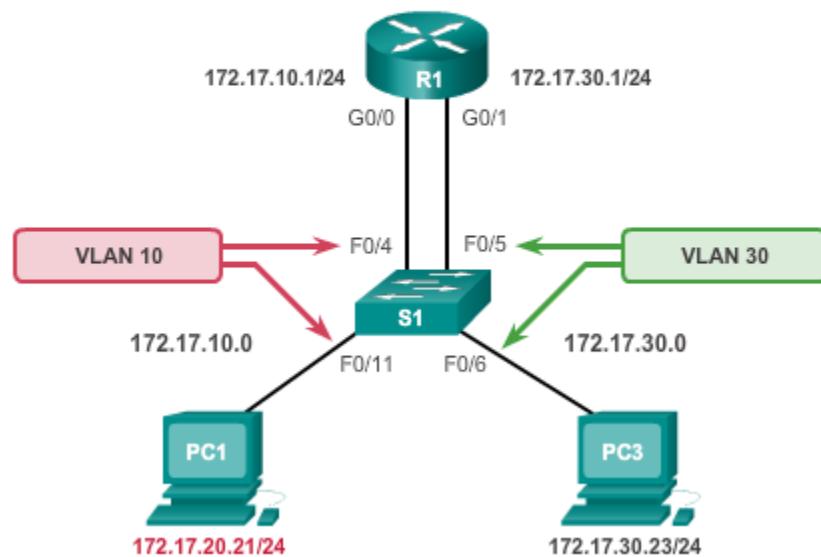
Los siguientes son algunos errores comunes de direccionamiento IP:

- Como se muestra en la figura 1, el router R1 se configuró con la dirección IP incorrecta en la interfaz G0/0. Esto evita que la PC1 pueda comunicarse con el router R1 en la VLAN 10. Para corregir este problema, asigne la dirección IP correcta a la interfaz G0/0 del router R1 mediante el comando **ip address 172.17.100.1 255.255.255.0**. Una vez asignada la interfaz del router a la dirección IP correcta, la PC1 puede utilizar la interfaz del router como gateway predeterminado para acceder a otras VLAN.
- En la figura 2, la PC1 se configuró con la dirección IP incorrecta para la subred asociada con la VLAN 10. Esto evita que la PC1 pueda comunicarse con el router R1 en la VLAN 10. Para corregir este problema, asigne la dirección IP correcta a PC1. Según el tipo de computadora que utilice, los detalles de configuración pueden ser diferentes.
- En la figura 3, la PC1 se configuró con la máscara de subred incorrecta. Según la máscara de subred configurada para PC1, PC1 está en la red 172.17.0.0. El resultado es que la PC1 calcula que la PC3, con la dirección IP 172.17.30.23, se encuentra en la misma subred que la PC1. La PC1 no reenvía el tráfico destinado a la PC3 a la interfaz G0/0 del router R1, por lo tanto, el tráfico nunca llega a la PC3. Para corregir este problema, cambie la máscara de subred en PC1 a 255.255.255.0. Según el tipo de computadora que utilice, los detalles de configuración pueden ser diferentes.

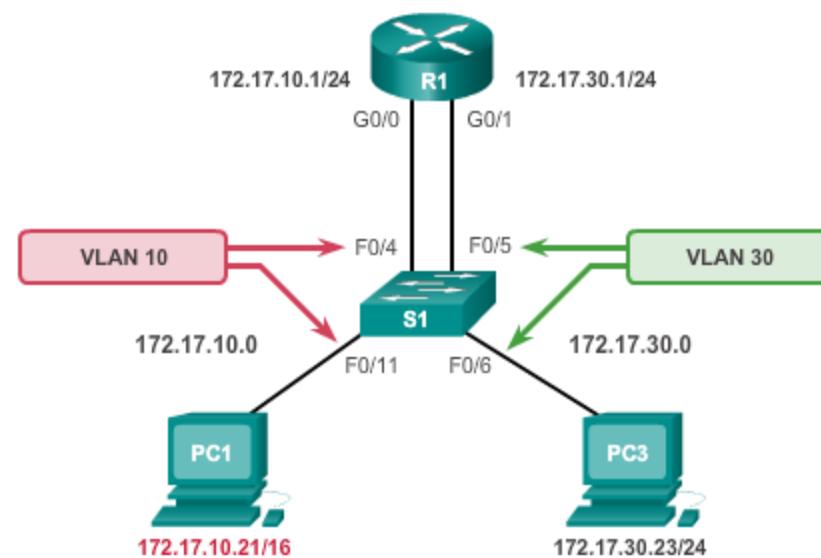
Topología 1



Topología 2



Topología 3



A cada interfaz o subinterfaz se le debe asignar una dirección IP que corresponda a la subred a la cual está conectada. Un error común es configurar incorrectamente una dirección IP para una subinterfaz. En la figura 1, se muestra el resultado del comando **show running-config**. El área resaltada muestra que la subinterfaz G0/0.10 en el router R1 tiene la dirección IP 172.17.20.1. La VLAN para esta subinterfaz debería admitir tráfico de la VLAN 10. La dirección IP se configuró de manera incorrecta. El comando **show ip interface** resulta útil en esta configuración. La segunda área resaltada muestra la dirección IP incorrecta.

Algunas veces, el problema es que el dispositivo de usuario final, como una computadora personal, está mal configurado. En la figura 2, se muestra la configuración IP para la PC1 que aparece en pantalla. La dirección IP es 172.17.20.21, con la máscara de subred 255.255.255.0. Sin embargo, en esta situación la PC1 debería estar en la VLAN 10, con la dirección 172.17.10.21 y la máscara de subred 255.255.255.0.

Nota: si bien la configuración de las ID de subinterfaz de manera que coincidan con el número de VLAN facilita la administración de la configuración entre VLAN, no es un requisito. Al trabajar en la resolución de problemas de direccionamiento, asegúrese de que la subinterfaz esté configurada con la dirección correcta para esa VLAN.

Problema del router

```
R1# show run
Building configuration...
<resultado omitido>
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
!
interface GigabitEthernet0/0.10
  encapsulation dot1Q 10
  ip address 172.17.20.1 255.255.255.0
!
interface GigabitEthernet0/0.30
<resultado omitido>
R1#
R1# show ip interface
<resultado omitido>
GigabitEthernet0/0.10 is up, line protocol is up
  Internet address is 172.17.20.1/24
  Broadcast address is 255.255.255.255
<resultado omitido>
R1#
```

Problema del direccionamiento IP de la computadora

```
Packet Tracer PC Command Line 1.0
PC1> ip config
Invalid Command.

PC1> ipconfig

IP Address.....: 172.17.20.21
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 172.17.10.1

PC1>



Esta PC1 debe estar en la subred VLAN 10  

    Entonces, esto debe ser 172.17.10.21, con la máscara de  

    subred 255.255.255.0


```

5.4 Conmutación de capa 3

5.4.1 Funcionamiento y configuración del switching de capa 3

El método router-on-a-stick es fácil de implementar porque los routers suelen estar disponibles en cada red. Como se muestra en la ilustración, la mayoría de las redes empresariales utilizan switches multicapa para obtener altas velocidades de procesamiento de paquetes con switching basado en hardware. Los switches de capa 3 suelen tener un rendimiento de switching de paquetes en el orden de los millones de paquetes por segundo (pps), mientras que los routers tradicionales proporcionan switching de paquetes en el orden de 100 000 a más de 1 millón de pps.

Todos los switches multicapa Catalyst admiten los siguientes tipos de interfaces de capa 3:

Puerto enrutado: una interfaz puramente de capa 3 similar a la interfaz física de un router IOS de Cisco.

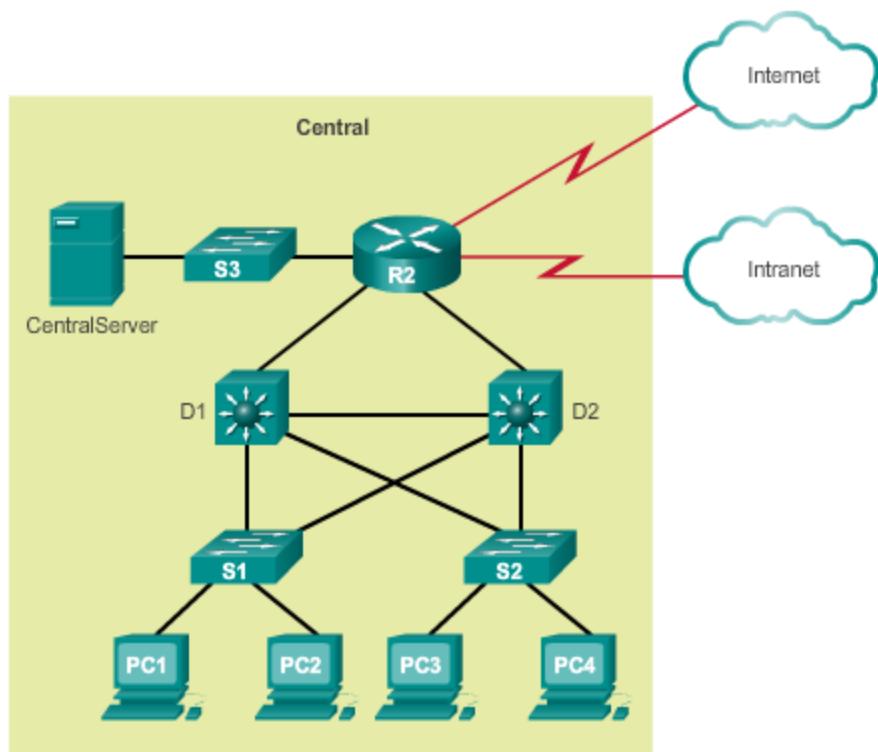
Interfaz virtual del switch (SVI): una interfaz VLAN virtual para routing entre VLAN. En otras palabras, las SVI son las interfaces VLAN enruteadas de manera virtual.

Los switches de alto rendimiento, como el Catalyst 6500 y el Catalyst 4500, realizan casi todas las funciones que incluyen a las capas 3 y superiores del modelo OSI con switching basado en hardware y en Cisco Express Forwarding.

Todos los switches Cisco Catalyst de capa 3 admiten protocolos de routing, pero varios modelos de switches Catalyst requieren un software mejorado para admitir características específicas de protocolos de routing. Los switches de la serie Catalyst 2960 que ejecutan IOS versión 12.2(55) o posterior admiten routing estático.

Los switches Catalyst utilizan diversas configuraciones predeterminadas para las interfaces. Todos los miembros de las familias de switches Catalyst 3560 y 4500 utilizan interfaces de capa 2 de

manera predeterminada, mientras que los miembros de la familia de switches Catalyst 6500 que ejecutan el IOS de Cisco utilizan interfaces de capa 3 de forma predeterminada. Las configuraciones de interfaz predeterminadas no aparecen en la configuración de inicio o en ejecución. Según la familia de switches Catalyst que se utilice, es posible que los comandos **switchport** o **no switchport** del modo de configuración de interfaz estén presentes en los archivos de configuración en ejecución o de configuración de inicio.



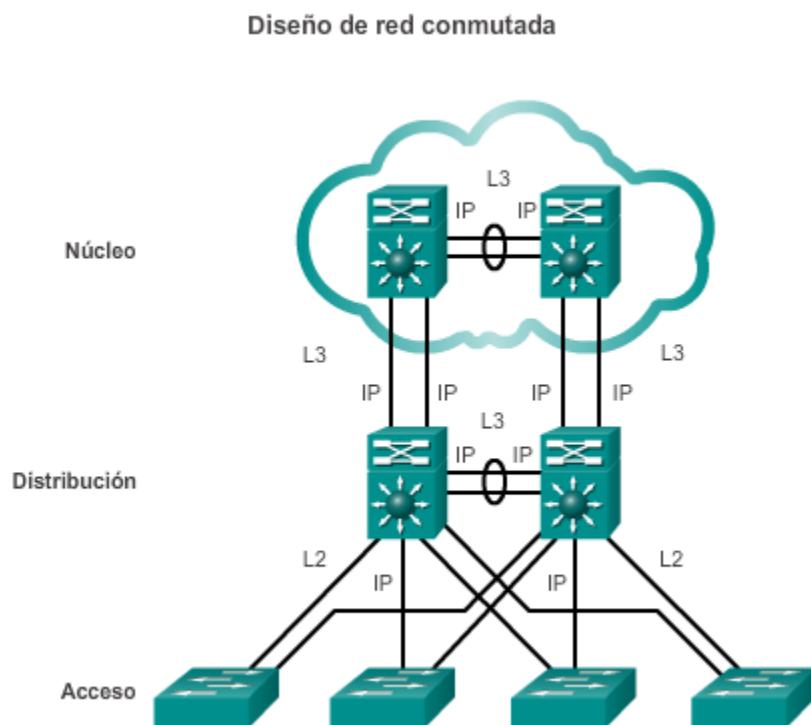
En los comienzos de las redes conmutadas, el switching era rápido (a menudo, tenía la velocidad del hardware, es decir que la velocidad era equivalente al tiempo físico que tomaba recibir las tramas y reenviarlas a otros puertos) y el routing era lento (debía procesarse mediante software). Esto hizo que los diseñadores de redes ampliaran la porción conmutada de la red al máximo posible. El acceso, la distribución y las capas de núcleo solían configurarse para comunicarse en la capa 2, pero esta topología generaba problemas de bucles. Para resolver estos problemas, se utilizaron tecnologías de árbol de expansión a fin de prevenir los bucles sin necesidad de renunciar a la flexibilidad y la redundancia de las conexiones entre switches.

Sin embargo, a medida que las tecnologías de redes evolucionaron, el routing se volvió más rápido y económico. Hoy en día, el routing se puede llevar a cabo a la velocidad del hardware. Una consecuencia de esta evolución es que el routing se puede transferir a las capas de núcleo y de distribución sin afectar el rendimiento de la red.

Muchos usuarios están en VLAN separadas, y cada VLAN suele ser una subred distinta. Por lo tanto, resulta lógico configurar los switches de distribución como gateways de capa 3 para los usuarios de la VLAN de cada switch de acceso. Esto significa que cada switch de distribución debe tener direcciones IP que coincidan con la VLAN de cada switch de acceso.

Los puertos de capa 3 (enrutados) se suelen implementar entre la capa de distribución y la capa de núcleo.

La arquitectura de red representada no depende del árbol de expansión, porque no existen bucles físicos en la porción de capa 2 de la topología.



Una SVI es una interfaz virtual configurada en un switch multicapa, como se muestra en la ilustración. Se puede crear una SVI para cualquier VLAN que exista en el switch. Una SVI se considera virtual porque no hay un puerto físico dedicado a la interfaz. Puede realizar las mismas funciones para la VLAN que una interfaz del router y puede configurarse de manera similar a una interfaz tal (es decir, dirección IP, ACL de entrada y de salida, etcétera). La SVI para la VLAN proporciona procesamiento de capa 3 para los paquetes que provienen de todos los puertos de switch asociados a dicha VLAN o que se dirigen a ella.

De manera predeterminada, se crea una SVI para la VLAN predeterminada (VLAN 10) a fin de permitir la administración remota del switch. Las SVI adicionales deben crearse de forma explícita. Las SVI se crean la primera vez que se ingresa al modo de configuración de interfaz de VLAN para una SVI de VLAN en particular, por ejemplo, cuando se introduce el comando **interface vlan 10**. El número de VLAN utilizado se corresponde con la etiqueta VLAN asociada con las tramas de datos en un enlace troncal encapsulado 802.1Q o bien con la ID de VLAN (VID) configurada para un puerto de acceso. Al crear una SVI como gateway para la VLAN 10, nombre "VLAN 10" a la interfaz SVI. Configure y asigne una dirección IP a cada SVI de VLAN.

Al crear una SVI, asegúrese de que esa VLAN en particular esté presente en la base de datos de VLAN. En la ilustración, el switch debe tener presentes las VLAN 10 y VLAN 20 en la base de datos de VLAN, de lo contrario, la interfaz SVI permanece desactivada.

A continuación se detallan algunos de los motivos para configurar una SVI:

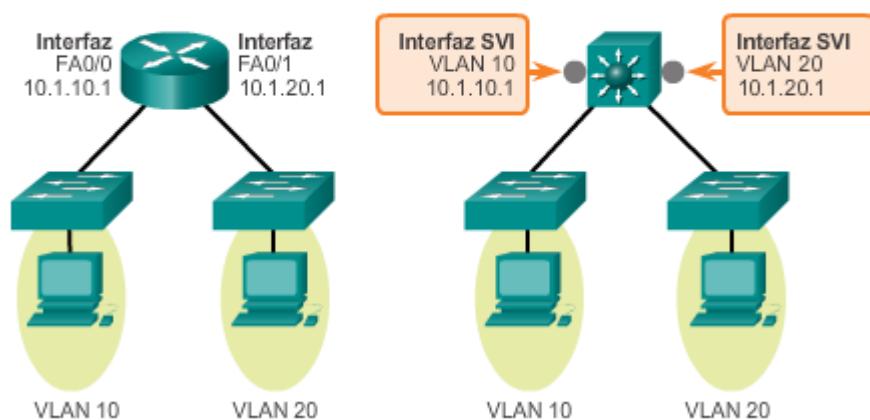
- Para proporcionar un gateway a una VLAN a fin de poder enrutar el tráfico dentro o fuera de esa VLAN.

- Para proporcionar conectividad IP de capa 3 al switch.
- Para admitir las configuraciones de puente y de protocolo de routing.

A continuación, se detallan algunas de las ventajas de las SVI (la única desventaja es que los switches multicapa son más costosos):

- Es mucho más veloz que router-on-a-stick, porque todo el switching y el routing se realizan por hardware.
- El routing no requiere enlaces externos del switch al router.
- No se limita a un solo enlace. Se pueden utilizar EtherChannels de capa 2 entre los switches para obtener más ancho de banda.
- La latencia es mucho menor, porque no hace falta que salga del switch.

Interfaz virtual de switch



Puertos enrutados y puertos de acceso en switches

Un puerto enrutado es un puerto físico que funciona de manera similar a una interfaz en un router. A diferencia de los puertos de acceso, los puertos enrutados no se asocian a una VLAN determinada. Los puertos enrutados se comportan como una interfaz del router normal. Además, debido a la eliminación de la funcionalidad de capa 2, los protocolos de capa 2 (tales como STP), no funcionan en interfaces enrutadas. Sin embargo, algunos protocolos, como LACP y EtherChannel, funcionan en la capa 3.

A diferencia de los routers IOS de Cisco, los puertos enrutados en un switch IOS de Cisco no admiten subinterfaces.

Los puertos enrutados se utilizan para enlaces punto a punto. Las conexiones de routers WAN y dispositivos de seguridad son ejemplos del uso de puertos enrutados. En una red conmutada, los

puertos enrutados se suelen configurar entre los switches de las capas de núcleo y de distribución. En la ilustración, se muestra un ejemplo de puertos enrutados en una red comutada de campus.

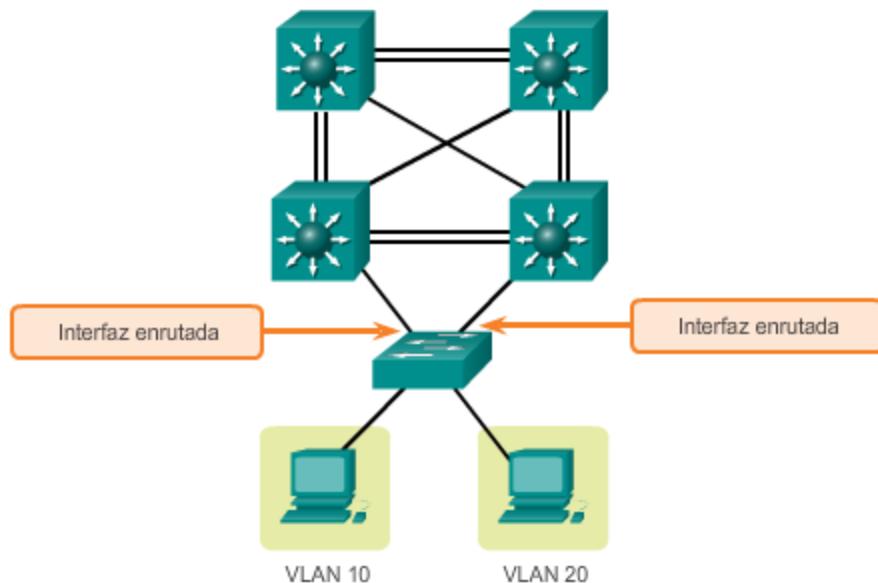
Para configurar los puertos enrutados, utilice el comando **no switchport** del modo de configuración de interfaz en los puertos adecuados. Por ejemplo, la configuración predeterminada de las interfaces en los switches Catalyst 3560 es de interfaces de capa 2, por lo que se deben configurar de forma manual como puertos enrutados. Además, asigne una dirección IP y otros parámetros de capa 3, según sea necesario. Después de asignar la dirección IP, verifique que el routing IP esté habilitado de manera global y que los protocolos de routing aplicables estén configurados.

A continuación, se detallan algunas de las ventajas de los puertos enrutados:

- Los switches multicapa puede tener tanto una SVI como puertos enrutados en un mismo switch.
- Los switches multicapa reenvían el tráfico de capa 2 o capa 3 mediante hardware, lo que contribuye a un routing más veloz.

Nota: los switches de la serie Catalyst 2960 no admiten puertos enrutados.

Puertos enrutados



Un switch Catalyst 2960 puede funcionar como un dispositivo de capa 3 y realizar enrutamiento entre VLAN y una cantidad limitada de rutas estáticas.

Switch Database Manager (SDM) de Cisco proporciona varias plantillas para el switch 2960. Las plantillas pueden habilitarse para admitir funciones específicas según el modo en que se utilice el switch en la red. Por ejemplo, la plantilla lanbase-routing de SDM se puede habilitar para permitir que el switch realice enrutamiento entre VLAN y admita el routing estático.

En la figura 1, se introduce el comando **show sdm prefer** en el switch S1 y se aplica la plantilla predeterminada. La plantilla predeterminada es la configuración predeterminada de fábrica de los switches Catalyst 2960. La plantilla predeterminada no admite routing estático. Si se habilitó el direccionamiento IPv6, la plantilla será dual-ipv4-and-ipv6 default.

La plantilla SDM se puede cambiar en el modo de configuración global con el comando **sdm prefer**.

Nota: en las figuras 2, 4, 6 y 7, el comando **do** se utiliza para ejecutar comandos de los modos EXEC del usuario o EXEC privilegiado desde otros modos de configuración del router.

En la figura 2, las opciones de plantillas SDM se muestran con el comando **sdm prefer?** La plantilla SDM cambia a lanbase-routing. El switch se debe volver a cargar para que la nueva plantilla tenga efecto.

En la figura 3, la plantilla lanbase-routing está activa en el S1. Con esa plantilla, se admite el routing estático para un máximo de 750 rutas estáticas.

En la figura 4, la interfaz F0/6 en el S1 está asignada a la VLAN 2. Las SVI para las VLAN 1 y 2 también se configuraron con las direcciones IP 192.168.1.1/24 y 192.168.2.1/24, respectivamente. El routing IP se habilita con el comando **ip routing** del modo de configuración global.

Nota: el comando **ip routing** se habilita de manera automática en los routers Cisco. Sin embargo, el comando correspondiente para IPv6, **ipv6 unicast-routing**, está deshabilitado de manera predeterminada en los routers y los switches Cisco.

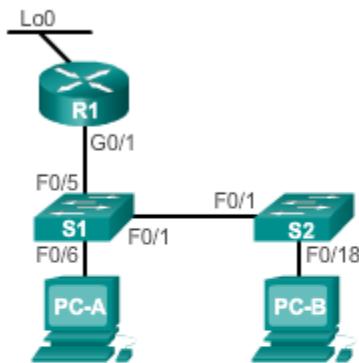
En la figura 5, el router R1 tiene dos redes IPv4 configuradas: la interfaz G0/1 tiene la dirección IP 192.168.1.10/24, y la interfaz loopback Lo0 tiene la dirección IP 209.165.200.225/27. Se muestra el resultado del comando **show ip route**.

En la figura 6, se muestra una ruta predeterminada configurada en el S1. Se muestra el resultado del comando **show ip route**.

En la figura 7, se muestra una ruta estática a la red remota 192.168.2.0/24 (VLAN 2) configurada en el R1. Se muestra el resultado del comando **show ip route**.

En la Figura 8, la PC-A está configurada con la dirección IP 192.168.2.2/24 en la VLAN 2, y la PC-B está configurada con la dirección IP 192.168.1.2/24 en la VLAN 1. La PC-B puede hacer ping a la PC-B y la interfaz loopback en el R1.

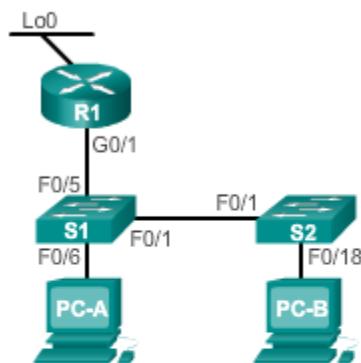
En la figura 9, utilice el verificador de sintaxis para configurar el routing estático en el S1.

Plantilla de Switch Database Manager

```
S1# show sdm prefer
The current template is "default" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

number of unicast mac addresses:          8K
number of IPv4 IGMP groups:              0.25K
number of IPv4/MAC qos aces:             0.125k
number of IPv4/MAC security aces:        0.375k
```

Plantilla de SDM

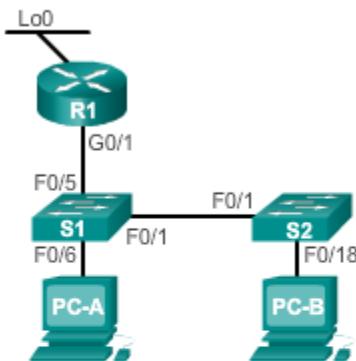


```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# sdm prefer ?
  default          Default bias
  dual-ipv4-and-ipv6  Support both IPv4 and IPv6
  lanbase-routing    Supports both IPv4 and IPv6 Static Routing
  qos               QoS bias

S1(config)# sdm prefer lanbase-routing
Changes to the running SDM preferences have been stored, but cannot
take effect
until the next reload.
Use 'show sdm prefer' to see what SDM preference is currently
active.
Switch(config)# do reload

System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
```

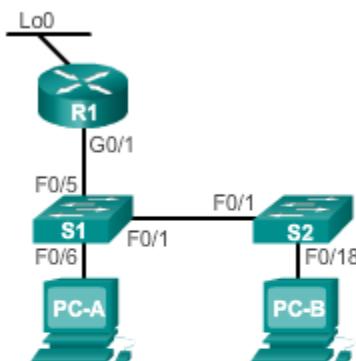
Compatibilidad con rutas estáticas en un switch Catalyst 2960



```
Switch# show sdm prefer
The current template is "lanbase-routing" template.
The selected template optimizes the resources in
the switch to support this level of features for
0 routed interfaces and 255 VLANs.

number of unicast mac addresses: 4K
number of IPv4 IGMP groups + multicast routes: 0.25K
number of IPv4 unicast routes: 0.75K
number of directly-connected IPv4 hosts: 0.75K
```

Habilitación de la funcionalidad de routing IPv4 en un switch Catalyst 2960



```

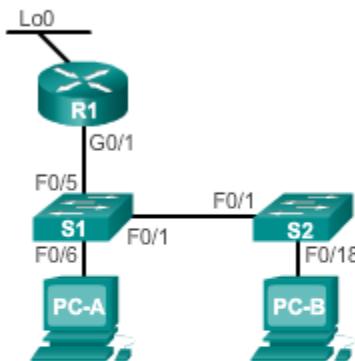
S1(config)# interface f0/6
S1(config-if)# switchport access vlan 2
S1(config-if)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# interface vlan 2
S1(config-if)# ip address 192.168.2.1 255.255.255.0
S1(config-if)# no shutdown
Mar 20 01:00:25.021: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan2, changed state to up
S1(config)# ip routing
S1(config)# do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - EGP, 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,
       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

          192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1
L        192.168.1.1/32 is directly connected, Vlan1
          192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan2
L        192.168.2.1/32 is directly connected, Vlan2

```

Router que participa en routing con un switch

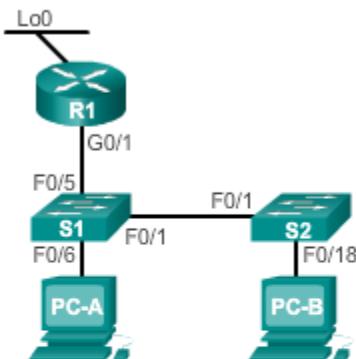


```
R1# show ip route
Codes: L - local, C - static, R - RIP, M - mobile,
      B - EGP, D - EIGRP, EX - EIGRP external, O - OSPF,
      IA - OSPF inter area, N1 - OSPF NSSA external type 1,
      N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
      E2 - OSPF external type 2, i - IS-IS, su - 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,
      U - per-user static route, o - ODR,
      P - periodic downloaded static route, H - NHRP, 1 - LISP
      + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.10/32 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/27 is directly connected, Loopback0
L        209.165.200.225/32 is directly connected, Loopback0
```

Configuración de una ruta estática en un switch Catalyst 2960

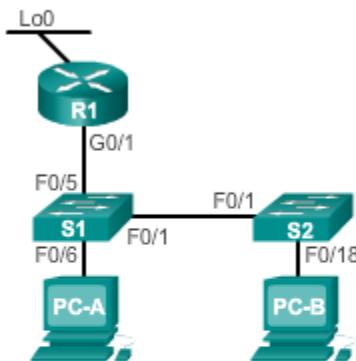


```
S1(config)# ip route 0.0.0.0 0.0.0.0 192.168.1.10
S1(config)# do show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
      B - EGP, D - EIGRP, EX - EIGRP external, O - OSPF,
      IA - OSPF inter area, N1 - OSPF NSSA external type 1,
      N2 - OSPF NSSA external type 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 routes, o - ODR,
      P - periodic downloaded static route, H - NHRP, 1 - LISP
      + - replicated route, % - next hop override

Gateway of last resort is 192.168.1.10 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.1.10
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1
L        192.168.1.1/32 is directly connected, Vlan1
```

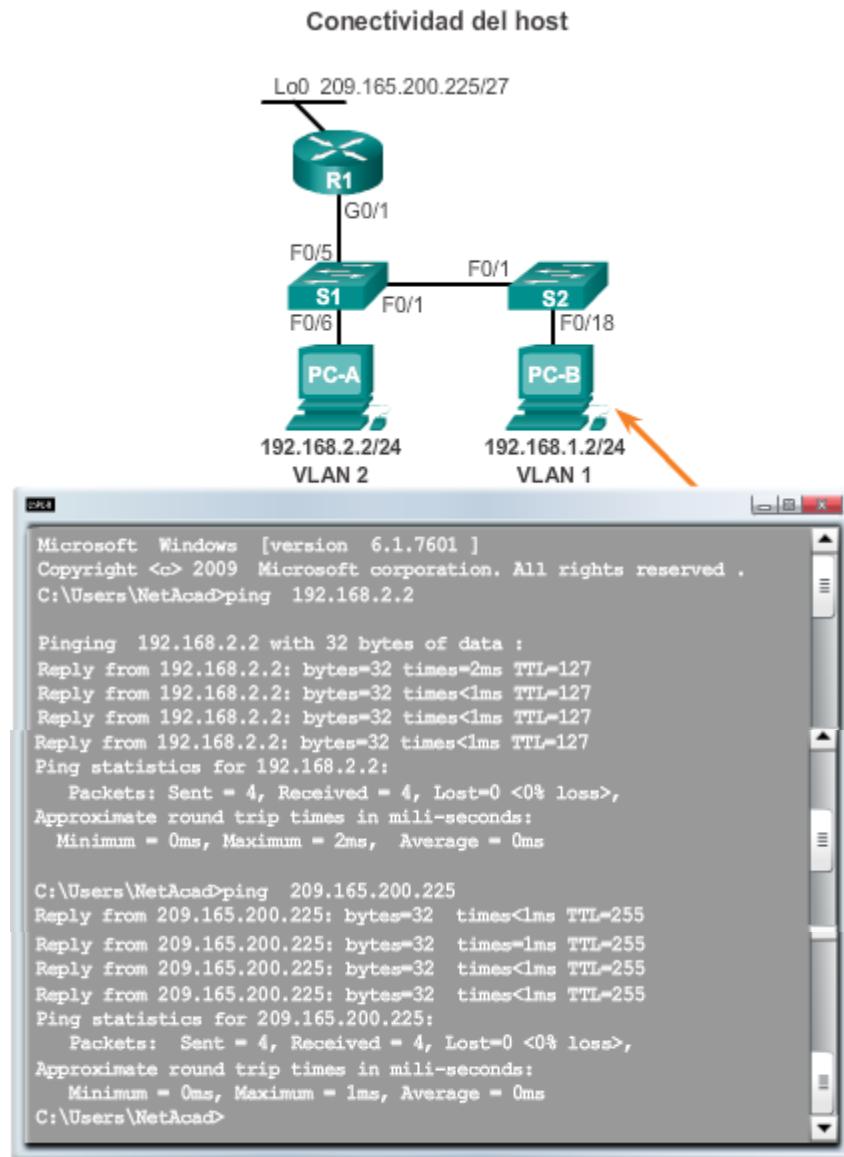
Tabla de routing final en el router



```
R1(config)# ip route 192.168.2.0 255.255.255.0 g0/1
R1(config)# do 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, 1 - LISP
      + - replicated route, % - next hop override

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, GigabitEthernet0/1
L        192.168.1.10/32 is directly connected, GigabitEthernet0/1
S        192.168.2.0/24 is directly connected, GigabitEthernet0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C          209.165.200.224/27 is directly connected, Loopback0
L          209.165.200.225/32 is directly connected, Loopback0
```



5.5 Conmutación de capa 3

5.5.1 Resolución de problemas de switching de capa 3

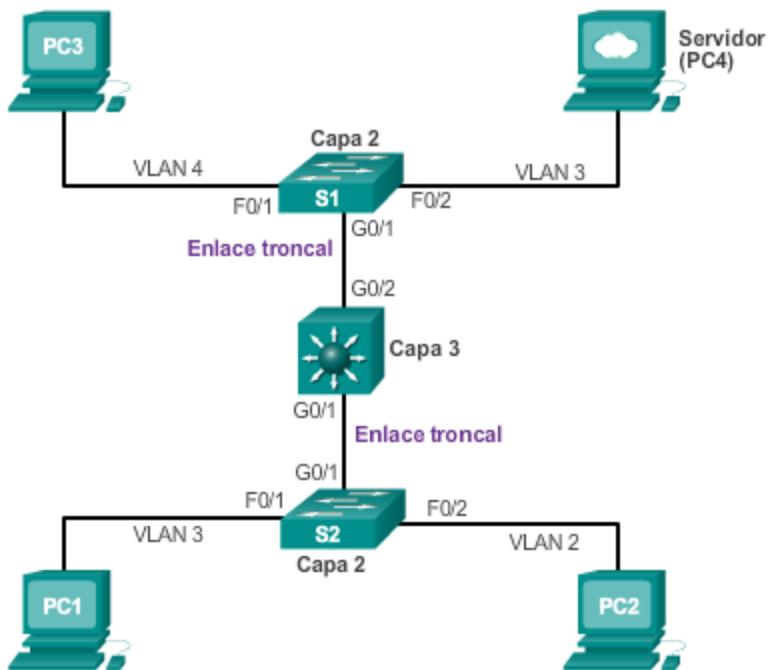
Los problemas comunes al routing entre VLAN antiguo y con router-on-a-stick también se manifiestan en el contexto de switching de capa 3. Para resolver problemas de switching de capa 3, se debe revisar la corrección de los siguientes elementos:

- **VLAN:** las VLAN deben estar definidas en todos los switches. Las VLAN deben estar habilitadas en los puertos de enlace troncal. Los puertos deben estar en las VLAN correctas.
- **SVI:** la SVI debe tener la dirección IP o la máscara de subred correcta. La SVI debe estar activada. La SVI debe coincidir con el número de VLAN.
- **Routing:** el routing debe estar habilitado. Cada interfaz o red debe estar agregada al protocolo de routing.

- **Hosts:** los hosts deben tener la dirección IP o la máscara de subred correcta. Los hosts deben contar con un gateway predeterminado asociado con una SVI o un puerto enruteado.

Para resolver problemas de switching de capa 3, debe familiarizarse con la implementación y el diseño de la disposición de la topología.

Problemas de configuración de switch de capa 3



5.6 Resumen

El enruteamiento inter VLAN es el proceso de tráfico de enruteamiento entre diferentes VLAN, mediante un router dedicado o un switch multicapa. El enruteamiento inter VLAN facilita la comunicación entre los dispositivos aislados por los límites de la VLAN.

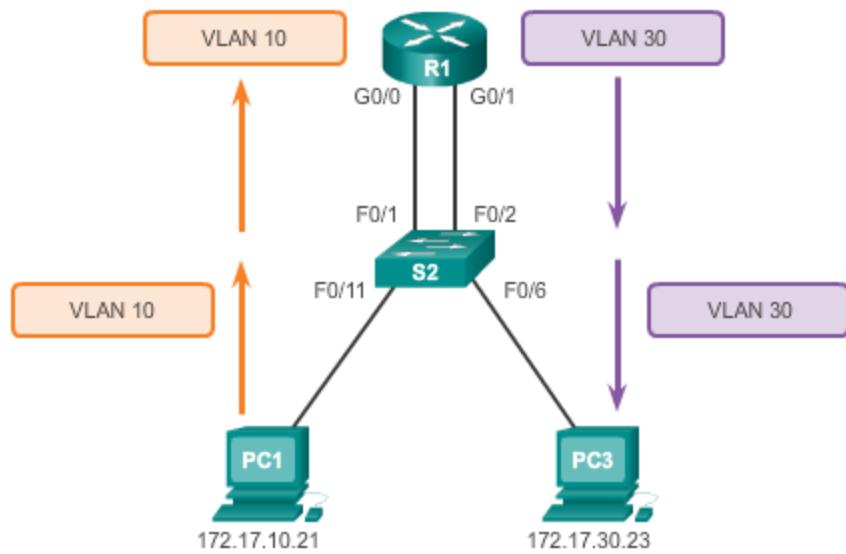
El routing entre VLAN antiguo dependía de que un puerto de router físico estuviera disponible para cada VLAN configurada. Esto fue reemplazado por la topología de router-on-a-stick, que depende de un router externo con subinterfaces de enlace troncal a un switch de capa 2. Con la opción de router-on-a-stick, se deben configurar en cada subinterfaz lógica el direccionamiento IP y la información de VLAN adecuados, y se debe configurar una encapsulación de enlace troncal que coincida con la interfaz troncal del switch.

También existe la opción de multicapa entre VLAN mediante switching de capa 3. El switching de capa 3 incluye SVI y puertos enruteados. El switching de capa 3 se suele configurar en las capas de distribución y de núcleo del modelo de diseño jerárquico. El switching de capa 3 con SVI es una forma de routing entre VLAN. Un puerto enruteado es un puerto físico que funciona de manera similar a una interfaz en un router. A diferencia de los puertos de acceso, los puertos enruteados no se asocian a una VLAN determinada.

Los switches Catalyst 2960 se pueden utilizar para routing multicapa entre VLAN. Estos switches admiten routing estático, pero no son compatibles con protocolos de routing dinámico. Para habilitar el routing IP en los switches 2960, son necesarias plantillas SDM.

La resolución de problemas de routing entre VLAN con un router o con un switch de capa 3 es similar. Los errores comunes suelen estar relacionados con las configuraciones de VLAN, enlace troncal, la interfaz de capa 3 y las direcciones IP.

¿Qué es el enruteamiento entre VLAN?



El enruteamiento entre VLAN basado en routers es un proceso para reenviar el tráfico de la red desde una VLAN a otra mediante un router.

6 Enrutamiento estático

6.1 Introducción

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

Los routers descubren redes remotas de manera dinámica, mediante protocolos de routing, de manera manual, o por medio de rutas estáticas. En muchos casos, los routers utilizan una combinación de protocolos de routing dinámico y rutas estáticas. Este capítulo trata sobre el enrutamiento estático.

Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que los protocolos de routing dinámico.

En este capítulo, se utilizarán topologías de ejemplo para configurar las rutas estáticas IPv4 e IPv6 y para presentar técnicas de resolución de problemas. A lo largo del proceso, se analizarán varios comandos importantes de IOS y los resultados que generan. Se incluirá una introducción a la tabla de routing con redes conectadas directamente y rutas estáticas.

En este capítulo, también se compara el routing con clase con los métodos de routing sin clase ampliamente implementados. Abarcará el routing entre dominios sin clase (CIDR) y los métodos de máscara de subred de longitud variable (VLSM). El CIDR y los VLSM ayudaron a conservar el espacio de direcciones IPv4 mediante el uso de la división en subredes y técnicas de sumarización.

Después de completar este capítulo, podrá hacer lo siguiente:

- Explicar las ventajas y desventajas del routing estático.
- Explicar la finalidad de los diferentes tipos de rutas estáticas.
- Configurar rutas estáticas IPv4 e IPv6 especificando una dirección del siguiente salto.
- Configurar rutas IPv4 e IPv6 predeterminadas.
- Explicar el uso del direccionamiento con clase antiguo en la implementación de redes.
- Explicar la finalidad de CIDR en el reemplazo del direccionamiento con clase.
- Diseñar e implementar un esquema de direccionamiento jerárquico.
- Configurar una dirección de red resumida IPv4 e IPv6, a fin de reducir el número de actualizaciones de la tabla de routing.
- Configurar una ruta estática flotante para proporcionar una conexión de respaldo.
- Explicar la forma en que un router procesa paquetes cuando se configura una ruta estática.
- Resolver problemas comunes de configuración de rutas estáticas y predeterminadas.



6.2 Implementación del routing estático

6.2.1 Enrutamiento estático

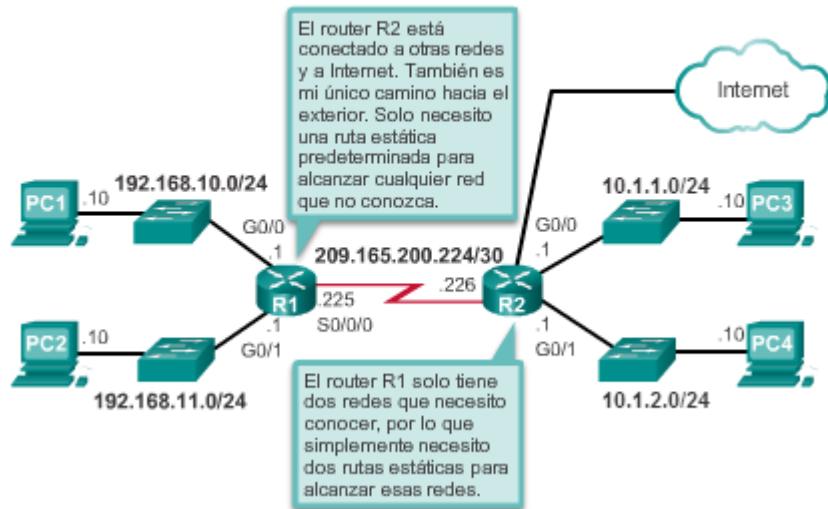
Un router puede descubrir redes remotas de dos maneras:

- **Manualmente:** las redes remotas se introducen de forma manual en la tabla de rutas por medio de rutas estáticas.
- **Dinámicamente:** las rutas remotas se descubren de forma automática mediante un protocolo de routing dinámico.

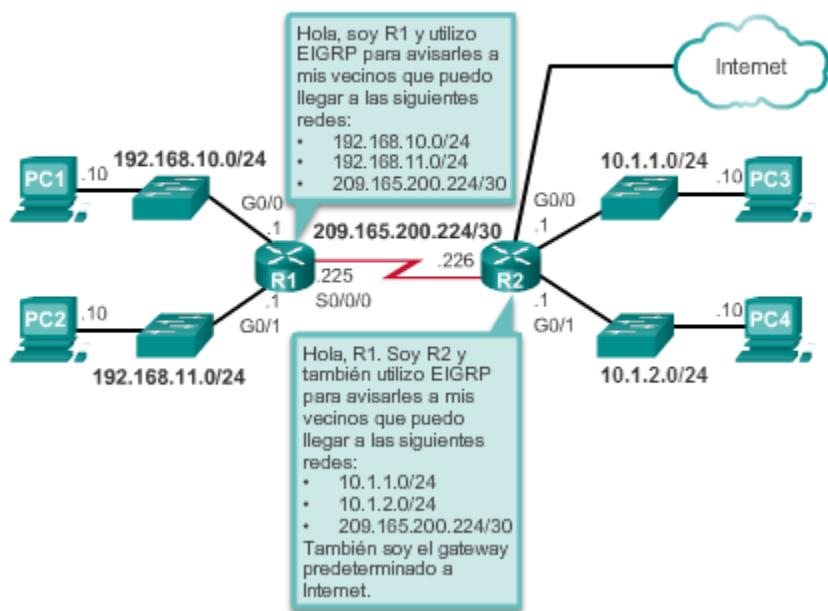
En la figura 1, se proporciona una situación de ejemplo de routing estático. En la figura 2, se proporciona una situación de ejemplo de routing dinámico con EIGRP.

Un administrador de red puede configurar una ruta estática de forma manual 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 de forma manual 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.

Situación de rutas estáticas y predeterminadas



Situación de routing dinámico



El routing estático proporciona algunas ventajas en comparación con el routing dinámico, por ejemplo:

- Las rutas estáticas no se anuncian a través de la red, lo cual aumenta la seguridad.
- Las rutas estáticas consumen menos ancho de banda que los protocolos de routing dinámico. No se utiliza ningún ciclo de CPU para calcular y comunicar las rutas.
- La ruta que usa una ruta estática para enviar datos es conocida.

El routing estático tiene las siguientes desventajas:

- La configuración inicial y el mantenimiento son prolongados.
- La configuración es propensa a errores, especialmente en redes extensas.
- Se requiere la intervención del administrador para mantener la información cambiante de la ruta.
- No se adapta bien a las redes en crecimiento; el mantenimiento se torna cada vez más complicado.
- Requiere un conocimiento completo de toda la red para una correcta implementación.

En la ilustración, se comparan las características del routing dinámico y el routing estático. Observe que las ventajas de un método son las desventajas del otro.

Las rutas estáticas son útiles para redes más pequeñas con solo una ruta hacia una red externa. También proporcionan seguridad en una red más grande para ciertos tipos de tráfico o enlaces a otras redes que necesitan más control. 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. Esto puede ocasionar que el router tenga varias rutas a una red de destino a través de rutas estáticas y rutas descubiertas dinámicamente. Sin embargo, la distancia administrativa (AD) a una ruta estática es 1. Por lo tanto, una ruta estática tendrá prioridad sobre todas las rutas descubiertas dinámicamente.

Comparación entre routing dinámico y estático

	Enrutamiento dinámico	Enrutamiento estático
Complejidad de la configuración	Generalmente independiente del tamaño de la red	Aumentos en el tamaño de la red
Cambios de topología	Se adapta automáticamente a los cambios de topología	Se requiere intervención del administrador
Escalamiento	Adecuado para topologías simples y complejas	Adecuado para topologías simples
Seguridad	Menos segura	Más segura
Uso de recursos	Utiliza CPU, memoria y ancho de banda de enlace	Sin necesidad de recursos adicionales
Facilidad de pronóstico	La ruta depende de la topología actual	La ruta a destino siempre es la misma

El routing estático tiene tres usos principales:

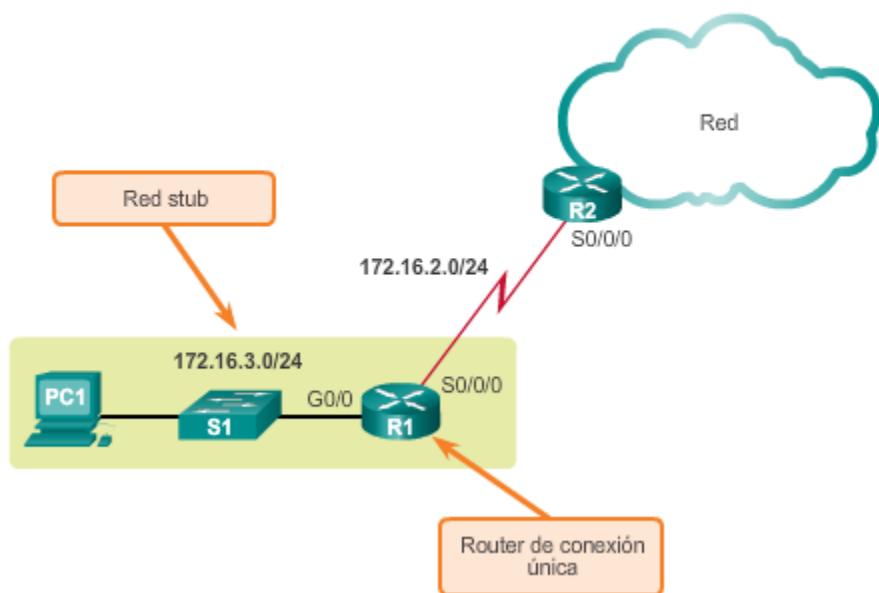
- Facilita el mantenimiento de la tabla de enrutamiento en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
- Proporciona routing hacia las redes de rutas internas y desde estas. Una red de rutas internas es aquella a la cual se accede a través de una única ruta y cuyo 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.

En la ilustración, se muestra un ejemplo de la conexión de una red de rutas internas y de la conexión de una ruta predeterminada. En dicha ilustración, observe que cualquier red conectada al R1 solo tiene una manera de alcanzar otros destinos, ya sean redes conectadas al R2 o destinos más allá del R2. Por lo tanto, la red 172.16.3.0 es una red de rutas internas y el R1 es un router de rutas internas. Al ejecutar un protocolo de routing entre el R2 y el R1, se desperdician recursos.

En este ejemplo, se puede configurar una ruta estática en el R2 para alcanzar la LAN del R1. Además, como el R1 tiene solo una forma de enviar tráfico no local, se puede configurar una ruta estática predeterminada en el R1 para señalar al R2 como el siguiente salto para todas las otras redes.

Redes y routers de rutas internas



	Beneficios	Desventajas
La complejidad de la configuración aumenta con el tamaño de la red.		✓
No se necesitan recursos adicionales (CPU, ancho de banda, etc.).	✓	
Los cambios en la topología afectan la configuración.		✓
La ruta al destino siempre es la misma.	✓	
Las tablas de routing son pequeñas y el mantenimiento es mínimo.	✓	
No se realizarán actualizaciones automáticas a la tabla de routing si la topología se modifica.		✓

6.2.2 Tipos de rutas estáticas

Como se muestra en la ilustración, las rutas estáticas suelen usarse con más frecuencia para conectarse a una red específica o para proporcionar un gateway de último recurso para una red de rutas internas. También pueden utilizarse para lo siguiente:

- Reducir el número de rutas anunciadas mediante el resumen de varias redes contiguas como una sola ruta estática.
- Crear una ruta de respaldo en caso de que falle un enlace de la ruta principal.

Se analizarán los siguientes tipos de rutas estáticas IPv4 e IPv6:

- Ruta estática estándar
- Ruta estática predeterminada
- Ruta estática resumida
- Ruta estática flotante

Utilice las rutas estáticas para...

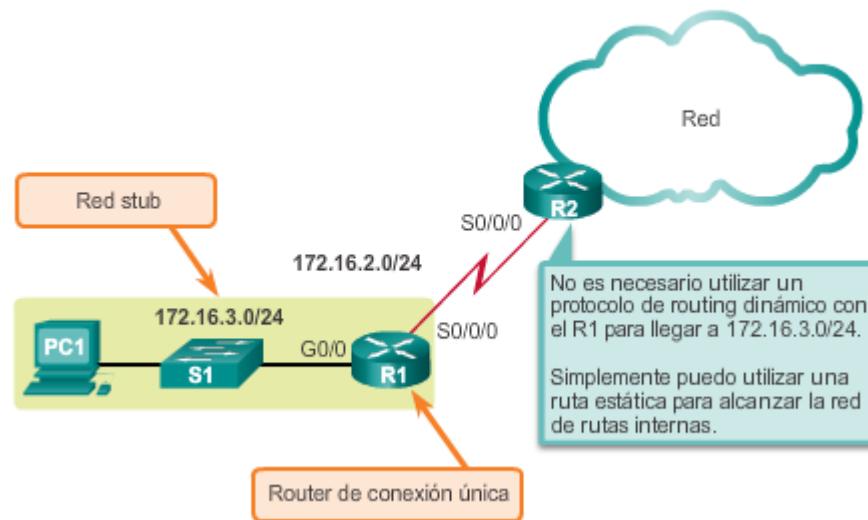
- conectarse a una red específica;
- conectar un router de rutas internas;
- resumir entradas de la tabla de routing;
- crear una ruta de respaldo.

IPv4 e IPv6 admiten la configuración de rutas estáticas. Las rutas estáticas son útiles para conectarse a una red remota específica.

En la ilustración, se muestra que el R2 se puede configurar con una ruta estática para alcanzar la red de rutas internas 172.16.3.0/24.

Nota: en el ejemplo, se resalta una red de rutas internas, pero, de hecho, una ruta estática se puede utilizar para conectarse a cualquier red.

Conexión a una red de rutas internas



Una ruta estática predeterminada es aquella que coincide con todos los paquetes. Una ruta predeterminada identifica la dirección IP del gateway al cual el router envía todos los paquetes IP para los que no tiene una ruta descubierta o estática. Una ruta estática predeterminada es simplemente una ruta estática con 0.0.0.0/0 como dirección IPv4 de destino. Al configurar una ruta estática predeterminada, se crea un gateway de último recurso.

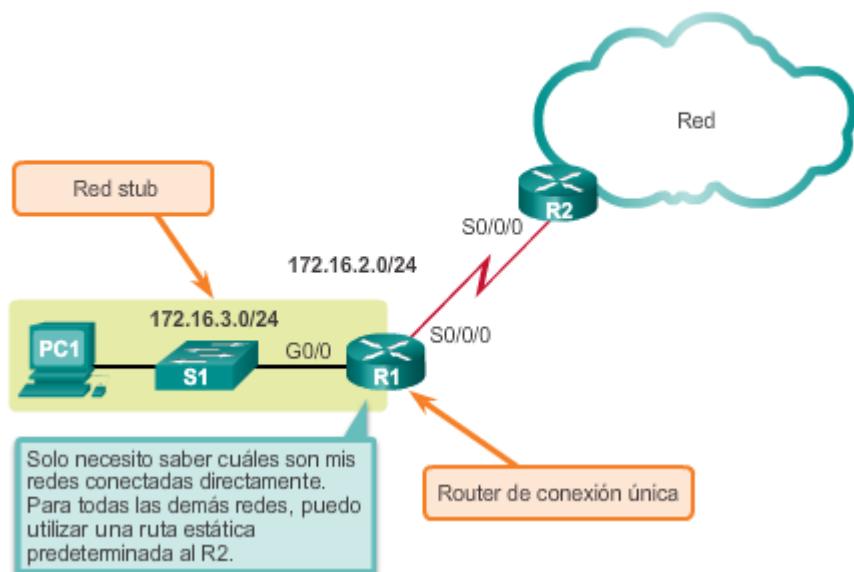
Nota: todas las rutas que identifican un destino específico con una máscara de subred más grande tienen prioridad sobre la ruta predeterminada.

Las rutas estáticas predeterminadas se utilizan en los siguientes casos:

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

Consulte la ilustración para ver una situación de ejemplo de implementación de routing estático predeterminado.

Conexión de un router de rutas internas

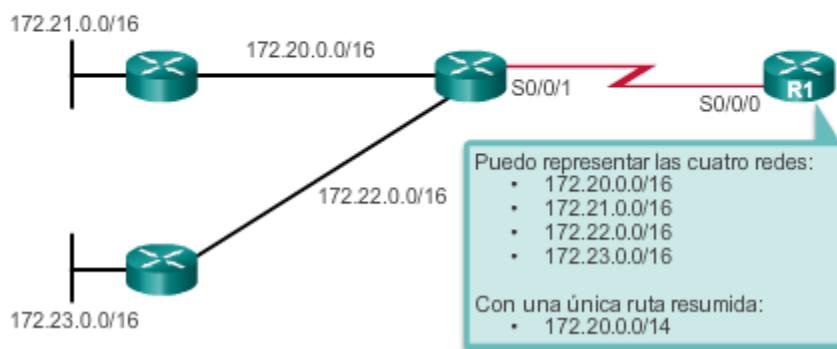


Para reducir el número de entradas en la tabla de routing, se pueden resumir varias rutas estáticas en una única ruta estática si se presentan las siguientes condiciones:

- Las redes de destino son contiguas y se pueden resumir en una única dirección de red.
- Todas las rutas estáticas utilizan la misma interfaz de salida o la dirección IP del siguiente salto.

En la ilustración, el R1 requiere cuatro rutas estáticas separadas para alcanzar las redes 172.20.0.0/16 a 172.23.0.0/16. En cambio, una ruta estática resumida puede configurarse y aún proporcionar conectividad a esas redes.

Uso de una única ruta estática resumida



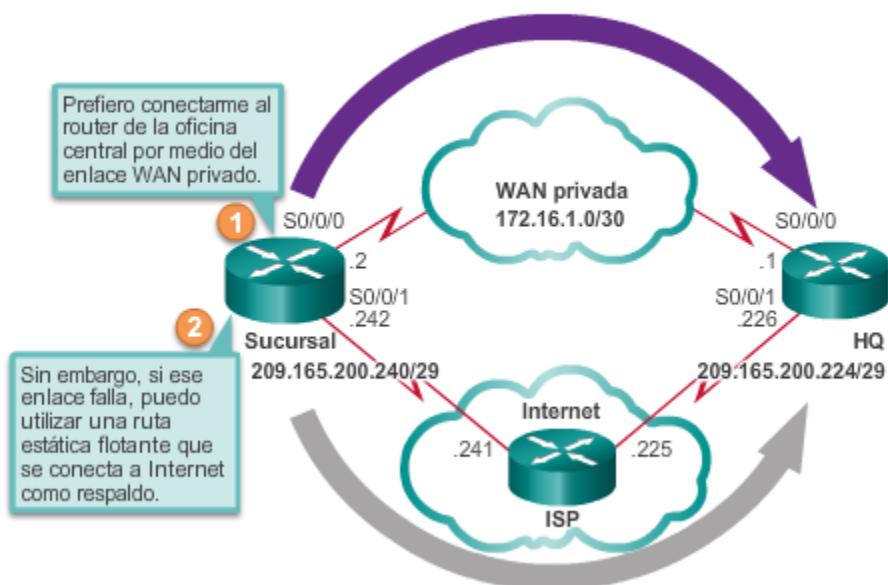
Otro tipo de ruta estática es una ruta estática flotante. Las rutas estáticas flotantes son rutas estáticas que se utilizan para proporcionar una ruta de respaldo a una ruta estática o dinámica principal, en el caso de una falla del enlace. La ruta estática flotante se utiliza únicamente cuando la ruta principal no está disponible.

Para lograrlo, la ruta estática flotante se configura con una distancia administrativa mayor que la ruta principal. Recuerde que la distancia administrativa representa la confiabilidad de una ruta. Si existen varias rutas al destino, el router elegirá la que tenga una menor distancia administrativa.

Por ejemplo, suponga que un administrador desea crear una ruta estática flotante como respaldo de una ruta descubierta por EIGRP. La ruta estática flotante se debe configurar con una distancia administrativa mayor que el EIGRP. El EIGRP tiene una distancia administrativa de 90. Si la ruta estática flotante se configura con una distancia administrativa de 95, se prefiere la ruta dinámica descubierta por el EIGRP a la ruta estática flotante. Si se pierde la ruta descubierta por el EIGRP, en su lugar se utiliza la ruta estática flotante.

En la ilustración, el router de la sucursal generalmente reenvía todo el tráfico al router de la oficina central (HQ) mediante el enlace WAN privado. En este ejemplo, los routers intercambian información de la ruta utilizando el EIGRP. Una ruta estática flotante, con una distancia administrativa de 91 o superior, se puede configurar para que funcione como ruta de respaldo. Si el enlace WAN privado falla y la ruta EIGRP desaparece de la tabla de routing, el router selecciona la ruta estática flotante como la mejor ruta para alcanzar la LAN de la oficina central.

Configuración de una ruta de respaldo



	Estándar	Predeterminado	Resumen	Flotante
Respalda una ruta ya descubierta por un protocolo de routing dinámico.				✓
Utiliza una dirección de red única para enviar varias rutas estáticas a una dirección de destino.			✓	
Hace coincidir todos los paquetes y los envía a un gateway predeterminado específico.		✓		
Es útil al conectarse a una red de rutas internas.	✓			
Está configurada con una distancia administrativa mayor que el protocolo de routing dinámico original.				✓
Suele utilizarse con routers perimetrales para conectarse a la red ISP.		✓		

6.3 Configuración de rutas estáticas y predeterminadas

6.3.1 Configuración de rutas estáticas IPv4

Las rutas estáticas se configuran con el comando **ip route** de configuración global. La sintaxis del comando es la siguiente:

```
Router(config)# ip route dirección-red máscara-subred {dirección-ip | tipo-interfaz número-interfaz [ dirección-ip ] [ distancia ] [ name name ] [ permanent ] [ tag etiqueta ] }
```

Se requieren los siguientes parámetros para configurar el routing estático:

- *dirección-red*: dirección de red de destino de la red remota que se agrega a la tabla de routing, también llamada “prefijo”.
- *máscara-subred*: máscara de subred, o simplemente máscara, de la red remota que se agrega a la tabla de routing. La máscara de subred puede modificarse para resumir un grupo de redes.

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

- *dirección-ip*: dirección IP del router de conexión que se va a utilizar para reenviar el paquete a la red de destino remota. Se la suele denominar “siguiente salto”.
- *interfaz-salida*: interfaz de salida que se va a utilizar para reenviar el paquete al siguiente salto.

Como se muestra en la ilustración, la sintaxis del comando que suele utilizarse es **ip route dirección-red máscara-subred {dirección-ip | interfaz-salida}**.

El parámetro *distancia* se utiliza para crear una ruta estática flotante al establecer una distancia administrativa mayor que la de una ruta descubierta de forma dinámica.

Nota: los parámetros restantes no son relevantes en este capítulo o para estudios de CCNA.

Sintaxis del comando ip route

```
Router(config)# ip route network-address subnet-mask
(ip-address | exit-intf)
```

Parámetro	Descripción
dirección-red	Dirección de la red de destino de la red remota que será agregada a la tabla de enrutamiento.
máscara-subred	<ul style="list-style-type: none"> Máscara de subred de la red remota que será agregada a la tabla de enrutamiento. La máscara de subred puede modificarse para resumir un grupo de redes.
dirección-ip	<ul style="list-style-type: none"> Se le denomina comúnmente como dirección IP del router del siguiente salto. Suele utilizarse para la conexión a un medio de difusión (es decir, Ethernet). Por lo general, crea una búsqueda recursiva.
interfaz-salida	<ul style="list-style-type: none"> Use la interfaz de salida para reenviar paquetes a la red de destino. También se la denomina "ruta estática conectada directamente". Suele utilizarse para conectarse en una configuración punto a punto.

En este ejemplo, las figuras 1 a 3 muestran las tablas de routing de los routers R1, R2 y R3. Observe que cada router tiene entradas solo para redes conectadas directamente y sus direcciones locales asociadas. Ninguno de los routers tiene conocimiento de las redes que están fuera de las interfaces conectadas directamente.

Por ejemplo, el R1 no tiene conocimiento de las redes:

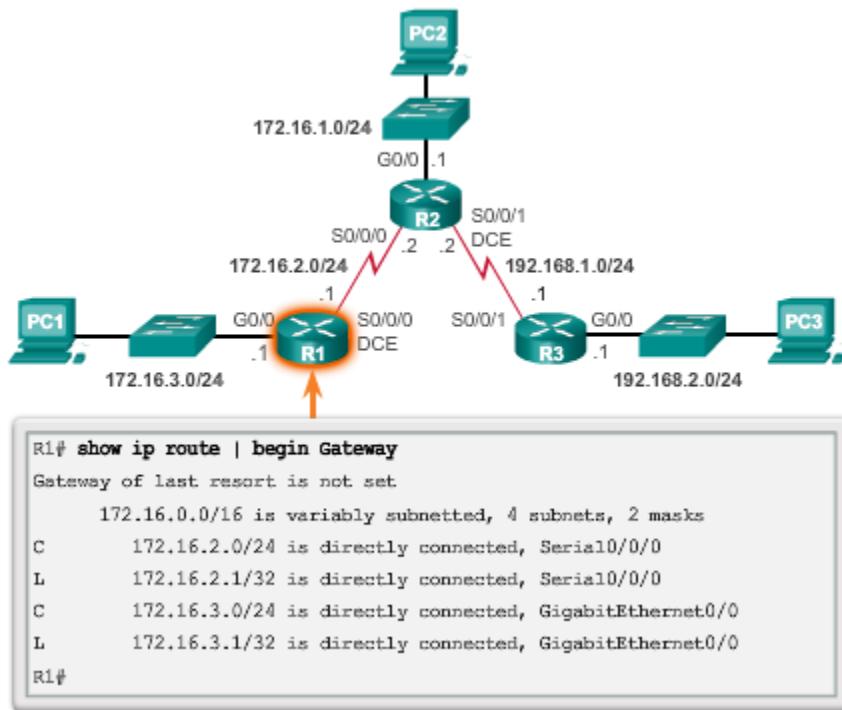
- 172.16.1.0/24: LAN en el R2
- 192.168.1.0/24: red serial entre el R2 y el R3
- 192.168.2.0/24: LAN en el R3

En la figura 4, se muestra un ping correcto del R1 al R2. En la figura 5, se muestra un ping incorrecto a la LAN del R3. Esto se debe a que el R1 no tiene una entrada en su tabla de routing para la red LAN del R3.

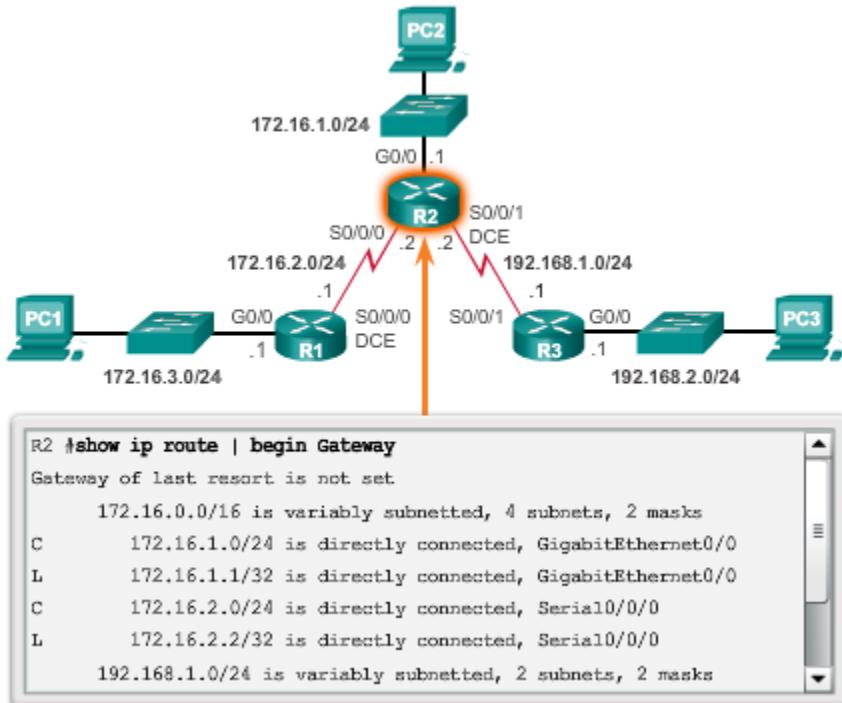
El siguiente salto se puede identificar mediante una dirección IP, una interfaz de salida, o ambas. El modo en que se especifica el destino genera uno de los siguientes tres tipos de ruta:

- **Ruta del siguiente salto:** solo se especifica la dirección IP del siguiente salto.
- **Ruta estática conectada directamente:** solo se especifica la interfaz de salida del router.
- **Ruta estática completamente especificada:** se especifican la dirección IP del siguiente salto y la interfaz de salida.

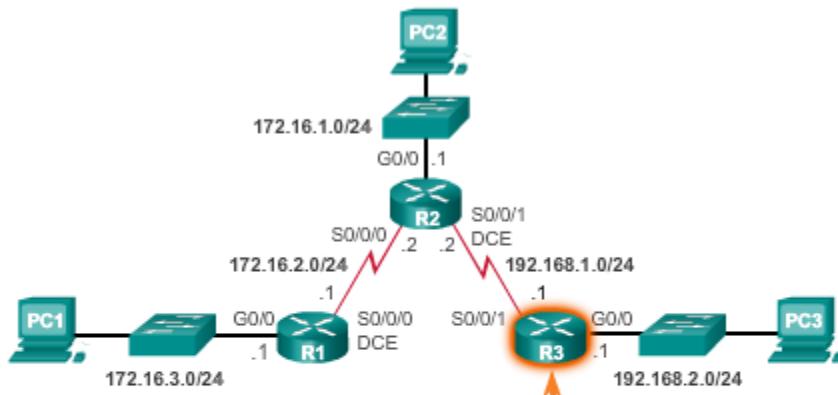
Verificación de la tabla de routing del R1



Verificación de la tabla de routing del R2

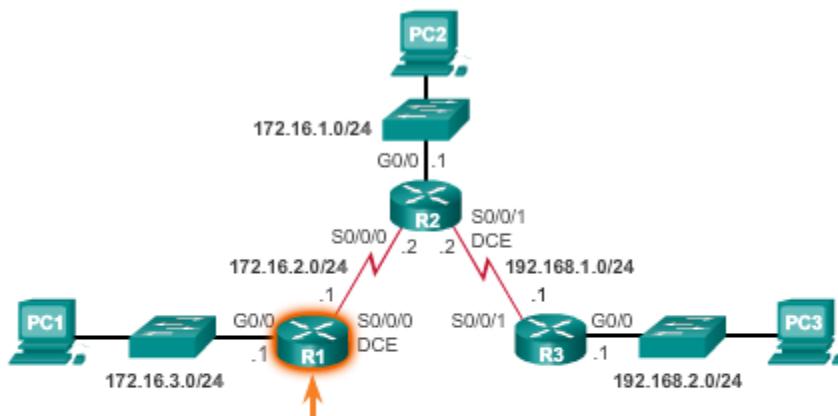


Verificación de la tabla de routing del R3



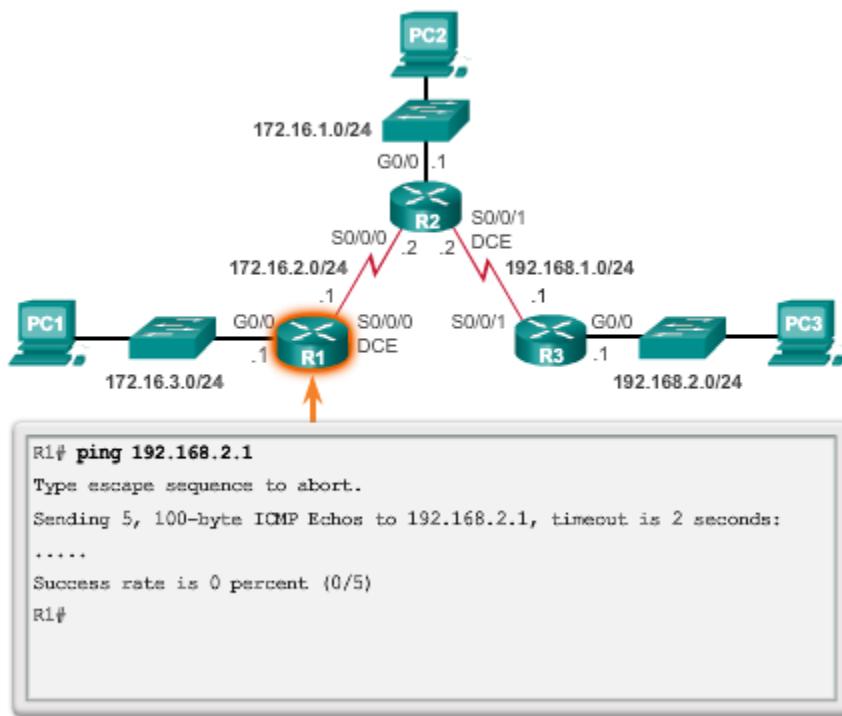
```
R3# show ip route | include C
Codes:L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
C      192.168.1.0/24 is directly connected, Serial0/0/1
C      192.168.2.0/24 is directly connected, GigabitEthernet0/0
R3#
```

Verificación de la conectividad del R1 al R2



```
R1# ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16
ms
R1#
```

Verificación de la conectividad del R1 a la LAN del R3



En una ruta estática de siguiente salto, solo se especifica la dirección IP del siguiente salto. La interfaz de salida se deriva del siguiente salto. Por ejemplo, en la figura 1, se configuran tres rutas estáticas de siguiente salto en el R1 con la dirección IP del siguiente salto, el R2.

Antes de que un router reenvíe un paquete, el proceso de la tabla de enrutamiento debe determinar qué interfaz de salida utilizará para reenviar el paquete. A esto se lo conoce como resolución de rutas. El proceso de resolución de la ruta varía en función del tipo de mecanismo de reenvío que utiliza el router. CEF (Cisco Express Forwarding) es el comportamiento predeterminado en la mayoría de las plataformas que ejecutan el IOS 12.0 o posterior.

En la figura 2, se detalla el proceso básico de reenvío de paquetes en la tabla de routing para el R1 sin el uso de CEF. Cuando un paquete está destinado a la red 192.168.2.0/24, el R1:

1. Busca una coincidencia en la tabla de routing y encuentra que debe reenviar paquetes a la dirección IPv4 172.16.2.2 del siguiente salto, tal como lo indica la etiqueta 1 en la ilustración. Todas las rutas que hacen referencia solo a la dirección IPv4 del siguiente salto y que no hacen referencia a una interfaz de salida deben resolver la dirección IPv4 del siguiente salto con otra ruta de la tabla de routing que tenga una interfaz de salida.
2. En esta instancia, el R1 debe determinar cómo alcanzar la dirección 172.16.2.2. Por lo tanto, busca por segunda vez si existe una coincidencia para 172.16.2.2. En este caso, la dirección IPv4 hace coincidir la ruta de la red conectada directamente 172.16.2.0/24 con la interfaz de salida Serial 0/0/0, tal como lo indica la etiqueta 2 en la ilustración. Esta búsqueda le comunica al proceso de la tabla de routing que este paquete se reenvía fuera de esa interfaz.

En realidad, se requieren dos procesos de búsqueda en la tabla de routing para reenviar cualquier paquete a la red 192.168.2.0/24. Cuando el router realiza varias búsquedas en la tabla de routing

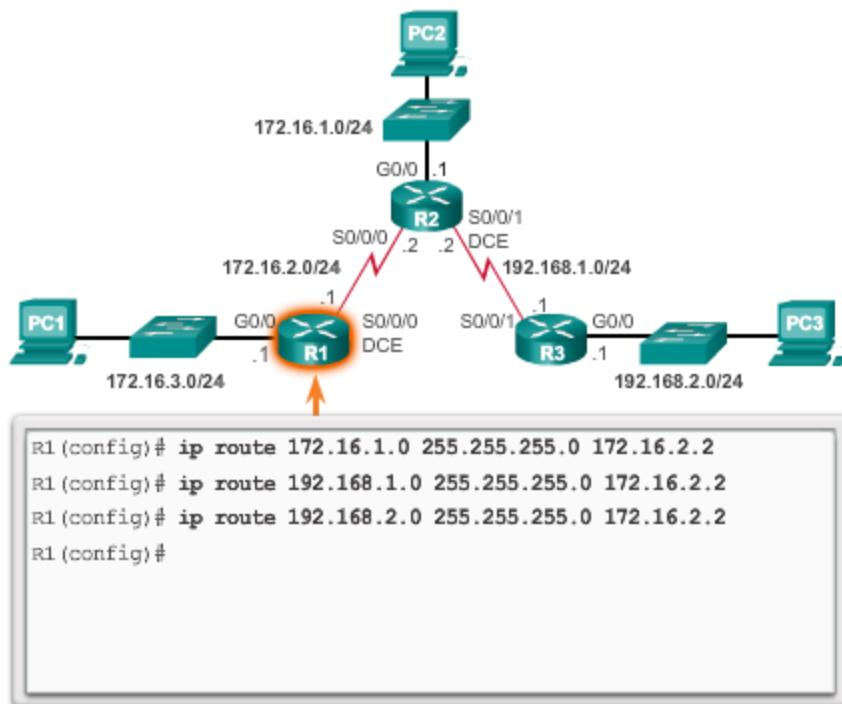
antes de reenviar un paquete, lleva a cabo un proceso que se conoce como “búsqueda recursiva”. Debido a que las búsquedas recursivas consumen recursos del router, deben evitarse siempre que sea posible.

Una ruta estática recursiva es válida (es decir, es candidata para agregarse a la tabla de routing) solo cuando el siguiente salto especificado resuelve a una interfaz de salida válida, ya sea de forma directa o indirecta.

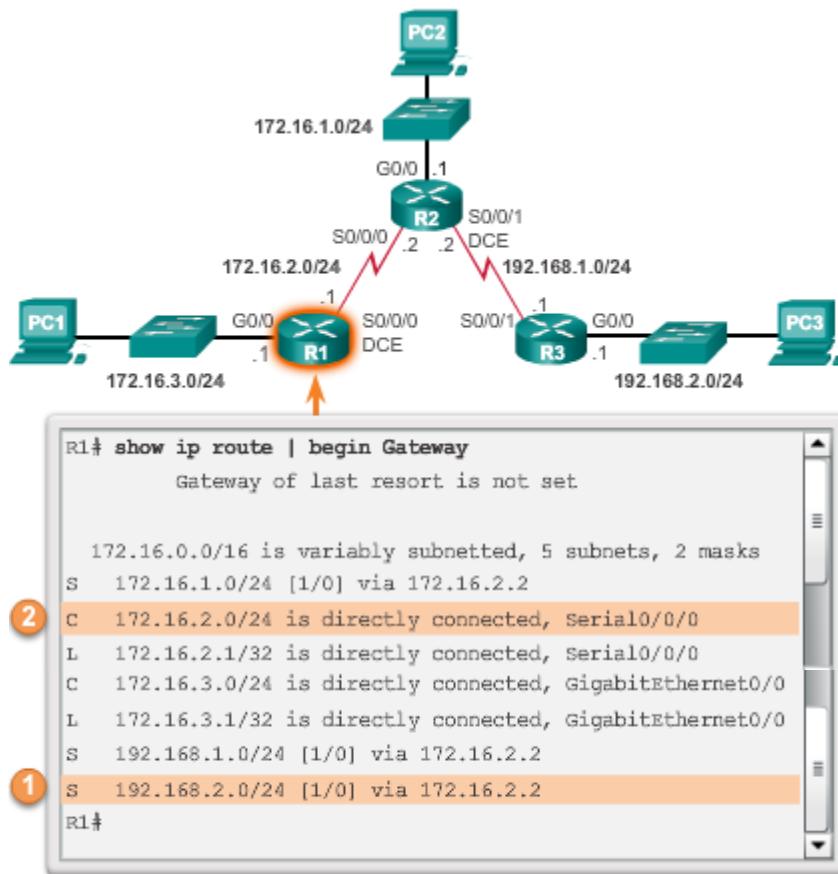
Nota: CEF proporciona búsquedas optimizadas para el reenvío de paquetes eficaz mediante dos estructuras de datos principales almacenadas en el plano de datos: una base de información de reenvío (FIB), que es una copia de la tabla de routing y la tabla de adyacencia que incluye información de direccionamiento de la capa 2. La información combinada en estas dos tablas trabaja en conjunto de manera que no sea necesario realizar una búsqueda recursiva para encontrar direcciones IP del siguiente salto. Es decir, una ruta estática que utiliza una IP del siguiente salto solo requiere una única búsqueda cuando CEF está habilitado en el router.

Utilice el verificador de sintaxis en las figuras 3 y 4 para configurar y verificar las rutas estáticas del siguiente salto en el R2 y el R3.

Configuración de rutas estáticas de siguiente salto en el R1



Verificación de la tabla de routing del R1



Al configurar una ruta estática, otra opción es utilizar la interfaz de salida para especificar la dirección del siguiente salto. En versiones anteriores de IOS, antes de CEF, este método se utiliza para evitar el problema de búsquedas recursivas.

En la figura 1, se configuran tres rutas estáticas conectadas directamente en el R1 mediante la interfaz de salida. La tabla de routing para el R1 en la figura 2 muestra que cuando un paquete está destinado a la red 192.168.2.0/24, el R1 busca una coincidencia en la tabla de routing y encuentra que puede reenviar el paquete desde su interfaz serial 0/0/0. No se necesita ninguna otra búsqueda.

Observe que la tabla de routing se ve diferente para la ruta configurada con una interfaz de salida que para la ruta configurada con una entrada recursiva.

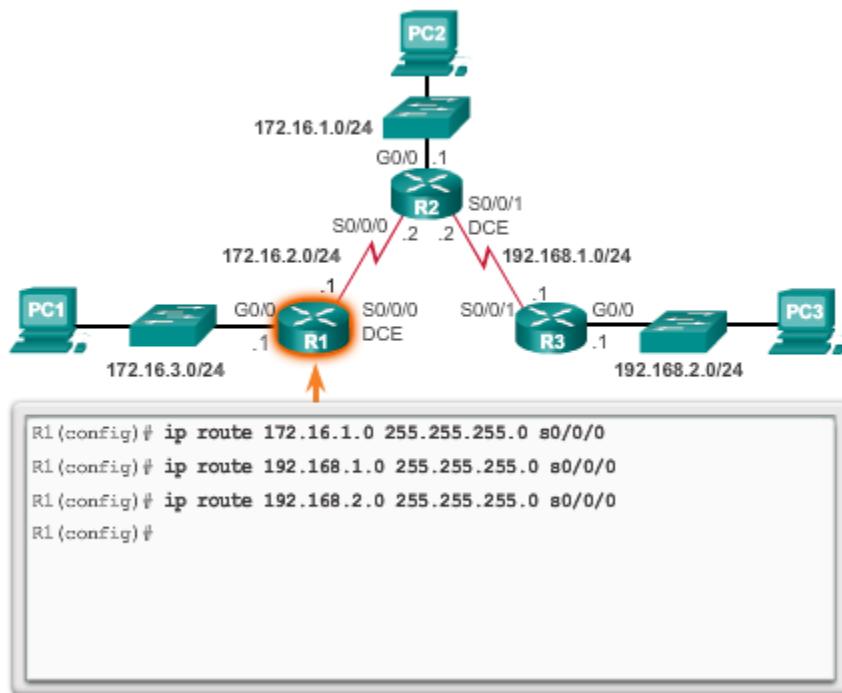
La configuración de una ruta estática conectada directamente con una interfaz de salida permite que la tabla de routing resuelva esta interfaz en una única búsqueda, no en dos. Aunque la entrada de la tabla de routing indica “conectado directamente”, la distancia administrativa de la ruta estática sigue siendo 1. Solo una interfaz conectada directamente puede tener una distancia administrativa de 0.

Nota: para las interfaces punto a punto, puede utilizar rutas estáticas que señalan a la interfaz de salida o a la dirección del siguiente salto. Para interfaces multipunto o de difusión, es más conveniente utilizar rutas estáticas que señalen a una dirección del siguiente salto.

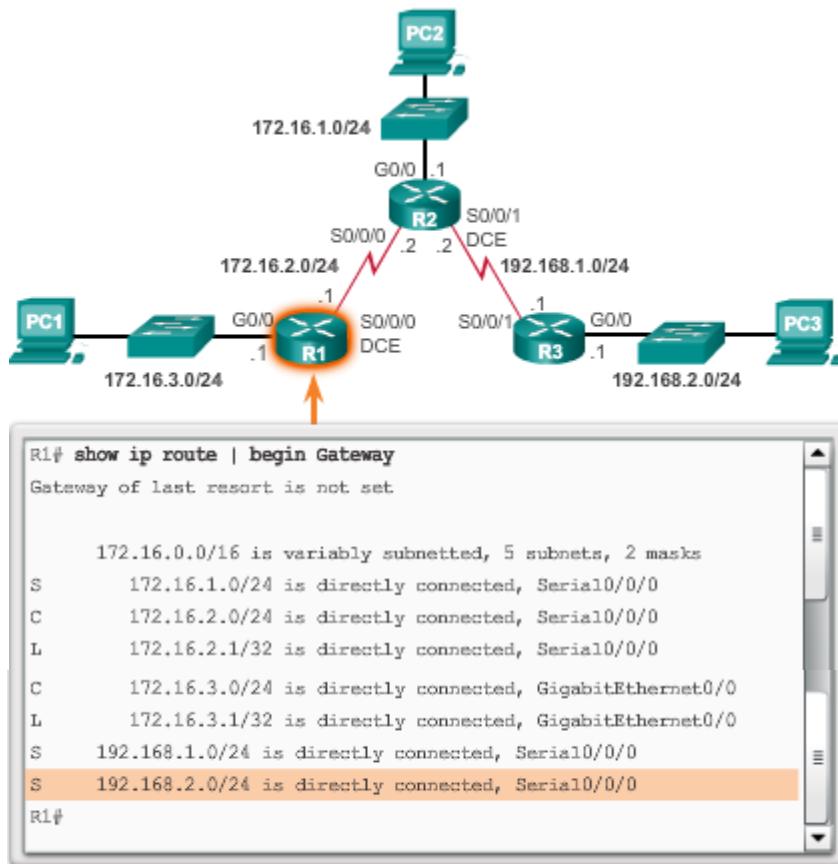
Utilice el verificador de sintaxis en las figuras 3 y 4 para configurar y verificar las rutas estáticas conectadas directamente en el R2 y el R3.

Aunque son comunes las rutas estáticas que utilizan solo una interfaz de salida en redes punto a punto, el uso del mecanismo de reenvío CEF predeterminado hace que esta práctica sea innecesaria.

Configuración de rutas estáticas conectadas directamente en el R1



Verificación de la tabla de routing del R1



Ruta estática completamente especificada

Una ruta estática completamente especificada tiene determinadas tanto la interfaz de salida como la dirección IP del siguiente salto. Este es otro tipo de ruta estática que se utiliza en versiones más antiguas de IOS, antes de CEF. Esta forma de ruta estática se utiliza cuando la interfaz de salida es una interfaz de accesos múltiples y se debe identificar explícitamente el siguiente salto. El siguiente salto debe estar conectado directamente a la interfaz de salida especificada.

Suponga que el enlace de red entre el R1 y el R2 es un enlace Ethernet y que la interfaz GigabitEthernet 0/1 del R1 está conectada a dicha red, como se muestra en la figura 1. CEF no está habilitado. Para eliminar la búsqueda recursiva, se puede implementar una ruta estática conectada directamente utilizando el siguiente comando:

```
R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/1
```

Sin embargo, esto puede causar resultados incongruentes o inesperados. La diferencia entre una red Ethernet de accesos múltiples y una red serial punto a punto es que esta última solo tiene un dispositivo más en esa red, el router que se encuentra en el otro extremo del enlace. Con las redes Ethernet, es posible que existan muchos dispositivos diferentes que comparten la misma red de accesos múltiples, incluyendo hosts y hasta routers múltiples. La designación de la interfaz de salida Ethernet en la ruta estática por sí sola no provee al router información suficiente para determinar qué dispositivo es el dispositivo del siguiente salto.

El R1 sabe que el paquete se debe encapsular en una trama de Ethernet y que se debe enviar desde la interfaz GigabitEthernet 0/1. Sin embargo, el R1 no conoce la dirección IPv4 del siguiente salto; por lo tanto, no puede determinar la dirección MAC de destino para la trama de Ethernet.

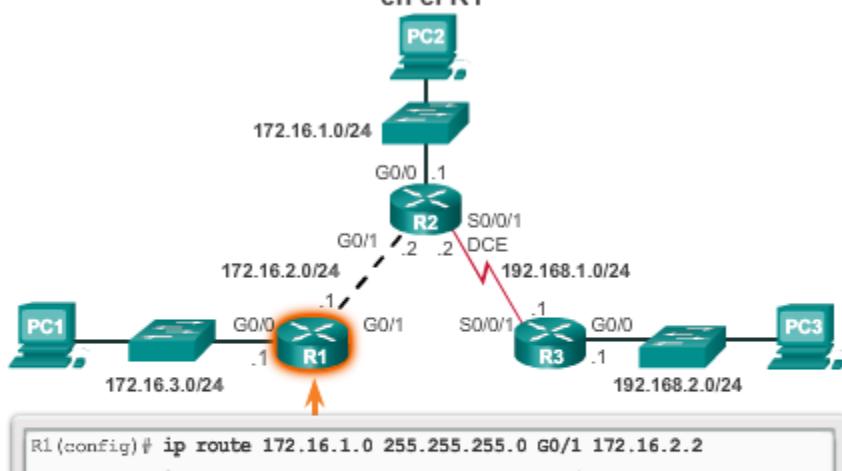
Según la topología y las configuraciones de otros routers, esta ruta estática puede funcionar o no. Cuando la interfaz de salida sea una red Ethernet, se recomienda utilizar una ruta estática completamente especificada que incluya la interfaz de salida y la dirección del siguiente salto.

Como se muestra en la figura 2, al reenviar paquetes al R2, la interfaz de salida es GigabitEthernet 0/1 y la dirección IPv4 del siguiente salto es 172.16.2.2.

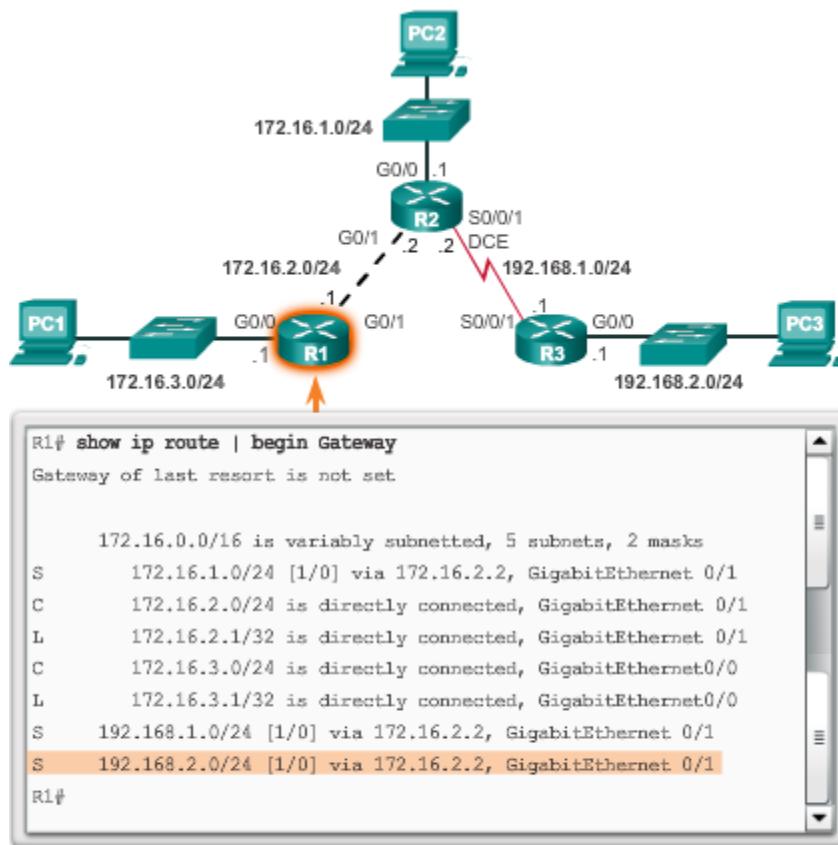
Nota: si se utiliza CEF, ya no se necesita una ruta estática completamente especificada. Debe utilizarse una ruta estática con una dirección del siguiente salto.

Utilice el verificador de sintaxis en las figuras 3 y 4 para configurar y verificar las rutas estáticas completamente especificadas en el R2 y el R3.

Configuración de rutas estáticas completamente especificadas en el R1



Verificación de la tabla de routing del R1



Además de los comandos **ping** y **traceroute**, otros comandos útiles para verificar las rutas estáticas son los siguientes:

- **show ip route**
- **show ip route static**
- **show ip route Capa de red**

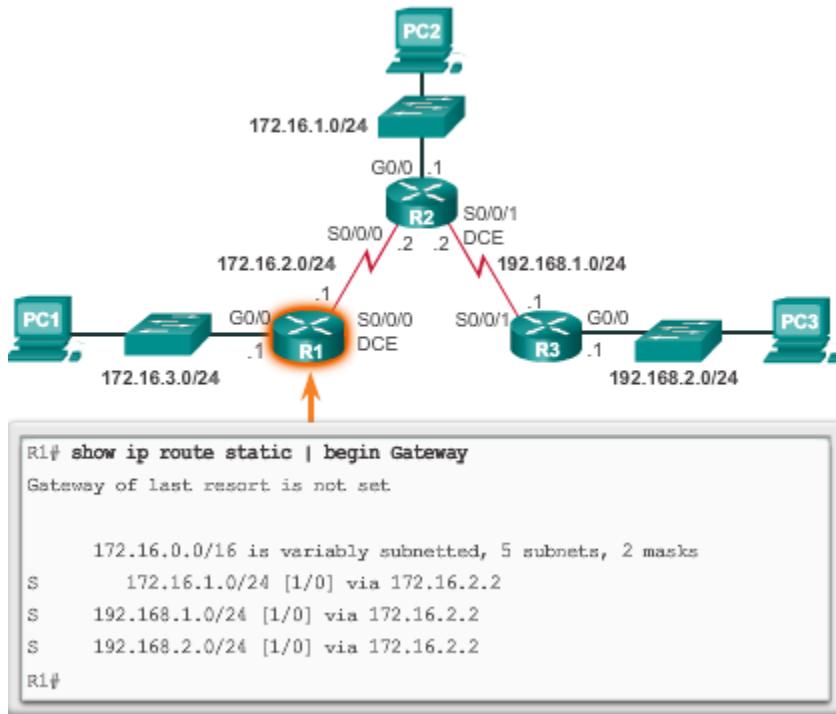
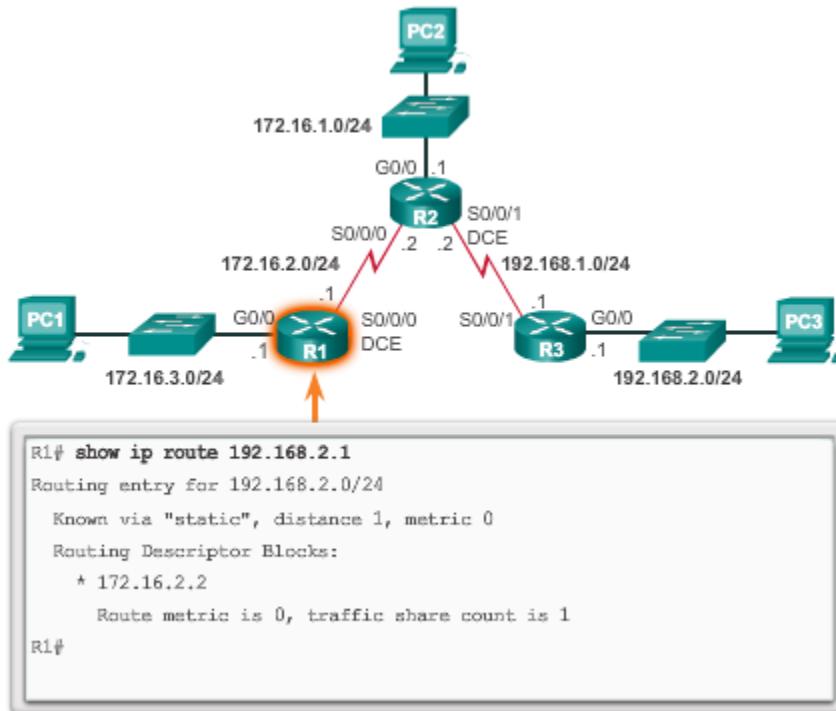
En la figura 1, se muestra un ejemplo del resultado que genera el comando **show ip route static**. En el ejemplo, el resultado se filtra con la barra vertical y el parámetro **begin**. El resultado refleja el uso de rutas estáticas con la dirección del siguiente salto.

En la figura 2, se muestra un ejemplo del resultado del comando **show ip route 192.168.2.1**.

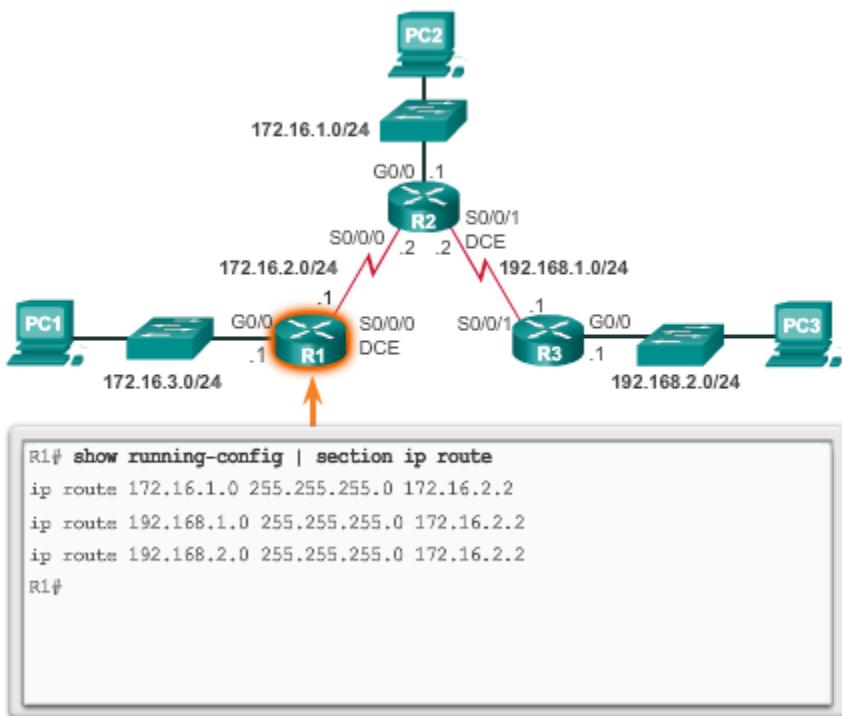
En la figura 3, se verifica la configuración de **ip route** en la configuración en ejecución.

Utilice el verificador de sintaxis de la figura 4 para verificar la configuración del routing del R2.

Utilice el verificador de sintaxis de la figura 5 para verificar la configuración del routing del R3.

Verificación de la tabla de routing del R1**Verificación de una entrada específica en la tabla de routing**

Verificación de la configuración de rutas estáticas



6.3.2 Configuración de rutas predeterminadas IPv4

Una ruta predeterminada es una ruta estática que coincide con todos los paquetes. En lugar de almacenar todas las rutas para todas las redes en la tabla de routing, un router puede almacenar una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing.

Los routers suelen utilizar rutas predeterminadas configuradas de forma local, o bien, descubiertas por otro router, mediante un protocolo de routing dinámico. Una ruta predeterminada se utiliza cuando ninguna otra ruta de la tabla de routing coincide con la dirección IP de destino del paquete. Es decir, si no existe una coincidencia más específica, entonces se utiliza la ruta predeterminada como el gateway de último recurso.

En general, las rutas estáticas predeterminadas se utilizan al conectar:

- Un router perimetral a la red de un proveedor de servicios
- Un router de rutas internas (aquel con solo un router vecino ascendente)

Como se muestra en la ilustración, la sintaxis del comando para una ruta estática predeterminada es similar a la sintaxis del comando de cualquier otra ruta estática, con la excepción de que la dirección de red es **0.0.0.0** y la máscara de subred es **0.0.0.0**. La sintaxis del comando básico de una ruta estática predeterminada es la siguiente:

- **ip route 0.0.0.0 0.0.0.0 {dirección-ip | interfaz-salida}**

Nota: una ruta estática predeterminada IPv4 suele llamarse “ruta de cuádruple cero”.

Sintaxis de ruta estática predeterminada

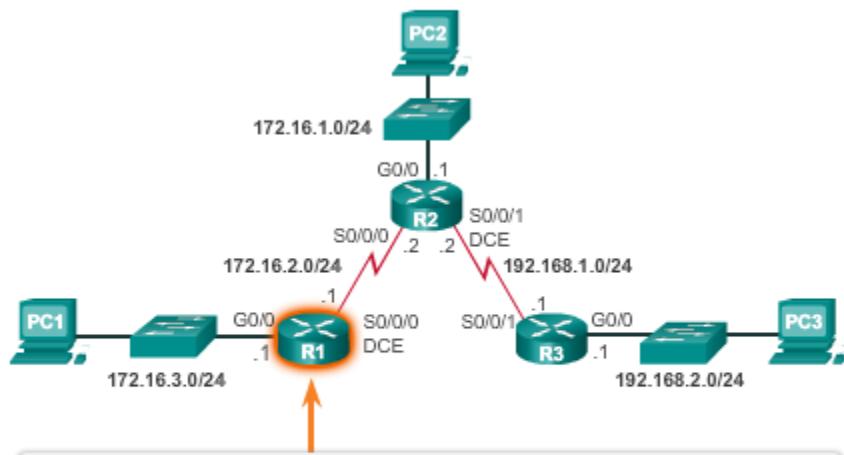
```
Router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

Parámetro	Descripción
0.0.0.0	Coincide con cualquier dirección de red.
0.0.0.0	Coincide con cualquier máscara de subred.
dirección-ip	<ul style="list-style-type: none"> Se le denomina comúnmente como dirección IP del router del siguiente salto. Suele utilizarse para la conexión a un medio de difusión (es decir, Ethernet). Por lo general, crea una búsqueda recursiva.
interfaz-salida	<ul style="list-style-type: none"> Use la interfaz de salida para reenviar paquetes a la red de destino. También se la denomina "ruta estática conectada directamente". Suele utilizarse para conectarse en una configuración punto a punto.

El R1 puede configurarse con tres rutas estáticas para alcanzar todas las redes remotas en la topología de ejemplo. Sin embargo, el R1 es un router de rutas internas, ya que está conectado únicamente al R2. Por lo tanto, sería más eficaz configurar una ruta estática predeterminada.

En el ejemplo de la ilustración, se configura una ruta estática predeterminada en el R1. Con la configuración del ejemplo, cualquier paquete que no coincida con entradas más específicas de la ruta se reenvía a 172.16.2.2.

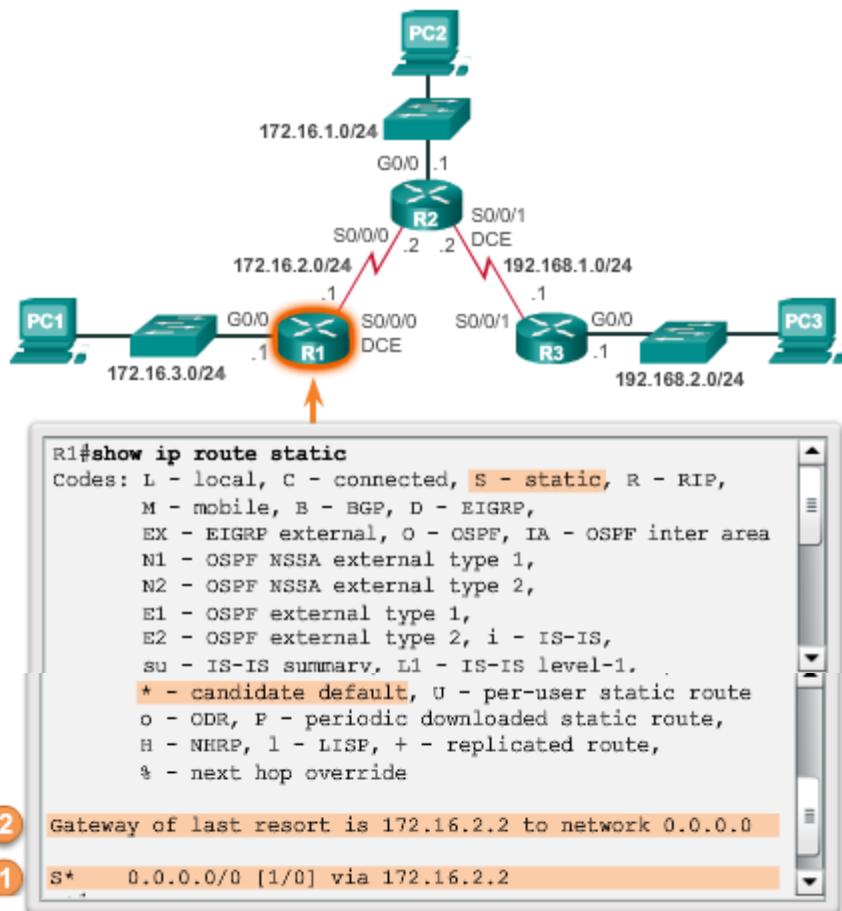
Configuración de una ruta estática predeterminada



En la ilustración, el resultado del comando **show ip route static** muestra el contenido de la tabla de routing. Observe el asterisco (*) junto a la ruta con el código "S". Como se muestra en la tabla de códigos de la ilustración, el asterisco indica que esta ruta estática es una ruta predeterminada candidata, razón por la cual se la selecciona como gateway de último recurso.

La clave para esta configuración es la máscara /0. Recuerde que la máscara de subred en una tabla de routing determina cuántos bits deben coincidir entre la dirección IP de destino del paquete y la ruta en la tabla de routing. Un 1 binario indica que los bits deben coincidir. Un 0 binario indica que los bits no tienen que coincidir. Una máscara /0 en esta entrada de ruta indica que no se requiere que ninguno de los bits coincida. La ruta estática predeterminada coincide con todos los paquetes para los cuales no existe una coincidencia más específica.

Verificación de la tabla de routing del R1



6.3.3 Configuración de rutas estáticas IPv6

Las rutas estáticas para IPv6 se configuran con el comando **ipv6 route** de configuración global. En la figura 1, se muestra la versión simplificada de la sintaxis del comando:

```
Router(config)# ipv6 route prefijo-ipv6/longitud-prefijo {dirección-ipv6 | interfaz-salida}
```

La mayoría de los parámetros son idénticos a la versión IPv4 del comando. Las rutas estáticas IPv6 también se pueden implementar como:

- Ruta estática estándar IPv6
- Ruta estática predeterminada IPv6

- Ruta estática resumida IPv6
- Ruta estática flotante IPv6

Al igual que con IPv4, estas rutas pueden configurarse como recursivas, conectadas directamente o completamente especificadas.

El comando de configuración global **ipv6 unicast-routing** debe configurarse para que habilite al router para que reenvíe paquetes IPv6. En la figura 2, se muestra la habilitación del routing de unidifusión IPv6.

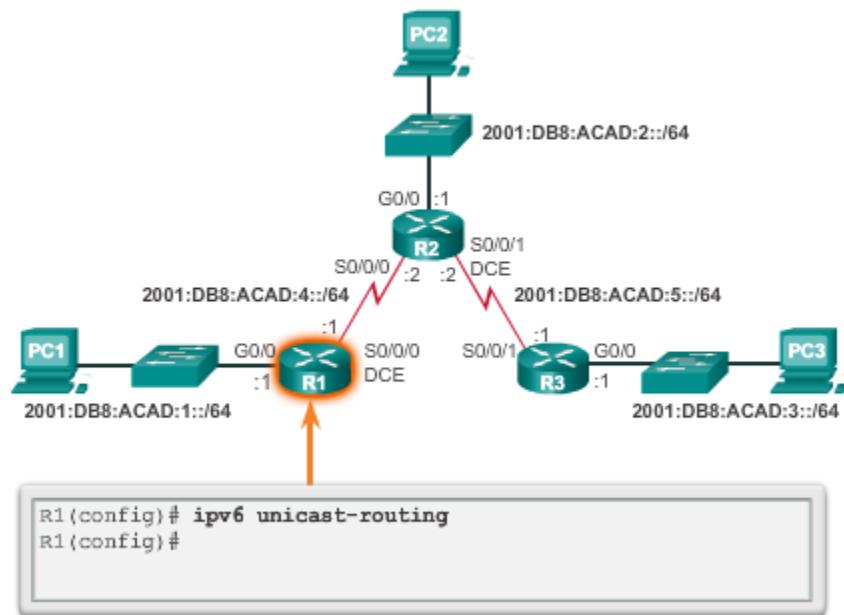
Utilice el verificador de sintaxis en las figuras 3 y 4 para habilitar el routing de unidifusión IPv6 en los routers R2 y R3.

Sintaxis del comando IPv6

```
Router(config)# ipv6 route ipv6-prefix/prefix-length
{ ipv6-address | exit-intf}
```

Parámetro	Descripción
prefijo-ipv6	Dirección de la red de destino de la red remota que será agregada a la tabla de enrutamiento.
longitud-prefijo	Longitud de prefijo de la red remota que se agregará a la tabla de routing.
dirección-ipv6	<ul style="list-style-type: none"> • Se le denomina comúnmente como dirección IP del router del siguiente salto. • Suele utilizarse para la conexión a un medio de difusión (es decir, Ethernet). • Por lo general, crea una búsqueda recursiva.
interfaz-salida	<ul style="list-style-type: none"> • Use la interfaz de salida para reenviar paquetes a la red de destino. • También se la denomina "ruta estática conectada directamente". • Suele utilizarse para conectarse en una configuración punto a punto.

Habilitación del routing de unidifusión IPv6



En este ejemplo, las figuras 1 a 3 muestran las tablas de routing de los routers R1, R2 y R3. Cada router tiene entradas solo para redes conectadas directamente y sus direcciones locales asociadas. Ninguno de los routers tiene conocimiento de las redes que están fuera de las interfaces conectadas directamente.

Por ejemplo, el R1 no tiene conocimiento de las redes:

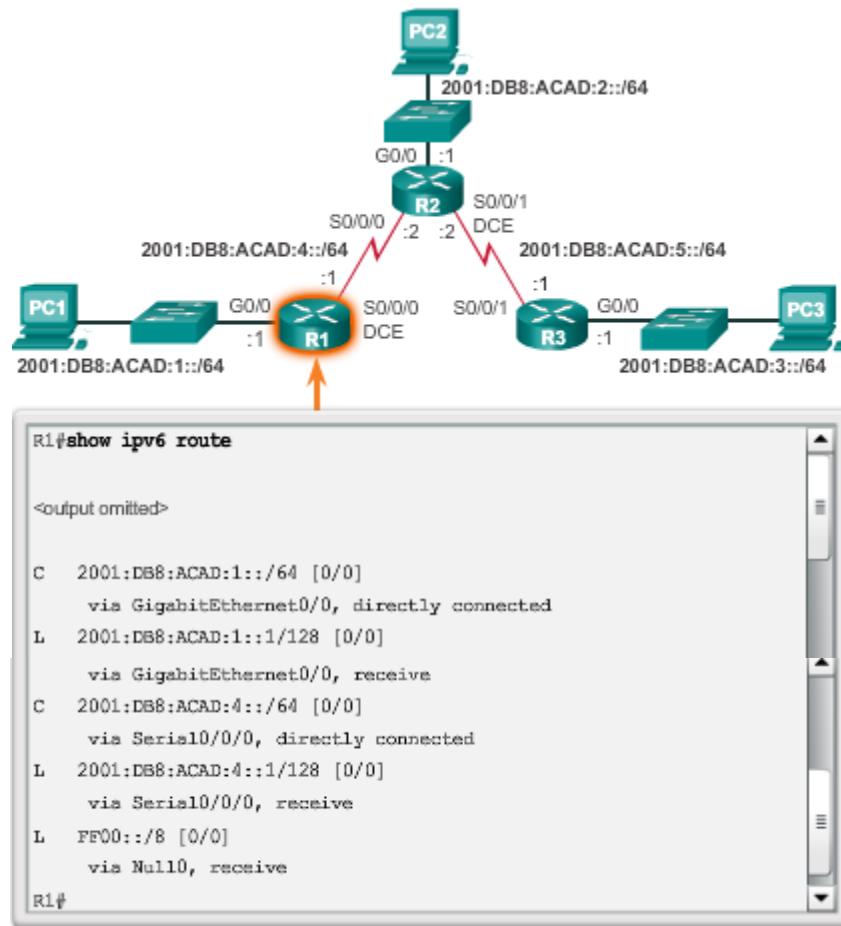
- 2001:DB8:ACAD:2::/64: LAN en el R2
- 2001:DB8:ACAD:5::/64: red serial entre el R2 y el R3
- 2001:DB8:ACAD:3::/64: LAN en el R3

En la figura 4, se muestra un ping correcto del R1 al R2. En la figura 5, se muestra un ping incorrecto a la LAN del R3. Esto se debe a que el R1 no tiene una entrada en su tabla de routing para esa red.

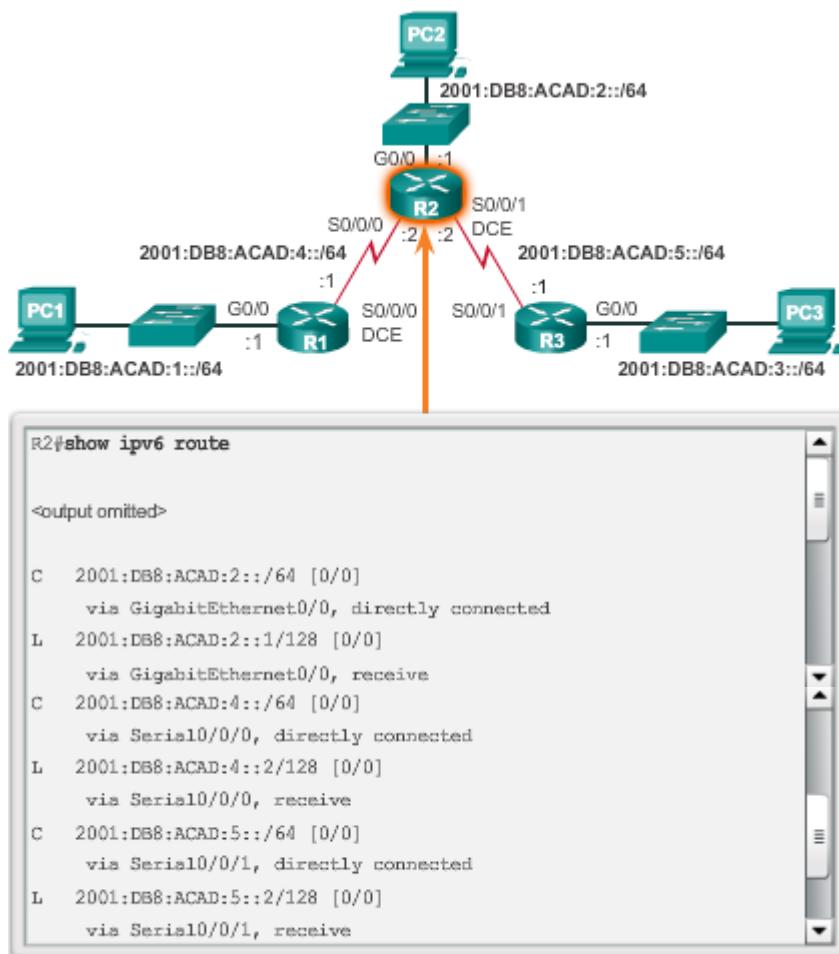
El siguiente salto se puede identificar mediante una dirección IPv6, una interfaz de salida, o ambas. El modo en que se especifica el destino genera uno de los siguientes tres tipos de ruta:

- **Ruta estática IPv6 de siguiente salto:** solo se especifica la dirección IPv6 del siguiente salto.
- **Ruta estática IPv6 conectada directamente:** solo se especifica la interfaz de salida del router.
- **Ruta estática IPv6 completamente especificada:** se especifican la dirección IPv6 del siguiente salto y la interfaz de salida.

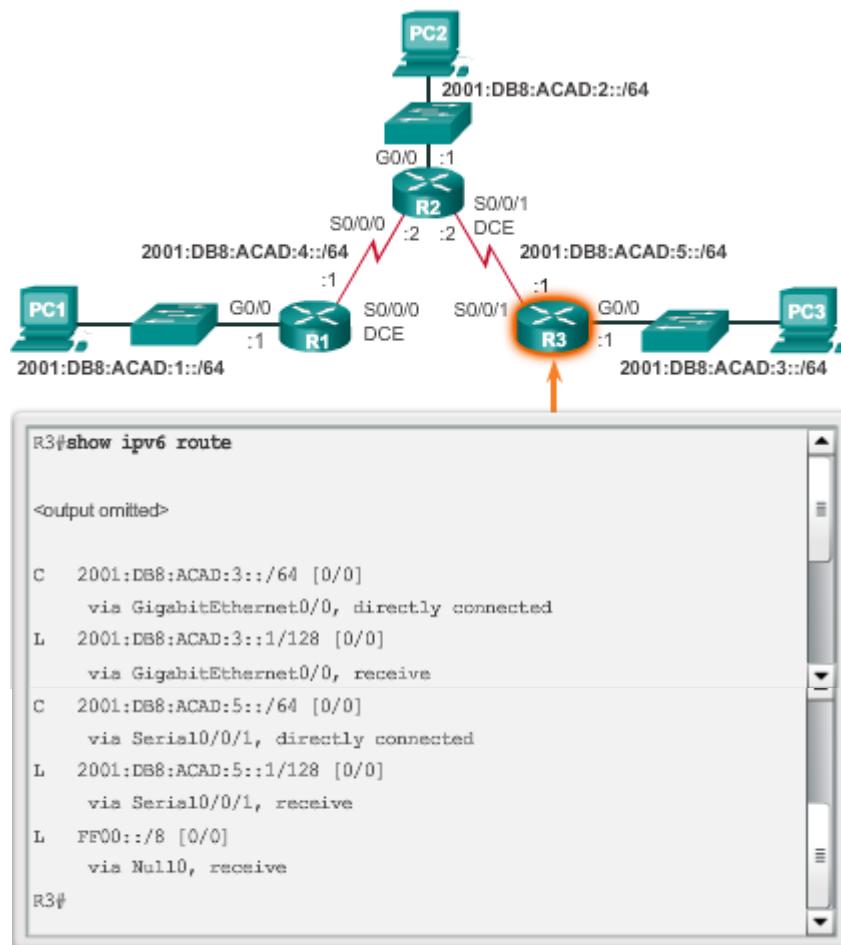
Verificación de la tabla de routing IPv6 del R1



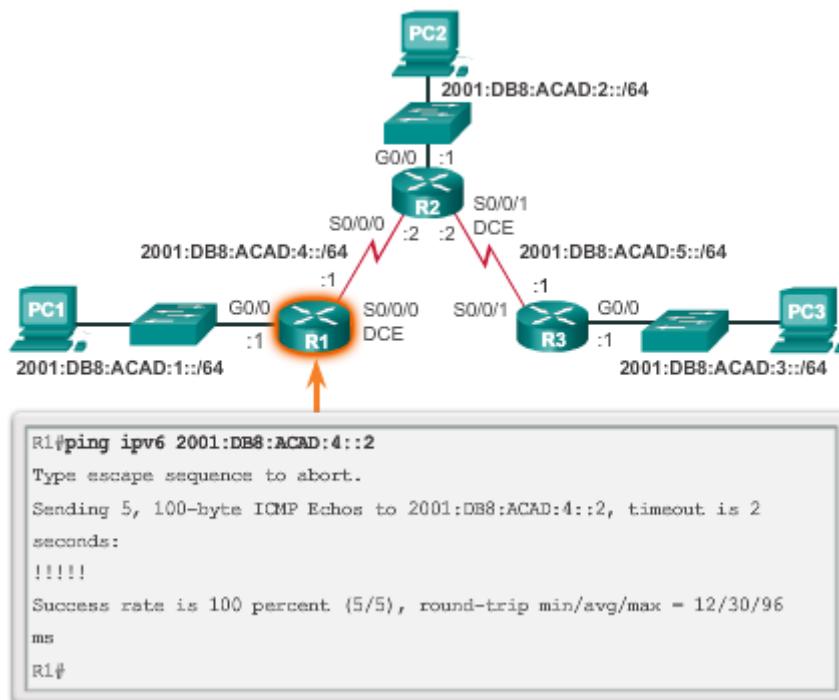
Verificación de la tabla de routing IPv6 del R2



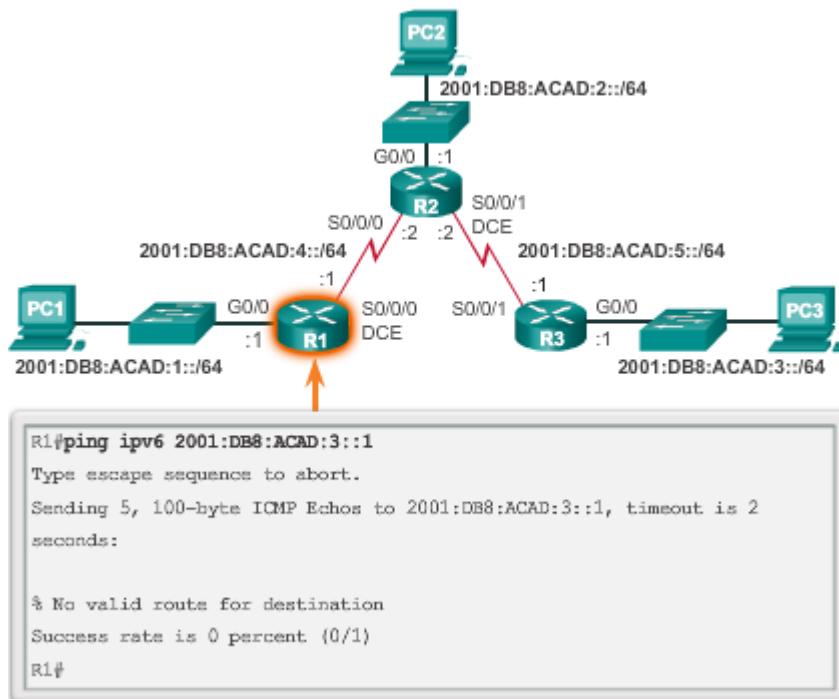
Verificación de la tabla de routing IPv6 del R3



Verificación de la conectividad del R1 al R2



Verificación de la conectividad del R1 a la LAN del R3



En una ruta estática de siguiente salto, solo se especifica la dirección IPv6 del siguiente salto. La interfaz de salida se deriva del siguiente salto. Por ejemplo, en la figura 1, se configuran tres rutas estáticas de siguiente salto en el R1.

Al igual que con IPv4, antes de que un router reenvíe un paquete, el proceso de la tabla de routing debe resolver la ruta para determinar qué interfaz de salida se utilizará para reenviar el paquete. El proceso de resolución de la ruta varía en función del tipo de mecanismo de reenvío que utiliza el router. CEF (Cisco Express Forwarding) es el comportamiento predeterminado en la mayoría de las plataformas que ejecutan el IOS 12.0 o posterior.

En la figura 2, se detalla el proceso básico de resolución de la ruta para el reenvío de paquetes en la tabla de routing para el R1 sin el uso de CEF. Cuando un paquete está destinado a la red 2001:DB8:ACAD:3::/64, el R1:

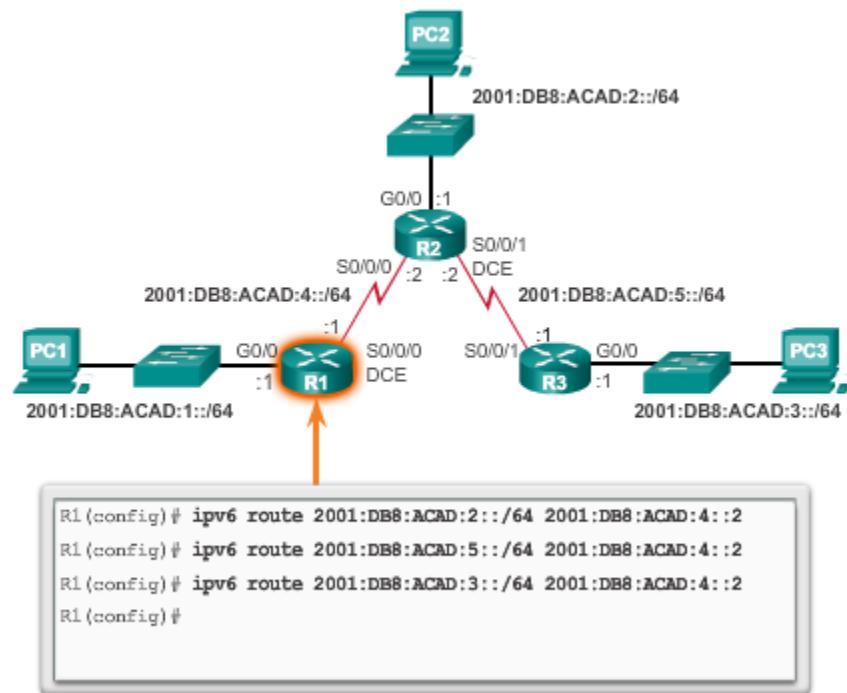
1. Busca una coincidencia en la tabla de routing y encuentra que debe reenviar paquetes a la dirección IPv6 2001:DB8:ACAD:4::2 del siguiente salto. Todas las rutas que hacen referencia solo a la dirección IPv6 del siguiente salto y que no hacen referencia a una interfaz de salida deben resolver la dirección IPv6 del siguiente salto con otra ruta de la tabla de routing que tenga una interfaz de salida.
2. En esta instancia, el R1 debe determinar cómo alcanzar la dirección 2001:DB8:ACAD:4::2. Por lo tanto, busca una coincidencia por segunda vez. En este caso, la dirección IPv6 coincide con la ruta para la red conectada directamente 2001:DB8:ACAD:4::/64 con la interfaz de salida Serial 0/0/0. Esta búsqueda le comunica al proceso de la tabla de routing que este paquete se reenvía fuera de esa interfaz.

Por lo tanto, en realidad, se requieren dos procesos de búsqueda en la tabla de routing para reenviar cualquier paquete a la red 2001:DB8:ACAD:3::/64. Cuando el router tiene que realizar múltiples búsquedas en la tabla de enrutamiento antes de reenviar un paquete, éste realiza un proceso que se conoce como búsqueda recurrente.

Una ruta estática IPv6 recursiva es válida (es decir, es candidata para agregarse a la tabla de routing) solo cuando el siguiente salto especificado resuelve a una interfaz de salida válida, ya sea de forma directa o indirecta.

Utilice el verificador de sintaxis en las figuras 3 y 4 para configurar las rutas estáticas IPv6 de siguiente salto.

Configuración de rutas estáticas IPv6 de siguiente salto



Verificación de una búsqueda de siguiente salto de IPv6

```
R1# show ipv6 route
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,
       OM2 - OSPF NSSA ext 2
C  2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
S  2001:DB8:ACAD:2::/64 [1/0]
    via 2001:DB8:ACAD:4::2
1  S  2001:DB8:ACAD:3::/64 [1/0]
    via 2001:DB8:ACAD:4::2
2  C  2001:DB8:ACAD:4::/64 [0/0]
    via Serial0/0/0, directly connected
L  2001:DB8:ACAD:4::1/128 [0/0]
    via Serial0/0/0, receive
S  2001:DB8:ACAD:5::/64 [1/0]
    via 2001:DB8:ACAD:4::2
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

Al configurar una ruta estática en redes punto a punto, una alternativa al uso de la dirección IPv6 de siguiente salto es especificar la interfaz de salida. Esto es una alternativa utilizada en IOS más antiguos o cada vez que se deshabilita CEF, para evitar el problema de búsquedas recursivas.

Por ejemplo, en la figura 1, se configuran tres rutas estáticas conectadas directamente en el R1 mediante la interfaz de salida.

La tabla de routing IPv6 para el R1 en la figura 2 muestra que cuando un paquete está destinado a la red 2001:DB8:ACAD:3::/64, el R1 busca una coincidencia en la tabla de routing y encuentra que puede reenviar el paquete desde su interfaz serial 0/0/0. No se necesita ninguna otra búsqueda.

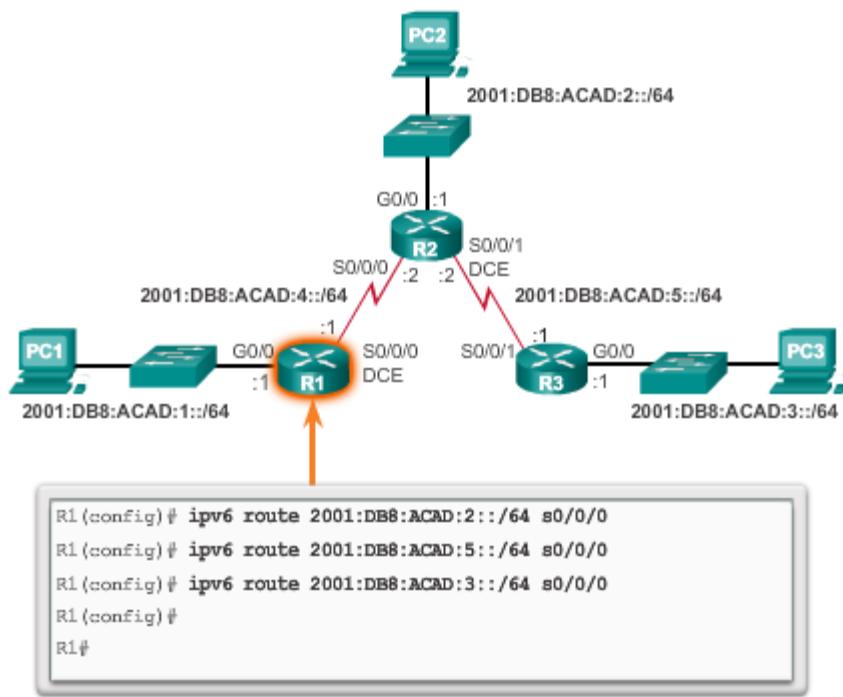
Observe que la tabla de routing se ve diferente para la ruta configurada con una interfaz de salida que para la ruta configurada con una entrada recursiva.

La configuración de una ruta estática conectada directamente con una interfaz de salida permite que la tabla de routing resuelva esta interfaz en una única búsqueda, no en dos. Recuerde que con el uso del mecanismo de reenvío CEF, las rutas estáticas con una interfaz de salida se consideran

innecesarias. Se realiza una única búsqueda utilizando una combinación de la FIB y la tabla de adyacencia almacenadas en el plano de datos.

Utilice el verificador de sintaxis en las figuras 3 y 4 para configurar las rutas estáticas IPv6 conectadas directamente en el R1.

Configuración de rutas estáticas IPv6 conectadas directamente en el R1



Verificación de la tabla de routing del R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-
user Static route
          B - EGP, 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
C  2001:DB8:ACAD:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L  2001:DB8:ACAD:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
S  2001:DB8:ACAD:2::/64 [1/0]
    via Serial0/0/0, directly connected
S  2001:DB8:ACAD:3::/64 [1/0]
    via Serial0/0/0, directly connected
C  2001:DB8:ACAD:4::/64 [0/0]
    via Serial0/0/0, directly connected
L  2001:DB8:ACAD:4::1/128 [0/0]
    via Serial0/0/0, receive
S  2001:DB8:ACAD:5::/64 [1/0]
    via Serial0/0/0, directly connected
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

Una ruta estática completamente especificada tiene determinadas tanto la interfaz de salida como la dirección IPv6 del siguiente salto. De modo similar a las rutas estáticas completamente especificadas que se utilizan con IPv4, esto se usaría si CEF no estuviera habilitado en el router y la interfaz de salida estuviera en una red multiacceso. Con CEF, una ruta estática que solo utiliza una dirección IPv6 del siguiente salto sería el método preferido incluso cuando la interfaz de salida sea una red multiacceso.

A diferencia de IPv4, hay una situación en IPv6 que se da cuando se debe utilizar una ruta estática completamente especificada. Si la ruta estática IPv6 usa una dirección IPv6 link-local como la dirección del siguiente salto, debe utilizarse una ruta estática completamente especificada que incluya la interfaz de salida. En la figura 1, se muestra un ejemplo de una ruta estática IPv6 completamente calificada que utiliza una dirección IPv6 link-local como la dirección del siguiente salto.

La razón por la cual se debe utilizar una ruta estática completamente especificada es que las direcciones IPv6 link-local no están incluidas en la tabla de routing IPv6. Las direcciones link-local solo son exclusivas en una red o un enlace dados. La dirección link-local del siguiente salto puede ser una dirección válida en varias redes conectadas al router. Por lo tanto, es necesario que la interfaz de salida se incluya.

En la figura 1, se configura una ruta estática completamente especificada con la dirección link-local del R2 como dirección del siguiente salto. Observe que el IOS requiere que se especifique una interfaz de salida.

En la figura 2, se muestra la entrada de la tabla de routing IPv6 para esta ruta. Observe que la dirección link-local del siguiente salto y la interfaz de salida están incluidas.

Utilice el verificador de sintaxis en la figura 3 para configurar las rutas estáticas IPv6 completamente especificadas en el R2, a fin de que alcancen la LAN del R1 mediante una dirección link-local.

Configuración de rutas estáticas IPv6 completamente especificadas en el R1



```
R1(config)# ipv6 route 2001:db8:acad:2::/64 fe80::2
% Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:2::/64 s0/0/0 fe80::2
R1(config)#End
```

Verificación de la tabla de routing del R1

```
R1# show ipv6 route static | begin 2001:DB8:ACAD:2::/64
S 2001:DB8:ACAD:2::/64 [1/0]
via FE80::2, Serial0/0/0
```

Además de los comandos **ping** y **traceroute**, otros comandos útiles para verificar las rutas estáticas son los siguientes:

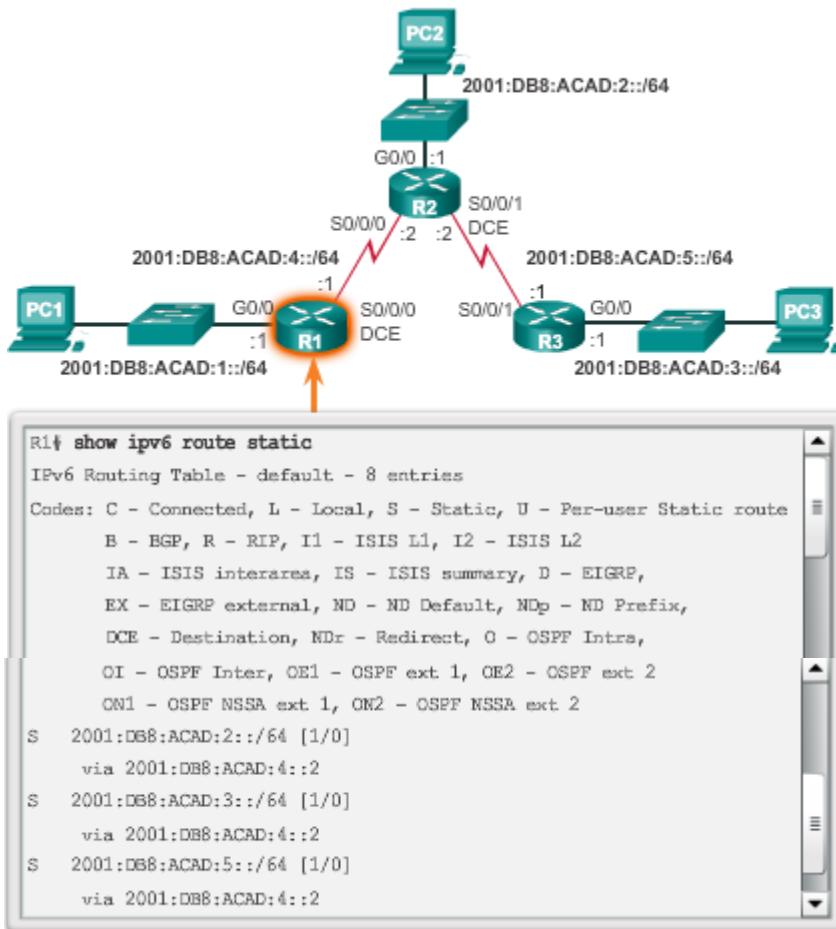
- **show ipv6 route**
- **show ipv6 route static**
- **show ipv6 route Capa de red**

En la figura 1, se muestra un ejemplo del resultado que genera el comando **show ipv6 route static**. El resultado refleja el uso de rutas estáticas con las direcciones de unidifusión global del siguiente salto.

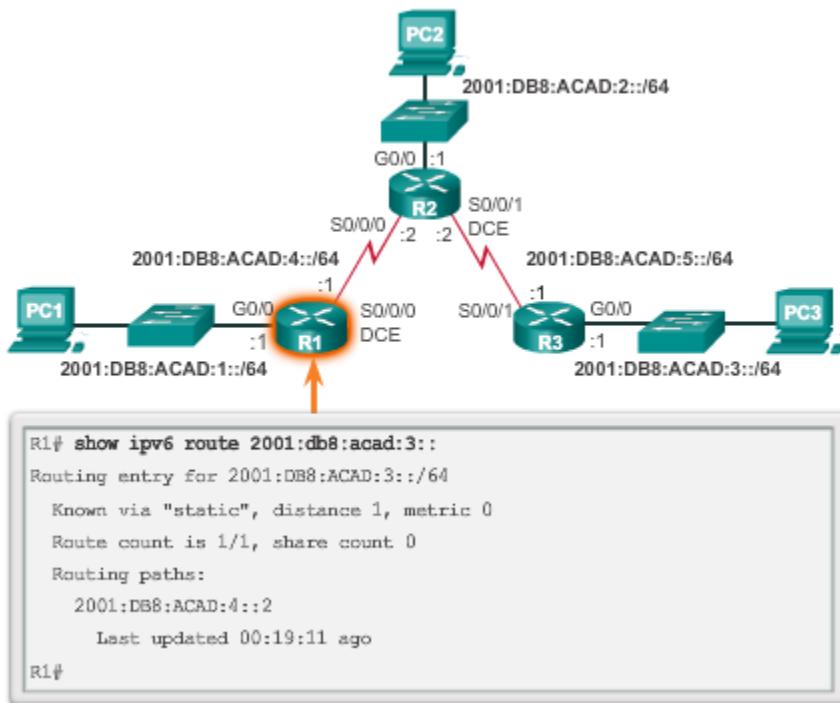
En la figura 2, se muestra un ejemplo del resultado que genera el comando **show ip route 2001:DB8:ACAD:3::**.

En la figura 3, se verifica la configuración de **ipv6 route** en la configuración en ejecución.

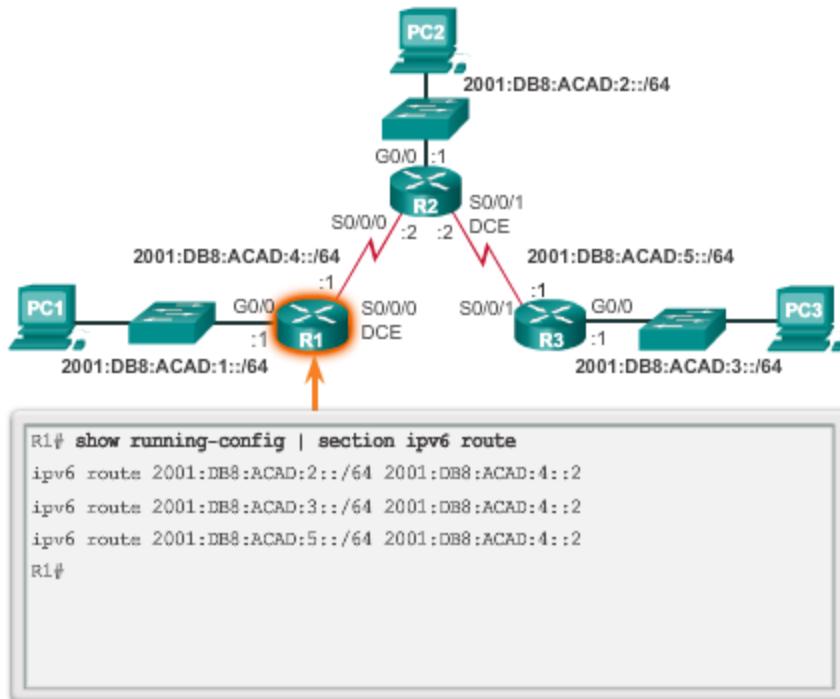
Verificación de la tabla de routing del R1



Verificación de una entrada específica en la tabla de routing



Verificación de la configuración de rutas estáticas



6.3.4 Configuración de rutas IPv6 predeterminadas

Una ruta predeterminada es una ruta estática que coincide con todos los paquetes. En lugar de almacenar rutas para todas las redes en Internet, los routers pueden almacenar una única ruta predeterminada que represente cualquier red que no esté en la tabla de routing.

Los routers suelen utilizar rutas predeterminadas configuradas de forma local, o bien, descubiertas por otro router, mediante un protocolo de routing dinámico. Se utilizan cuando ninguna otra ruta coincide con la dirección IP de destino del paquete en la tabla de routing. Es decir, si no existe una coincidencia más específica, entonces se utiliza la ruta predeterminada como el gateway de último recurso.

En general, las rutas estáticas predeterminadas se utilizan al conectar:

- El router perimetral de una empresa a la red de un proveedor de servicios.
- Un router con solo un router vecino ascendente. El router no tiene otros vecinos y, por lo tanto, se denomina “router de rutas internas”.

Como se muestra en la ilustración, la sintaxis del comando para una ruta estática predeterminada es similar a la sintaxis del comando de cualquier otra ruta estática, excepto que prefijo-ipv6/longitud-prefijo es **::/0**, y coincide con todas las rutas.

La sintaxis del comando básico de una ruta estática predeterminada es la siguiente:

- **ipv6 route ::/0 { dirección-ipv6 | interfaz-salida }**

Sintaxis de ruta estática predeterminada IPv6

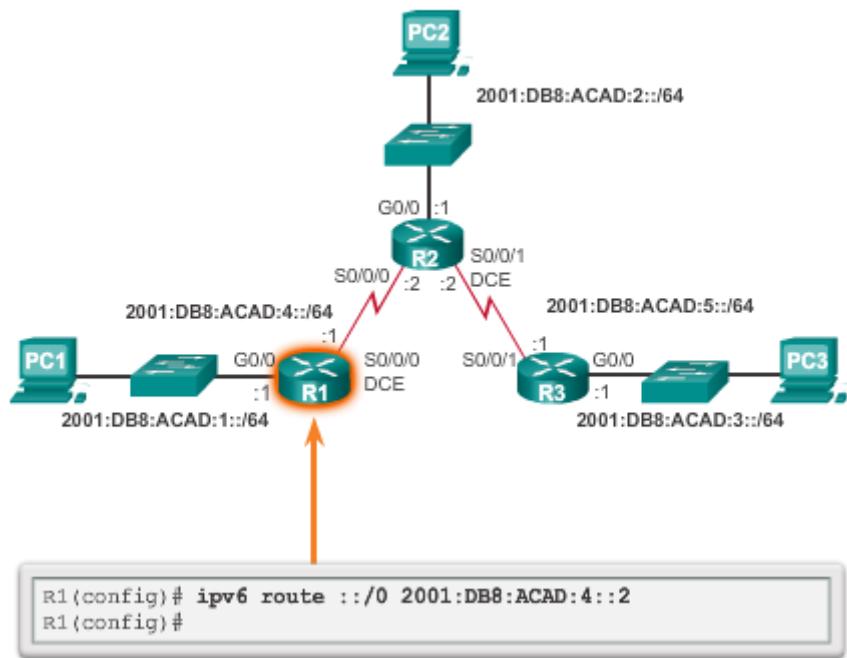
```
Router(config)# ipv6 route ::/0 (ipv6-address | exit-intf)
```

Parámetro	Descripción
::/0	Coincide con cualquier prefijo IPv6 independientemente de la longitud de prefijo.
dirección-ipv6	<ul style="list-style-type: none"> • Se la suele denominar “dirección IPv6 del router de siguiente salto”. • Suele utilizarse para la conexión a un medio de difusión (es decir, Ethernet). • Por lo general, crea una búsqueda recursiva.
interfaz-salida	<ul style="list-style-type: none"> • Use la interfaz de salida para reenviar paquetes a la red de destino. • También se la denomina “ruta estática conectada directamente”. • Suele utilizarse para conectarse en una configuración punto a punto.

El R1 puede configurarse con tres rutas estáticas para alcanzar todas las redes remotas en la topología. Sin embargo, el R1 es un router de rutas internas, ya que está conectado únicamente al R2. Por lo tanto, sería más eficaz configurar una ruta estática predeterminada IPv6.

El ejemplo en la ilustración muestra una configuración de una ruta estática predeterminada IPv6 en el R1.

Configuración de una ruta estática predeterminada IPv6



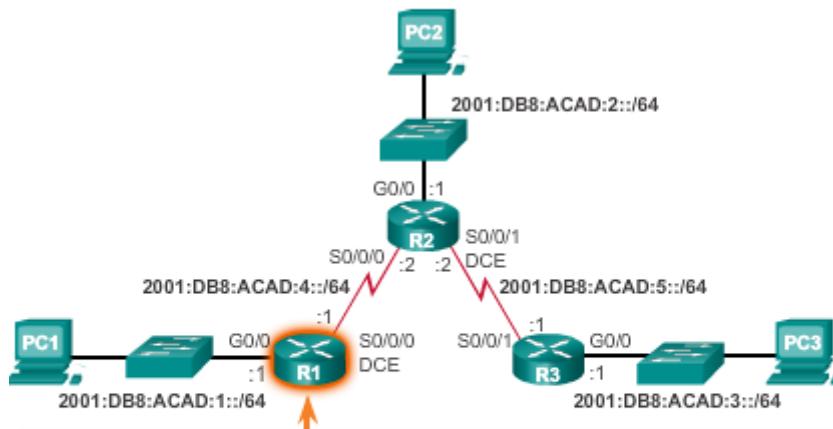
En la figura 1, el resultado del comando **show ipv6 route static** muestra el contenido de la tabla de routing.

A diferencia de IPv4, IPv6 no establece en forma explícita que la ruta estática predeterminada IPv6 es el gateway de último recurso.

La clave para esta configuración es la máscara **::/0**. Recuerde que la longitud-de-prefijo de ipv6 en una tabla de routing determina cuántos bits deben coincidir entre la dirección IP de destino del paquete y la ruta en la tabla de routing. La máscara **::/0** indica que no se requiere que ninguno de los bits coincida. Mientras no exista una coincidencia más específica, la ruta estática predeterminada IPv6 coincide con todos los paquetes.

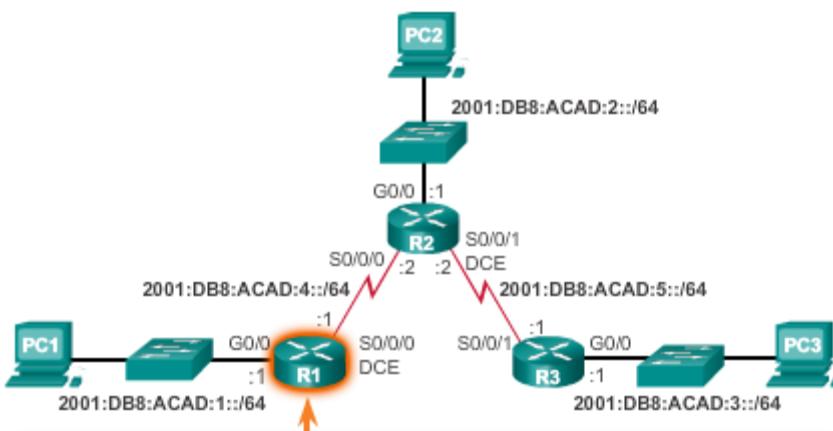
En la figura 2, se muestra un ping correcto a la interfaz LAN del R3.

Verificación de la tabla de routing del R1



```
R1# show ipv6 route static
IPv6 Routing Table - default - 6 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
S  ::/0 [1/0]
      via 2001:DB8:ACAD:4::2
R1#
```

Verificación de la conectividad a la LAN del R3



```
R1# ping 2001:0DB8:ACAD:3::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:3::1,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max
= 28/28/28 ms
R1#
```

6.4 Revisión de CIDR y VLSM

6.4.1 Direccionamiento con clase

Lanzadas en 1981, RFC 790 y RFC 791 describen cómo se asignaron inicialmente las direcciones de red IPv4 según un sistema de clasificación. En la especificación original de IPv4, los autores establecieron las clases para proporcionar tres tamaños distintos de redes para organizaciones grandes, medianas y pequeñas. Por consiguiente, se definieron las direcciones de clase A, B y C con un formato específico para los bits de orden superior. Los bits de orden superior son los bits del extremo izquierdo en una dirección de 32 bits.

Como se muestra en la figura:

- **Direcciones de clase A que comienzan con 0:** diseñadas para organizaciones grandes. Esta clase incluye todas las direcciones de 0.0.0.0 (**00000000**) a 127.255.255.255 (**01111111**). La dirección 0.0.0.0 se reserva para el routing predeterminado y la dirección 127.0.0.0, para la prueba de loopback.
- **Direcciones de clase B que comienzan con 10:** diseñadas para organizaciones medianas a grandes. Esta clase incluye todas las direcciones de 128.0.0.0 (**10000000**) a 191.255.255.255 (**10111111**).
- **Direcciones de clase C que comienzan con 110:** diseñadas para organizaciones pequeñas a medianas. Esta clase incluye todas las direcciones de 192.0.0.0 (**11000000**) a 223.255.255.255 (**11011111**).

Las direcciones restantes se reservaron para multicasting y futuros usos.

- **Direcciones de multidifusión de clase D que comienzan con 1110:** las direcciones de multidifusión se utilizan para identificar un grupo de hosts que forman parte de un grupo de multidifusión. Esto ayuda a reducir la cantidad de procesamientos de paquetes que realizan los hosts, en especial en los medios de difusión (es decir, las LAN Ethernet). Los protocolos de routing, como RIPv2, EIGRP y OSPF, utilizan direcciones de multidifusión designadas (RIP = 224.0.0.9, EIGRP = 224.0.0.10, OSPF 224.0.0.5 y 224.0.0.6).
- **Direcciones IP de clase E reservadas que comienzan con 1111:** estas direcciones se reservaron para uso experimental y futuro.

Enlaces:

"Internet Protocol", (Protocolo de Internet):<http://www.ietf.org/rfc/rfc791.txt>

"Internet Multicast Addresses", (Direcciones multicast de Internet):<http://www.iana.org/assignments/multicast-addresses>

Bits de orden superior

Clase	Bits de orden superior	Inicio	Finalizar
Clase A	0xxxxxx	0.0.0.0	127.255.255.255
Clase B	10xxxxx	128.0.0.0	191.255.255.255
Clase C	110xxxx	192.0.0.0	223.255.255.255
Clase D (multidifusión)	1110xxx	224.0.0.0	239.255.255.255
Clase E (reservada)	1111xxx	240.0.0.0	255.255.255.255

Como se especifica en RFC 790, cada clase de red tiene asociada una máscara de subred predeterminada.

Como se muestra en la figura 1, las redes de clase A utilizan el primer octeto para identificar la porción de red de la dirección. Esto se traduce a una máscara de subred con clase 255.0.0.0. Debido a que solo se dejaron 7 bits en el primer octeto (recuerde que el primer bit es siempre 0), se elevó el 2 a la 7.a potencia, o se generaron 128 redes. El número real es de 126 redes, porque hay dos direcciones reservadas de clase A (es decir, 0.0.0.0/8 y 127.0.0.0/8). Con 24 bits en la porción de host, cada dirección de clase A tenía capacidad para más de 16 millones de direcciones host individuales.

Como se muestra en la figura 2, las redes de clase B utilizan los dos primeros octetos para identificar la porción de red de la dirección de red. Con los primeros dos bits ya establecidos en 1 y 0, quedaban 14 bits en los primeros dos octetos para asignar redes, lo que produjo 16 384 direcciones de red de clase B. Debido a que cada dirección de red de clase B contenía 16 bits en la porción de host, controlaba 65 534 direcciones. (Recuerde que dos direcciones se reservaron para las direcciones de red y de difusión).

Como se muestra en la figura 3, las redes de clase C utilizan los dos primeros octetos para identificar la porción de red de la dirección de red. Con los primeros tres bits establecidos en 1 y 1, y 0, quedaban 21 bits para asignar redes para más de 2 millones de redes de clase C. Pero cada red de clase C sólo tenía 8 bits en la porción de host o 254 direcciones host posibles.

Una ventaja de asignar máscaras de subred predeterminadas específicas a cada clase es que reduce los mensajes de actualización de routing. Los protocolos de routing con clase no incluyen la información de la máscara de subred en las actualizaciones. El router receptor aplica la máscara predeterminada según el valor del primer octeto que identifica la clase.

Redes de clase A

	1er. octeto	2º octeto	3er. octeto	4º octeto
Siempre comienza con binario 0:	0xxxxxx			
Equivalente decimal:	0-127			

	Red	Host	Host	Host
Máscara de subred	255	.0	.0	.0

Redes de clase B

	1er. octeto	2º octeto	3er. octeto	4º octeto
Siempre comienza con binario 10:	10xxxxxx	xxxxxxx		
Equivalente decimal:	128-191	0-255		

	Red	Red	Host	Host
Máscara de subred	255	.255	.0	.0

Redes de clase C

	1er. octeto	2º octeto	3er. octeto	4º octeto
Siempre comienza con binario 110:	110xxxxx	xxxxxxx	xxxxxxx	
Equivalente decimal:	192-223	0-255	0-255	

	Red	Red	Red	Host
Máscara de subred	255	.255	.255	.0

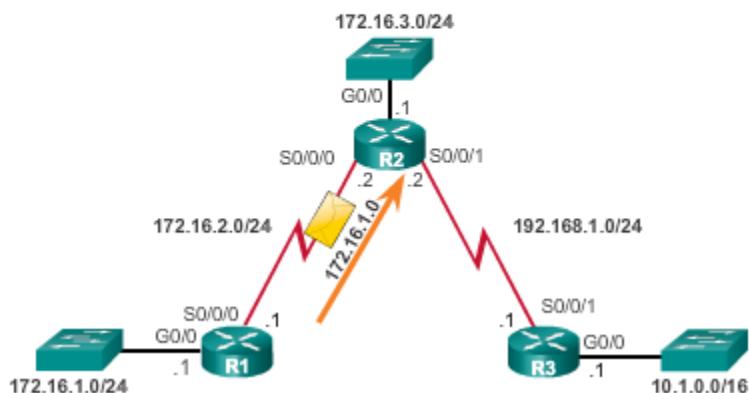
El uso de direcciones IP con clase significaba que la máscara de subred podía determinarse por el valor del primer octeto, o más precisamente, los primeros tres bits de la dirección. Los protocolos de routing, como RIPv1, solo necesitan propagar la dirección de red de las rutas conocidas y no

necesitan incluir la máscara de subred en la actualización de routing. Esto se debe a que el router que recibe la actualización de routing determina la máscara de subred con solo examinar el valor del primer octeto de la dirección de red o al aplicar su máscara de interfaz de entrada para las rutas divididas en subredes. La máscara de subred estaba directamente relacionada con la dirección de red.

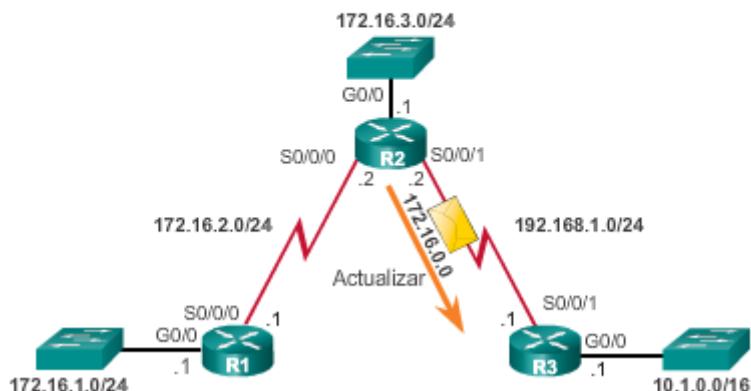
En la figura 1, el R1 envía una actualización al R2. En el ejemplo, R1 tiene información de que la subred 172.16.1.0 pertenece a la misma red principal con clase que la interfaz saliente. Por lo tanto, le envía una actualización RIP a R2 que contiene la subred 172.16.1.0. Cuando R2 recibe la actualización, aplica la máscara de subred de la interfaz receptora (/24) a la actualización y agrega 172.16.1.0 a la tabla de enrutamiento.

En la figura 2, el R2 envía una actualización al R3. Cuando se envían actualizaciones a R3, R2 resume las subredes 172.16.1.0/24, 172.16.2.0/24 y 172.16.3.0/24 en la red principal con clase 172.16.0.0. Debido a que el R3 no tiene ninguna subred que pertenezca a 172.16.0.0, aplica la máscara con clase para una red de clase B, /16.

Actualizaciones de routing con clase



Actualizaciones de routing con clase



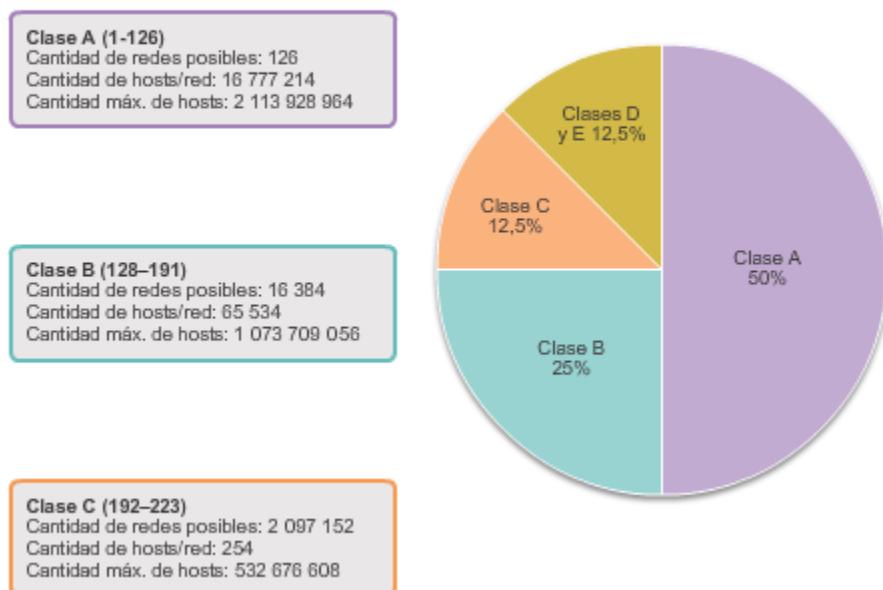
El direccionamiento con clase especificado en las RFC 790 y 791 generaba un enorme desperdicio de espacio de direcciones. En los albores de Internet, se asignó a las organizaciones una dirección de red con clase completa de clase A, B o C.

Como se muestra en la ilustración:

- La clase A tenía el 50% del espacio de direcciones total. Sin embargo, solo podía asignarse una dirección de red de clase A a 126 organizaciones. Lo ridículo era que cada una de estas organizaciones podía proporcionar direcciones para un máximo de 16 millones de hosts. A las organizaciones muy grandes se les asignaban bloques de direcciones enteros de clase A. Algunas empresas y organizaciones gubernamentales aún tienen direcciones de clase A. Por ejemplo, General Electric posee 3.0.0.0/8, Apple Computer, 17.0.0.0/8, y el servicio postal de los Estados Unidos, 56.0.0.0/8.
- La clase B tenía el 25% del espacio de direcciones total. Hasta 16 384 organizaciones podían tener asignada una dirección de red de clase B, y cada una de estas redes podía admitir hasta 65 534 hosts. Sólo las organizaciones más grandes y los gobiernos podían llegar a usar alguna vez las 65 000 direcciones. Al igual que las redes de clase A, muchas direcciones IP en el espacio de direcciones de clase B se perdían.
- La clase C tenía el 12,5% del espacio de direcciones total. Muchas más organizaciones podían obtener las redes de clase C, pero estaban limitadas en el número total de hosts que podían conectar. De hecho, en muchos casos, las direcciones de clase C eran a menudo demasiado pequeñas para la mayoría de las organizaciones medianas.
- Las clases D y E se utilizan para direcciones de multidifusión y reservadas.

El resultado general fue que el direccionamiento con clase era un esquema de direccionamiento que generaba mucho desperdicio. Debía desarrollarse una mejor solución para el direccionamiento de red. Por este motivo, en 1993, se introdujo el routing entre dominios sin clase (CIDR).

Asignación de dirección IP con clase = ineficaz



6.4.2 CIDR

Del mismo modo en que Internet crecía a un ritmo exponencial a principios de la década de los noventa, el tamaño de las tablas de routing que los routers de Internet mantenían también crecía bajo el direccionamiento IP con clase. Por este motivo, la IETF introdujo el CIDR en la RFC 1517 en 1993.

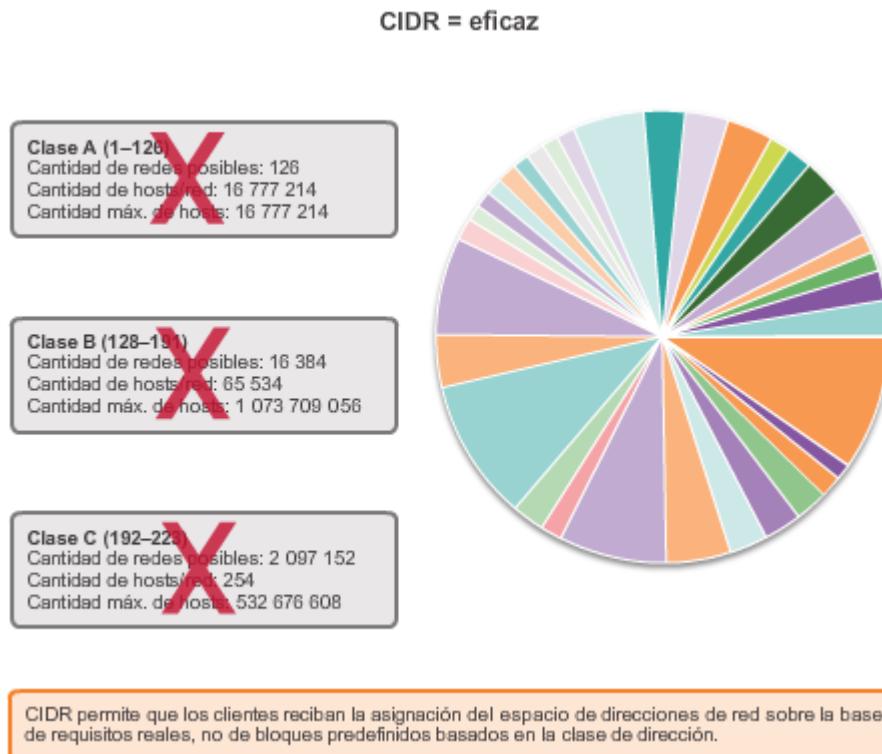
El CIDR reemplazó las asignaciones de red con clase y las clases de direcciones (A, B, C) se volvieron obsoletas. Con el CIDR, el valor del primer octeto ya no determina la dirección de red. En cambio, la porción de red de la dirección la determina la máscara de subred, también conocida como “prefijo de red” o “longitud de prefijo” (es decir, /8, /19, etc.).

Los ISP ya no están limitados a una máscara de subred de /8, /16 o /24. Ahora pueden asignar espacio de direcciones de manera más eficaz mediante el uso de cualquier longitud de prefijo que comience con /8 y valores superiores (es decir, /8, /9, /10, etc.). En la ilustración, se muestra de qué manera los bloques de direcciones IP se pueden asignar a una red en función de los requisitos del cliente, que pueden variar de unos pocos hosts a cientos o miles de hosts.

El CIDR también reduce el tamaño de las tablas de routing y administra el espacio de direcciones IPv4 con mayor eficacia mediante:

- **Sumarización de ruta:** también conocida como “agregación de prefijos”. Las rutas se resumen en una única ruta para ayudar a reducir el tamaño de las tablas de routing. Por ejemplo, una ruta estática resumida puede reemplazar varias instrucciones de rutas estáticas específicas.
- **Creación de superredes:** ocurre cuando la máscara de sumarización de ruta es un valor menor que la máscara con clase predeterminada tradicional.

Nota: una superred siempre es un resumen de rutas, pero un resumen de rutas no siempre es una superred.



En la ilustración, observe que el ISP1 tiene cuatro clientes y que cada uno tiene una cantidad variable de espacio de direcciones IP. El espacio de direcciones de los cuatro clientes puede resumirse en un anuncio para el ISP2. La ruta 192.168.0.0/20 resumida o agregada incluye todas las redes que pertenecen a los clientes A, B, C y D. Este tipo de ruta se conoce como “ruta de superred”. Una superred resume varias direcciones de red con una máscara menor que la máscara con clase.

La determinación de la ruta resumida y la máscara de subred para un grupo de redes se puede realizar en tres pasos:

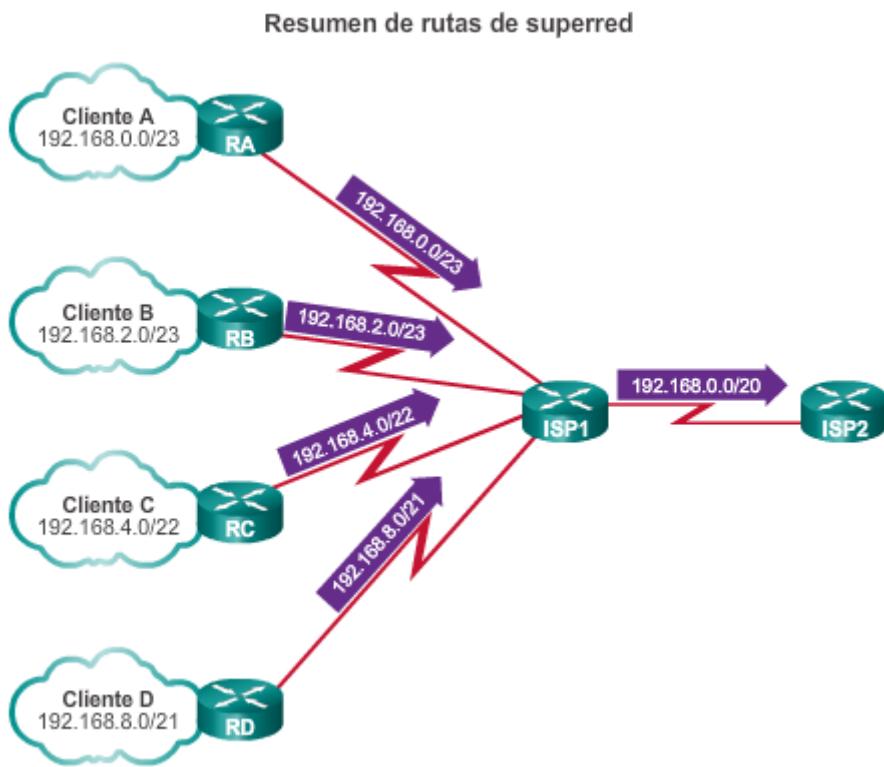
Paso 1. Enumere las redes en formato binario.

Paso 2. Cuente el número de bits coincidentes del extremo izquierdo. Esta es la longitud de prefijo o máscara de subred de la ruta resumida.

Paso 3. Copie los bits coincidentes y luego agregue los bits 0 al resto de la dirección para determinar la dirección de red resumida.

La dirección de red sumarizada y la máscara de subred ahora pueden usarse como ruta sumarizada para este grupo de redes.

Las rutas resumidas pueden configurarse por medio de rutas estáticas y protocolos de routing sin clase.

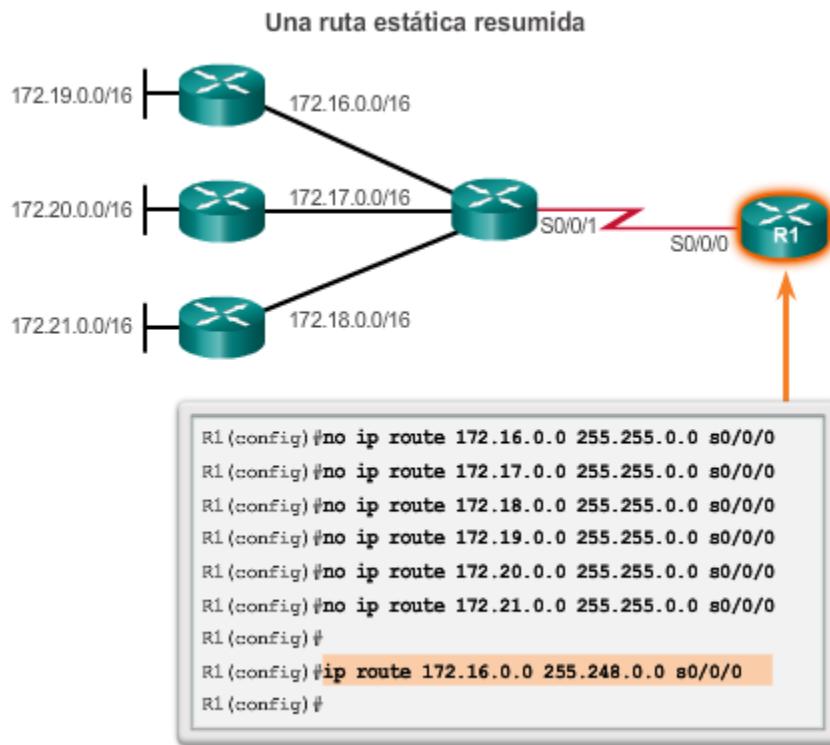
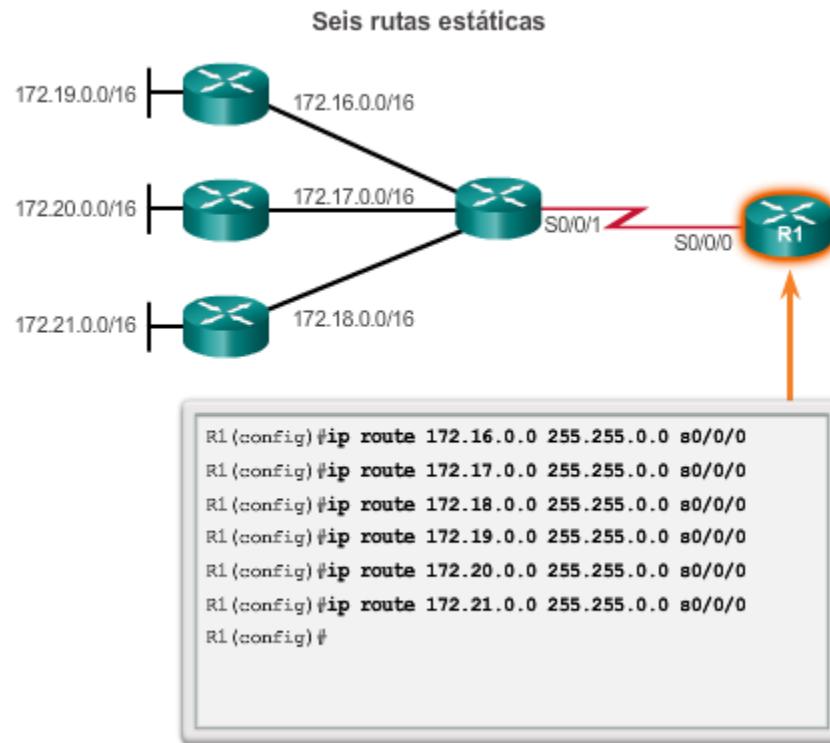


La creación de tablas de enrutamiento más pequeñas hace que el proceso de búsqueda en la tabla de enrutamiento sea más eficaz ya que existen menos rutas para buscar. Si se puede utilizar una ruta estática en lugar de varias, se reduce el tamaño de la tabla de routing. En muchos casos, se puede usar una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

Las rutas resumidas CIDR se pueden configurar mediante rutas estáticas. Esto contribuye a reducir el tamaño de las tablas de routing.

En la figura 1, el R1 se configuró para alcanzar las redes identificadas en la topología. Si bien es aceptable, sería más eficaz configurar una ruta estática resumida.

En la figura 2, se proporciona una solución con utilizando la summarización CIDR. Las seis entradas de ruta estática se podrían reducir a la entrada 172.16.0.0/13. En el ejemplo, se eliminan las seis entradas de ruta estática y se las reemplaza con una ruta estática resumida.

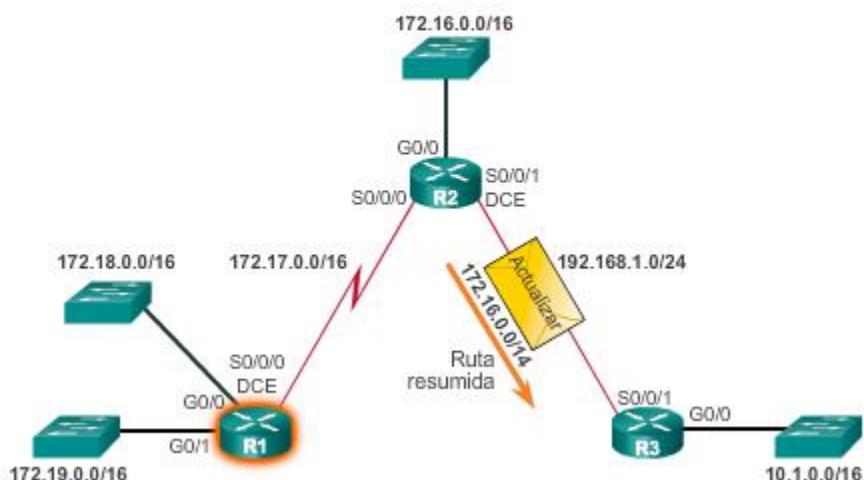


Los protocolos de routing con clase no pueden enviar rutas de superred. Esto se debe a que el router receptor aplica de forma automática la máscara de subred con clase predeterminada a la dirección de red en la actualización de routing. Si la topología en la ilustración tuviera un protocolo de routing con clase, entonces el R3 solo instalaría 172.16.0.0/16 en la tabla de routing.

La propagación de las rutas VLSM y de superred requiere un protocolo de routing sin clase, como RIPv2, OSPF o EIGRP. Los protocolos de routing sin clase anuncian las direcciones de red junto con las máscaras de subred asociadas. Con un protocolo de routing sin clase, el R2 puede resumir las redes 172.16.0.0/16, 172.17.0.0/16, 172.18.0.0/16 y 172.19.0.0/16, y anunciar una ruta estática resumida de superred 172.16.0.0/14 al R3. A continuación, el R3 instala la ruta de superred 172.16.0.0/14 en la tabla de routing.

Nota: cuando una ruta de superred se encuentra en una tabla de routing, por ejemplo, como una ruta estática, un protocolo de routing con clase no incluye esa ruta en las actualizaciones.

Actualización de routing sin clase



6.4.3 VLSM

Con la máscara de subred de longitud fija (FLSM), se asigna la misma cantidad de direcciones a cada subred. Si todas las subredes tuvieran los mismos requisitos en cuanto a la cantidad de hosts, estos bloques de direcciones de tamaño fijo serían suficientes. Sin embargo, esto no es lo que suele suceder.

Nota: la FLSM también se suele denominar “división tradicional en subredes”.

La topología que se muestra en la figura 1 requiere que la dirección de red 192.168.20.0/24 se subdivida en siete subredes: una para cada una de las cuatro LAN (Edificios A a D) y una para cada una de las tres conexiones WAN entre los routers.

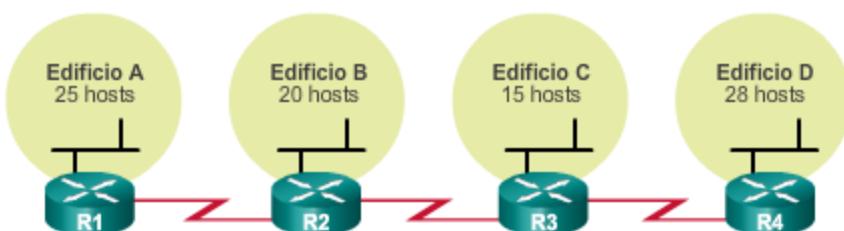
En la figura 2, se destaca la manera en que la división en subredes tradicional puede tomar prestados 3 bits de la porción de host en el último octeto para cumplir con el requisito de siete subredes. Por ejemplo, en la porción de host, la porción de subred destaca cómo el préstamo de 3 bits crea 8 subredes, mientras que la porción de host destaca 5 bits del host que proporcionan 30 direcciones IP de hosts utilizables por subred. Mediante este esquema, se crean las subredes necesarias y se cumplen los requisitos de host de la LAN más grande.

Si bien la división en subredes tradicional satisface las necesidades de la LAN más grande y divide el espacio de direcciones en una cantidad adecuada de subredes, da como resultado un desperdicio significativo de direcciones sin utilizar.

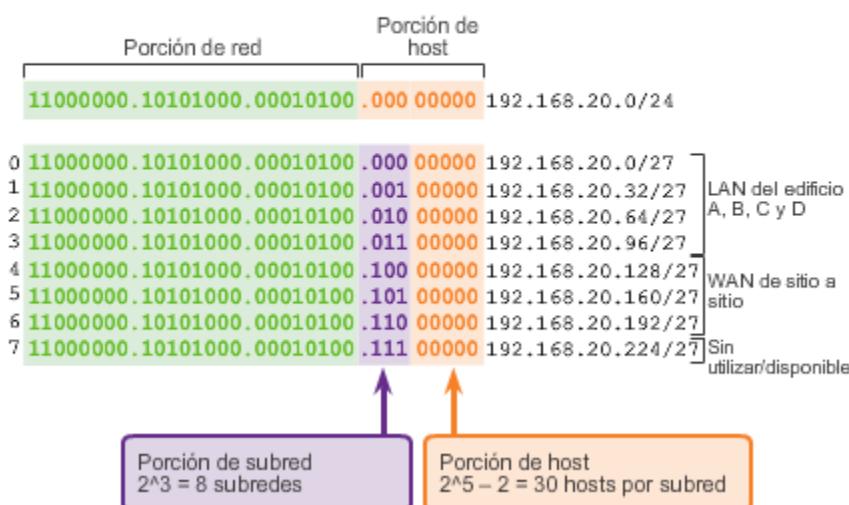
Por ejemplo, solo se necesitan dos direcciones en cada subred para los tres enlaces WAN. Dado que cada subred tiene 30 direcciones utilizables, hay 28 direcciones sin utilizar en cada una de estas subredes. Como se muestra en la figura 3, esto da como resultado 84 direcciones sin utilizar (28×3). Además, de esta forma se limita el crecimiento futuro al reducir el número total de subredes disponibles. Este uso ineficiente de las direcciones es característico de la división en subredes tradicional de redes con clase.

La aplicación de un esquema de división en subredes tradicional a esta situación no resulta muy eficiente y genera desperdicio. De hecho, este ejemplo es un modelo satisfactorio para mostrar cómo la división en subredes de una subred puede utilizarse para maximizar el uso de la dirección. La subdivisión de subredes, o el uso de una máscara de subred de longitud variable (VLSM), se diseñó para evitar que se desperdicien direcciones.

Topología de la red: subredes básicas



Esquema de subredes básico



Direcciones sin utilizar en subredes WAN

4 **11000000.10101000.00010100 .100 00000** 192.168.20.128/27
 5 **11000000.10101000.00010100 .101 00000** 192.168.20.160/27
 6 **11000000.10101000.00010100 .110 00000** 192.168.20.192/27

Nueva porción de host
 $2^5 - 2 = 30$ hosts por subred

$30 - 2 = 28$
 Cada subred WAN desperdicia 28 direcciones

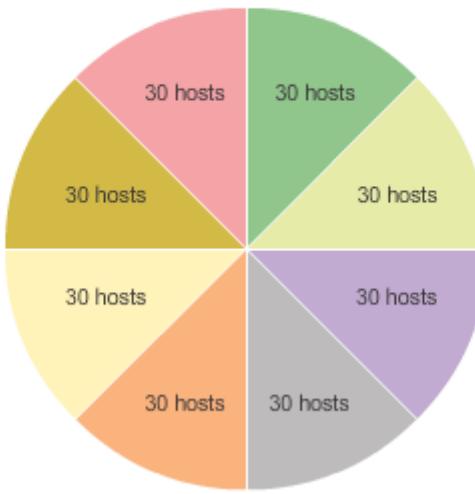
$28 \times 3 = 84$
 Hay 84 direcciones sin utilizar

En la división en subredes tradicional se aplica la misma máscara de subred a todas las subredes. Esto significa que cada subred tiene la misma cantidad de direcciones de host disponibles.

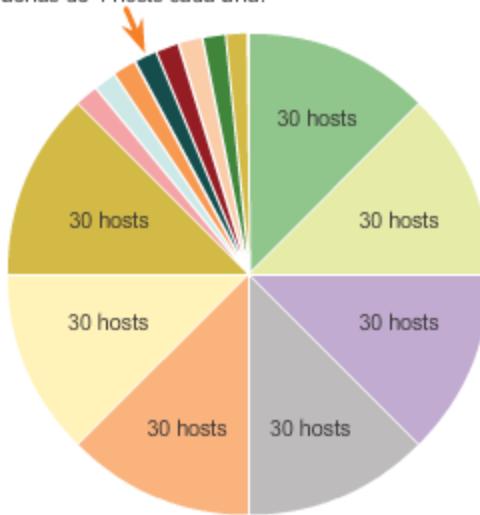
Como se ilustra en la figura 1, mediante la división en subredes tradicional se crean subredes de igual tamaño. Cada subred en un esquema tradicional utiliza la misma máscara de subred.

Con VLSM, la longitud de la máscara de subred varía según la cantidad de bits que se toman prestados para una subred específica, de lo cual deriva la parte “variable” de la máscara de subred de longitud variable. Como se muestra en la figura 2, VLSM permite dividir un espacio de red en partes desiguales.

La división en subredes de VLSM es similar a la división en subredes tradicional en cuanto a que se toman prestados bits para crear subredes. Las fórmulas para calcular la cantidad de hosts por subred y la cantidad de subredes que se crean también son válidas para VLSM. La diferencia es que la división en subredes no es una actividad que conste de un único paso. Con VLSM, la red primero se divide en subredes y, a continuación, las subredes se vuelven a dividir en subredes. Este proceso se puede repetir varias veces crear subredes de diversos tamaños.

La división en subredes tradicional crea subredes de igual tamaño**Subredes de distintos tamaños**

Una subred se subdividió para crear 8 subredes más pequeñas de 4 hosts cada una.



VLSM permite el uso de diferentes máscaras para cada subred. Después de que una dirección de red se divide en subredes, esas subredes también se pueden dividir en subredes. VLSM simplemente subdivide una subred. Se puede considerar a VLSM como una división en sub-subredes.

La figura muestra la red 10.0.0.0/8 que se ha dividido en subredes usando la máscara de subred de /16, lo que produce 256 subredes. Es decir 10.0.0.0/16, 10.1.0.0/16, 10.2.0.0/16, ..., 10.255.0.0/16. En la ilustración, se muestran cuatro de estas subredes de /16. Cualquiera de las subredes /16 pueden subdividirse aún más.

Haga clic en el botón Reproducir en la ilustración para ver la animación. En la animación:

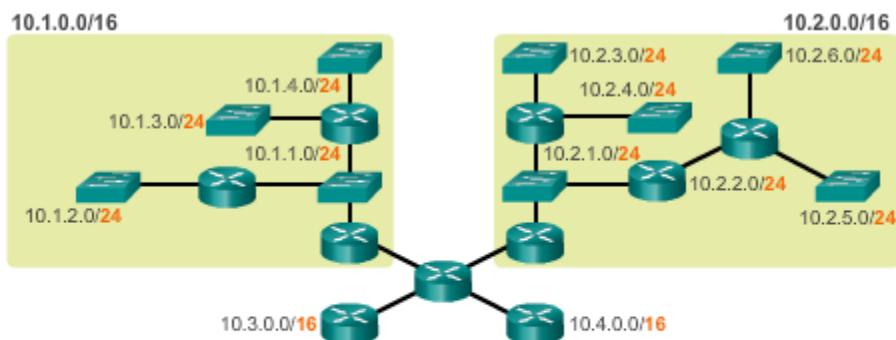
- La subred 10.1.0.0/16 se vuelve a dividir en subredes con la máscara /24.
- La subred 10.2.0.0/16 se vuelve a dividir en subredes con la máscara /24.
- La subred 10.3.0.0/16 se vuelve a dividir en subredes con la máscara /28.
- La subred 10.4.0.0/16 se vuelve a dividir en subredes con la máscara /20.

Las direcciones host individuales se asignan a partir de las direcciones de "sub-subredes". Por ejemplo, la figura muestra la subred 10.1.0.0/16 dividida en subredes de /24. La dirección 10.1.4.10 sería ahora miembro de la subred más específica 10.1.4.0/24.

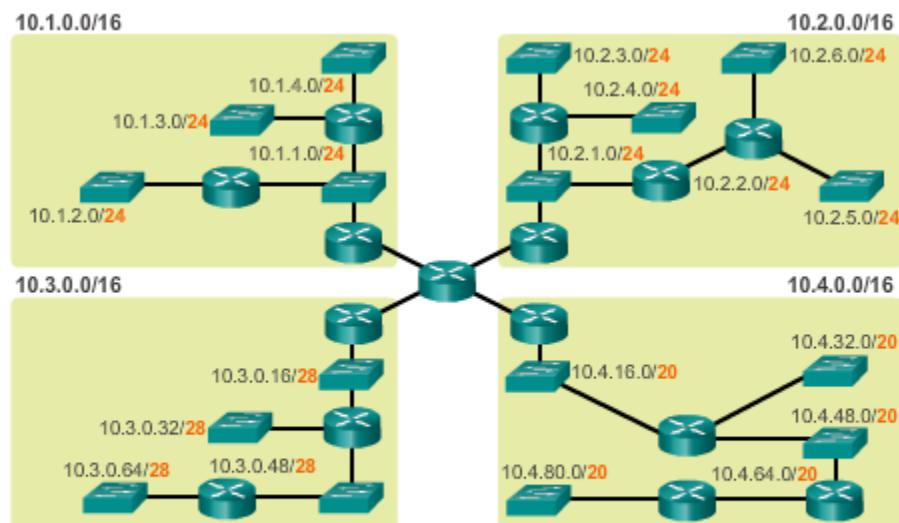
Subredes VLSM



La subred 10.0.0.0/8 se subdividió mediante la máscara de subred /16.



Cualquiera de las subredes /16 pueden subdividirse aún más. En este ejemplo, 10.1.0.0/16 y 10.2.0.0/16 se dividieron en subredes con la máscara /24.



En este ejemplo, 10.3.0.0/16 se dividió en subredes utilizando la máscara /28 y 10.4.0.0/16 se dividió en subredes utilizando la máscara /20.

Las direcciones host individuales se asignan a partir de las "sub-subredes".

Otra forma de ver las subredes de VLSM es enumerar cada subred y sus sub-subredes.

En la figura 1, la red 10.0.0.0/8 es el espacio de direcciones inicial y está dividida en subredes con una máscara /16. El préstamo de 8 bits (que van de /8 a /16) crea 256 subredes que van de 10.0.0.0/16 a 10.255.0.0/16.

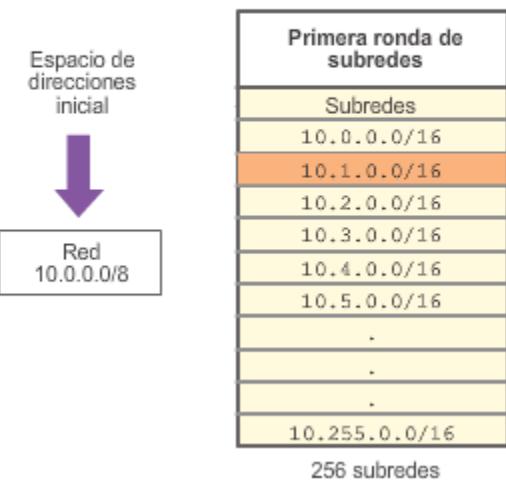
En la figura 2, la subred 10.1.0.0/16 se vuelve a dividir en subredes al tomar prestados 8 bits más. Esto crea 256 subredes con una máscara /24. Esta máscara permite que haya 254 direcciones host por subred. Las subredes comprendidas entre 10.1.0.0/24 y 10.1.255.0/24 son subredes de la subred 10.1.0.0/16.

En la figura 3, la subred 10.2.0.0/16 se vuelve a dividir en subredes con una máscara /24, lo que permite que haya 254 direcciones host por subred. Las subredes comprendidas entre 10.2.0.0/24 y 10.2.255.0/24 son subredes de la subred 10.2.0.0/16.

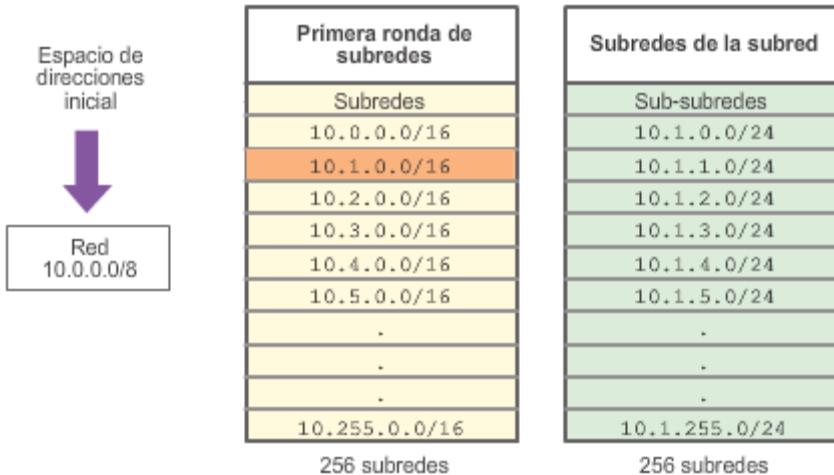
En la figura 4, la subred 10.3.0.0/16 se vuelve a dividir en subredes con una máscara /28. De esta manera, crea 4096 subredes y permite que haya 14 direcciones host por subred. Las subredes comprendidas entre 10.3.0.0/28 y 10.3.255.240/28 son subredes de la subred 10.3.0.0/16.

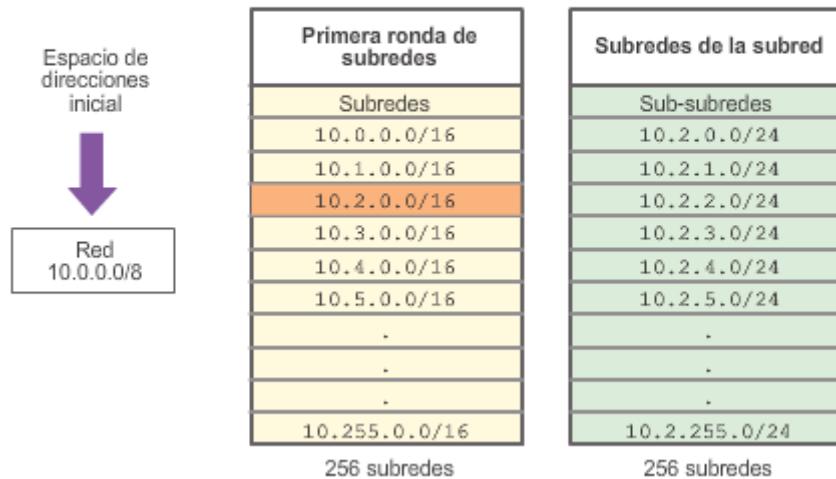
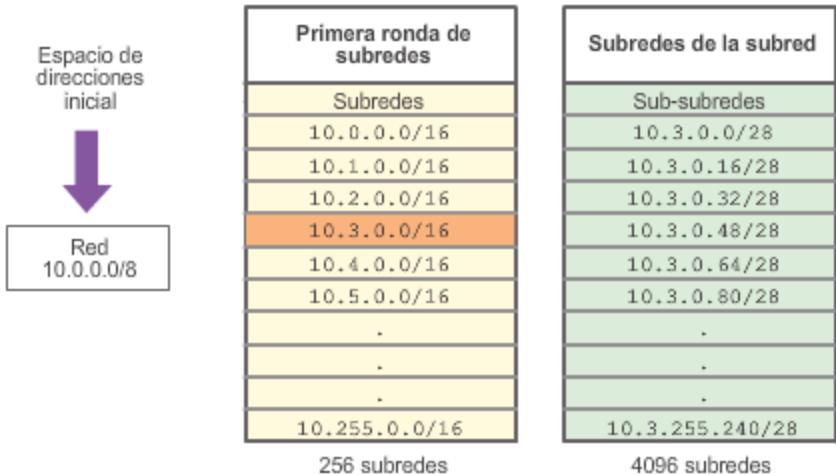
En la figura 5, la subred 10.4.0.0/16 se vuelve a dividir en subredes con una máscara /20. De esta manera, crea 16 subredes y permite que haya 4094 direcciones host por subred. Las subredes comprendidas entre 10.4.0.0/20 y 10.4.240.0/20 son subredes de la subred 10.4.0.0/16. Estas subredes /20 son lo suficientemente grandes como para dividirse aún más veces y permitir que haya más redes.

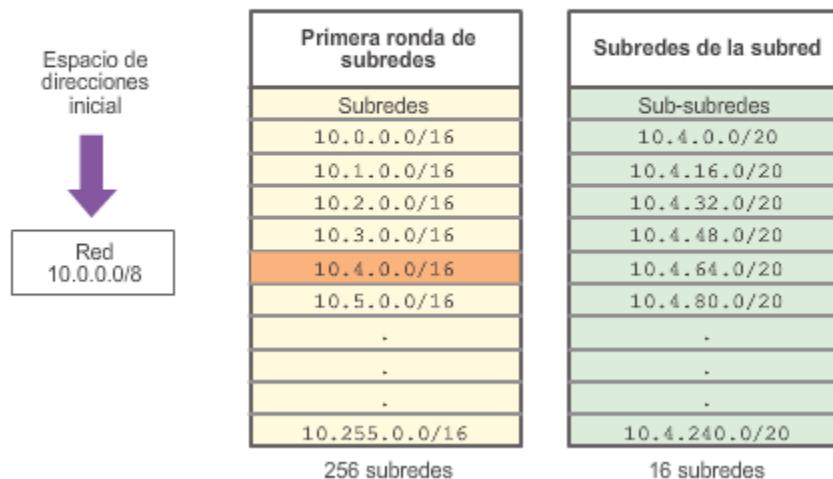
División en subredes 10.0.0.0/8 a 10.0.0.0/16



División en subredes de la subred 10.1.0.0/16 a 10.1.0.0/24



División en subredes de la subred 10.2.0.0/16 a 10.2.0.0/24**División en subredes de la subred 10.3.0.0/16 a 10.3.0.0/28**

División en subredes de la subred 10.4.0.0/16 a 10.4.0.0/20

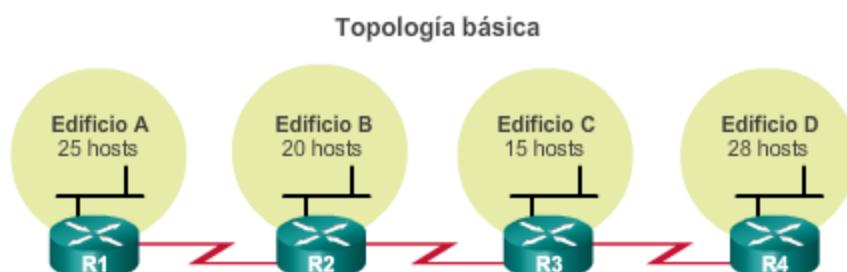
Se debe prestar particular atención al diseño de un esquema de direccionamiento de red. Por ejemplo, la topología de ejemplo en la figura 1 requiere siete subredes.

Al utilizar la división en subredes tradicional, los primeros siete bloques de direcciones se asignan a las LAN y WAN, tal como se muestra en la figura 2. Este esquema da como resultado 8 subredes con 30 direcciones utilizables cada una (/27). Si bien este esquema funciona para los segmentos LAN, se desperdician muchas direcciones en los segmentos WAN.

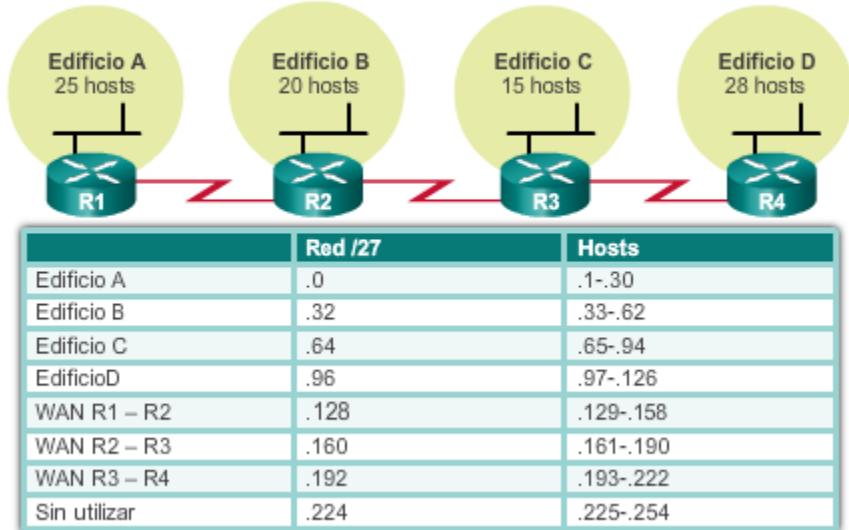
Si se diseña un esquema de direccionamiento de una red nueva, los bloques de direcciones pueden asignarse de manera tal que se minimice el desperdicio y que los bloques de direcciones sin utilizar sean contiguos. Agregar esto a una red existente puede ser más difícil.

Como se muestra en la figura 3, para utilizar el espacio de direcciones de manera más eficaz, se crean subredes /30 para los enlaces WAN. A fin de mantener juntos los bloques de direcciones sin utilizar, la última subred /27 se vuelve a dividir en subredes para crear subredes /30. Las primeras tres subredes se asignaron a los enlaces WAN que crearon las subredes 192.168.20.224/30, 192.168.20.228/30 y 192.168.20.232/30. Si se diseña el esquema de direccionamiento de esta manera, quedan tres subredes /27 y cinco subredes /30 sin utilizar.

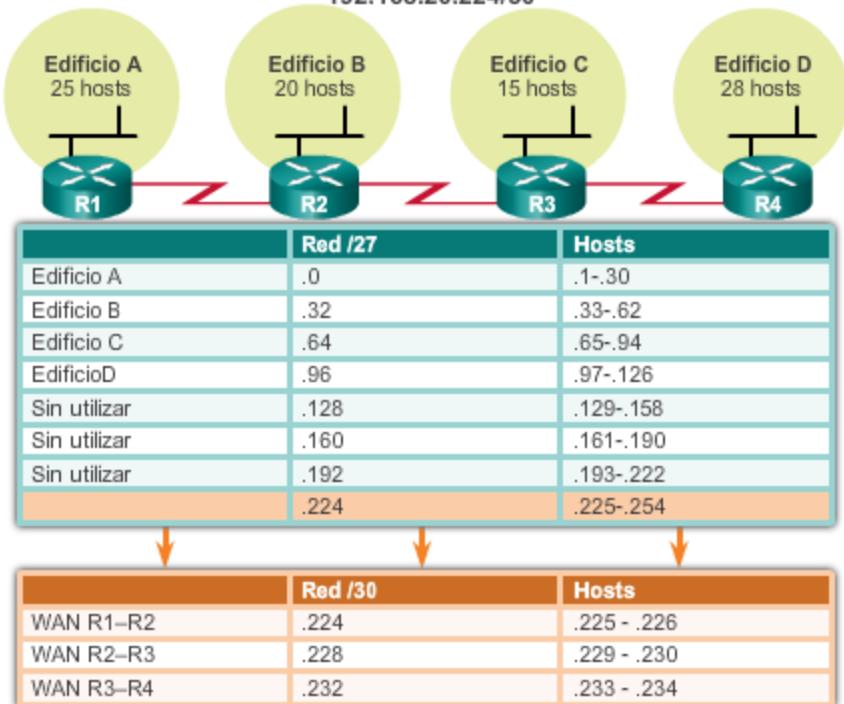
En las figuras 4 a 7, se muestran configuraciones de ejemplo en los cuatro routers para implementar el esquema de direccionamiento VLSM.



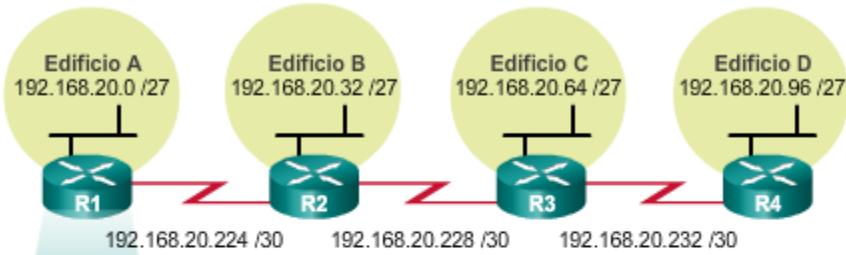
División en subredes 192.168.20.0/24 a 192.168.20.0/27



División en subredes de la subred 192.168.20.224/27 a 192.168.20.224/30

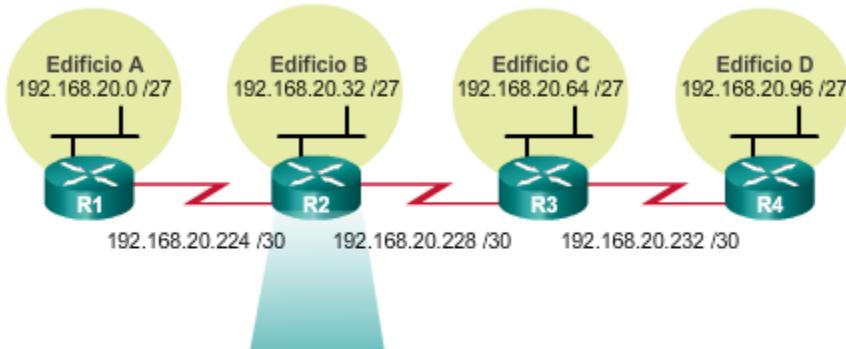


Configuración de VLSM en el R1



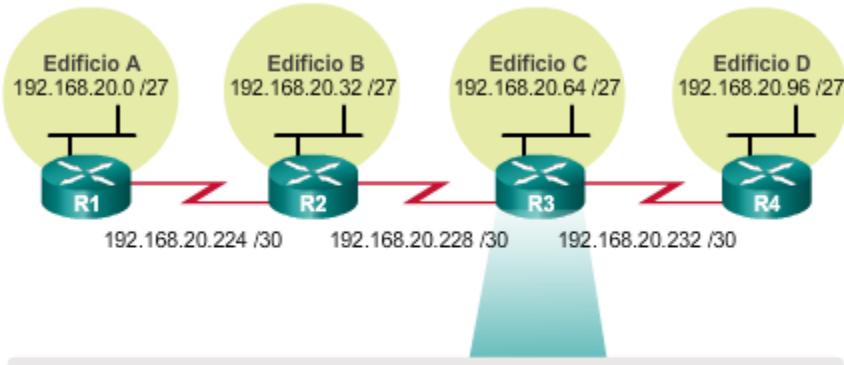
```
R1(config)# interface gigabitethernet 0/0
R1(config-if)# ip address 192.168.20.1 255.255.255.224
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 192.168.20.225 255.255.255.252
R1(config-if)# end
R1#
```

Configuración de VLSM en el R2



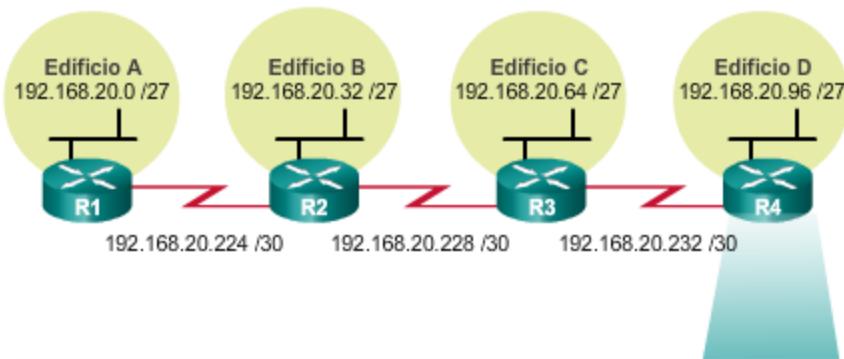
```
R2(config)# interface gigabitethernet 0/0
R2(config-if)# ip address 192.168.20.33 255.255.255.224
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.20.226 255.255.255.252
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config)# ip address 192.168.20.229 255.255.255.252
R2(config-if)# end
R2#
```

Configuración de VLSM en el R3



```
R3(config)# interface gigabitethernet 0/0
R3(config-if)# ip address 192.168.20.65 255.255.255.224
R3(config-if)# exit
R3(config)# interface serial 0/0/0
R3(config-if)# ip address 192.168.20.230 255.255.255.252
R3(config-if)# exit
R3(config)# interface serial 0/0/1
R3(config)# ip address 192.168.20.233 255.255.255.252
R3(config-if)# end
R3#
```

Configuración de VLSM en el R4



```
R4(config)# interface gigabitethernet 0/0
R4(config-if)# ip address 192.168.20.97 255.255.255.224
R4(config-if)# exit
R4(config)# interface serial 0/0/0
R4(config-if)# ip address 192.168.20.234 255.255.255.252
R4(config-if)# end
R4#
```

6.5 Configuración de rutas resumidas y estáticas flotantes

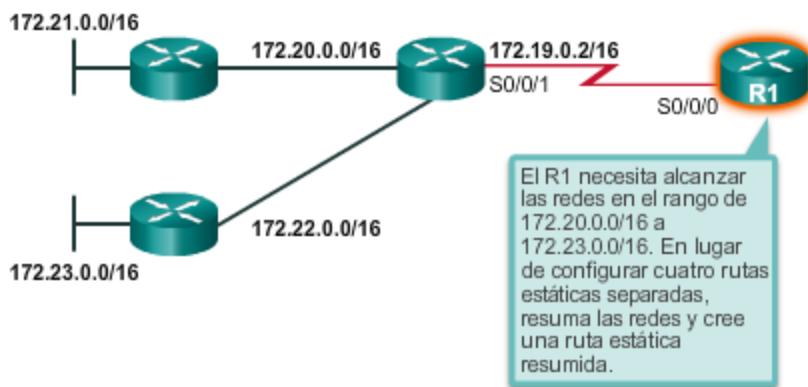
6.5.1 Configuración de rutas resumidas IPv4

La summarización de ruta, también conocida como “agregación de rutas”, es el proceso de anunciar un conjunto de direcciones contiguas como una única dirección, con una máscara de subred más corta y menos específica. CIDR es una forma de summarización de ruta y es un sinónimo del término “creación de superredes”.

CIDR omite la restricción de límites con clase y permite la summarización con máscaras más pequeñas que las de la máscara con clase predeterminada. Este tipo de summarización ayuda a reducir la cantidad de entradas en las actualizaciones de enrutamiento y disminuye 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.

En la ilustración, el R1 requiere una ruta estática resumida para alcanzar las redes en el rango de 172.20.0.0/16 a 172.23.0.0/16.

Topología básica



La summarización de redes en una única dirección y máscara se puede realizar en tres pasos:

Paso 1. Enumere las redes en formato binario. En la figura 1 se indican las redes 172.20.0.0/16 a 172.23.0.0/16 en formato binario.

Paso 2. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara de la ruta resumida. En la figura 2, se destacan los 14 bits coincidentes que se encuentran en el extremo izquierdo. Este es el prefijo, o la máscara de subred, para la ruta resumida: /14 o 255.252.0.0.

Paso 3. Copie los bits coincidentes y luego agregue los bits 0 para determinar la dirección de red resumida. En la figura 3, se muestra que los bits coincidentes con ceros al final producen la dirección de red 172.20.0.0. Las cuatro redes (172.20.0.0/16, 172.21.0.0/16, 172.22.0.0/16 y 172.23.0.0/16) pueden sumarizarse en una única dirección de red y prefijo 172.20.0.0/14.

En la figura 4, se muestra el R1 configurado con una ruta estática resumida para alcanzar las redes 172.20.0.0/16 a 172.23.0.0/16.

Cálculo de un resumen de rutas

Paso 1: enumerar las redes en formato binario.

172.20.0.0	10101100 . 00010100 . 00000000 . 00000000
172.21.0.0	10101100 . 00010101 . 00000000 . 00000000
172.22.0.0	10101100 . 00010110 . 00000000 . 00000000
172.23.0.0	10101100 . 00010111 . 00000000 . 00000000

Paso 2: contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara.

Respuesta: 14 bits coincidentes = /14 o 255.252.0.0

Cálculo de un resumen de rutas

Paso 1: enumerar las redes en formato binario.

172.20.0.0	10101100 . 00010100 . 00000000 . 00000000
172.21.0.0	10101100 . 00010101 . 00000000 . 00000000
172.22.0.0	10101100 . 00010110 . 00000000 . 00000000
172.23.0.0	10101100 . 00010111 . 00000000 . 00000000

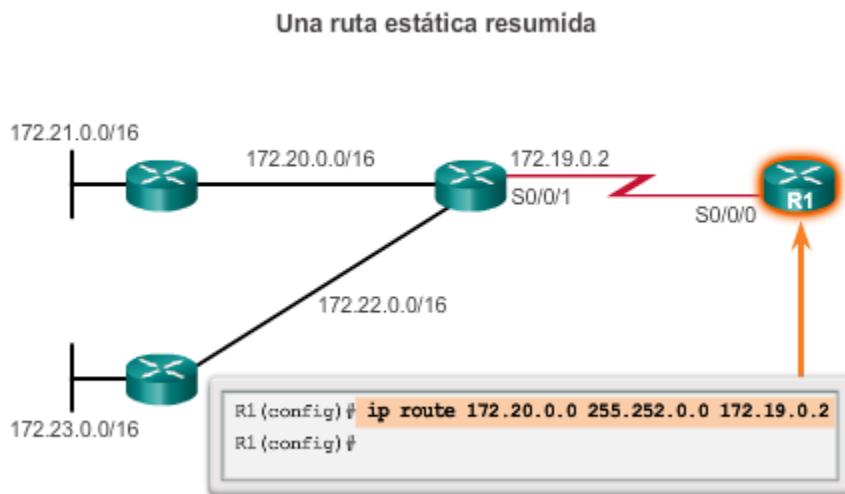
Paso 2: contar el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la máscara.

Respuesta: 14 bits coincidentes = /14 o 255.252.0.0

Paso 3: copiar los bits coincidentes y luego agregar los bits 0 para determinar la dirección de red resumida.

10101100 . 00010100 . 00000000 . 00000000
_____ Copiar _____ Agregar bits cero _____

Respuesta: 172.20.0.0



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

- Las redes de destino son contiguas y se pueden resumir en una única dirección de red.
- Todas las rutas estáticas utilizan la misma interfaz de salida o la dirección IP del siguiente salto.

Considere el ejemplo de la figura 1. Todos los routers tienen conectividad mediante rutas estáticas.

En la figura 2, se muestran las entradas de la tabla de routing estático para el R3. Observe que tiene tres rutas estáticas que pueden resumirse, porque comparten los mismos dos primeros octetos.

En la figura 3, se muestran los pasos para resumir esas tres redes:

Paso 1. Escriba las redes que se van a resumir en formato binario.

Paso 2. Para encontrar la máscara de subred para la sumarización, comience con el bit del extremo izquierdo y vaya hacia la derecha. Verá que todos los bits coinciden de forma consecutiva hasta una columna en la cual los bits no coinciden, la cual identifica el límite del resumen.

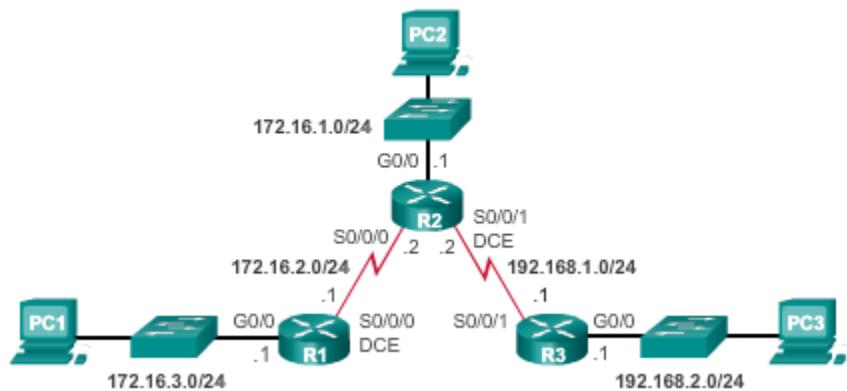
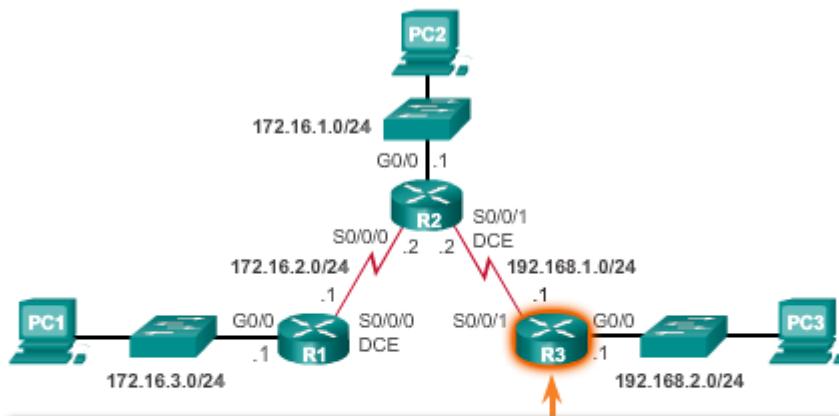
Paso 3. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo. En el ejemplo, es 22. Este número identifica la máscara de subred de la ruta resumida como /22 o 255.255.252.0.

Paso 4. 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.

Después de identificar la ruta resumida, reemplace las rutas existentes por esta ruta.

En la figura 4, se muestra cómo se eliminan las tres rutas existentes y, luego, cómo se configura la nueva ruta estática resumida.

En la figura 5, se confirma que la ruta estática resumida está en la tabla de routing del R3.

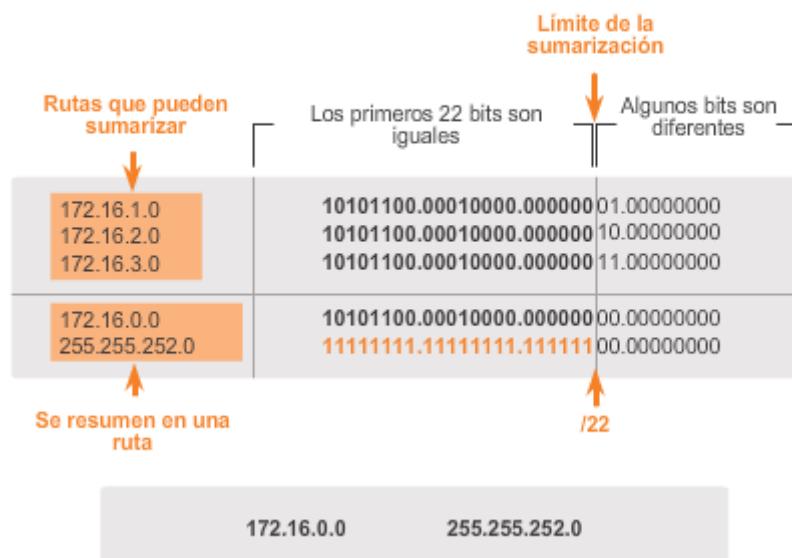
Topología básica**Verificación de la tabla de routing**

```
R3# show ip route static | begin Gateway
Gateway of last resort is not set

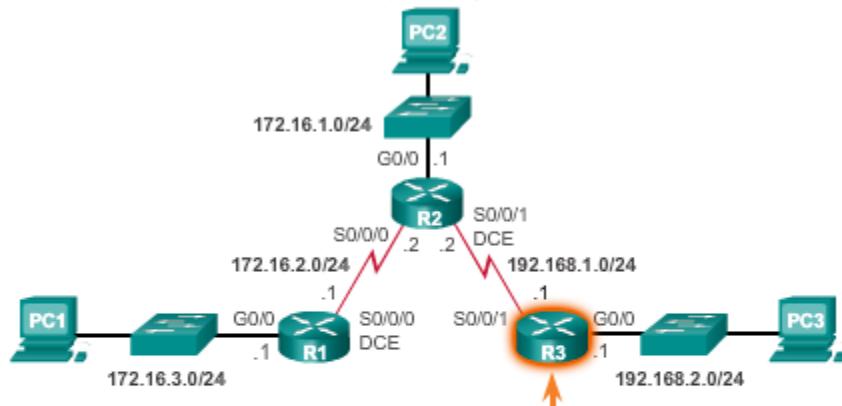
    172.16.0.0/24 is subnetted, 3 subnets
S        172.16.1.0 [1/0] via 192.168.1.2
S        172.16.2.0 [1/0] via 192.168.1.2
S        172.16.3.0 [1/0] via 192.168.1.2

R3#
```

Resumen de redes



Eliminación de rutas estáticas y configuración de la ruta estática resumida

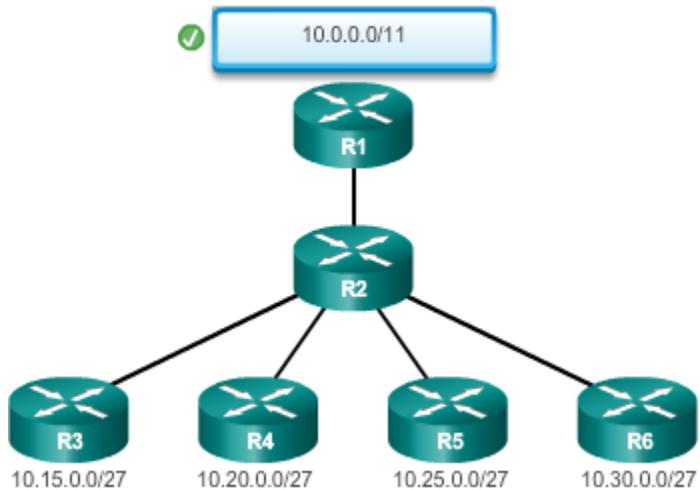
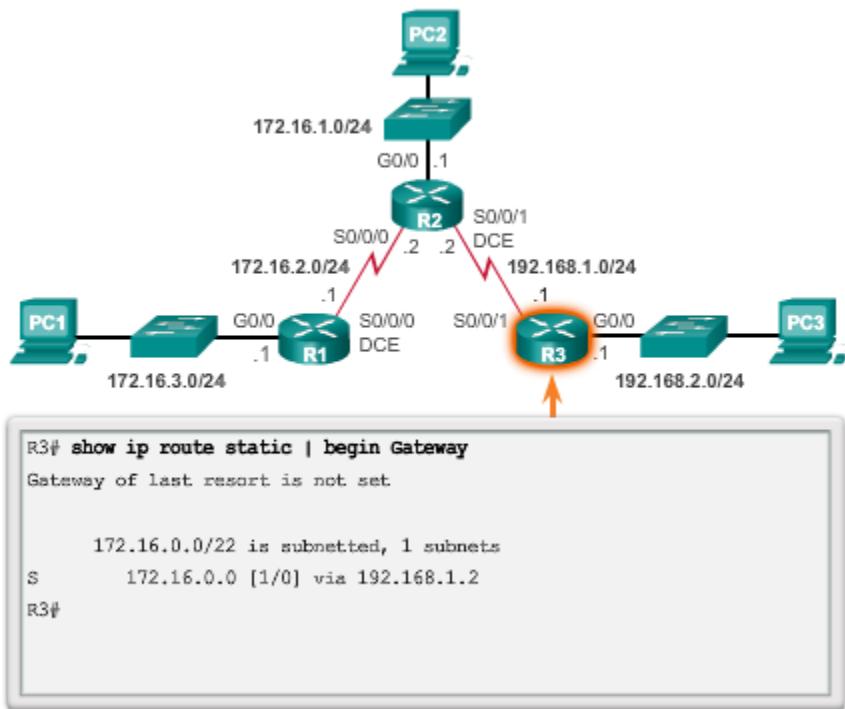


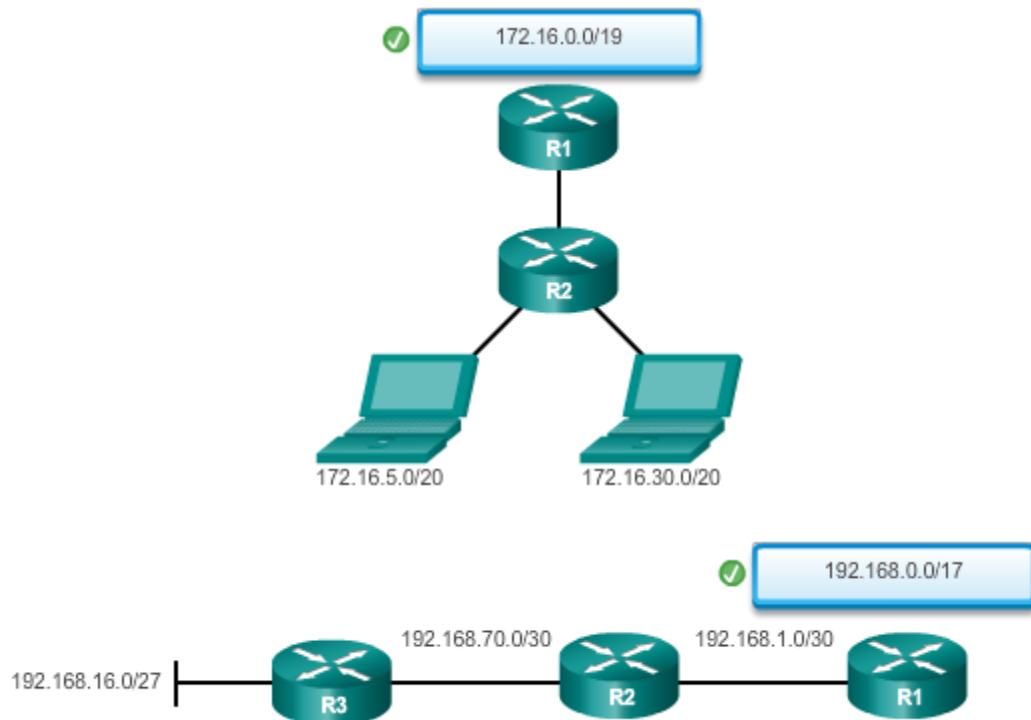
```

R3(config)# no ip route 172.16.1.0 255.255.255.0 192.168.1.2
R3(config)# no ip route 172.16.2.0 255.255.255.0 192.168.1.2
R3(config)# no ip route 172.16.3.0 255.255.255.0 192.168.1.2
R3(config)# ip route 172.16.0.0 255.255.252.0 192.168.1.2
R3(config)#

```

Verificación de la ruta estática resumida





6.5.2 Configuración de rutas resumidas IPv6

Aparte del hecho de que las direcciones IPv6 tienen una longitud de 128 bits y están escritas en hexadecimales, el resumen de direcciones IPv6 es muy similar al resumen de las direcciones IPv4. Solo requiere de algunos pasos más debido a las direcciones IPv6 abreviadas y a la conversión hexadecimal.

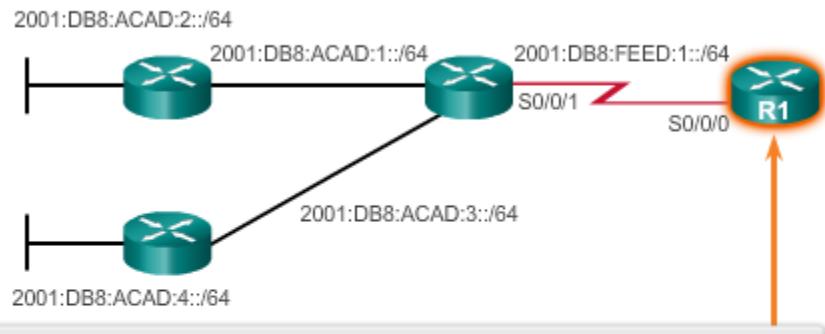
Varias rutas estáticas IPv6 se pueden resumir en una única ruta estática IPv6 si:

- Las redes de destino son contiguas y se pueden resumir en una única dirección de red.
- Todas las rutas estáticas utilizan la misma interfaz de salida o la dirección IPv6 del siguiente salto.

Consulte la red de la figura 1. Actualmente, el R1 tiene cuatro rutas estáticas IPv6 para alcanzar las redes 2001:DB8:ACAD:1::/64 a 2001:DB8:ACAD:4::/64.

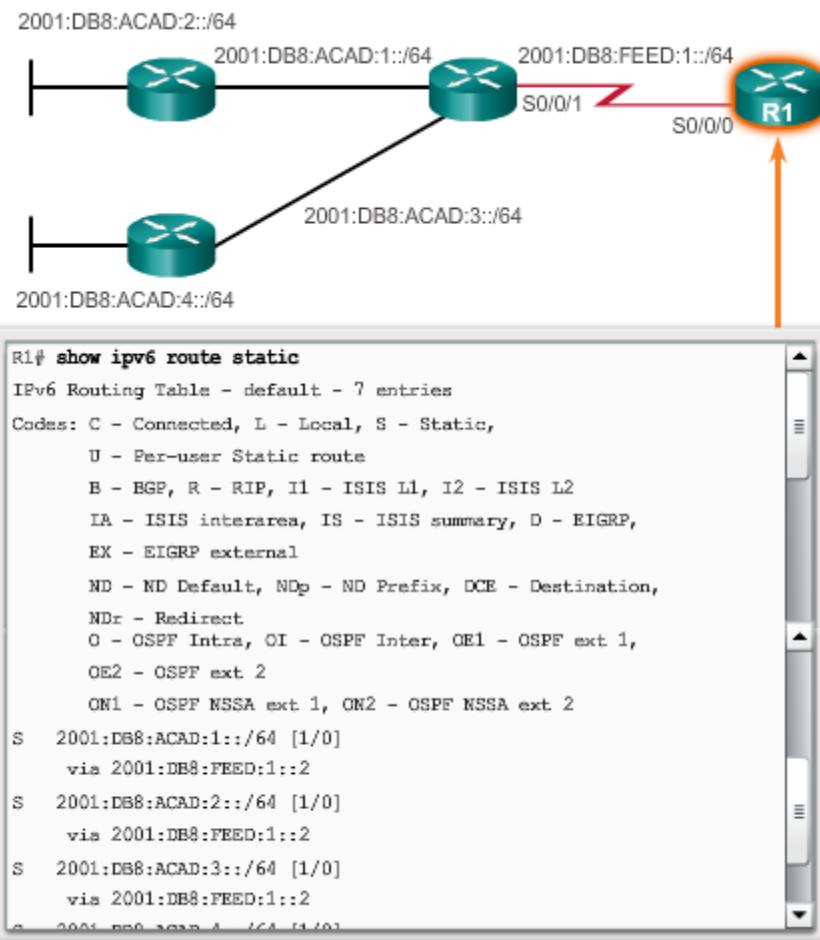
En la figura 2, se muestran las rutas estáticas IPv6 instaladas en la tabla de routing IPv6.

Topología básica



```
R1(config)# ipv6 route 2001:DB8:ACAD:1::/64 2001:db8:feed:1::2
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 2001:db8:feed:1::2
R1(config)# ipv6 route 2001:DB8:ACAD:3::/64 2001:db8:feed:1::2
R1(config)# ipv6 route 2001:DB8:ACAD:4::/64 2001:db8:feed:1::2
R1(config)#
```

Verificación de la tabla de routing del R1



El resumen de redes IPv6 en un único prefijo IPv6 y una única longitud de prefijo se puede realizar en siete pasos, tal como se muestra en las figuras 1 a 7:

Paso 1. Enumere las direcciones de red (prefijos) e identifique la parte en la cual las direcciones difieren.

Paso 2. Expanda la IPv6 si está abreviada.

Paso 3. Convierta la sección diferente de sistema hexadecimal a binario.

Paso 4. Cuente el número de bits coincidentes que se encuentran en el extremo izquierdo para determinar la longitud de prefijo para la ruta resumida.

Paso 5. Copie los bits coincidentes y luego agregue los bits 0 para determinar la dirección de red resumida (prefijo).

Paso 6. Convierta la sección binaria de nuevo en hexadecimal.

Paso 7. Agregue el prefijo de la ruta resumida (resultado del paso 4).

Identificación de la parte en la que difieren las direcciones

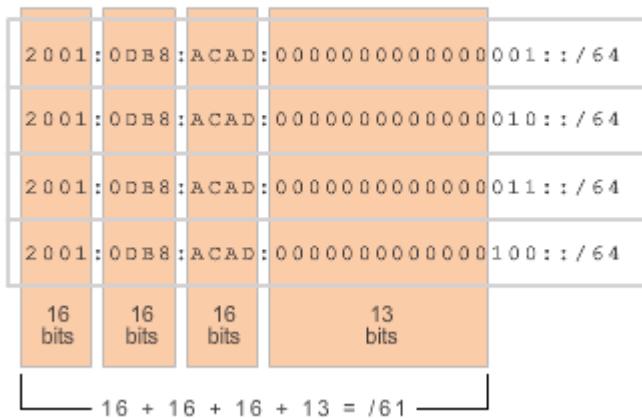
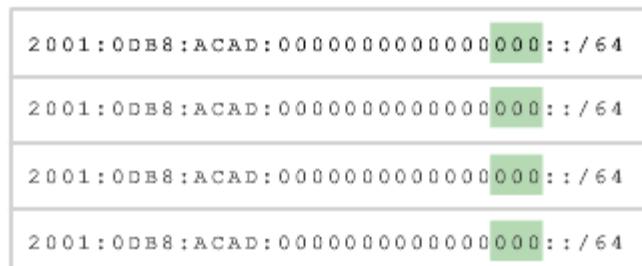
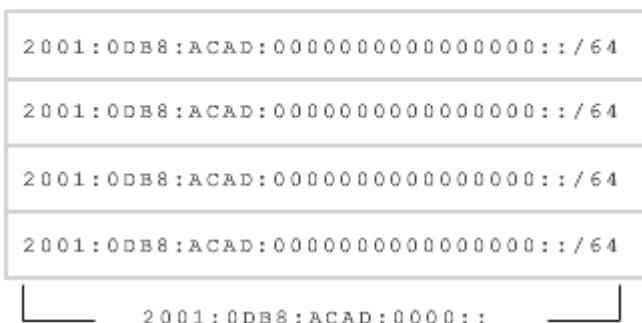
2001:0DB8:ACAD:1::/64
2001:0DB8:ACAD:2::/64
2001:0DB8:ACAD:3::/64
2001:0DB8:ACAD:4::/64

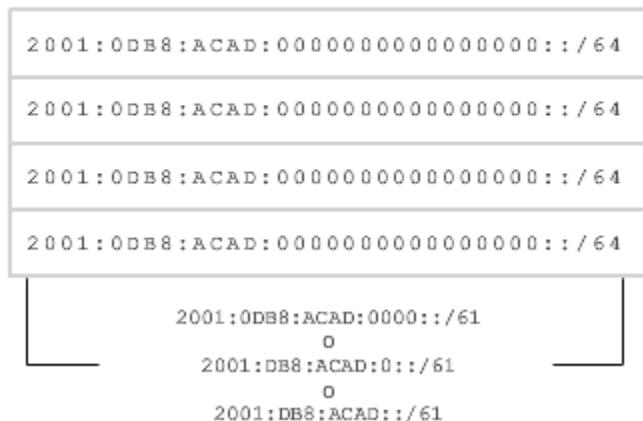
Identificación de la parte en la que difieren las direcciones

2001:0DB8:ACAD:0001::/64
2001:0DB8:ACAD:0002::/64
2001:0DB8:ACAD:0003::/64
2001:0DB8:ACAD:0004::/64

Conversión de la sección de sistema hexadecimal a binario

2001:0DB8:ACAD:0000000000000001::/64
2001:0DB8:ACAD:00000000000000010::/64
2001:0DB8:ACAD:00000000000000011::/64
2001:0DB8:ACAD:000000000000000100::/64

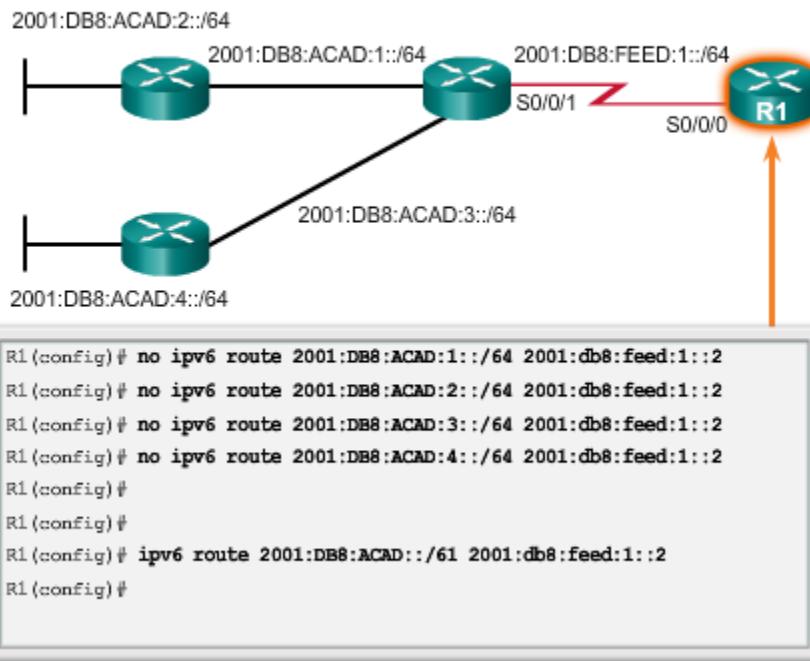
Conteo del número de bits coincidentes del extremo izquierdo**Agregado de los bits 0 para determinar la dirección de red resumida****Conversión de la sección binaria de nuevo en hexadecimal**

Conteo del número de bits coincidentes del extremo izquierdo

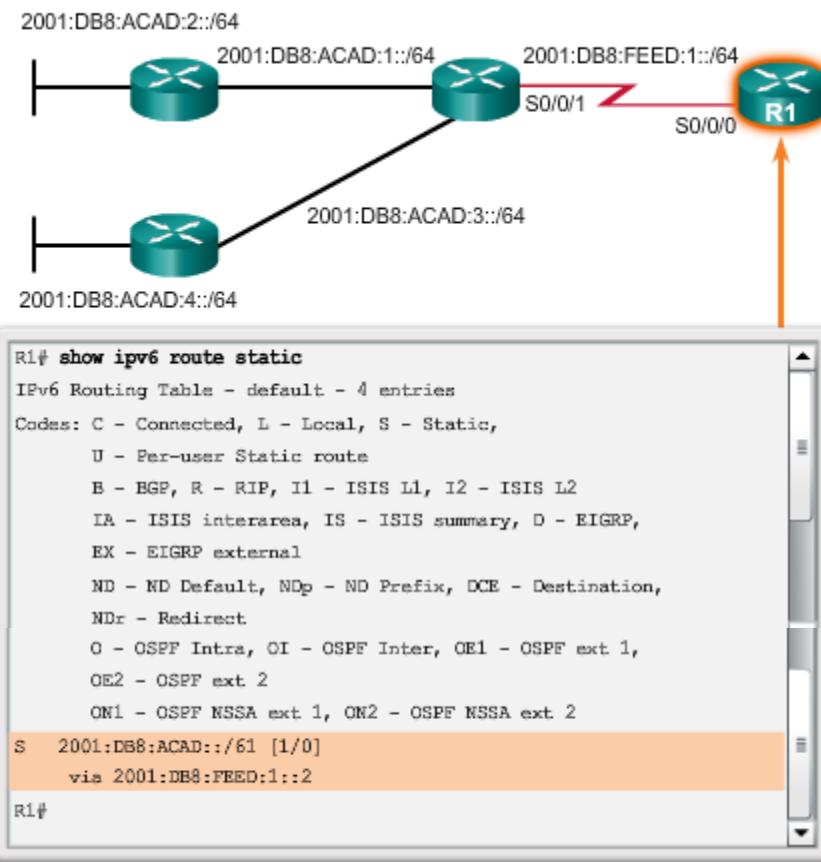
Después de identificar la ruta resumida, reemplace las rutas existentes por esta ruta.

En la figura 1, se muestra cómo se eliminan las cuatro rutas existentes y, luego, cómo se configura la nueva ruta estática resumida IPv6.

En la figura 2, se confirma que la ruta estática resumida está en la tabla de routing del R1.

Eliminación de rutas estáticas y configuración de la ruta resumida IPv6

Verificación de la ruta resumida IPv6



6.5.3 Configuración de rutas estáticas flotantes

Las rutas estáticas flotantes son rutas estáticas que tienen una distancia administrativa mayor que la de otra ruta estática o la de rutas dinámicas. Son muy útiles para proporcionar un respaldo a un enlace principal, como se muestra en la ilustración.

De manera predeterminada, las rutas estáticas tienen una distancia administrativa de 1, lo que las hace preferibles a las rutas descubiertas mediante protocolos de routing dinámico. Por ejemplo, las distancias administrativas de algunos protocolos de routing dinámico comunes son las siguientes:

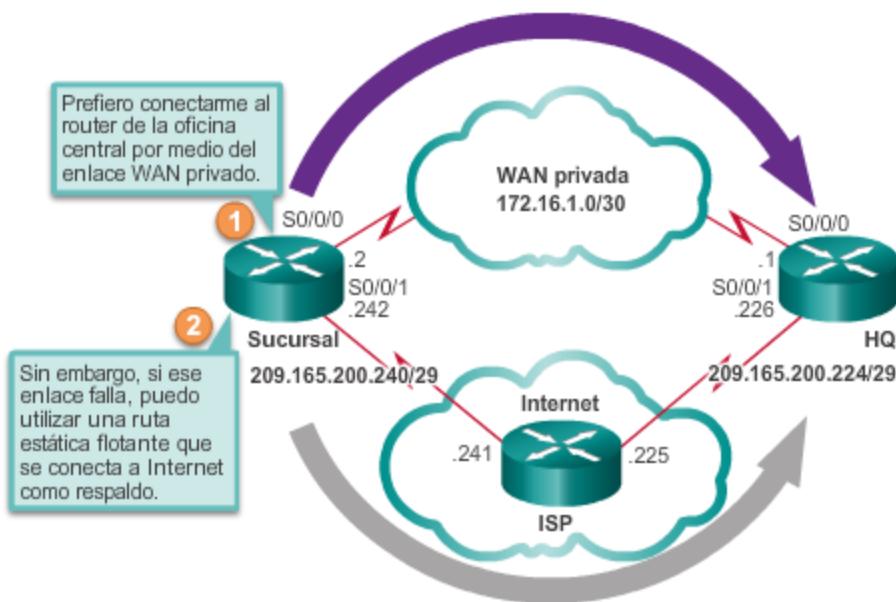
- EIGRP = 90
- IGRP = 100
- OSPF = 110
- IS-IS = 115
- RIP = 120

La distancia administrativa de una ruta estática se puede aumentar para hacer que la ruta sea menos deseable que la ruta de otra ruta estática o una ruta descubierta mediante un protocolo de routing dinámico. De esta manera, la ruta estática “flota” y no se utiliza cuando está activa la ruta con la mejor distancia administrativa. Sin embargo, si se pierde la ruta de preferencia, la ruta estática flotante puede tomar el control, y se puede enviar el tráfico a través de esta ruta alternativa.

Una ruta estática flotante se puede utilizar para proporcionar una ruta de respaldo a varias interfaces o redes en un router. También es independiente de la encapsulación, lo que significa que puede utilizarse para reenviar paquetes desde cualquier interfaz, sin importar el tipo de encapsulación.

Es importante tener en cuenta que el tiempo de convergencia afecta una ruta estática flotante. Una ruta que pierde y restablece una conexión de manera continua puede hacer que la interfaz de respaldo se active innecesariamente.

¿Por qué configurar una ruta estática flotante?



Para configurar rutas estáticas IPv4, se utiliza el comando **ip route** de configuración global y se especifica una distancia administrativa. Si no se configura ninguna distancia administrativa, se utiliza el valor predeterminado (1).

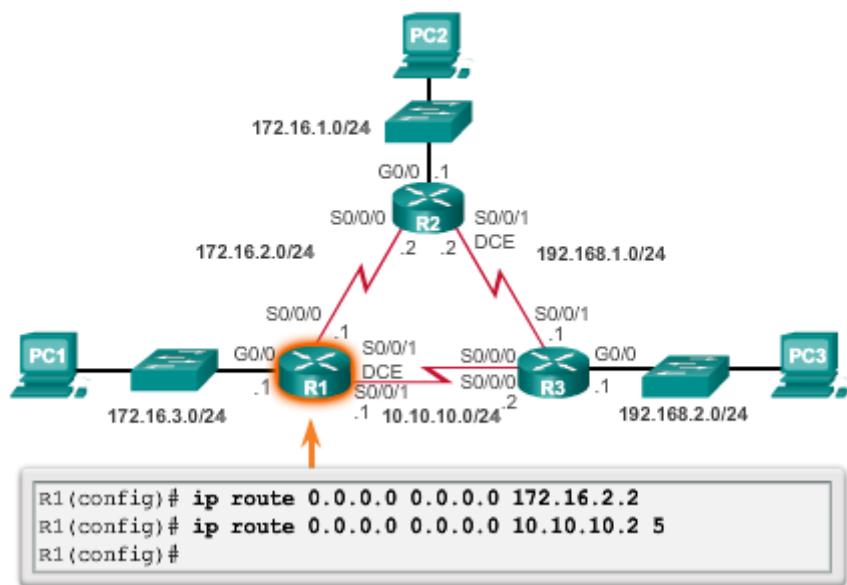
Consulte la topología en la figura 1. En esta situación, la ruta preferida del R1 es al R2. La conexión al R3 se debe utilizar solo para respaldo.

El R1 se configura con una ruta estática predeterminada que apunte al R2. Debido a que no está configurada ninguna distancia administrativa, se utiliza el valor predeterminado (1) para esta ruta estática. El R1 también está configurado con una ruta estática flotante predeterminada que apunta al R3 con una distancia administrativa de 5. Este valor es mayor que el valor predeterminado 1, y, por lo tanto, esta ruta flota y no está presente en la tabla de routing, a menos que la ruta preferida falle.

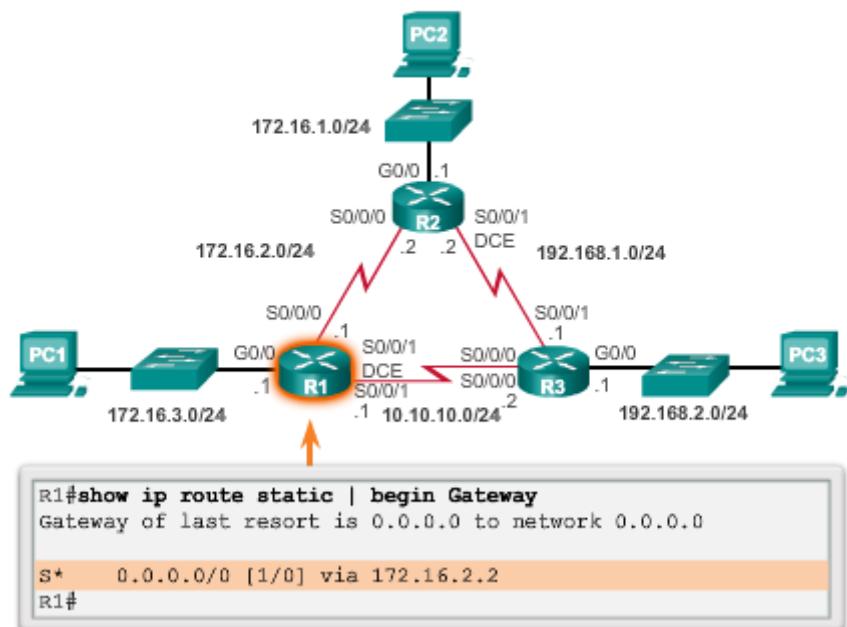
En la figura 2, se verifica que la ruta predeterminada al R2 esté instalada en la tabla de routing. Observe que la ruta de respaldo al R3 no está presente en la tabla de routing.

Utilice el verificador de sintaxis en la figura 3 para configurar el R3 de modo similar al R1.

Configuración de una ruta estática flotante al R3



Verificación de la tabla de routing del R1



Debido a que la ruta estática predeterminada en el R1 al R2 tiene una distancia administrativa de 1, el tráfico del R1 al R3 debe pasar por el R2. El resultado en la figura 1 confirma que el tráfico entre el R1 y el R3 atraviesa el R2.

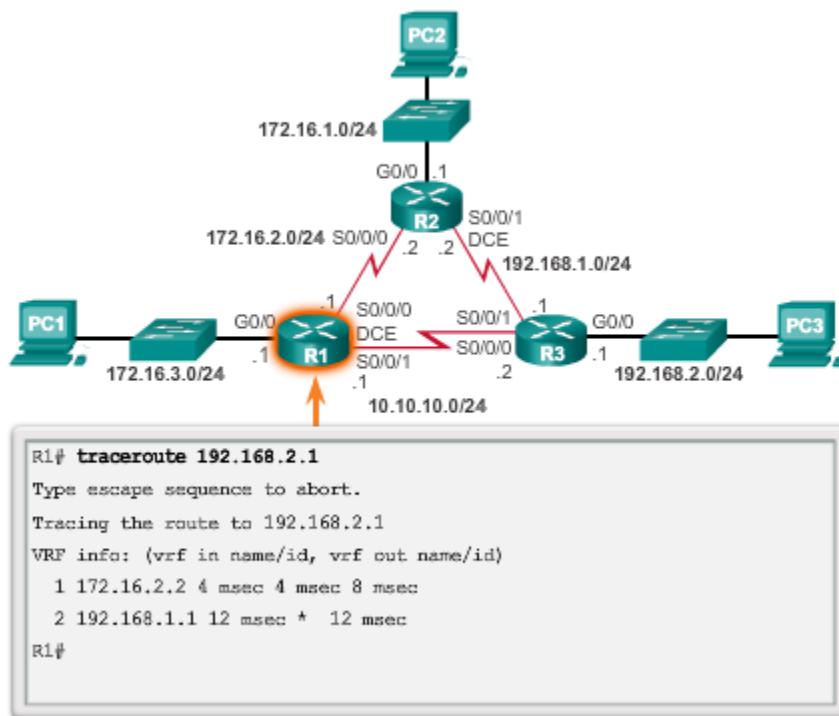
¿Qué ocurriría si el R2 falla? Para simular esta falla, se desactivan ambas interfaces seriales del R2, como se muestra en la figura 2.

Observe en la figura 3 que el R1 genera mensajes de forma automática que indican que la interfaz serial al R2 está inactiva. Al revisar la tabla de routing, se puede verificar que la ruta predeterminada ahora apunta al R3 que utiliza la ruta estática flotante predeterminada que se configuró para el siguiente salto 10.10.10.2.

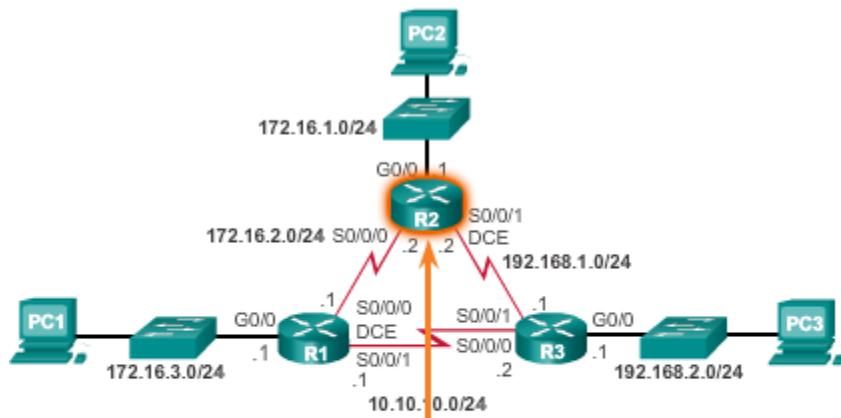
El resultado en la figura 4 confirma que el tráfico ahora fluye directamente entre el R1 y el R3.

Nota: la configuración de rutas estáticas flotantes IPv6 está fuera del ámbito de este capítulo.

Verificación de la ruta a la LAN del R3

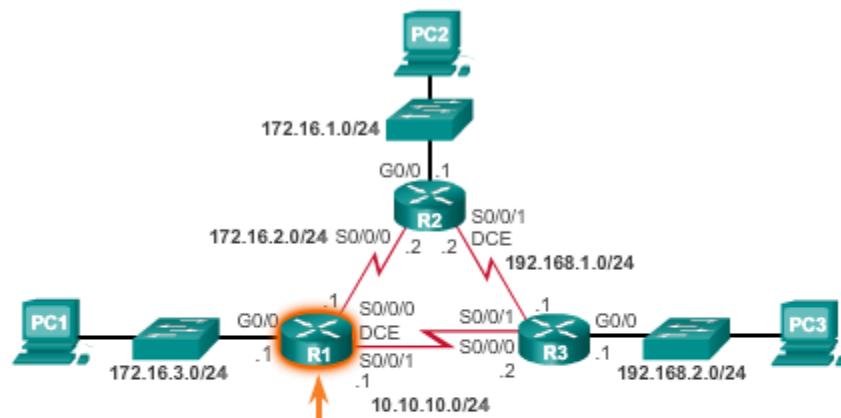


Simulación de una falla del router en el R2



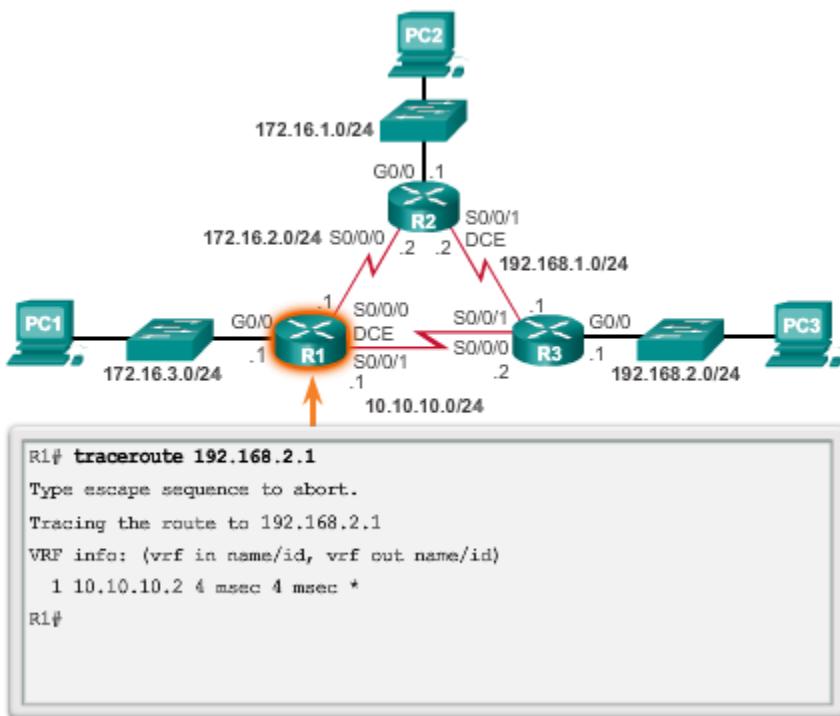
```
R2(config)# int s0/0/0
R2(config-if)# shut
*Feb 21 16:33:35.939: %LINK-5-CHANGED: Interface Serial0/0/0, changed
state to administratively down
*Feb 21 16:33:36.939: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R2(config-if)# int s0/0/1
R2(config-if)# shut
R2(config-if)#
*Feb 21 16:33:42.543: %LINK-5-CHANGED: Interface Serial0/0/1, changed
state to administratively down
*Feb 21 16:33:43.543: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
```

Verificación de la ruta predeterminada en el R1



```
state to down
*Feb 21 16:35:59.435: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed state to down
R1#
R1# sho ip route static | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*      0.0.0.0/0 [5/0] via 10.10.10.2
R1#
```

Verificación de la ruta a la LAN del R3



6.6 Resolución de problemas de rutas estáticas y predeterminadas

6.6.1 Procesamiento de paquetes con rutas estáticas

En el siguiente ejemplo, se describe el proceso de reenvío de paquetes con rutas estáticas.

Haga clic en el botón Reproducir de la ilustración para ver una animación en la que la PC1 envía un paquete a la PC3.

- El paquete llega a la interfaz GigabitEthernet 0/0 del R1.
- R1 no tiene una ruta específica hacia la red de destino, 192.168.2.0/24; por lo tanto, R1 utiliza la ruta estática predeterminada.
- R1 encapsula el paquete en una nueva trama. Debido a que el enlace a R2 es un enlace punto a punto, R1 agrega una dirección de "todos 1 (unos)" para la dirección de destino de Capa 2.
- La trama se reenvía a través de la interfaz serial 0/0/0. El paquete llega a la interfaz serial 0/0/0 en R2.
- El R2 desencapsula la trama y busca una ruta hacia el destino. El R2 tiene una ruta estática a 192.168.2.0/24 que sale de la interfaz serial 0/0/1.
- El R2 encapsula el paquete en una nueva trama. Debido a que el enlace al R3 es un enlace punto a punto, el R2 agrega una dirección de todos unos (1) para la dirección de destino de capa 2.

7. La trama se reenvía a través de la interfaz serial 0/0/1. El paquete llega a la interfaz serial 0/0/1 en el R3.

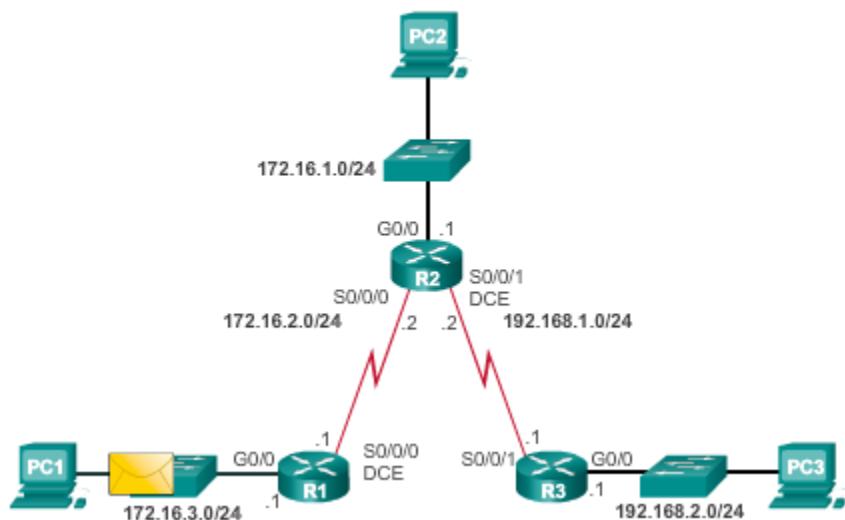
8. El R3 desencapsula la trama y busca una ruta hacia el destino. El R3 tiene una ruta conectada a 192.168.2.0/24 que sale de la interfaz serial GigabitEthernet 0/0.

9. El R3 busca la entrada en la tabla ARP para 192.168.2.10 para encontrar la dirección de control de acceso a los medios (MAC) de capa 2 para la PC3. Si no existe una entrada, el R3 envía una solicitud de protocolo de resolución de direcciones (ARP) a través de la interfaz GigabitEthernet 0/0 y la PC3 responde con una respuesta de ARP, la cual incluye la dirección MAC de la PC3.

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

11. La trama se reenvía a través la interfaz GigabitEthernet 0/0. El paquete llega a la interfaz de la tarjeta de interfaz de red (NIC) de la PC3.

Rutas estáticas y envío de paquetes



6.6.2 Resolución de problemas de configuración de rutas estáticas y predeterminadas IPv4

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

- falla una interfaz,
- un proveedor de servicios desactiva una conexión,
- los enlaces se sobresaturan,
- un administrador ingresa una configuración incorrecta.

Cuando se produce un cambio en la red, es posible que se pierda la conectividad. Los administradores de red son responsables de identificar y solucionar el problema. Para encontrar y resolver estos problemas, un administrador de red debe conocer las herramientas que lo ayudarán a aislar los problemas de routing de manera rápida.

Entre los comandos comunes para la resolución de problemas de IOS, se encuentran los siguientes:

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

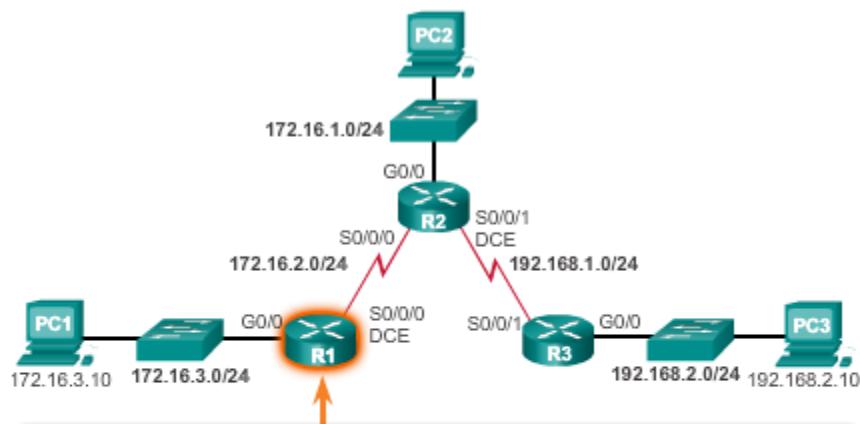
En la figura 1, se muestra el resultado de un ping extendido de la interfaz de origen del R1 a la interfaz LAN del R3. Un ping extendido se da cuando se especifican la interfaz de origen o la dirección IP de origen.

En la figura 2, se muestra el resultado de un comando traceroute del R1 a la LAN del R3.

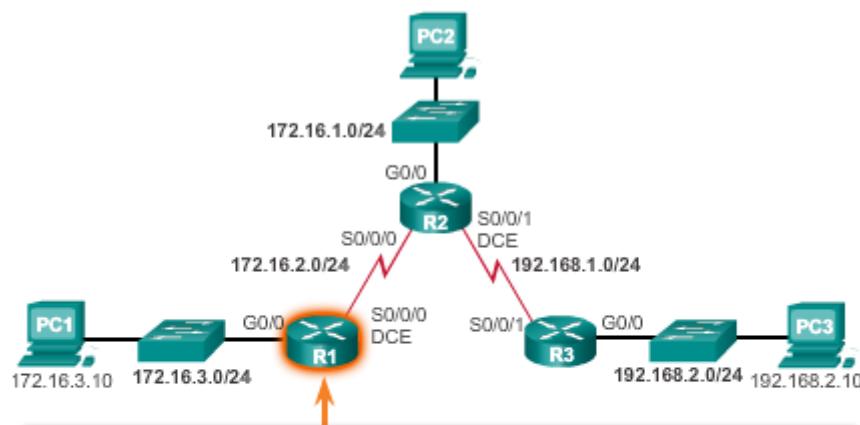
En la figura 3, se muestra la tabla de routing del R1.

En la figura 4, se proporciona un estado rápido de todas las interfaces del router.

En la figura 5, se proporciona una lista de dispositivos Cisco conectados directamente. Este comando valida la conectividad de la capa 2 (y, por lo tanto, la de la capa 1). Por ejemplo, si en el resultado del comando se indica un dispositivo vecino, pero no se puede hacer ping a este, entonces se debe investigar el direccionamiento de la capa 3.

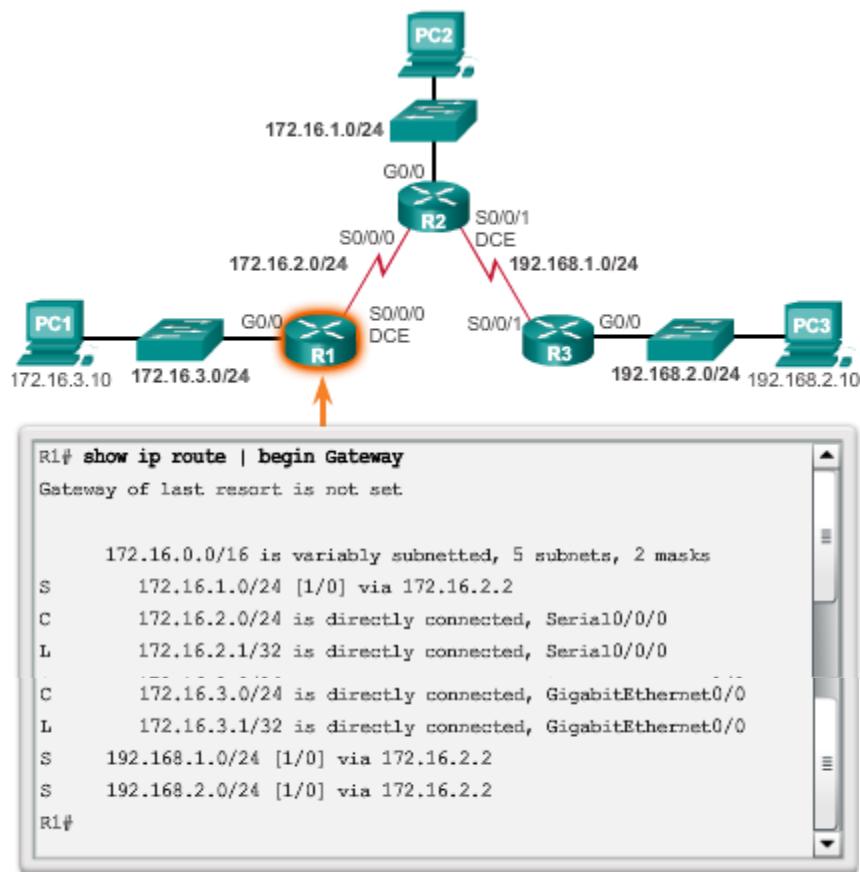
Ping extendido

```
R1# ping 192.168.2.1 source 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28
ms
R1#
```

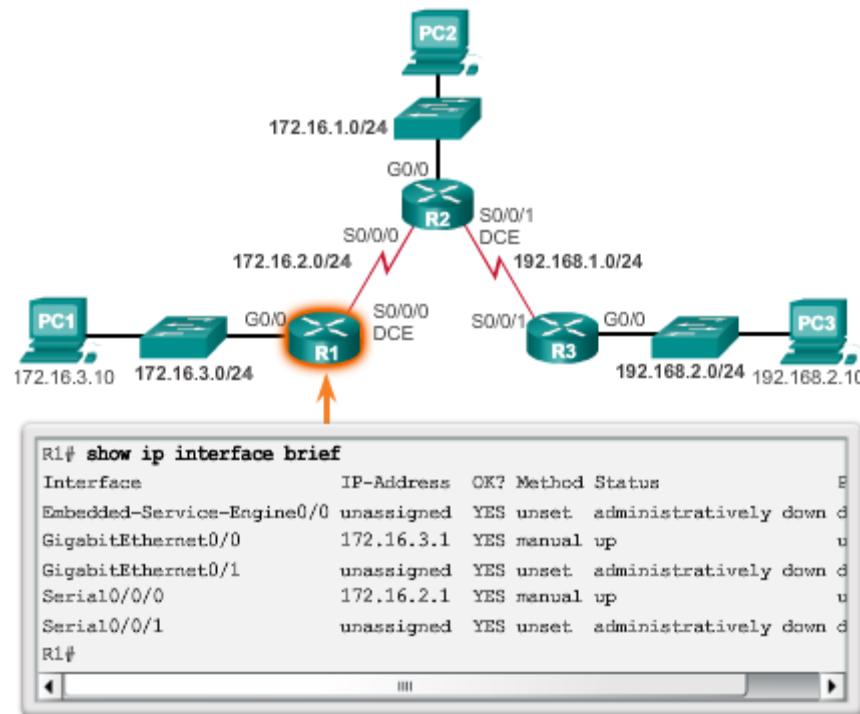
Traceroute del R1 al R3

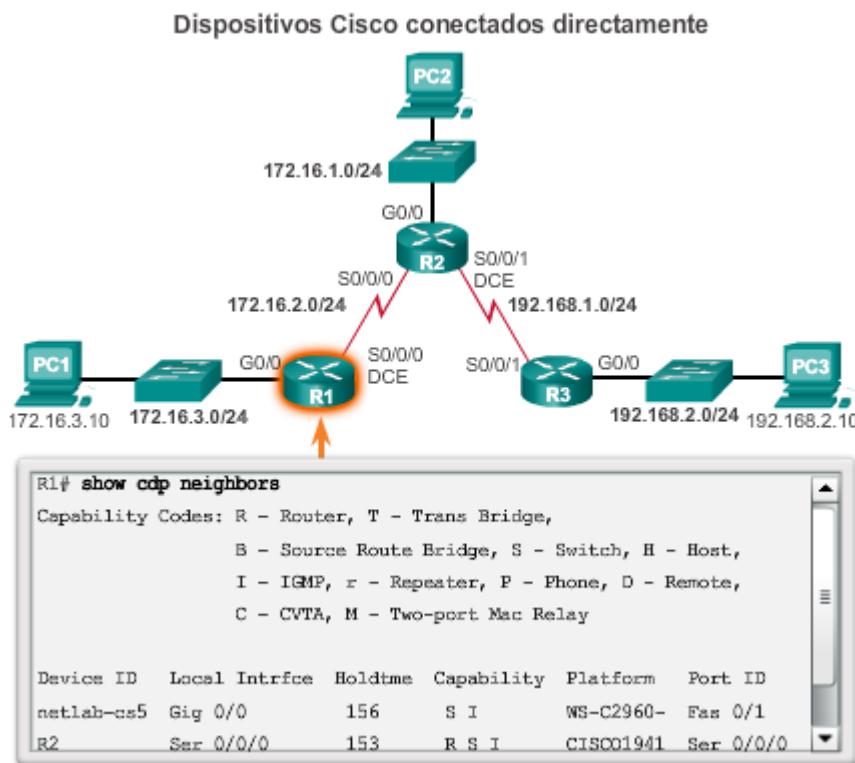
```
R1# traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.2.2 4 msec 4 msec 8 msec
 2 192.168.1.1 12 msec 12 msec *
R1#
```

Verificación de la tabla de routing



Estado de la interfaz





Encontrar una ruta que falta (o que está mal configurada) es un proceso relativamente sencillo, si se utilizan las herramientas adecuadas de manera metódica.

En este ejemplo, el usuario en la PC1 informa que no puede acceder a los recursos en la LAN del R3. Esto puede confirmarse haciendo ping en la interfaz LAN del R3 que utiliza la interfaz LAN del R1 como origen (consulte la figura 1). Los resultados muestran que no hay conectividad entre estas LAN.

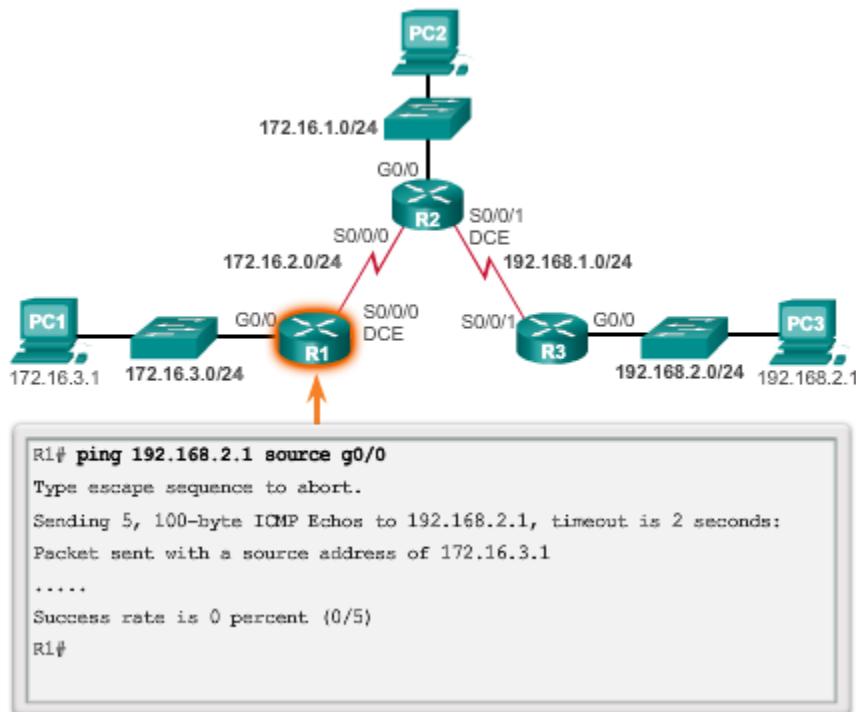
Un comando traceroute en la figura 2 muestra que el R2 no responde como se esperaba. Por alguna razón, el R2 reenvía el comando traceroute de nuevo al R1. El R1 lo devuelve al R2. Este bucle continuaría hasta que el valor del tiempo de vida (TTL) disminuya a cero, en cuyo caso, el router enviaría al R1 un mensaje de destino inalcanzable del protocolo de mensajes de control de Internet (ICMP).

El siguiente paso es investigar la tabla de routing del R2, porque es el router que muestra un patrón extraño de reenvío. La tabla de routing en la figura 3 muestra que la red 192.168.2.0/24 está configurada de manera incorrecta. Se configuró una ruta estática a la red 192.168.2.0/24 con la dirección del siguiente salto 172.16.2.1. Mediante la dirección del siguiente salto configurada, los paquetes destinados a la red 192.168.2.0/24 se devuelven al R1. La topología deja en claro que la red 192.168.2.0/24 está conectada al R3, no al R1. Por lo tanto, la ruta estática a la red 192.168.2.0/24 en el R2 debe utilizar el siguiente salto 192.168.1.1, no 172.16.2.1.

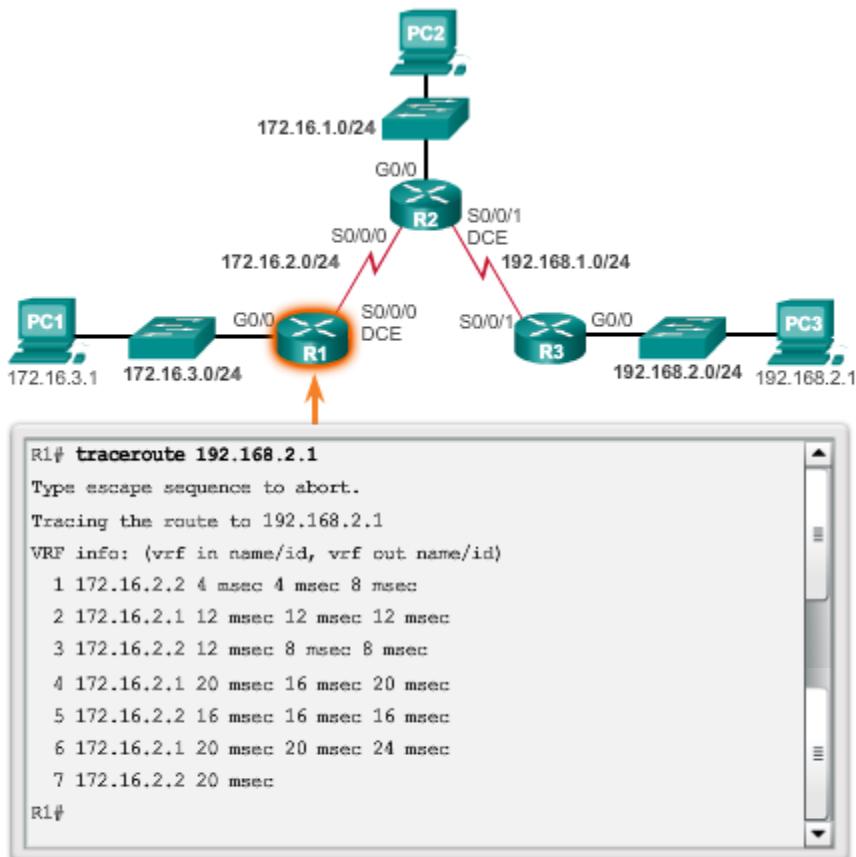
En la figura 4, se muestra el resultado de la configuración en ejecución que revela la instrucción incorrecta de **ip route**. Se elimina la ruta incorrecta y luego se introduce la correcta.

En la figura 5, se verifica si el R1 puede alcanzar la interfaz LAN del R3. Como último paso de confirmación, el usuario de la PC1 también debe probar la conectividad a la LAN 192.168.2.0/24.

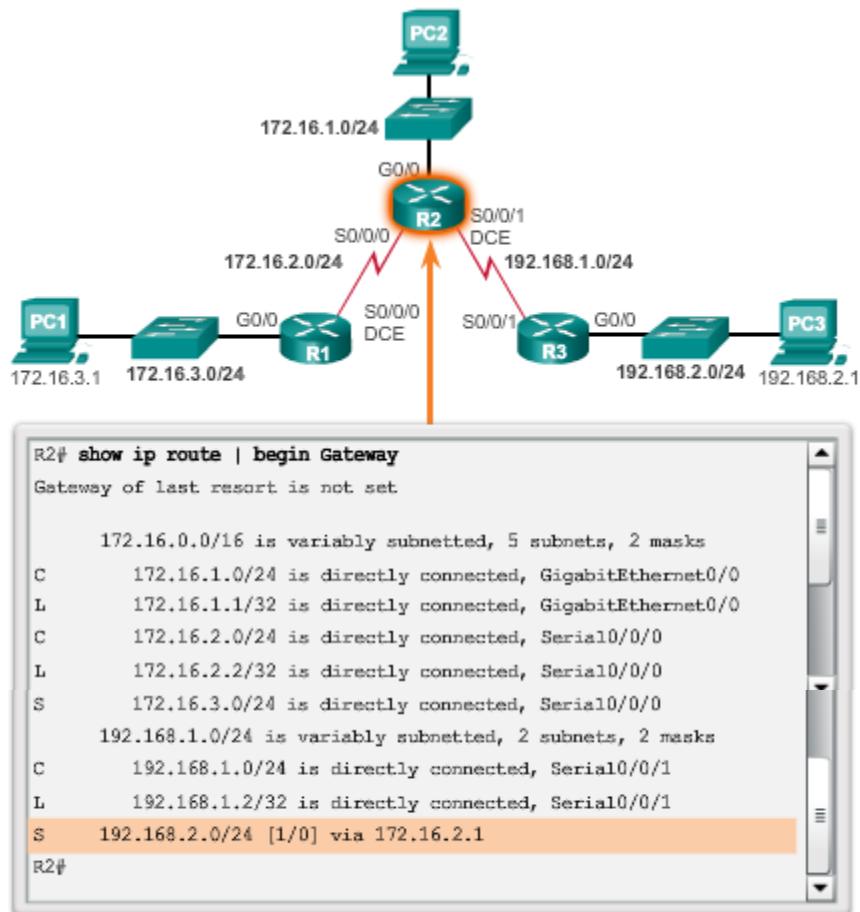
Verificación de la conectividad a la LAN del R3



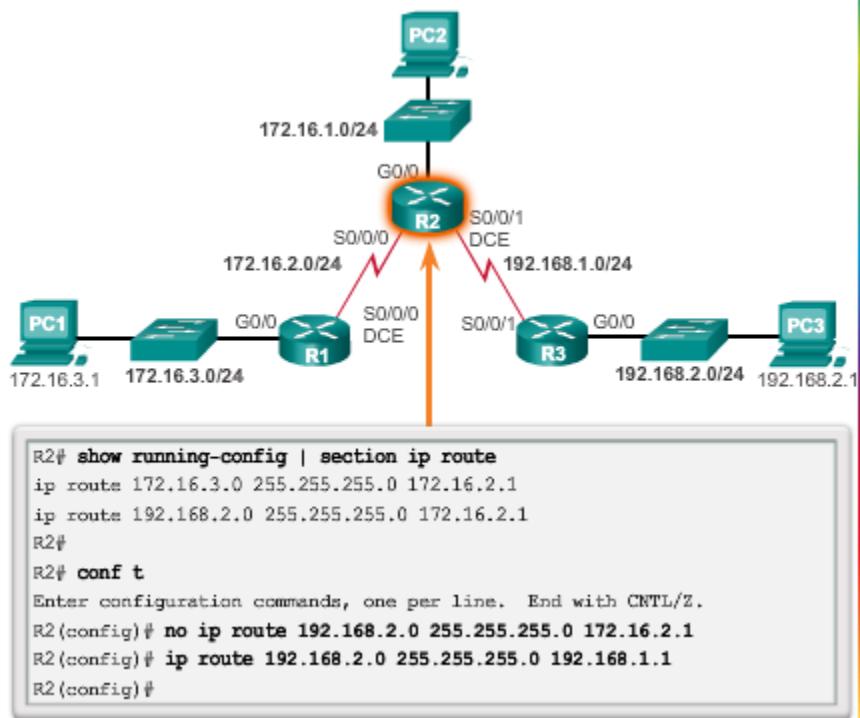
Verificación de la conectividad de salto a salto

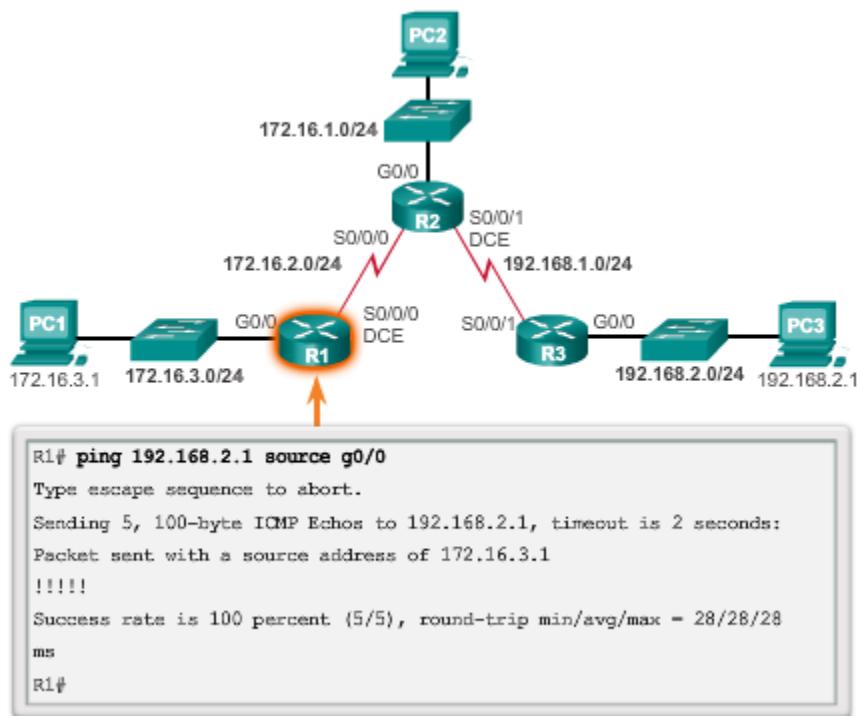


Verificación de la tabla de routing



Identificación y solución del problema



Verificación de la conectividad a la LAN del R3**6.7 Resumen**

En este capítulo, aprendió cómo pueden utilizarse las rutas estáticas IPv4 e IPv6 para alcanzar redes remotas. Las redes remotas son redes a las que se puede llegar únicamente mediante el envío del paquete a otro router. Las rutas estáticas son fáciles de configurar. Sin embargo, en redes de gran tamaño, esta operación manual puede ser complicada. Las rutas estáticas aún se utilizan, incluso cuando se implementa un protocolo de routing dinámico.

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

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

Solo se introduce una ruta estática en la tabla de routing si la dirección IP del siguiente salto se puede resolver a través de una interfaz de salida. Ya sea que la ruta estática esté configurada con una dirección IP del siguiente salto o una interfaz de salida, la ruta estática no se incluye en la tabla de routing si la interfaz de salida que se utiliza para reenviar ese paquete no se encuentra en esa tabla.

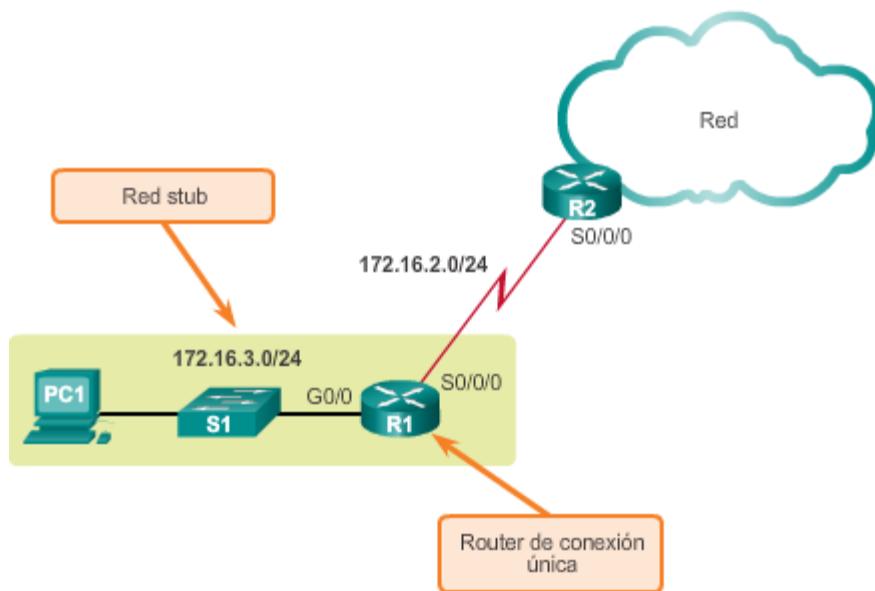
Con el CIDR, pueden configurarse varias rutas estáticas como única ruta resumida. Esto significa que habrá menos entradas en la tabla de enrutamiento y que el proceso de búsqueda en la tabla de enrutamiento será más rápido. El CIDR también administra el espacio de direcciones IPv4 con más eficacia.

La división en subredes de VLSM es similar a la división en subredes tradicional en cuanto a que se toman prestados bits para crear subredes. Con VLSM, la red primero se divide en subredes y, a continuación, las subredes se vuelven a dividir en subredes. Este proceso se puede repetir varias veces para crear subredes de diversos tamaños.

La ruta resumida final es una ruta predeterminada, configurada con una dirección de red 0.0.0.0 y una máscara de subred 0.0.0.0 para IPv4, y el prefijo/longitud de prefijo ::/0 para IPv6. Si no existe una coincidencia más específica en la tabla de routing, dicha tabla utiliza la ruta predeterminada para reenviar el paquete a otro router.

Una ruta estática flotante se puede configurar para respaldar un enlace principal al manipular su valor administrativo.

Redes y routers de rutas internas



7 Routing dinámico

7.1 Introducción

Las redes de datos que usamos en nuestras vidas cotidianas para aprender, jugar y trabajar varían desde pequeñas redes locales hasta grandes internetworks globales. En el hogar, un usuario puede tener un router y dos o más computadoras. En el trabajo, una organización probablemente tenga varios routers y switches para atender las necesidades de comunicación de datos de cientos o hasta miles de computadoras.

Los routers reenvían paquetes mediante el uso de la información de la tabla de routing. Los routers pueden descubrir las rutas hacia las redes remotas de dos maneras: de forma estática y de forma dinámica.

En una red grande con muchas redes y subredes, la configuración y el mantenimiento de rutas estáticas entre dichas redes conllevan una sobrecarga administrativa y operativa. Esta sobrecarga administrativa es especialmente tediosa cuando se producen cambios en la red, como un enlace fuera de servicio o la implementación de una nueva subred. Implementar protocolos de routing dinámico puede aliviar la carga de las tareas de configuración y de mantenimiento, además de proporcionar escalabilidad a la red.

En este capítulo, se presentan los protocolos de routing dinámico, se exploran los beneficios de utilizar esta clase de protocolos, la forma en que se clasifican los distintos protocolos de routing y las métricas que utilizan los protocolos de routing para determinar la mejor ruta para el tráfico de la red. Entre otros temas que se analizan en este capítulo, se encuentran las características de los protocolos de routing dinámico y la forma en que se diferencian los distintos protocolos de routing. Los profesionales de red deben comprender cuáles son los diferentes protocolos de routing disponibles a fin de decidir fundamentalmente cuándo utilizar routing dinámico o estático. También necesitan saber cuál es el protocolo de routing dinámico más adecuado en un entorno de red determinado.

Después de completar este capítulo, podrá hacer lo siguiente:

- Explicar el propósito de los protocolos de routing dinámico.
- Explicar el uso del routing dinámico en comparación con el routing estático.
- Explicar la forma en que los protocolos de routing dinámico comparten información de la ruta y logran la convergencia.
- Comparar las distintas categorías de los protocolos de routing.
- Describir el algoritmo que utilizan los protocolos de routing vector distancia para determinar la mejor ruta.
- Identificar los tipos de protocolos de routing vector distancia.
- Configurar el protocolo de routing RIP.
- Configurar el protocolo de routing RIPng.
- Describir el algoritmo que utilizan los protocolos de routing de estado de enlace para determinar la mejor ruta.
- Explicar la forma en que el protocolo de routing de estado de enlace utiliza la información enviada en una actualización de estado de enlace.
- Explicar las ventajas y desventajas que implica utilizar protocolos de routing de estado de enlace.
- Determinar el origen de la ruta, la distancia administrativa y la métrica para una ruta determinada.
- Explicar el concepto de la relación de nivel principal/secundario en una tabla de routing creada de forma dinámica.
- Comparar el proceso de búsqueda de rutas IPv4 sin clase y el proceso de búsqueda IPv6.
- Analizar una tabla de routing para determinar cuál ruta se utilizará para reenviar un paquete.



La mejor ruta de routing puede encontrarse mediante el uso de distintos protocolos y métricas.

Entre las métricas utilizadas se incluyen las siguientes:

- Ancho de banda
- Costo
- Retardo
- Saltos

7.2 Protocolos de enrutamiento dinámico

7.2.1 Funcionamiento del protocolo de enrutamiento dinámico

Los protocolos de routing dinámico se utilizan en el ámbito de las redes desde finales de la década de los ochenta. Uno de los primeros protocolos de routing fue el protocolo de información de routing (RIP). Si bien el protocolo RIP versión 1 (RIPv1) se lanzó en 1988, ya en 1969 se utilizaban algunos de los algoritmos básicos en dicho protocolo en la Advanced Research Projects Agency Network (ARPANET).

A medida que las redes evolucionaron y se volvieron más complejas, surgieron nuevos protocolos de routing. El protocolo de routing RIP se actualizó a RIPv2 a fin de admitir el crecimiento del entorno de red. Sin embargo, la versión más nueva de RIP aún no es escalable a las implementaciones de red más extensas de la actualidad. Con el objetivo de satisfacer las necesidades de las redes más grandes, se desarrollaron dos protocolos de routing: el protocolo OSPF (Open Shortest Path First) e Intermediate System-to-Intermediate System (IS-IS). Cisco desarrolló el protocolo de routing de gateway interior (IGRP) e IGRP mejorado (EIGRP), que también tiene buena escalabilidad en implementaciones de redes más grandes.

Asimismo, surgió la necesidad de conectar distintas internetworks y proporcionar routing entre ellas. En la actualidad, se utiliza el protocolo de gateway fronterizo (BGP) entre proveedores de servicios de Internet (ISP). El protocolo BGP también se utiliza entre los ISP y sus clientes privados más grandes para intercambiar información de routing.

En la figura 1, se muestra la línea cronológica de la introducción de los diversos protocolos.

En la figura 2, se clasifican los protocolos.

Con la llegada de numerosos dispositivos que usan IP para consumidores, el espacio de direccionamiento IPv4 quedó prácticamente agotado, por lo que surgió IPv6. A fin de admitir la comunicación basada en IPv6, se desarrollaron versiones más nuevas de los protocolos de routing IP (consulte la fila de IPv6 en la ilustración).

RIP es el más simple de los protocolos de routing dinámico y, en esta sección, se utiliza para proporcionar un nivel básico de comprensión sobre los protocolos de routing.

	Protocolos de gateway interior				Protocolos de gateway exterior
	Vector distancia		Estado de enlace		Vector ruta
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la elección de los mejores caminos que realiza el protocolo. El propósito de los protocolos de routing dinámico incluye lo siguiente:

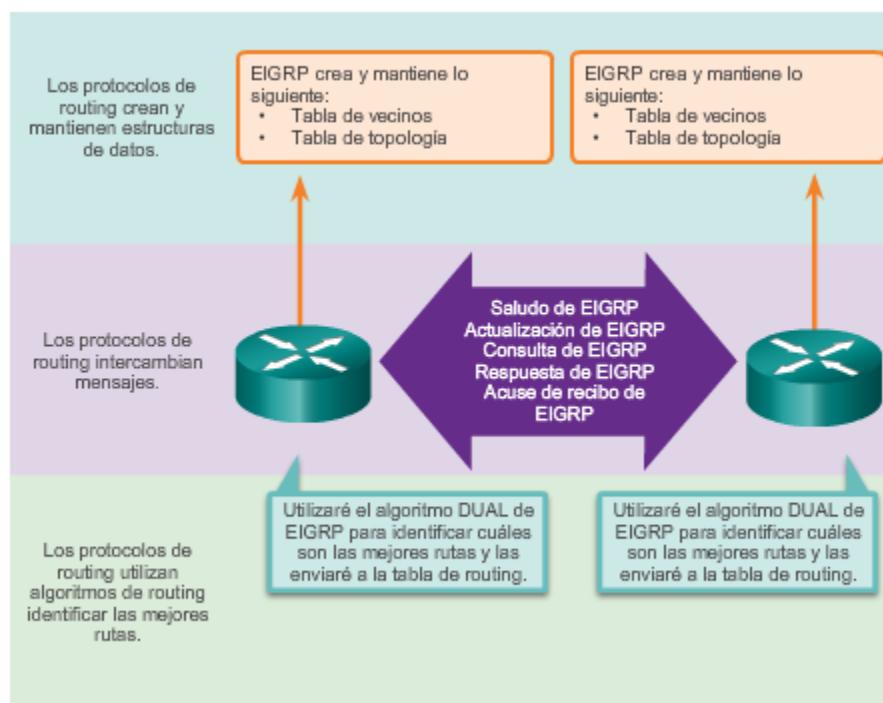
- Descubrir redes remotas
- Mantener la información de enrutamiento actualizada
- Escoger el mejor camino hacia las redes de destino
- Poder encontrar un mejor camino nuevo si la ruta actual deja de estar disponible

Los componentes principales de los protocolos de routing dinámico incluyen los siguientes:

- **Estructuras de datos:** por lo general, los protocolos de routing utilizan tablas o bases de datos para sus operaciones. Esta información se guarda en la RAM.
- **Mensajes del protocolo de routing:** los protocolos de routing usan varios tipos de mensajes para descubrir routers vecinos, intercambiar información de routing y realizar otras tareas para descubrir la red y conservar información precisa acerca de ella.
- **Algoritmo:** un algoritmo es una lista finita de pasos que se usan para llevar a cabo una tarea. Los protocolos de enrutamiento usan algoritmos para facilitar información de enrutamiento y para determinar el mejor camino.

En la ilustración, se destacan las estructuras de datos, los mensajes del protocolo de routing y el algoritmo de routing que utiliza EIGRP.

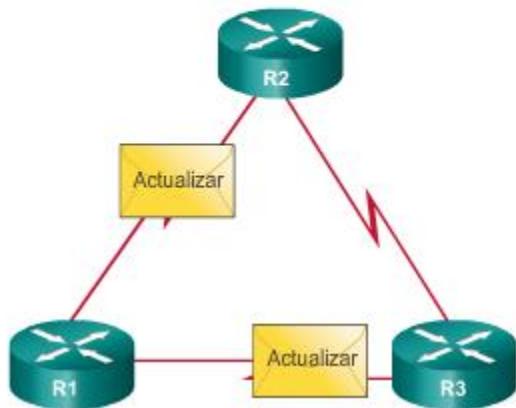
Componentes de los protocolos de routing



Los protocolos de routing permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esa información automáticamente a sus propias tablas de routing. Consulte la animación en la ilustración.

Los protocolos de routing determinan la mejor ruta hacia cada red y, a continuación, esa ruta se agrega a la tabla de routing. 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. Las redes con niveles moderados de complejidad pueden tener routing estático y routing dinámico configurados.

Los routers comparten actualizaciones en forma dinámica

7.2.2 Comparación entre routing dinámico y estático

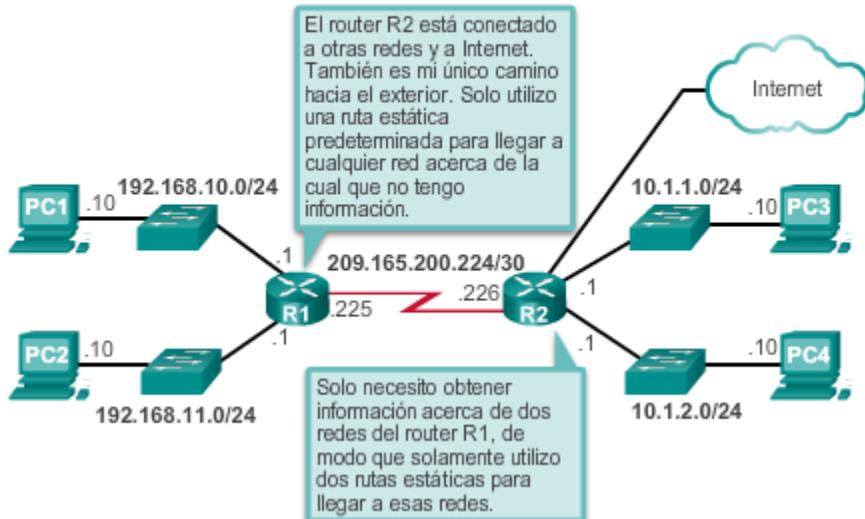
Antes de identificar los beneficios de los protocolos de routing dinámico, considere los motivos por los que los profesionales de red utilizan el routing estático. El routing dinámico definitivamente tiene varias ventajas sobre el routing estático, sin embargo, el routing estático todavía se utiliza en redes hoy en día. De hecho, las redes generalmente usan una combinación de enrutamiento estático y dinámico.

El enrutamiento estático tiene varios usos principales, entre ellos:

- Facilita el mantenimiento de la tabla de enrutamiento en redes más pequeñas en las cuales no está previsto que crezcan significativamente.
- Realiza routing desde y hacia una red de rutas internas, que es una red con una sola ruta predeterminada hacia fuera y sin conocimiento de redes remotas.
- Permite acceder a una única ruta predeterminada (la cual se utiliza para representar una ruta hacia cualquier red que no tiene una coincidencia más específica con otra ruta en la tabla de routing).

En la ilustración, se proporciona una situación de ejemplo de routing estático.

Situación de routing estático



En la tabla de la ilustración, se destacan las ventajas y las desventajas del routing estático. El routing estático es fácil de implementar en redes pequeñas. Las rutas estáticas permanecen sin alteraciones, lo que hace que sea relativamente fácil llevar a cabo la resolución de problemas. Las rutas estáticas no envían mensajes de actualización y, por lo tanto, ocasionan muy poca sobrecarga.

Las desventajas del routing estático incluyen las siguientes:

- No es fácil de implementar en redes grandes.
- La administración de las configuraciones estáticas puede llevar mucho tiempo.
- Si un enlace falla, una ruta estática no puede volver a enrutar el tráfico.

Ventajas y desventajas del enrutamiento estático

Ventajas	Desventajas
Fácil de implementar en una red pequeña.	Adecuado solamente para topologías simples o para fines específicos, como una ruta estática predeterminada. La complejidad de la configuración aumenta notablemente a medida que crece la red.
Muy seguro. No se envían anuncios, a diferencia del caso de los protocolos de routing dinámico.	La complejidad de la configuración aumenta significativamente cuando el tamaño de la red es mayor.
La ruta hacia el destino siempre es la misma.	Se requiere intervención manual para volver a enrutar el tráfico.
Dado que no se requieren algoritmos de routing ni mecanismos de actualización, no se necesitan recursos adicionales (CPU o RAM).	

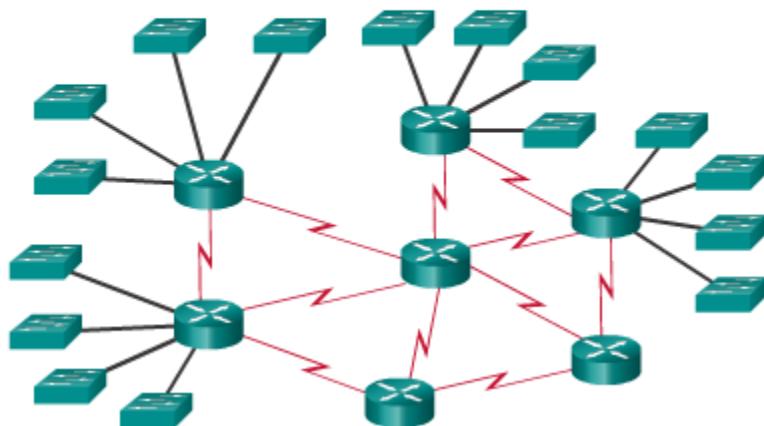
Los protocolos de routing dinámico ayudan al administrador de red a administrar el proceso riguroso y lento de configuración y mantenimiento de rutas estáticas.

Imagine tener que mantener las configuraciones de routing estático para los siete routers en figura 1.

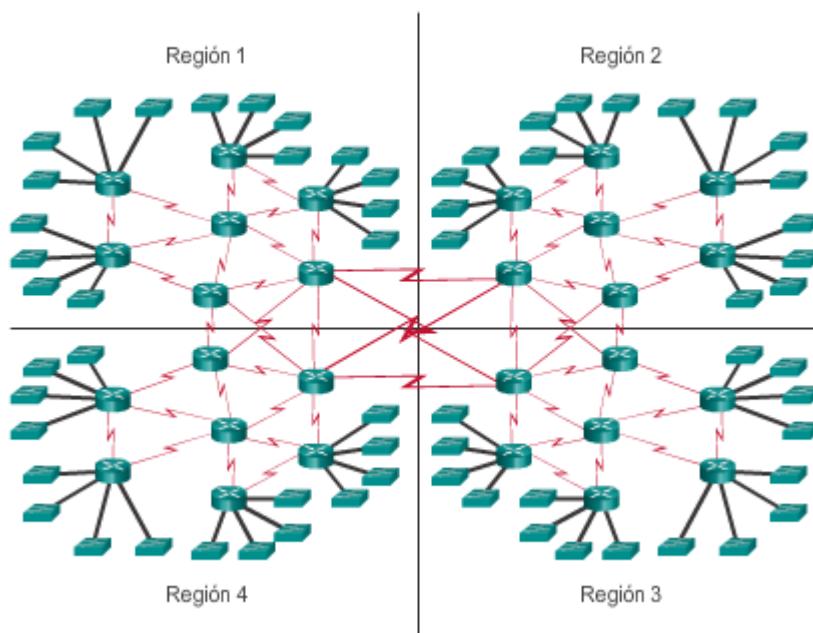
¿Qué sucedería si la empresa creciera y ahora tuviera cuatro regiones y 28 routers para administrar, como se muestra en la figura 2? ¿Qué sucede cuando un enlace deja de funcionar? ¿Cómo se asegura de que las rutas redundantes estén disponibles?

El routing dinámico es la mejor opción para redes grandes como la que se muestra.

Situación de routing dinámico



Situación de routing dinámico



En la tabla de la ilustración, se destacan las ventajas y las desventajas del routing dinámico. Los protocolos de routing dinámico funcionan bien en cualquier tipo de red conformada por varios routers. Son escalables y determinan automáticamente las mejores rutas si se produce un cambio en la topología. Si bien existen otros aspectos para tener en cuenta respecto de la configuración de los protocolos de routing dinámico, son más simples de configurar en redes grandes.

El routing dinámico presenta desventajas. Esta clase de routing requiere conocer comandos adicionales. Además, es menos seguro que el routing estático, porque las interfaces identificadas por el protocolo de routing envían actualizaciones de routing fuera de la red. Las rutas tomadas pueden variar entre paquetes. El algoritmo de routing utiliza CPU, RAM y ancho de banda de enlace adicionales.

Observe la forma en que el routing dinámico aborda las desventajas del routing estático.

Ventajas y desventajas del enrutamiento dinámico

Ventajas	Desventajas
Adecuado en todas las topologías donde se requieren varios routers.	La implementación puede ser más compleja.
Por lo general, es independiente del tamaño de la red.	Menos seguro. Se requieren opciones de configuración adicionales para proporcionarle protección.
Si es posible, adapta automáticamente la topología para volver a enrutar el tráfico.	La ruta depende de la topología actual.
	Requiere CPU, RAM y ancho de banda de enlace adicionales.

	Enrutamiento estático	Enrutamiento dinámico
Adecuado para topologías de varios routers.		✓
Cuando es posible, se adapta a los cambios de topología para volver a enrutar el tráfico.		✓
Fácil de implementar en una red pequeña.	✓	
Requiere más CPU, RAM y ancho de banda de enlace.		✓
La ruta hacia el destino siempre es la misma.	✓	

7.2.3 Aspectos básicos de la operación de los protocolos de routing

Todos los protocolos de routing están diseñados para descubrir redes remotas y adaptarse rápidamente cuando ocurre un cambio en la topología. El método que usa un protocolo de enrutamiento para lograr su propósito depende del algoritmo que use y de las características operativas de ese protocolo.

En general, las operaciones de un protocolo de enrutamiento dinámico pueden describirse de la siguiente manera:

1. El router envía y recibe mensajes de enrutamiento en sus interfaces.
2. El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.
3. Los routers intercambian información de enrutamiento para obtener información sobre redes remotas.
4. Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.

Todos los protocolos de routing siguen los mismos patrones de funcionamiento. Para ayudar a ilustrar esto, considere la siguiente situación en la que los tres routers ejecutan RIPv2.

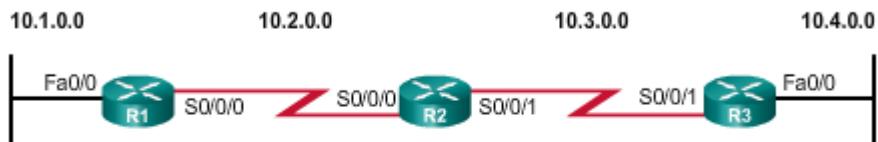
Cuando un router se enciende, no tiene ninguna información sobre la topología de la red. Ni siquiera tiene conocimiento de que existen dispositivos en el otro extremo de sus enlaces. La única información que tiene un router proviene de su propio archivo de configuración almacenado en la NVRAM. Una vez que se un router arranca correctamente, aplica la configuración guardada. Si el direccionamiento IP está configurado de forma correcta, en primer lugar el router detecta sus propias redes conectadas directamente.

Haga clic en Reproducir en la ilustración para ver una animación de la detección inicial de las redes conectadas para cada router.

Observe la forma en que los routers avanzan a través del proceso de arranque y luego detectan las redes conectadas directamente y las máscaras de subred. Esta información se agrega a sus tablas de routing de la siguiente manera:

- El R1 agrega la red 10.1.0.0 disponible a través de la interfaz FastEthernet 0/0, y 10.2.0.0 está disponible a través de la interfaz Serial 0/0/0.
- El R2 agrega la red 10.2.0.0 disponible a través de la interfaz Serial 0/0/0, y 10.3.0.0 está disponible a través de la interfaz Serial 0/0/1.
- El R3 agrega la red 10.3.0.0 disponible a través de la interfaz Serial 0/0/1, y 10.4.0.0 está disponible a través de la interfaz FastEthernet 0/0.

Con esta información inicial, los routers proceden a encontrar orígenes de ruta adicionales para sus tablas de routing.

Redes conectadas directamente detectadas

Red	Interfaz	Salto
10.1.0.0	Fa0/0	0
10.2.0.0	S0/0/0	0

Red	Interfaz	Salto
10.2.0.0	S0/0/0	0
10.3.0.0	S0/0/1	0

Red	Interfaz	Salto
10.3.0.0	S0/0/1	0
10.4.0.0	Fa0/0	0

Después del arranque inicial y del descubrimiento, la tabla de routing se actualiza con todas las redes conectadas directamente y las interfaces en las que residen dichas redes.

Si se configura un protocolo de routing, el siguiente paso es que el router comience a intercambiar actualizaciones de routing para obtener información sobre rutas remotas.

El router envía un paquete de actualización por todas las interfaces habilitadas en el router. La actualización contiene la información de la tabla de routing, que en este momento consta de todas las redes conectadas directamente.

Al mismo tiempo, el router también recibe y procesa actualizaciones similares de otros routers conectados. Una vez recibida la actualización, el router revisa si contiene información de red nueva, y se agrega a la tabla de routing toda red que no esté incluida en ella aún.

Para ver la configuración de la topología entre tres routers (R1, R2 y R3), consulte la ilustración. Sobre la base de esta topología, a continuación se muestra una lista de las distintas actualizaciones que el R1, el R2 y el R3 envían y reciben durante la convergencia inicial.

R1:

- Envía una actualización acerca de la red 10.1.0.0 desde la interfaz serial 0/0/0.
- Envía una actualización acerca de la red 10.2.0.0 desde la interfaz FastEthernet0/0.
- Recibe una actualización del R2 acerca de la red 10.3.0.0 e incrementa el conteo de saltos en 1.
- Almacena la red 10.3.0.0 en la tabla de enrutamiento con una métrica de 1.

R2:

- Envía una actualización acerca de la red 10.3.0.0 desde la interfaz serial 0/0/0.
- Envía una actualización acerca de la red 10.2.0.0 desde la interfaz serial 0/0/1.

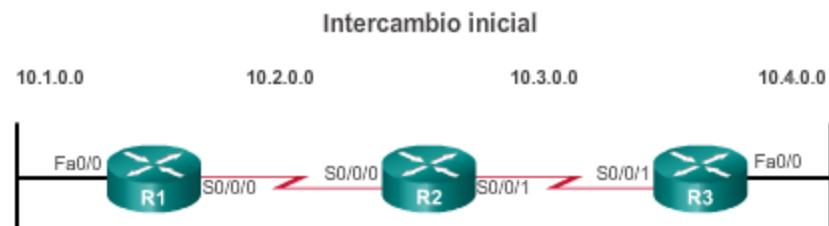
- Recibe una actualización del R1 acerca de la red 10.1.0.0 e incrementa el conteo de saltos en 1.
- Almacena la red 10.1.0.0 en la tabla de enrutamiento con una métrica de 1.
- Recibe una actualización del R3 acerca de la red 10.4.0.0 e incrementa el conteo de saltos en 1.
- Almacena la red 10.4.0.0 en la tabla de enrutamiento con una métrica de 1.

R3:

- Envía una actualización acerca de la red 10.4.0.0 desde la interfaz serial 0/0/1.
- Envía una actualización acerca de la red 10.3.0.0 desde la interfaz FastEthernet0/0.
- Recibe una actualización del R2 acerca de la red 10.2.0.0 e incrementa el conteo de saltos en 1.
- Almacena la red 10.2.0.0 en la tabla de enrutamiento con una métrica de 1.

Haga clic en Reproducir en la ilustración para ver una animación sobre la forma en que el R1, el R2 y el R3 comienzan el intercambio inicial.

Después de esta primera ronda de intercambios de actualizaciones, cada router tiene información acerca de las redes conectadas de sus vecinos conectados directamente. Sin embargo, ¿observó que R1 todavía no tiene información acerca de 10.4.0.0 al igual que R3 acerca de 10.1.0.0? La red convergente no tiene lugar ni se obtiene información completa hasta que se produce otro intercambio de información de routing.



Red	Interfaz	Salto	Red	Interfaz	Salto	Red	Interfaz	Salto
10.1.0.0	Fa0/0	0	10.2.0.0	S0/0/0	0	10.3.0.0	S0/0/1	0
10.2.0.0	S0/0/0	0	10.3.0.0	S0/0/1	0	10.4.0.0	Fa0/0	0
10.3.0.0	S0/0/0	1	10.1.0.0	S0/0/0	1	10.2.0.0	S0/0/1	1
			10.4.0.0	S0/0/1	1			

En este punto, los routers tienen información sobre sus propias redes conectadas directamente y las de sus vecinos más cercanos. Siguiendo el camino hacia la convergencia, los routers intercambian la siguiente ronda de actualizaciones periódicas. Cada router verifica las actualizaciones nuevamente para comprobar si hay información nueva.

Para ver la configuración de la topología entre tres routers (R1, R2 y R3), consulte la ilustración. Una vez que se completa el descubrimiento inicial, cada router continúa el proceso de convergencia mediante el envío y la recepción de las siguientes actualizaciones.

R1:

- Envía una actualización acerca de la red 10.1.0.0 por la interfaz Serial 0/0/0.
- Envía una actualización acerca de las redes 10.2.0.0 y 10.3.0.0 por la interfaz FastEthernet0/0.
- Recibe una actualización del R2 acerca de la red 10.4.0.0 e incrementa el conteo de saltos en 1.
- Almacena la red 10.4.0.0 en la tabla de routing con el valor de métrica 2.
- La misma actualización del R2 contiene información acerca de la red 10.3.0.0 con el valor de métrica 1. No se produce ningún cambio, por lo que la información de routing permanece igual.

R2:

- Envía una actualización acerca de las redes 10.3.0.0 y 10.4.0.0 por la interfaz Serial 0/0/0.
- Envía una actualización acerca de las redes 10.1.0.0 y 10.2.0.0 por la interfaz Serial 0/0/1.
- Recibe una actualización de R1 acerca de la red 10.1.0.0. No se produce ningún cambio, por lo que la información de routing permanece igual.
- Recibe una actualización de R3 acerca de la red 10.4.0.0. No se produce ningún cambio, por lo que la información de routing permanece igual.

R3:

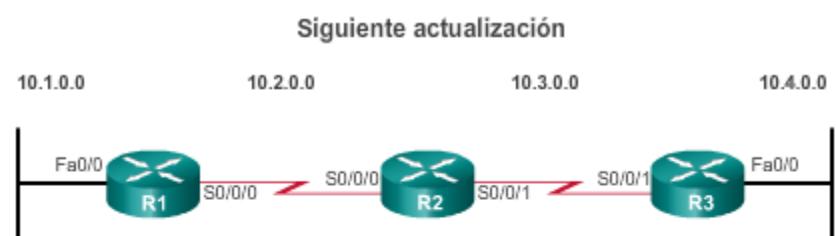
- Envía una actualización acerca de la red 10.4.0.0 desde la interfaz serial 0/0/1.
- Envía una actualización acerca de las redes 10.2.0.0 y 10.3.0.0 por la interfaz FastEthernet0/0.
- Recibe una actualización del R2 acerca de la red 10.1.0.0 e incrementa el conteo de saltos en 1.
- Almacena la red 10.1.0.0 en la tabla de routing con el valor de métrica 2.

- La misma actualización del R2 contiene información acerca de la red 10.2.0.0 con el valor de métrica 1. No se produce ningún cambio, por lo que la información de routing permanece igual.

Haga clic en Reproducir en la ilustración para ver una animación sobre la forma en que el R1, el R2 y el R3 envían la tabla de routing más reciente a sus vecinos.

Por lo general, los protocolos de routing vector distancia implementan una técnica para evitar los bucles de routing conocida como “horizonte dividido”. El horizonte dividido evita que la información se envíe desde la misma interfaz en la que se recibió dicha información. Por ejemplo, el R2 no envía una actualización que contenga la red 10.1.0.0 por la interfaz Serial 0/0/0, debido a que obtuvo información acerca de la red 10.1.0.0 a través de la interfaz Serial 0/0/0.

Una vez que los routers dentro de una red realizan la convergencia, el router puede utilizar la información que se encuentra en la tabla de rutas para determinar la mejor ruta para llegar a un destino. Los distintos protocolos de routing tienen diferentes maneras de calcular la mejor ruta.



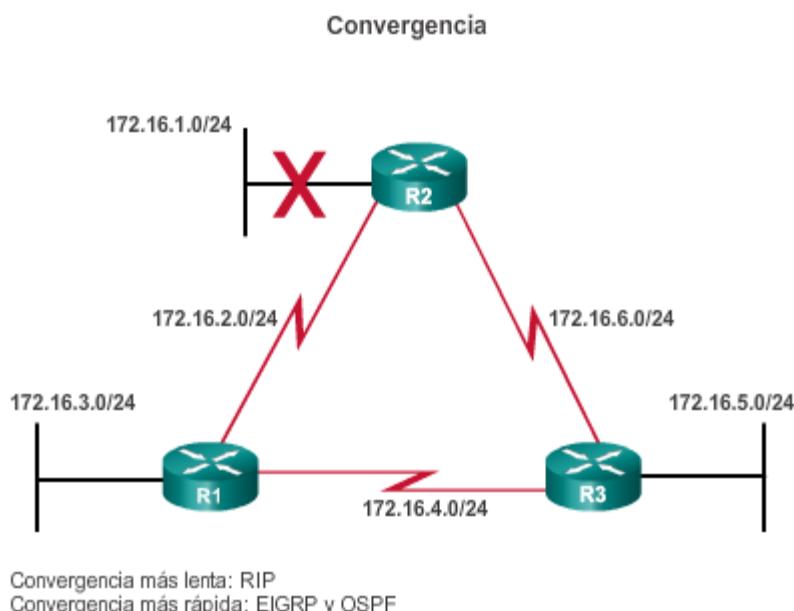
Red	Interfaz	Salto	Red	Interfaz	Salto	Red	Interfaz	Salto
10.1.0.0	Fa0/0	0	10.2.0.0	S0/0/0	0	10.3.0.0	S0/0/1	0
10.2.0.0	S0/0/0	0	10.3.0.0	S0/0/1	0	10.4.0.0	Fa0/0	0
10.3.0.0	S0/0/0	1	10.1.0.0	S0/0/0	1	10.2.0.0	S0/0/1	1
10.4.0.0	S0/0/0	2	10.4.0.0	S0/0/1	1	10.1.0.0	S0/0/1	2

La convergencia de la red se produce cuando todos los routers tienen información completa y precisa acerca de toda la red, como se muestra en la figura 1. El tiempo de convergencia es el tiempo que los routers tardan en compartir información, calcular las mejores rutas y actualizar sus tablas de enrutamiento. Una red no es completamente operativa hasta que la red haya convergido; por lo tanto, la mayoría de las redes requieren tiempos de convergencia breves.

La convergencia es cooperativa e independiente al mismo tiempo. Los routers comparten información entre sí, pero deben calcular en forma independiente los impactos del cambio de topología en sus propias rutas. Dado que establecen un acuerdo con la nueva topología en forma independiente, se dice que convergen sobre este consenso.

Las propiedades de convergencia incluyen la velocidad de propagación de la información de enrutamiento y el cálculo de los caminos óptimos. La velocidad de propagación se refiere al tiempo que tardan los routers dentro de la red en reenviar la información de routing.

Como se muestra en la figura 2, los protocolos de routing pueden clasificarse según la velocidad de convergencia: cuanto más rápida sea la convergencia, mejor será el protocolo de routing. Generalmente, los protocolos más antiguos, como RIP, tienen una convergencia lenta, mientras que los protocolos modernos, como EIGRP y OSPF, la realizan más rápidamente.



7.2.4 Tipos de protocolos de routing

Los protocolos de enrutamiento se pueden clasificar en diferentes grupos según sus características. Específicamente, los protocolos de routing se pueden clasificar según lo siguiente:

- **Propósito:** protocolo de gateway interior (IGP) o protocolo de gateway exterior (EGP)
- **Operación:** vector distancia, protocolo de estado de enlace, protocolo vector ruta
- **Comportamiento:** protocolo con clase (antiguo) o protocolo sin clase

Por ejemplo, los protocolos de routing IPv4 se clasifican de la siguiente manera:

- **RIPv1 (antiguo):** IGP, vector distancia, protocolo con clase
- **IGRP (antiguo):** IGP, vector distancia, protocolo con clase desarrollado por Cisco (cayó en desuso a partir del IOS 12.2)
- **RIPv2:** IGP, vector distancia, protocolo sin clase
- **EIGRP:** IGP, vector distancia, protocolo sin clase desarrollado por Cisco

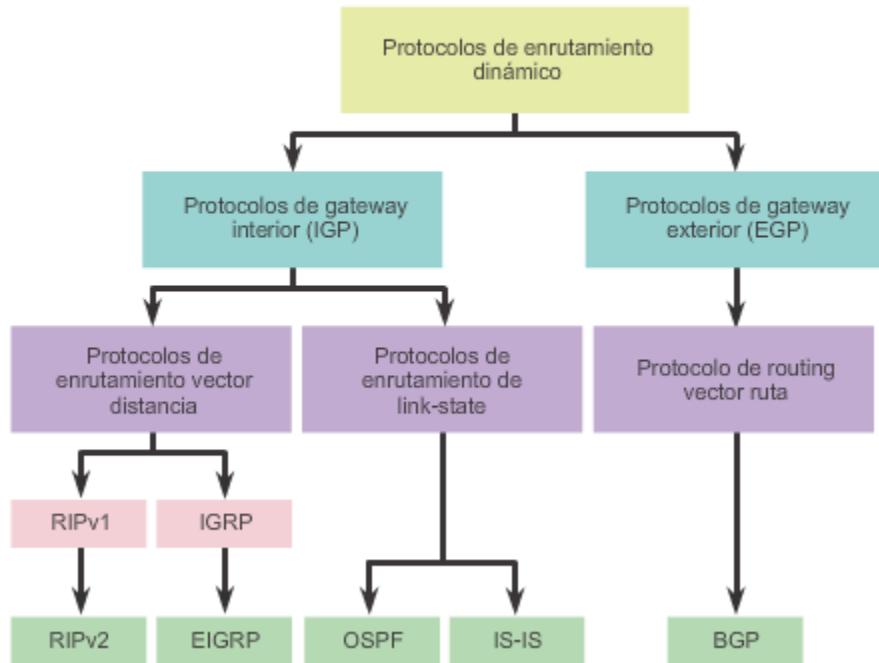
- **OSPF:** IGP, estado de enlace, protocolo sin clase
- **IS-IS:** IGP, estado de enlace, protocolo sin clase
- **BGP:** EGP, vector ruta, protocolo sin clase

Los protocolos de routing con clase, RIPv1 e IGRP, son protocolos antiguos y se utilizan solamente en redes antiguas. Estos protocolos de routing se convirtieron en los protocolos de routing sin clase RIPv2 y EIGRP, respectivamente. Los protocolos de routing de estado de enlace son protocolos sin clase naturalmente.

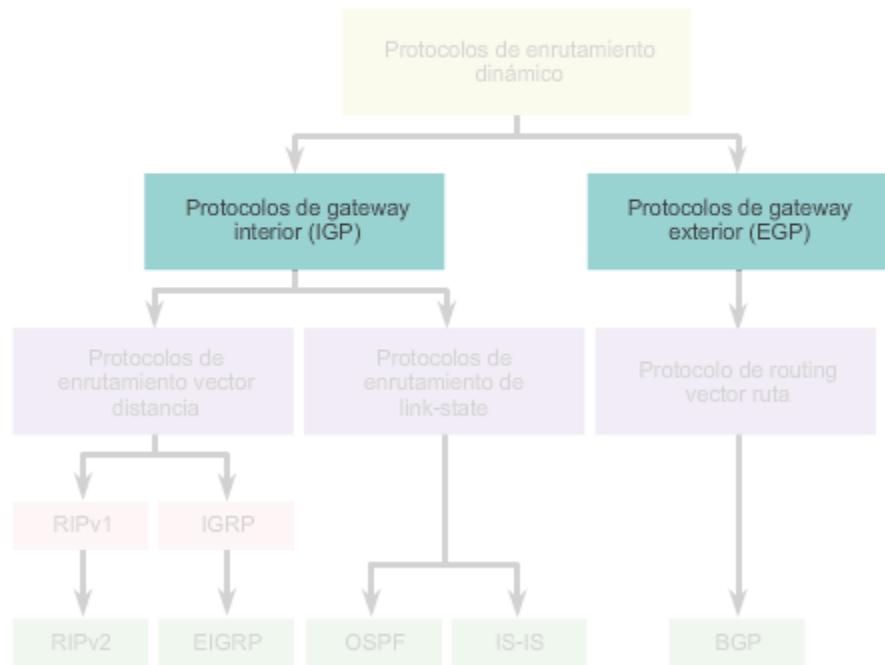
En la figura 1, se muestra una vista jerárquica de la clasificación de los protocolos de routing dinámico.

En las figuras 2 a 5, se destaca el propósito, la operación y el comportamiento de los diversos protocolos de routing.

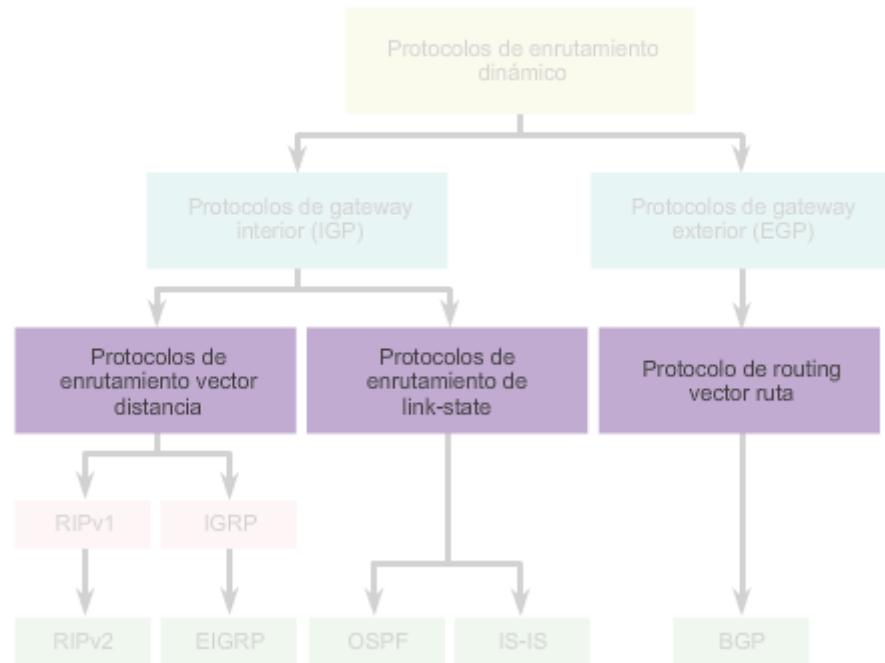
Clasificación de los protocolos de routing



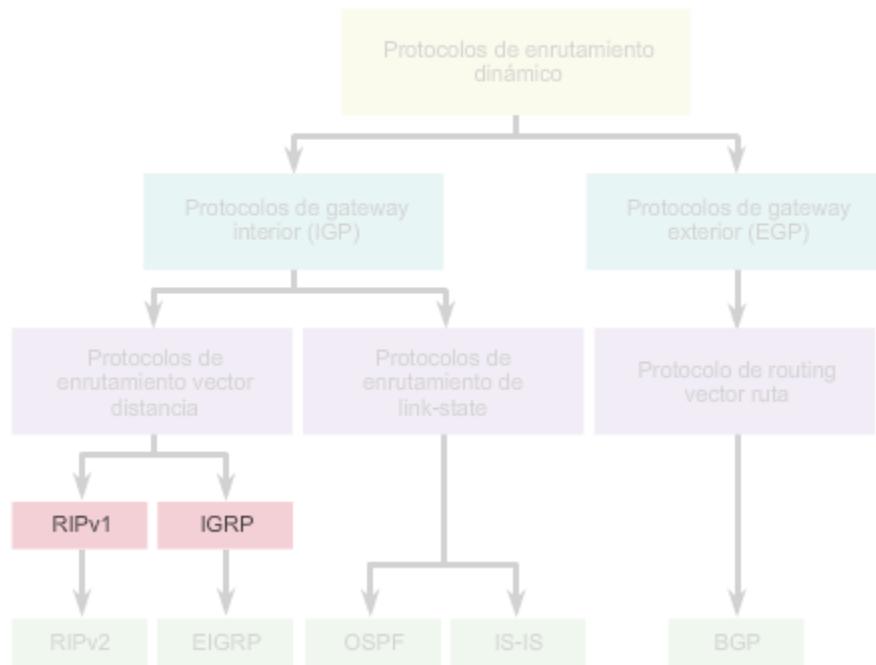
Clasificación de los protocolos de routing según su propósito



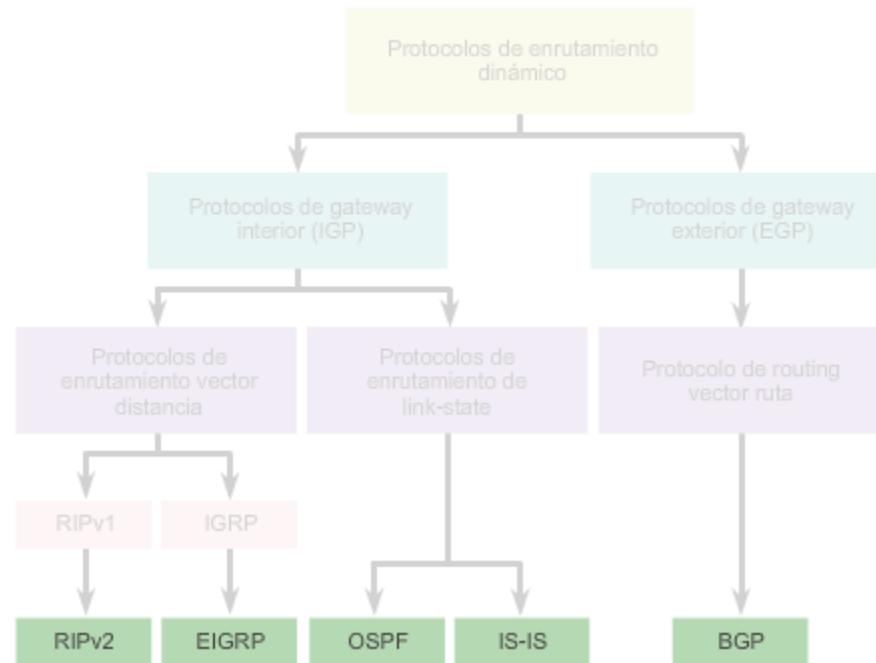
Clasificación de los protocolos de routing según su funcionamiento



Clasificación de protocolos según su comportamiento con clase



Clasificación de protocolos según su comportamiento sin clase



Un sistema autónomo (AS) es un conjunto de routers bajo una administración común, como una empresa o una organización. Los AS también se conocen como “dominios de routing”. Los ejemplos típicos de AS son la red interna de una empresa y la red de un ISP.

Debido a que Internet se basa en el concepto de AS, se requieren dos tipos de protocolos de routing:

- **Protocolo de gateway interior (IGP):** se utiliza para el routing dentro de un AS. También se lo denomina “routing interno de AS”. Las empresas, las organizaciones e incluso los proveedores de servicios utilizan un IGP en sus redes internas. Los IGP incluyen RIP, EIGRP, OSPF e IS-IS.
- **Protocolo de gateway exterior (EGP):** se utiliza para el routing entre AS. Los proveedores de servicios y las empresas grandes pueden interconectarse mediante un EGP. El protocolo de gateway fronterizo (BGP) es el único EGP viable actualmente y es el protocolo de routing oficial utilizado por Internet.

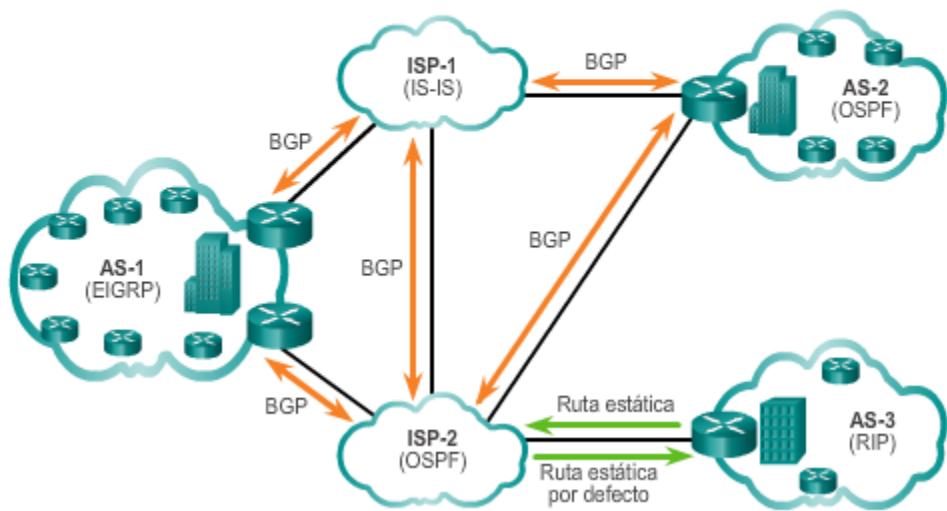
Nota: dado que BGP es el único EGP disponible, no se suele utilizar el término EGP. En cambio, la mayoría de los ingenieros simplemente hacen referencia a BGP.

En el ejemplo de la ilustración, se proporcionan situaciones simples en las que se destaca la implementación de IGP, de BGP y del routing estático:

- **ISP-1:** es un AS que utiliza IS-IS como IGP. Se interconecta con otros sistemas autónomos y proveedores de servicios que utilizan BGP para controlar explícitamente el modo en que se enruta el tráfico.
- **ISP-2:** es un AS que utiliza OSPF como IGP. Se interconecta con otros sistemas autónomos y proveedores de servicios que utilizan BGP para controlar explícitamente el modo en que se enruta el tráfico.
- **AS-1:** se trata de una organización grande que utiliza EIGRP como IGP. Dado que es un entorno de host múltiples (es decir, se conecta a dos proveedores de servicios distintos), utiliza BGP para controlar explícitamente la forma en que el tráfico ingresa al AS y sale de él.
- **AS-2:** se trata de una organización mediana y utiliza OSPF como IGP. También es un entorno de host múltiples, por lo que utiliza BGP para controlar explícitamente la forma en que el tráfico ingresa al AS y sale de él.
- **AS-3:** se trata de una organización pequeña con routers más antiguos dentro del AS y utiliza RIP como IGP. Dado que tiene conexión simple (es decir, conecta a solo un proveedor de servicios), no se requiere BGP. En cambio, se implementa routing estático entre el AS y el proveedor de servicios.

Nota: BGP excede el ámbito de este curso, motivo por el cual no se lo describe en detalle.

Comparación entre protocolos de routing IGP y EGP



“Vector distancia” significa que las rutas se anuncian proporcionando dos características:

- **Distancia**: identifica la distancia hasta la red de destino. Se basa en una métrica como el conteo de saltos, el costo, el ancho de banda y el retraso, entre otros.
- **Vector**: especifica el sentido en que se encuentra el router de siguiente salto o la interfaz de salida para llegar al destino.

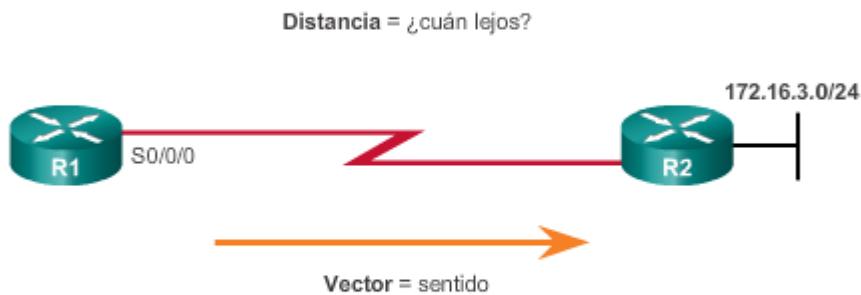
Por ejemplo, en la ilustración, el R1 tiene información de que la distancia para llegar a la red 172.16.3.0/24 es de un salto y de que el sentido es a través de la interfaz S0/0/0 hacia el R2.

Un router que utiliza un protocolo de enrutamiento vector distancia no tiene la información de la ruta completa hasta la red de destino. Los protocolos vector distancia utilizan routers como letreros a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento vector distancia no tienen un mapa en sí de la topología de la red.

Hay cuatro IGP vector distancia IPv4:

- **RIPv1**: protocolo antiguo de primera generación
- **RIPv2**: protocolo de routing vector distancia simple
- **IGRP**: protocolo exclusivo de Cisco de primera generación (obsoleto y reemplazado por EIGRP)
- **EIGRP**: versión avanzada del routing vector distancia

El significado de vector distancia



Para el R1, 172.16.3.0/24 está a un salto (distancia)
Puede alcanzarse a través del R2 (vector).

A diferencia de la operación del protocolo de routing vector distancia, un router configurado con un protocolo de routing de estado de enlace puede crear una “vista completa” o una topología de la red al reunir información proveniente de todos los demás routers.

Para continuar con nuestra analogía de letreros, el uso de un protocolo de enrutamiento de link-state es como tener un mapa completo de la topología de la red. Los letreros a lo largo de la ruta de origen a destino no son necesarios, debido a que todos los routers de estado de enlace usan un mapa de la red idéntico. Un router de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar la mejor ruta hacia todas las redes de destino en la topología.

Los routers con RIP habilitado envían actualizaciones periódicas de su información de routing a sus vecinos. Los protocolos de enrutamiento de link-state no usan actualizaciones periódicas. Una vez que se produjo la convergencia de la red, la actualización del estado de enlace solo se envía cuando se produce un cambio en la topología. Por ejemplo, la actualización del estado de enlace en la animación no se envía hasta que la red 172.16.3.0 se desactiva.

Haga clic en Reproducir en la ilustración para ver operaciones de estado de enlace.

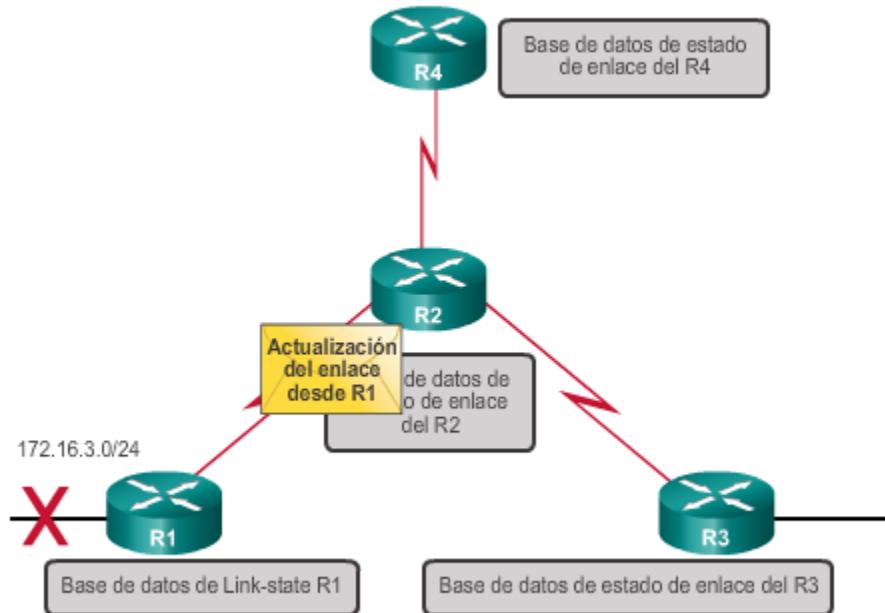
Los protocolos de link-state funcionan mejor en situaciones donde:

- El diseño de red es jerárquico, lo cual suele suceder en redes extensas.
- La rápida convergencia de la red es crucial.
- Los administradores tienen un conocimiento cabal del protocolo de routing de estado de enlace implementado.

Hay dos IGP de estado de enlace IPv4:

- **OSPF:** protocolo de routing muy popular basado en estándares
- **IS-IS:** popular en redes de proveedores

Funcionamiento del protocolo de link-state



Los protocolos de estado de enlace reenvían actualizaciones cuando cambia el estado de un enlace.

La mayor diferencia entre los protocolos de routing con clase y sin clase es que los protocolos de routing con clase no envían información de la máscara de subred en sus actualizaciones de routing. Los protocolos de routing sin clase incluyen información de la máscara de subred en las actualizaciones de routing.

Los dos protocolos de routing IPv4 originales que se desarrollaron fueron RIPv1 e IGRP, que se crearon cuando las direcciones de red se asignaban según las clases (es decir, clase A, B o C). En ese entonces, no era necesario que un protocolo de routing incluyera la máscara de subred en la actualización de routing, debido a que era posible determinar la máscara de red sobre la base del primer octeto de la dirección de red.

Nota: solo RIPv1 e IGRP son protocolos con clase. El resto de los protocolos de routing IPv4 e IPv6 son protocolos sin clase. El direccionamiento con clase nunca fue parte de IPv6.

El hecho de que RIPv1 e IGRP no incluyan información de la máscara de subred en sus actualizaciones significa que no pueden proporcionar máscaras de subred de longitud variable (VLSM) ni routing entre dominios sin clase (CIDR).

Los protocolos de routing con clase también generan problemas en las redes no contiguas. Que una red sea no contigua significa que las subredes de la misma dirección de red principal con clase están separadas por una dirección de red con clase diferente.

Consulte la topología que se muestra en la figura 1 para ver una ilustración de las limitaciones del routing con clase. Observe que las LAN del R1 (172.16.1.0/24) y del R3 (172.16.2.0/24) son subredes de la misma red de clase B (172.16.0.0/16), que están separadas por distintas direcciones de red con clase (192.168.1.0/30 y 192.168.2.0/30).

Cuando el R1 reenvía una actualización al R2, RIPv1 no incluye información de la máscara de subred con la actualización, sino que solamente reenvía la dirección de red de clase B 172.16.0.0.

El R2 recibe la actualización y la procesa. A continuación, crea una entrada para la red de clase B 172.16.0.0/16 y la agrega en la tabla de routing, como se muestra en la figura 2.

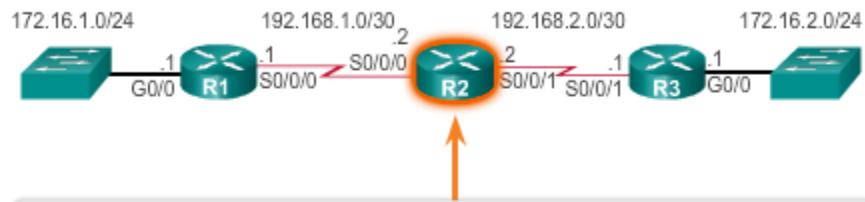
En la figura 3, se muestra que cuando el R3 reenvía una actualización al R2, tampoco incluye información de la máscara de subred y, por lo tanto, solamente reenvía la dirección de red con clase 172.16.0.0.

En la figura 4, el R2 recibe y procesa la actualización y agrega otra entrada para la dirección de red con clase 172.16.0.0/16 a su tabla de routing. Cuando hay dos entradas con métricas idénticas en la tabla de routing, el router comparte la carga de tráfico por igual entre los dos enlaces. Esto se conoce como “balanceo de carga”.

Como se muestra en la figura 5, esto tiene un efecto negativo sobre una red no contigua. Observe el comportamiento irregular de los comandos **ping** y **traceroute**.

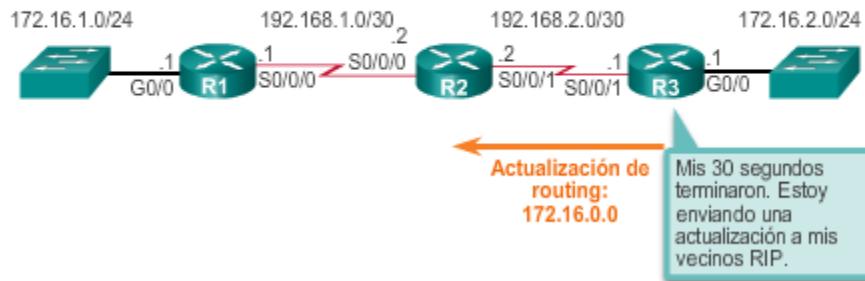
El R1 reenvía una actualización con clase al R2



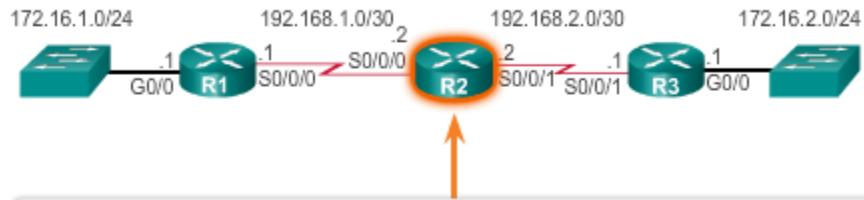
El R2 agrega la entrada para 172.16.0.0 a través del R1

```
R2# show ip route | begin Gateway
Gateway of last resort is not set

R    172.16.0.0/16 [120/1] via 192.168.1.1, 00:00:11,
      Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets,
      2 masks
C        192.168.1.0/30 is directly connected, Serial0/0/0
L        192.168.1.2/32 is directly connected, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets,
      2 masks
C        192.168.2.0/30 is directly connected, Serial0/0/1
L        192.168.2.2/32 is directly connected, Serial0/0/1
R2#
```

El R3 reenvia una actualización con clase al R2

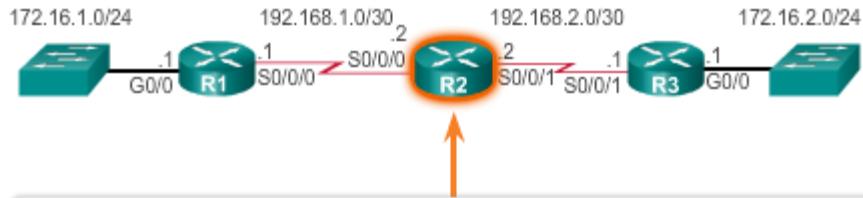
El R2 agrega la entrada para 172.16.0.0 a través del R3



```
R2# show ip route | begin Gateway
Gateway of last resort is not set

R    172.16.0.0/16 [120/1] via 192.168.2.1, 00:00:14,
      Serial0/0/1
      [120/1] via 192.168.1.1, 00:00:16,
      Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets,
      2 masks
C        192.168.1.0/30 is directly connected, Serial0/0/0
L        192.168.1.2/32 is directly connected, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets,
      2 masks
C        192.168.2.0/30 is directly connected, Serial0/0/1
L        192.168.2.2/32 is directly connected, Serial0/0/1
R2#
```

Falla de conectividad



```
R2# ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2
seconds:
U.U.U
Success rate is 0 percent (0/5)
R2#
R2# traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1  192.168.1.1 4 msec
      192.168.2.1 4 msec
      192.168.1.1 4 msec
R2#
```

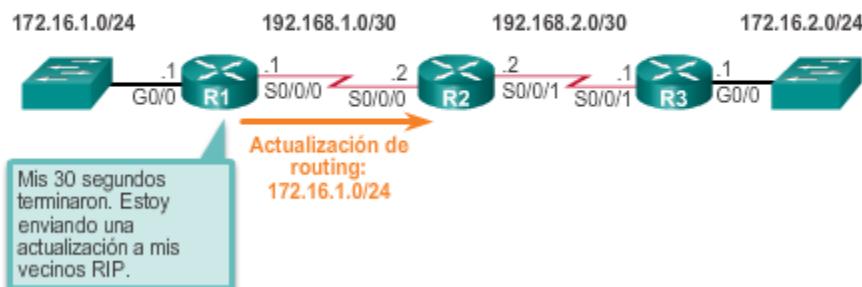
Las redes modernas ya no utilizan el direccionamiento IP con clase, y la máscara de subred no se puede determinar mediante el valor del primer octeto. Los protocolos de routing IPv4 sin clase (RIPv2, EIGRP, OSPF e IS-IS) incluyen la información de la máscara de subred con la dirección de red en las actualizaciones de routing. Los protocolos de routing sin clase admiten VLSM y CIDR.

Los protocolos de routing IPv6 son protocolos sin clase. Por lo general, la distinción entre los protocolos de routing con clase y sin clase se aplica únicamente a los protocolos de routing IPv4. Se considera que todos los protocolos de routing IPv6 son protocolos sin clase, dado que incluyen la duración de prefijo con la dirección IPv6.

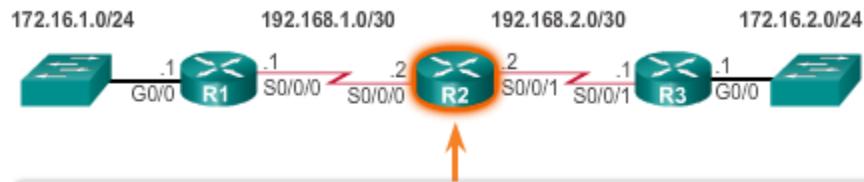
En las figuras 1 a 5, se ilustra la forma en que el routing sin clase resuelve los problemas que se generan con el routing con clase:

- **Figura 1:** en este diseño de red no contigua, se implementó el protocolo sin clase RIPv2 en los tres routers. Cuando el R1 reenvía una actualización al R2, RIPv2 incluye la información de la máscara de subred con la actualización 172.16.1.0/24.
- **Figura 2:** el R2 recibe, procesa y agrega dos entradas en la tabla de routing. En la primera línea, se muestra la dirección de red con clase 172.16.0.0 con la máscara de subred /24 de la actualización. Esto se conoce como “ruta principal”. En la segunda entrada, se muestra la dirección de red VLSM 172.16.1.0, con la dirección del siguiente salto y la salida. Esto se conoce como “ruta secundaria”. Las rutas principales nunca incluyen una interfaz de salida ni la dirección IP del siguiente salto.
- **Figura 3:** cuando el R3 reenvía una actualización al R2, RIPv2 incluye la información de la máscara de subred con la actualización 172.16.2.0/24.
- **Figura 4:** el R2 recibe, procesa y agrega otra entrada de ruta secundaria 172.16.2.0/24 debajo de la entrada de la ruta principal 172.16.0.0.
- **Figura 5:** ahora el R2 tiene información acerca de las redes divididas en subredes.

El R1 reenvía una actualización sin clase al R2



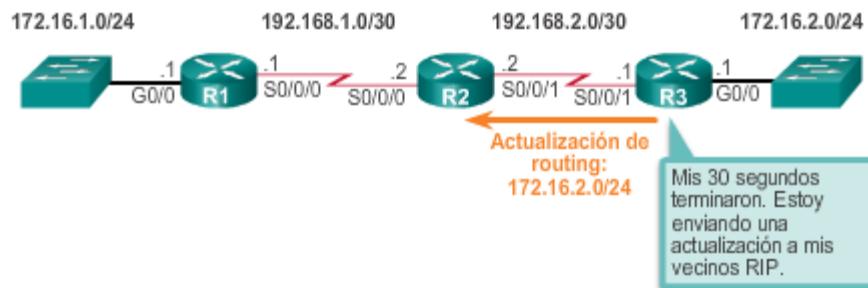
El R2 agrega la entrada para 172.16.0.0 a través del R1



```
R2# show ip route | begin Gateway
Gateway of last resort is not set

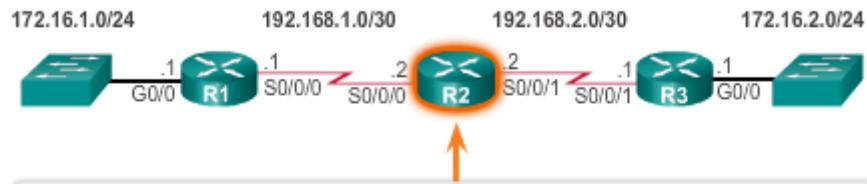
      172.16.0.0/24 is subnetted, 1 subnets
R          172.16.1.0 [120/1] via 192.168.1.1, 00:00:06,
                  Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets,
      2 masks
C            192.168.1.0/30 is directly connected, Serial0/0/0
L            192.168.1.2/32 is directly connected, Serial0/0/0
R2#
```

El R3 reenvía una actualización sin clase al R2



Mis 30 segundos terminaron. Estoy enviando una actualización a mis vecinos RIP.

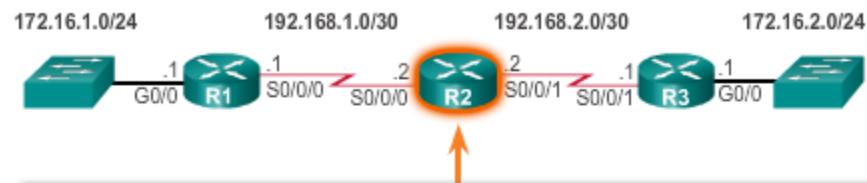
El R2 agrega la entrada para 172.16.0.0 a través del R3



```
R2# show ip route | begin Gateway
Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 2 subnets
R          172.16.1.0 [120/1] via 192.168.1.1, 00:00:03,
                  Serial0/0/0
R          172.16.2.0 [120/1] via 192.168.2.1, 00:00:03,
                  Serial0/0/1
      192.168.1.0/24 is variably subnetted, 2 subnets,
      2 masks
C              192.168.1.0/30 is directly connected, Serial0/0/0
L              192.168.1.2/32 is directly connected, Serial0/0/0
      192.168.2.0/24 is variably subnetted, 2 subnets,
      2 masks
C              192.168.2.0/30 is directly connected, Serial0/0/1
L              192.168.2.2/32 is directly connected, Serial0/0/1
R2#
```

Conectividad satisfactoria



```
R2# ping 172.16.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
12/14/16 ms
R2#
R2# traceroute 172.16.1.1
Type escape sequence to abort.
Tracing the route to 172.16.1.1
VRF info: (vrf in name/id, vrf out name/id)
  1 192.168.1.1 4 msec 4 msec *
R2#
```

Los protocolos de enrutamiento se pueden comparar según las siguientes características:

- **Velocidad de convergencia:** define cuán rápido comparten información de routing y alcanzan un estado de conocimiento coherente los routers de la topología de la red. Cuanto más rápida sea la convergencia, más preferible será el protocolo. Los loops de enrutamiento pueden ser el resultado de tablas de enrutamiento incongruentes que no se han actualizado debido a la lenta convergencia de una red sujeta a cambios.
- **Escalabilidad:** define cuán grande puede ser una red, según el protocolo de routing implementado. Cuanto más grande sea la red, más escalable debe ser el protocolo de enrutamiento.
- **Con clase o sin clase (uso de VLSM):** los protocolos de routing con clase no incluyen la máscara de subred y no admiten VLSM. Los protocolos de routing sin clase incluyen la máscara de subred en las actualizaciones. Los protocolos de routing sin clase admiten VLSM y una mejor summarización de ruta.
- **Uso de recursos:** incluye los requisitos de un protocolo de routing, como el espacio de memoria (RAM), la utilización de la CPU y el uso del ancho de banda del enlace. Una mayor cantidad de requisitos de recursos exige hardware más potente para admitir la operación del protocolo de routing además de los procesos de reenvío de paquetes.
- **Implementación y mantenimiento:** describen el nivel de conocimiento necesario para que un administrador de red ponga en funcionamiento y mantenga la red según el protocolo de routing implementado.

En la tabla de la ilustración, se resumen las características de cada protocolo de routing.

Comparación de los protocolos de routing

	Vector distancia				Estado de enlace	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Velocidad de convergencia	Lento	Lento	Lento	Rápido	Rápido	Rápido
Escalabilidad: tamaño de la red	Pequeño	Pequeño	Pequeño	Grande	Grande	Grande
Uso de VLSM	No	Sí	No	Sí	Sí	Sí
Uso de recursos	Bajo	Bajo	Bajo	Medio	Alto	Alto
Implementación y mantenimiento	Simple	Simple	Simple	Complejo	Complejo	Complejo

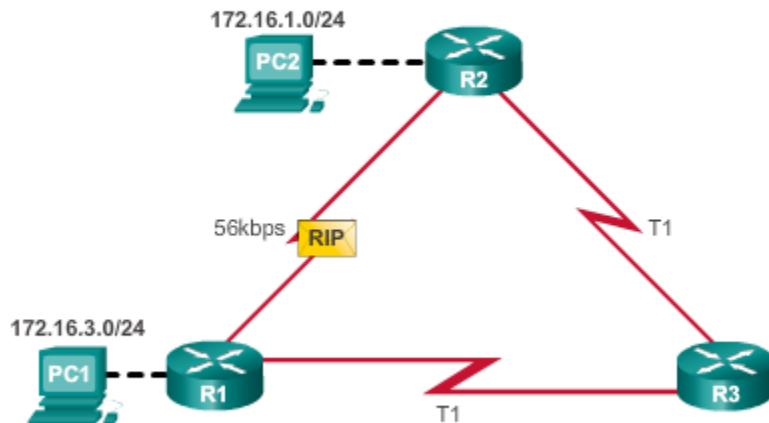
En algunos casos, un protocolo de enrutamiento obtiene información sobre más de una ruta hacia el mismo destino. Para seleccionar el mejor camino, el protocolo de enrutamiento debe poder evaluar y diferenciar entre las rutas disponibles. Esto se logra mediante el uso de métricas de routing.

Una métrica es un valor mensurable que el protocolo de routing asigna a distintas rutas según la utilidad que tengan. En situaciones donde hay varias rutas hacia la misma red remota, las métricas de routing se utilizan para determinar el “costo” total de una ruta de origen a destino. Los protocolos de routing determinan la mejor ruta sobre la base del costo más bajo.

Los diferentes protocolos de enrutamiento pueden usar diferentes métricas. La métrica utilizada por un protocolo de enrutamiento no es comparable con la métrica utilizada por otro protocolo de enrutamiento. Dos protocolos de routing distintos pueden elegir diferentes rutas hacia el mismo destino.

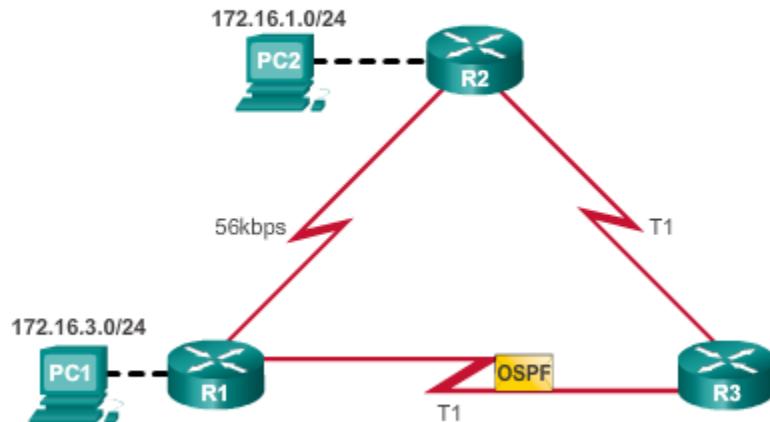
En la animación de la ilustración, se muestra que el protocolo RIP elegiría la ruta con la menor cantidad de saltos, mientras que el protocolo OSPF elegiría la ruta con el mayor ancho de banda.

Protocolos de routing y sus métricas

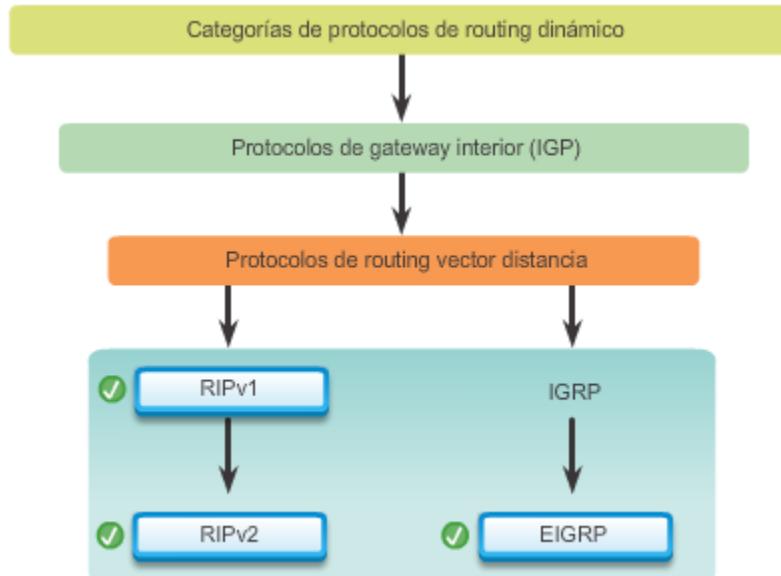


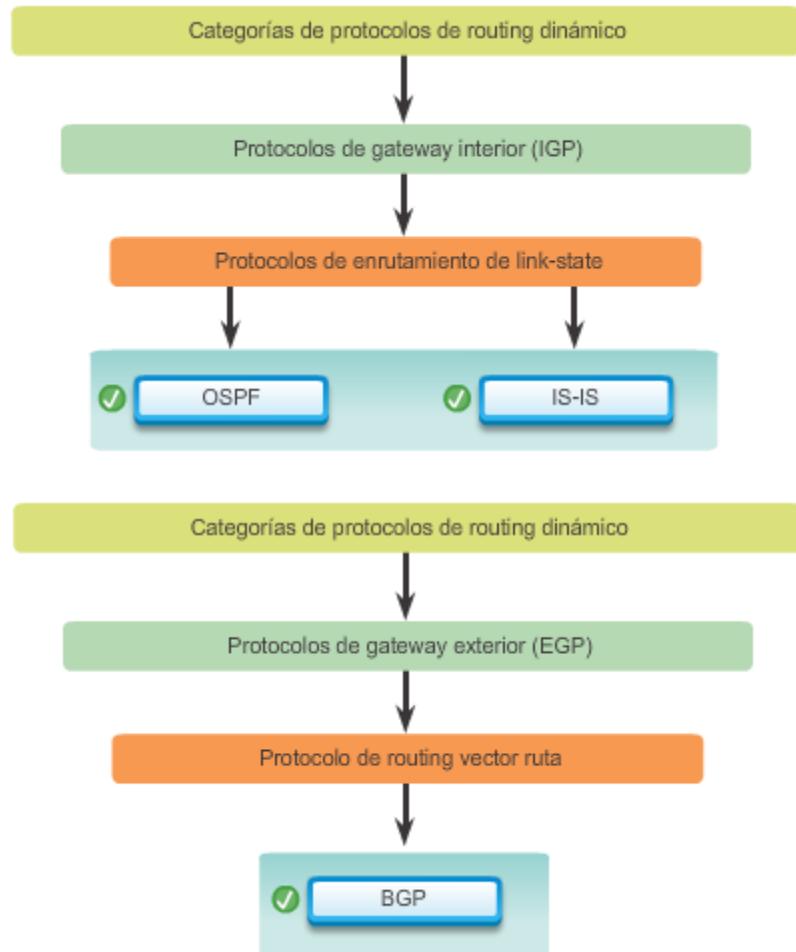
RIP selecciona la mejor ruta sobre la base del conteo de saltos.
OSPF selecciona la mejor ruta sobre la base del ancho de banda.

Protocolos de routing y sus métricas



RIP selecciona la mejor ruta sobre la base del conteo de saltos.
OSPF selecciona la mejor ruta sobre la base del ancho de banda.





Protocolos de routing vector distancia (actuales)		
RIPv2	EIGRP	Característica del protocolo de routing
✓ Lento	✓ Rápido	Velocidad de convergencia (lenta o rápida)
✓ Pequeño	✓ Grande	Escalabilidad de la red (pequeña o grande)
✓ Sí	✓ Sí	Compatibilidad con VLSM (sí o no)
✓ Bajo	✓ Medio	Consumo de recursos (alto, medio o bajo)
✓ Simple	✓ Complejo	Implementación y mantenimiento (simples o complejos)

Protocolos de enrutamiento de link-state

OSPF	IS-IS	Característica del protocolo de routing
Rápido	Rápido	Velocidad de convergencia (lenta o rápida)
Grande	Grande	Escalabilidad de la red (pequeña o grande)
Sí	Sí	Compatibilidad con VLSM (sí o no)
Alto	Alto	Consumo de recursos (alto, medio o bajo)
Complejo	Complejo	Implementación y mantenimiento (simples o complejos)

	EIGRP	OSPF	RIP
Métrica basada en conteo de saltos.			
Utiliza el costo (anchos de banda del enlace acumulativos) como métrica.			
Métrica basada en el retraso (tiempo de entrega de paquetes) y el ancho de banda.			
La métrica también puede basarse en la carga (cantidad de tráfico del enlace) y la confiabilidad (probabilidad de fallas del enlace).			

7.3 Routing dinámico vector distancia

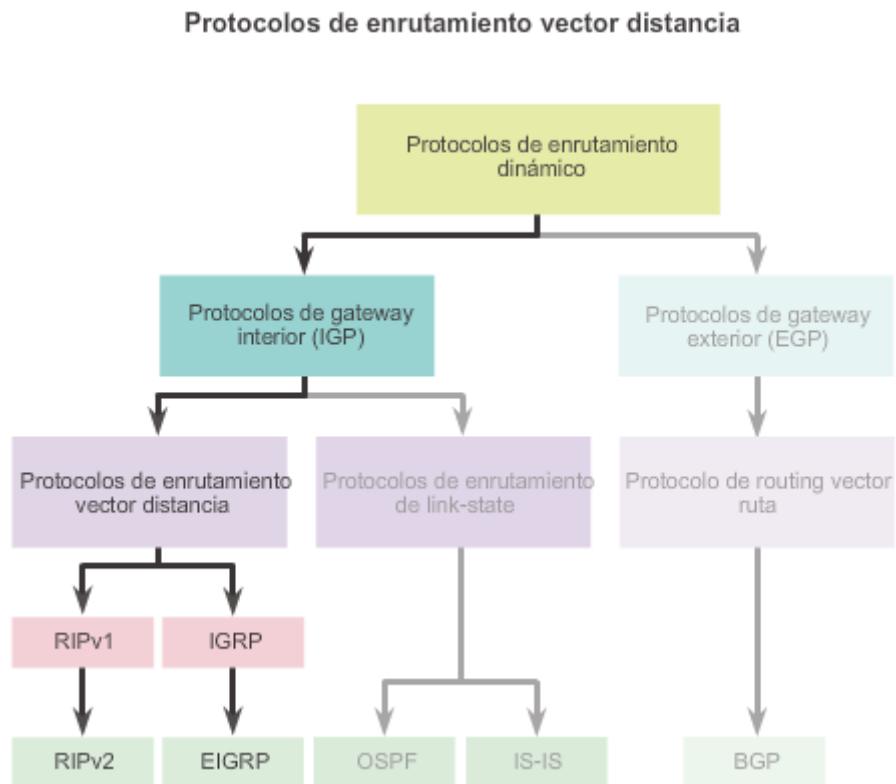
7.3.1 Funcionamiento del protocolo de enrutamiento vector distancia

Los protocolos de routing vector distancia comparten actualizaciones entre vecinos. Los vecinos son routers que comparten un enlace y que están configurados para usar el mismo protocolo de enrutamiento. El router sólo conoce las direcciones de red de sus propias interfaces y las direcciones de red remota que puede alcanzar a través de sus vecinos. Los routers que utilizan el enrutamiento vector distancia no tienen información sobre la topología de la red.

Algunos protocolos de routing vector distancia envían actualizaciones periódicas. Por ejemplo, RIP envía una actualización periódica a todos sus vecinos cada 30 segundos; incluso si no se produce un cambio en la topología, RIP continúa enviando actualizaciones. Para llegar a todos sus vecinos, RIPv1 envía actualizaciones a la dirección IPv4 de todos los hosts 255.255.255.255 mediante una difusión.

La difusión de actualizaciones periódicas es ineficiente, debido a que las actualizaciones consumen ancho de banda y recursos de la CPU del dispositivo de red. Cada dispositivo de red debe procesar un mensaje de difusión. En cambio, RIPv2 y EIGRP utilizan direcciones de multidifusión, de modo que solamente reciben las actualizaciones los vecinos que las necesitan. EIGRP también puede enviar un mensaje de unidifusión solamente al vecino afectado. Además, EIGRP envía una actualización solo cuando se la necesita, en lugar de hacerlo en forma periódica.

Como se muestra en la ilustración, los dos protocolos de routing vector distancia IPv4 modernos son RIPv2 y EIGRP. RIPv1 e IGRP se incluyen solamente por motivos de precisión histórica.



El algoritmo de routing se encuentra en el centro del protocolo vector distancia. El algoritmo se utiliza para calcular los mejores caminos y después enviar dicha información a los vecinos.

El algoritmo utilizado para los protocolos de enrutamiento define los siguientes procesos:

- El mecanismo para enviar y recibir información de routing.
- El mecanismo para calcular las mejores rutas e instalar rutas en la tabla de routing.
- El mecanismo para detectar cambios en la topología y reaccionar ante ellos.

En la animación de la ilustración, el R1 y el R2 están configurados con el protocolo de routing RIP. El algoritmo envía y recibe actualizaciones. Tanto R1 como R2 obtienen información nueva de la actualización. En este caso, cada router obtiene información acerca de una red nueva. El algoritmo de cada router realiza los cálculos de manera independiente y actualiza la tabla de enrutamiento con la información nueva. Cuando la LAN del R2 deja de funcionar, el algoritmo compone una actualización dirigida y la envía al R1. Luego, R1 elimina la red de la tabla de enrutamiento.

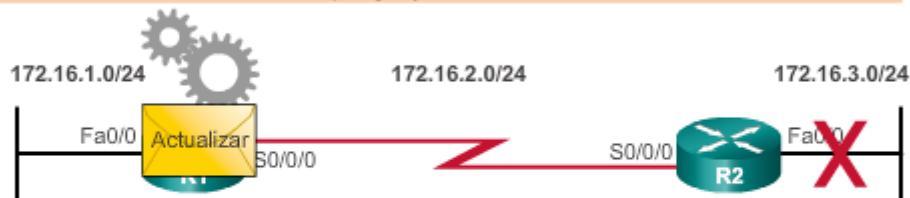
Los diferentes protocolos de enrutamiento utilizan diversos algoritmos para instalar rutas en la tabla de enrutamiento, enviar actualizaciones a los vecinos y determinar las rutas. Por ejemplo:

- RIP utiliza el algoritmo de Bellman-Ford como algoritmo de routing. Se basa en dos algoritmos desarrollados por Richard Bellman y Lester Ford júnior en 1958 y 1956.

- IGRP y EIGRP utilizan el algoritmo de actualización por difusión (DUAL) como algoritmo de routing, desarrollado por el Dr. J. J. Garcia-Luna-Aceves en SRI International.

Propósito de los algoritmos de routing

- Enviar y recibir actualizaciones.
- Calcular la mejor ruta e instalar rutas.
- Detectar cambios en la topología y reaccionar ante ellos.



Red	Interfaz	Salto
172.16.1.0/24	Fa0/0	0
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	S0/0/0	1

Red	Interfaz	Salto
172.16.2.0/24	S0/0/0	0
172.16.3.0/24	Fa0/0	0
172.16.1.0/24	S0/0/0	1

7.3.2 Tipos de protocolos de routing vector distancia

El protocolo de información de routing (RIP) era un protocolo de routing de primera generación para IPv4 especificado inicialmente en RFC 1058. Dado que es fácil de configurar, es una buena opción para redes pequeñas.

Las características clave del protocolo RIPv1 son las siguientes:

- Las actualizaciones de routing se transmiten por difusión (255.255.255.255) cada 30 segundos.
- Se utiliza el conteo de saltos como métrica para la selección de rutas.
- Se considera que un conteo de saltos de más de 15 saltos es infinito (demasiado alejado); el router del decimoquinto salto no propagaría la actualización de routing al siguiente router.

En 1993, RIPv1 evolucionó a un protocolo de routing sin clase conocido como "RIP versión 2" (RIPv2). RIPv2 introdujo las siguientes mejoras:

- Protocolo de routing sin clase:** admite VLSM y CIDR, debido a que incluye la máscara de subred en las actualizaciones de routing.
- Mayor eficiencia:** reenvía actualizaciones a la dirección de multidifusión 224.0.0.9, en lugar de a la dirección de difusión 255.255.255.255.

- **Entradas de routing reducidas:** admite la summarización de ruta manual en cualquier interfaz.
- **Protección:** admite un mecanismo de autenticación para proteger las actualizaciones de la tabla de routing entre vecinos.

En la tabla de la ilustración, se resumen las diferencias entre RIPv1 y RIPv2.

Las actualizaciones RIP se encapsulan en un segmento UDP, con los números de puerto de origen y de destino establecidos en el puerto UDP 520.

En 1997, se lanzó la versión de RIP con IPv6 habilitado. RIPng se basa en RIPv2. Aún tiene una limitación de 15 saltos, y la distancia administrativa es 120.

Comparación entre RIPv1 y RIPv2

Características y funciones	RIPv1	RIPv2
Métrica	Ambos usan el conteo de saltos como métrica. La cantidad máxima de saltos es 15.	
Dirección a la que se envían las actualizaciones	255.255.255.255	224.0.0.9
Admite VLSM	✗	✓
Admite CIDR	✗	✓
Admite summarización	✗	✓
Admite autenticación	✗	✓

El protocolo de routing de gateway interior (IGRP) fue el primer protocolo de routing IPv4 exclusivo desarrollado por Cisco en 1984. Tenía las siguientes características de diseño:

- Se utilizan el ancho de banda, el retraso, la carga y la confiabilidad para crear una métrica compuesta.
- De manera predeterminada, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

En 1992, el protocolo IGRP se vio reemplazado por IGRP mejorado (EIGRP). Al igual que RIPv2, EIGRP también introdujo compatibilidad con VLSM y CIDR. Con EIGRP se aumenta la eficiencia, se reducen las actualizaciones de routing y se admite el intercambio seguro de mensajes.

En la tabla de la ilustración, se resumen las diferencias entre IGRP y EIGRP.

EIGRP también introdujo lo siguiente:

- **Actualizaciones dirigidas limitadas:** no se envían actualizaciones periódicas. Solo se propagan los cambios de la tabla de routing, siempre que se produce un cambio. Esto reduce la cantidad de carga que el protocolo de routing coloca en la red. Que las actualizaciones sean dirigidas y limitadas significa que EIGRP solo envía actualizaciones a los vecinos que las necesitan. Se utiliza menos ancho de banda, especialmente en redes grandes con muchas rutas.
- **Mecanismo de saludo keepalive:** se intercambia periódicamente un pequeño mensaje de saludo para mantener adyacencias con los routers vecinos. Esto implica un uso muy bajo de los recursos de red durante el funcionamiento normal, en lugar de actualizaciones periódicas.
- **Mantenimiento de una tabla de topología:** se mantienen todas las rutas recibidas de los vecinos (no sólo las mejores rutas) en una tabla de topología. DUAL puede insertar rutas de respaldo en la tabla de topología de EIGRP.
- **Convergencia rápida:** en la mayoría de los casos, se trata del IGP más rápido para realizar la convergencia debido a que mantiene rutas alternativas, lo que permite una convergencia casi instantánea. Si una ruta principal falla, el router puede utilizar la ruta alternativa identificada. El cambio a la ruta alternativa es inmediato y no implica interacción con otros routers.
- **Compatibilidad con varios protocolos de capa de red:** EIGRP utiliza módulos dependientes de protocolo (PDM), lo que significa que es el único protocolo compatible con otros protocolos además de IPv4 e IPv6, como el IPX antiguo y AppleTalk.

Comparación entre IGRP y EIGRP

Características y funciones	IGRP	EIGRP
Métrica	Ambos utilizan una métrica compuesta que consta del ancho de banda y el retraso. La confiabilidad y la carga también se pueden incluir en el cálculo de la métrica.	
Dirección a la que se envían las actualizaciones	255.255.255.255	224.0.0.10
Admite VLSM	✗	✓
Admite CIDR	✗	✓
Admite sumarización	✗	✓
Admite autenticación	✗	✓

Descripción del protocolo de routing vector distancia	RIP O EIGRP
Envía paquetes de saludo.	EIGRP
La versión 2 admite VLSM y routing sin clase.	RIP
Límite máximo de 255 saltos.	EIGRP
Límite máximo de 15 saltos.	RIP
Crea adyacencias con los vecinos.	EIGRP

7.4 Routing RIP y RIPng

7.4.1 Configuración del protocolo RIP

Si bien el protocolo RIP se utiliza con muy poca frecuencia en las redes modernas, es útil como base para comprender el routing de red básico. Por este motivo, en esta sección se proporciona una breve descripción general de la forma en que se configuran los parámetros básicos de RIP y de la manera en que se verifica RIPv2.

Consulte la topología de referencia en la figura 1 y la tabla de direccionamiento en la figura 2. En esta situación, todos los routers se configuraron con funciones de administración básicas, y todas las interfaces identificadas en la topología de referencia están configuradas y habilitadas. No hay rutas estáticas configuradas ni protocolos de routing habilitados, por lo que el acceso remoto de red es imposible en ese momento. RIPv2 se utiliza como protocolo de routing dinámico. Para habilitar RIP, utilice el comando **router rip**, como se muestra en la figura 3. Este comando no inicia en forma directa el proceso del RIP. En cambio, proporciona acceso al modo de configuración del router, donde se configuran los parámetros de routing RIP.

Para deshabilitar y eliminar RIP, utilice el comando de configuración global **no router rip**. Este comando detiene el proceso RIP y elimina todas las configuraciones RIP existentes.

En la figura 4, se muestran los diversos comandos RIP que se pueden configurar. En esta sección, se abordan las palabras clave resaltadas.

Topología de referencia

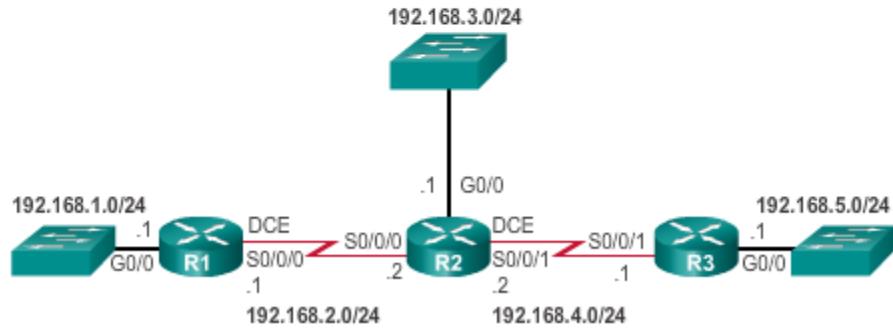


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred
R1	G0/0	192.168.1.1	255.255.255.0
	S0/0/0	192.168.2.1	255.255.255.0
R2	G0/0	192.168.3.1	255.255.255.0
	S0/0/0	192.168.2.2	255.255.255.0
	S0/0/1	192.168.4.2	255.255.255.0
R3	G0/0	192.168.5.1	255.255.255.0
	S0/0/1	192.168.4.1	255.255.255.0

Ingreso al modo de configuración de routing

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# router rip
R1(config-router)#

```

Opciones de configuración de RIP

```
R1(config-router) # ?
Router configuration commands:
  address-family      Enter Address Family command mode
  auto-summary        Enable automatic network number
                      summarization
  default             Set a command to its defaults
  default-information Control distribution of default
                      information
  default-metric      Set metric of redistributed routes
  distance            Define an administrative distance
  distribute-list     Filter networks in routing updates
  exit                Exit from routing protocol
                      configuration mode
  flash-update-threshold Specify flash update threshold in
                           second
  help                Description of the interactive help
                      system
  input-queue          Specify input queue depth
```

Al ingresar en el modo de configuración de router RIP, el router recibe instrucciones para que ejecute el RIP. Pero el router aún necesita conocer las interfaces locales que deberá utilizar para comunicarse con otros routers, así como las redes conectadas en forma local que deberá publicar a dichos routers.

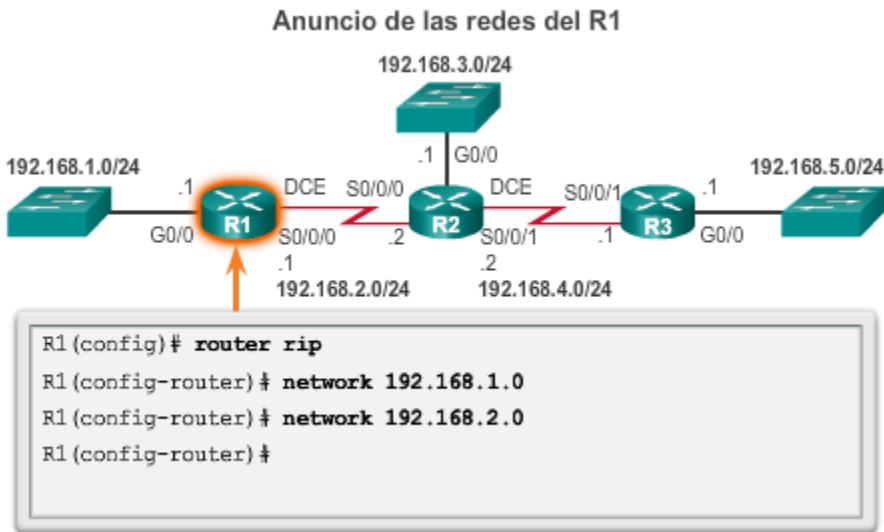
Para habilitar el routing RIP para una red, utilice el comando del modo de configuración del router **network dirección-red**. Introduzca la dirección de red con clase para cada red conectada directamente. Este comando realiza lo siguiente:

- Habilita el RIP en todas las interfaces que pertenecen a una red específica. Hace que las interfaces asociadas ahora envíen y reciban actualizaciones RIP.
- Publica la red especificada en las actualizaciones de enrutamiento RIP enviadas a otros routers cada 30 segundos.

Nota: si se introduce una dirección de subred, el IOS la convierte automáticamente a la dirección de red con clase. Recuerde que RIPv1 es un protocolo de routing con clase para IPv4. Por ejemplo, si se introduce el comando **network 192.168.1.32**, se convertiría automáticamente a **network 192.168.1.0** en el archivo de configuración en ejecución. El IOS no proporciona un mensaje de error, sino que corrige la entrada e introduce la dirección de red con clase.

En la figura 1, el comando **network** se utiliza para anunciar las redes conectadas directamente al R1.

Utilice el verificador de sintaxis de la figura 2 para establecer una configuración similar en el R2 y en el R3.



El comando **show ip protocols** muestra los parámetros del protocolo de routing IPv4 configurados actualmente en el router. Este resultado que se muestra en la figura 1 confirma la mayoría de los parámetros de RIP, incluido lo siguiente:

1. El routing RIP está configurado y en ejecución en el router R1.
2. Los valores de diversos temporizadores; por ejemplo, el R1 envía la siguiente actualización de routing en 16 segundos.
3. La versión de RIP configurada actualmente es RIPv1.
4. El R1 realiza la summarización en el límite de la red con clase.
5. El R1 anuncia las redes con clase. Estas son las redes que el R1 incluye en sus actualizaciones RIP.
6. Los vecinos RIP se indican mediante la inclusión de la dirección IP del siguiente salto, la AD asociada que el R2 utiliza para las actualizaciones enviadas por ese vecino y el momento en que dicho vecino recibió la última actualización.

Nota: este comando también resulta muy útil para verificar las operaciones de otros protocolos de routing (es decir, EIGRP y OSPF).

El comando **show ip route** muestra las rutas RIP instaladas en la tabla de routing. En la figura 2, el R1 ahora tiene información acerca de las redes resaltadas.

Utilice el verificador de sintaxis de la figura 3 para verificar las rutas RIP y la configuración de RIP del R2 y del R3.

Verificación de la configuración de RIP en el R1

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

1 Routing Protocol is "rip"
    Outgoing update filter list for all interfaces is not set
    Incoming update filter list for all interfaces is not set
2 Sending updates every 30 seconds, next due in 16 seconds
    Invalid after 180 seconds, hold down 180, flushed after 240
    Redistributing: rip

3 Default version control: send version 1, receive any version
    Interface          Send   Recv   Triggered   RIP   Key-chain
    GigabitEthernet0/0   1      1     2
    Serial0/0/0          1      1     2

4 Automatic network summarization is in effect
5 Maximum path: 4
6 Routing for Networks:
    192.168.1.0
    192.168.2.0

7 Routing Information Sources:
    Gateway          Distance      Last Update
    192.168.2.2        120          00:00:15
    Distance: (default is 120)

R1#
```

Verificación de las rutas RIP en el R1

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

    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
    192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.2.0/24 is directly connected, Serial0/0/0
L       192.168.2.1/32 is directly connected, Serial0/0/0
R       192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R       192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
R       192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:24, Serial0/0/0
R1#
```

De manera predeterminada, cuando hay un proceso de RIP configurado en un router Cisco, este ejecuta RIPv1, como se muestra en la figura 1. Sin embargo, a pesar de que el router sólo envía mensajes de RIPv1, puede interpretar los mensajes de RIPv1 y RIPv2. Los routers RIPv1 simplemente ignoran los campos de RIPv2 en la entrada de ruta.

Utilice el comando del modo de configuración del router **version 2** para habilitar RIPv2, como se muestra en la figura 2. Observe la forma en que el comando **show ip protocols** verifica que el R2 ahora está configurado para enviar y recibir solamente mensajes de versión 2. El proceso de RIP ahora incluye la máscara de subred en todas las actualizaciones, lo que hace que RIPv2 sea un protocolo de routing sin clase.

Nota: la configuración de **version 1** habilita RIPv1 solamente, mientras que configurar **no version** revierte el router a la configuración predeterminada, mediante la cual se envían actualizaciones de versión 1 pero se está a la escucha de actualizaciones de versión 1 y de versión 2.

En la figura 3, se verifica que ya no haya rutas RIP en la tabla de routing. Esto se debe a que el R1 ahora está a la escucha de actualizaciones RIPv2 únicamente. El R2 y el R3 todavía envían actualizaciones RIPv1. Por lo tanto, se debe configurar el comando **version 2** en todos los routers en el dominio de routing.

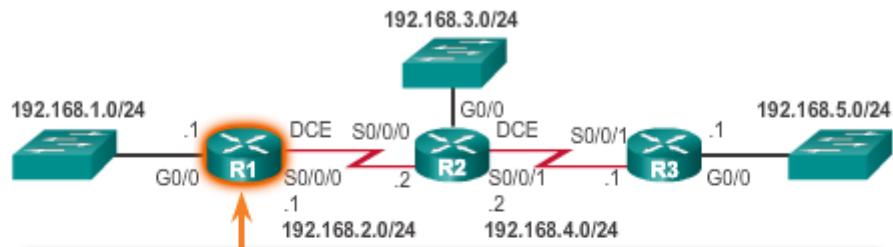
Utilice el verificador de sintaxis de la figura 4 para habilitar RIPv2 en el R2 y en el R3.

Verificación de la configuración de RIP en el R1

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

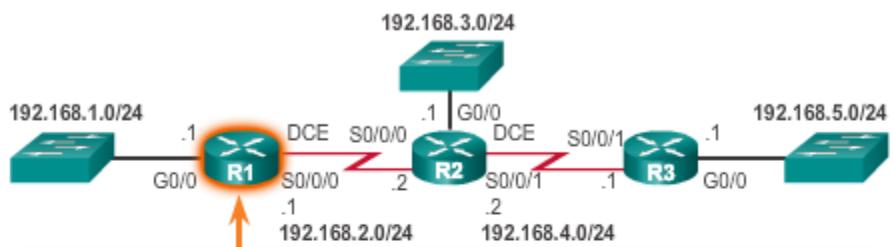
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not
set
  Incoming update filter list for all interfaces is not
set
  Sending updates every 30 seconds, next due in 16 seconds
    Invalid after 180 seconds, hold down 180, flushed after
240
  Redistributing: rip
  Default version control: send version 1, receive any
version
      Interface      Send   Recv Triggered RIP  Key-chain
      GigabitEthernet0/0  1     1 2
      Serial0/0/0       1     1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway          Distance      Last Update
```

Habilitación y verificación de RIPv2 en el R1



```
R1(config)# router rip
R1(config-router)# version 2
R1(config-router)# ^Z
R1#
R1# show ip protocols | section Default
Default version control: send version 2, receive version 2
  Interface      Send   Recv  Triggered RIP  Key-chain
  GigabitEthernet0/0    2      2
  Serial0/0/0          2      2
R1#
```

Verificación de las rutas del R1



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

  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
  192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R1#
```

Como se muestra en la figura 1, RIPv2 resume automáticamente las redes en los límites de red principales de manera predeterminada, al igual que RIPv1.

Para modificar el comportamiento predeterminado de RIPv2 de summarización automática, utilice el comando del modo de configuración del router **no auto-summary**, como se muestra en la figura 2. Este comando no tiene ningún efecto cuando se utiliza RIPv1. Cuando se deshabilita la summarización automática, RIPv2 ya no resume las redes a su dirección con clase en routers fronterizos. RIPv2 ahora incluye todas las subredes y sus máscaras correspondientes en sus actualizaciones de routing. El comando **show ip protocols** ahora indica lo siguiente: automatic network summarization is not in effect (la summarización de red automática no está operativa).

Nota: se debe habilitar RIPv2 antes de deshabilitar la summarización automática.

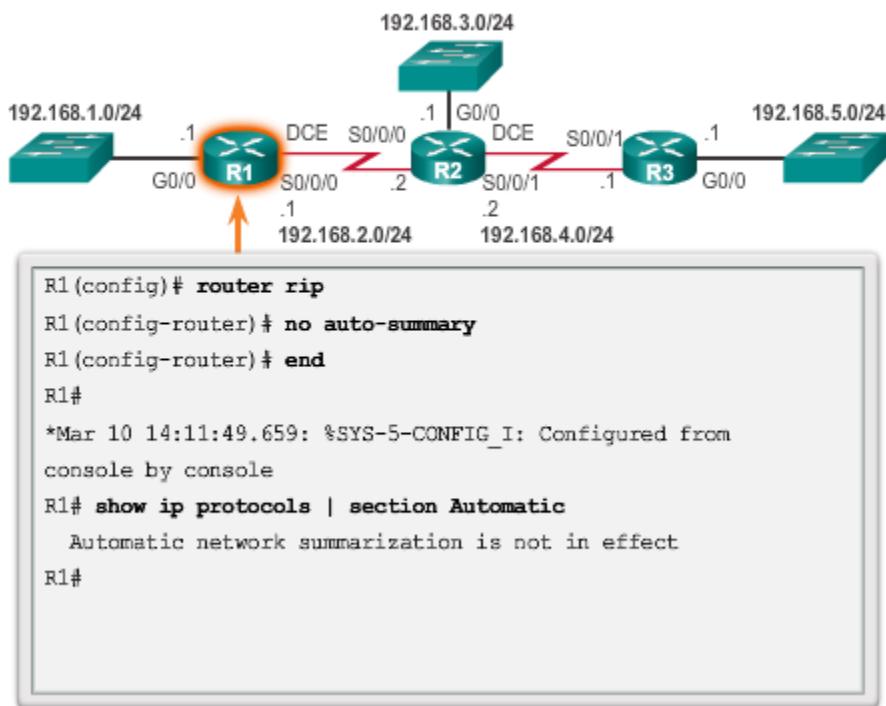
Utilice el verificador de sintaxis de la figura 3 para deshabilitar la summarización automática en el R2 y en el R3.

Sumarización automática con RIPv2

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

Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 16 seconds
  Invalid after 180 seconds, hold down 180, flushed after
  240
  Redistributing: rip
  Default version control: send version 2, receive version 2
    Interface      Send   Recv   Triggered RIP  Key-chain
      GigabitEthernet0/0    1     1 2
      Serial0/0/0        1     1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.1.0
    192.168.2.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    192.168.2.2        120          00:00:15
  Distance: (default is 120)
R1#
```

Deshabilitación de la sumarización automática en el R1



De manera predeterminada, las actualizaciones RIP se reenvían por todas las interfaces con RIP habilitado. Sin embargo, en realidad las actualizaciones RIP solo deben reenviarse por las interfaces que se conectan a otros routers con RIP habilitado.

Por ejemplo, consulte la topología en la figura 1. RIP envía actualizaciones por su interfaz G0/0, aunque no existe ningún dispositivo RIP en esa LAN. No hay manera de que el R1 tenga información acerca de esto y, como resultado, envía una actualización cada 30 segundos. El envío de actualizaciones innecesarias a una LAN impacta en la red de tres maneras:

- **Desperdicio de ancho de banda:** se utiliza ancho de banda para transportar actualizaciones innecesarias. Dado que las actualizaciones RIP se transmiten por difusión o multidifusión, los switches también reenvían las actualizaciones por todos los puertos.
- **Desperdicio de recursos:** todos los dispositivos en la LAN deben procesar la actualización hasta las capas de transporte, punto en el cual los dispositivos descartan la actualización.
- **Riesgo de seguridad:** el anuncio de actualizaciones en una red de difusión constituye un riesgo de seguridad. Las actualizaciones RIP pueden interceptarse con software analizador de protocolos. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico.

Utilice el comando de configuración del router **passive-interface** para evitar que las actualizaciones de routing se transmitan a través de una interfaz del router y permitir que esa red se siga anunciando a otros routers. El comando detiene las actualizaciones de routing a través de la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada aún se anuncia en las actualizaciones de routing enviadas a otras interfaces.

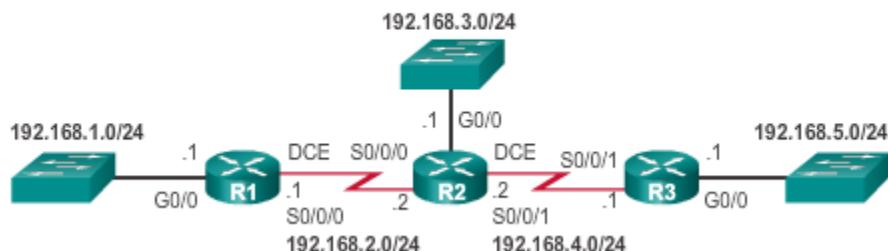
No es necesario que el R1, el R2, y el R3 reenvíen actualizaciones RIP por sus interfaces LAN. En la configuración de la figura 2, se identifica la interfaz G0/0 del R1 como pasiva. El comando **show ip protocols** se utiliza para verificar que la interfaz Gigabit Ethernet es pasiva. Observe que ya no se indica que la interfaz G0/0 envía o recibe actualizaciones de versión 2, sino que se encuentra en la sección Passive Interface(s) (Interfaces pasivas). Asimismo, observe que la red 192.168.1.0 aún se encuentra bajo Routing for Networks (Routing para redes), lo cual significa que esta red aún está incluida como una entrada de ruta en las actualizaciones RIP que se envían al R2.

Nota: todos los protocolos de routing admiten el comando **passive-interface**.

Utilice el verificador de sintaxis de la figura 3 para configurar la interfaz LAN como interfaz pasiva en el R2 y en el R3.

Como alternativa, todas las interfaces se pueden convertir en pasivas con el comando **passive-interface default**. Las interfaces que no deben ser pasivas se pueden volver a habilitar con el comando **no passive-interface**.

Configuración de interfaces pasivas en el R1



Configuración y verificación de una interfaz pasiva en el R1

```
R1(config)# router rip
R1(config-router)# passive-interface g0/0
R1(config-router)# end
R1#
R1# show ip protocols | begin Default
Default version control: send version 2, receive version 2
  Interface          Send   Recv Triggered RIP  Key-chain
  Serial0/0/0           2      2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  192.168.1.0
  192.168.2.0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway          Distance      Last Update
  192.168.2.2        120          00:00:06
Distance: (default is 120)

R1#
```

Consulte la Figura 1. En esta situación, el R1 tiene conexión simple a un proveedor de servicios. Por lo tanto, para que el R1 llegue a Internet, solo se requiere una ruta estática predeterminada desde la interfaz Serial 0/0/1.

Se podrían configurar rutas estáticas predeterminadas similares en el R2 y en el R3, pero es mucho más escalable introducirla una vez en el router perimetral R1 y, a continuación, hacer que el R1 la propague al resto de los routers mediante RIP. Para proporcionarle conectividad a Internet a todas las demás redes del dominio de enrutamiento RIP, la ruta estática predeterminada debe publicarse a todos los demás routers que usan el protocolo de enrutamiento dinámico.

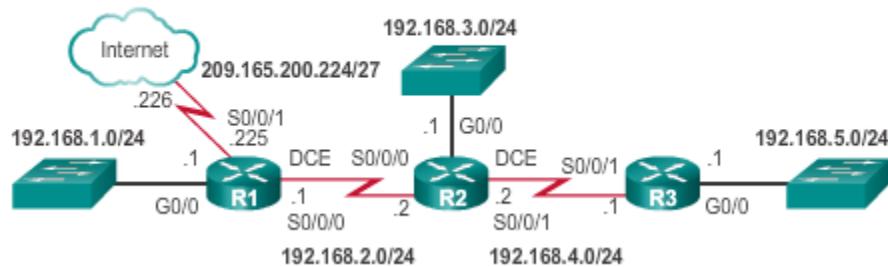
Para propagar una ruta predeterminada, el router perimetral debe estar configurado con lo siguiente:

- Una ruta estática predeterminada mediante el comando **ip route 0.0.0.0 0.0.0.0 interfaz-salida ip-siguiente-salto**.
- El comando de configuración del **routerdefault-information originate**. Esto le ordena al router R1 que produzca información predeterminada mediante la propagación de la ruta estática predeterminada en actualizaciones RIP.

En el ejemplo de la figura 2, se configura una ruta estática predeterminada completamente especificada al proveedor de servicios y, a continuación, se propaga la ruta mediante RIP. Observe que ahora el R1 tiene un gateway de último recurso y una ruta predeterminada instalados en su tabla de routing.

Utilice el verificador de sintaxis de la figura 3 para verificar que la ruta predeterminada se haya propagado al R2 y al R3.

Propagación de una ruta predeterminada en el R1



Configuración y verificación de una ruta predeterminada en el R1

```
R1(config)# ip route 0.0.0.0 0.0.0.0 S0/0/1 209.165.200.226
R1(config)# router rip
R1(config-router)# default-information originate
R1(config-router)# ^z
R1#
*Mar 10 23:33:51.801: %SYS-5-CONFIG_I: Configured from console by
console
R1# 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, serial0/0/1
      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
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Serial0/0/0
L        192.168.2.1/32 is directly connected, Serial0/0/0
R        192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:08,
Serial0/0/0
R        192.168.4.0/24 [120/1] via 192.168.2.2, 00:00:08,
Serial0/0/0
R        192.168.5.0/24 [120/2] via 192.168.2.2, 00:00:08,
Serial0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/24 is directly connected, Serial0/0/1
```

7.4.2 Configuración del protocolo RIPng

Al igual que su equivalente para IPv4, RIPng no se suele utilizar en las redes modernas, pero también resulta útil como base para comprender el routing de red básico. Por este motivo, en esta sección se proporciona una breve descripción general de cómo configurar RIPng básico.

Consulte la topología de referencia en la ilustración. En esta situación, todos los routers se configuraron con funciones de administración básicas, y todas las interfaces identificadas en la topología de referencia están configuradas y habilitadas. No hay rutas estáticas configuradas ni protocolos de routing habilitados, por lo que el acceso remoto de red es imposible en ese momento.

Para habilitar un router IPv6 para que reenvíe paquetes IPv6, se debe configurar el comando **ipv6 unicast-routing**.

A diferencia de RIPv2, RIPng se habilita en una interfaz y no en el modo de configuración del router. De hecho, no hay un comando **network dirección-reddisponible** en RIPng. En cambio, utilice el comando de configuración de interfaz **ipv6 rip nombre-dominio enable**.

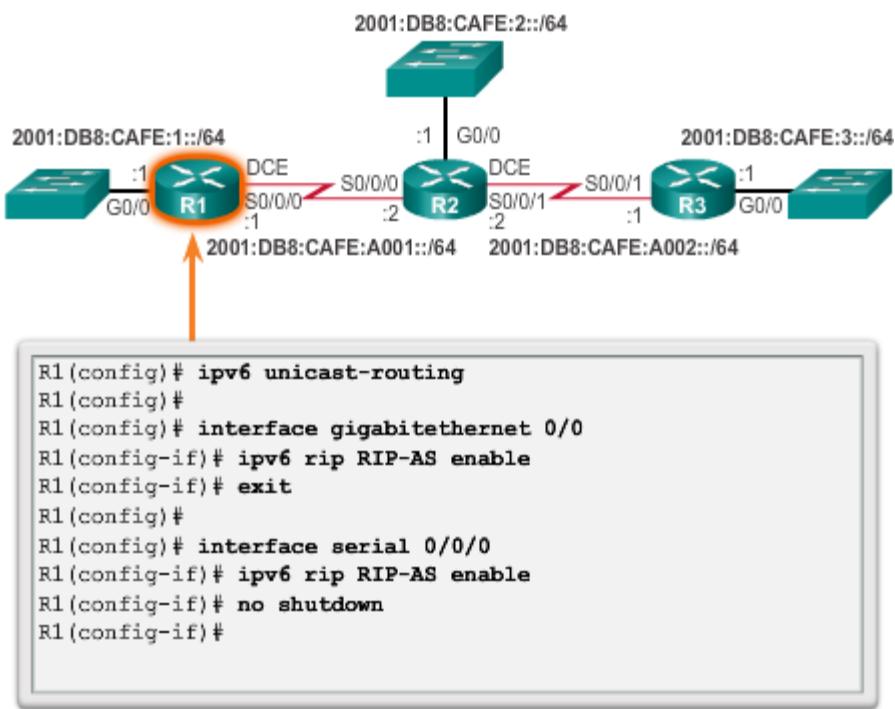
En la figura 1, se habilita el routing de unidifusión IPv6 y se habilitan las interfaces Gigabit Ethernet 0/0 y Serial 0/0/0 para RIPng mediante el nombre de dominio RIP-AS.

Utilice el verificador de sintaxis de la figura 2 para establecer una configuración similar en el R2 y en el R3.

El proceso para propagar una ruta predeterminada en RIPng es idéntico al de RIPv2, excepto que se debe especificar una ruta estática predeterminada IPv6. Por ejemplo, suponga que el R1 tenía una conexión a Internet de una interfaz Serial 0/0/1 a la dirección IP 2001:DB8:FEED:1::1/64. Para propagar una ruta predeterminada, el R3 debería configurarse con lo siguiente:

- Una ruta estática predeterminada mediante el comando de configuración global **ipv6 route 0::/0 2001:DB8:FEED:1::1**.
- El comando del modo de configuración de interfaz **ipv6 rip nombre-dominio default-information originate**. Esto ordena al R3 que sea el origen de la información de la ruta predeterminada y que propague la ruta estática predeterminada en las actualizaciones RIPng enviadas por la interfaz configurada.

Habilitación de RIPng para IPv6 en las interfaces del R1



En la figura 1, el comando **show ipv6 protocols** no proporciona la misma cantidad de información que su equivalente para IPv4. Sin embargo, confirma los siguientes parámetros:

1. El routing RIPng está configurado y en ejecución en el router R1.

2. Las interfaces están configuradas con RIPng.

El comando **show ipv6 route** muestra las rutas instaladas en la tabla de routing, como se muestra en la figura 2. El resultado confirma que el R1 ahora tiene información acerca las redes RIPng resaltadas.

Observe que la LAN del R2 se anuncia como a dos saltos de distancia. Esto se debe a que hay una diferencia en la forma en que RIPv2 y RIPng calculan los conteos de saltos. Con RIPv2 (y RIPv1), la métrica hasta la LAN del R2 sería un salto. Esto se debe a que la métrica (el conteo de saltos) que se muestra en la tabla de routing IPv4 es la cantidad de saltos requeridos para llegar a la red remota (contando el router del siguiente salto como primer salto). En RIPng, el router emisor se considera a sí mismo a un salto de distancia, por lo tanto, el R2 anuncia su LAN con un valor de métrica 1. Cuando el R1 recibe la actualización, agrega otro conteo de saltos de 1 a la métrica. Por lo tanto, el R1 considera que la LAN del R2 está a dos saltos de distancia. De manera similar, considera que la LAN del R3 está a tres saltos de distancia.

Si se agrega la palabra clave **rip** al comando, como se muestra en la figura 3, solo se indican las redes RIPng.

Utilice el verificador de sintaxis de la figura 4 para verificar el R2 y el R3.

Verificación de la configuración de RIP en el R1

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
1 IPv6 Routing Protocol is "rip RIP-AS"
2 Interfaces:
    Serial0/0/0
    GigabitEthernet0/0
Redistribution:
    None
R1#
```

Verificación de rutas en el R1

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 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
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
R  2001:DB8:CAFE:2::/64 [120/2]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R  2001:DB8:CAFE:3::/64 [120/3]
    via FE80::FE99:47FF:FE71:78A0, 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
R  2001:DB8:CAFE:A002::/64 [120/2]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
L  FF00::/8 [0/0]
    via Null0, receive
R1#
```

Verificación de rutas RIPng en el R1

```
R1# show ipv6 route rip
IPv6 Routing Table - default - 8 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
R  2001:DB8:CAFE:2::/64 [120/2]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R  2001:DB8:CAFE:3::/64 [120/3]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R  2001:DB8:CAFE:A002::/64 [120/2]
    via FE80::FE99:47FF:FE71:78A0, Serial0/0/0
R1#
```

7.5 Routing dinámico de estado de enlace

7.5.1 Funcionamiento del protocolo de routing de estado de enlace

A los protocolos de enrutamiento de link-state también se les conoce como protocolos shortest path first y se desarrollan en torno al algoritmo shortest path first (SPF) de Edsger Dijkstra. El algoritmo SPF se analiza más detalladamente en una sección posterior.

En la ilustración, se muestran los protocolos de routing de estado de enlace IPv4:

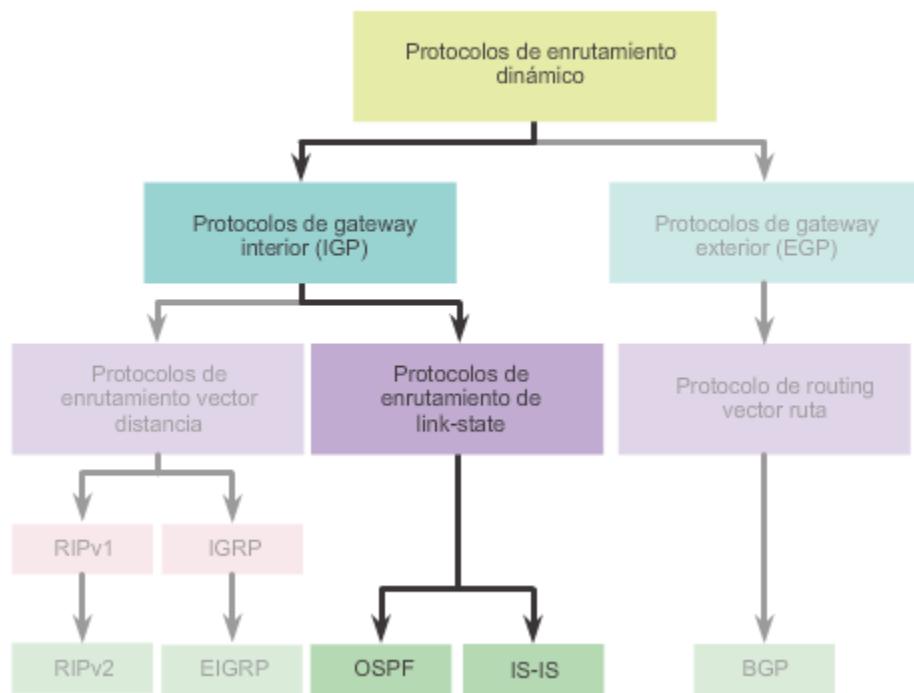
- Open Shortest Path First (OSPF)
- Intermediate-System-to-Intermediate-System (IS-IS)

Los protocolos de enrutamiento de link-state son conocidos por presentar una complejidad bastante mayor que sus vectores distancia equivalentes. Sin embargo, la funcionalidad básica y la configuración de los protocolos de routing de estado de enlace son igualmente sencillas.

Al igual que RIP y EIGRP, las operaciones básicas de OSPF se pueden configurar mediante los siguientes comandos:

- **router ospf *id-proceso*** (comando de configuración global)
- **network** para anunciar redes

Protocolos de enrutamiento de link-state



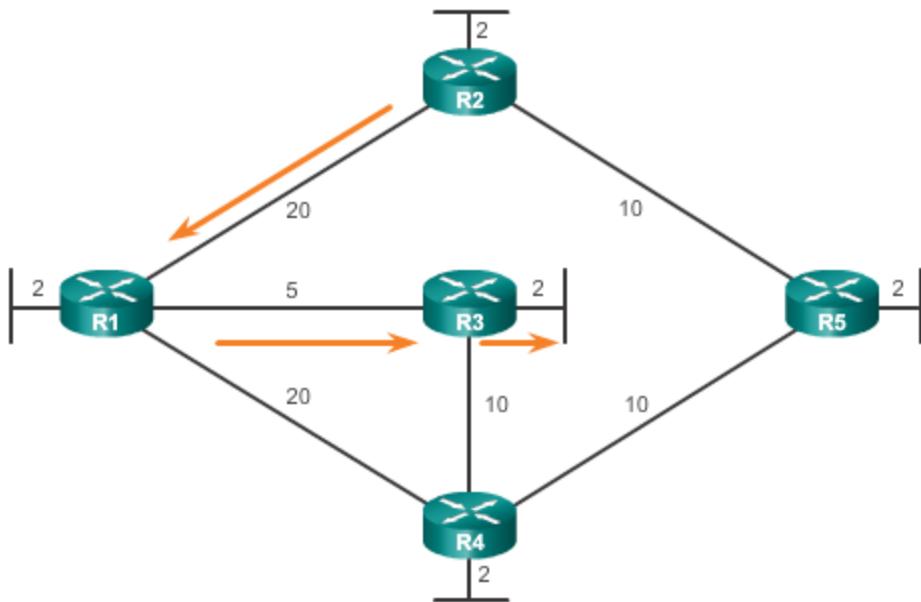
Todos los protocolos de routing de estado de enlace aplican el algoritmo de Dijkstra para calcular la mejor ruta. A este algoritmo se le llama comúnmente “algoritmo SPF” (Shortest Path First). Para determinar el costo total de una ruta, este algoritmo utiliza costos acumulados a lo largo de cada ruta, de origen a destino.

En la figura, cada ruta se rotula con un valor arbitrario para el costo. El costo de la ruta más corta para que el R2 envíe paquetes a la LAN conectada al R3 es 27. Cada router determina su propio costo hacia cada destino en la topología. En otros términos, cada router calcula el algoritmo SPF y determina el costo desde su propia perspectiva.

Nota: el objetivo central de esta sección es analizar el costo, el cual está determinado por el árbol SPF. Por este motivo, en los gráficos de esta sección se muestran las conexiones del árbol SPF y no la topología. Todos los enlaces se representan mediante una línea negra continua.

Algoritmo Shortest Path First de Dijkstra

Ruta más corta para que el host en la LAN del R2 alcance al host en la LAN del R3:
Del R2 al R1 (20) + del R1 al R3 (5) + del R3 a la LAN (2) = 27

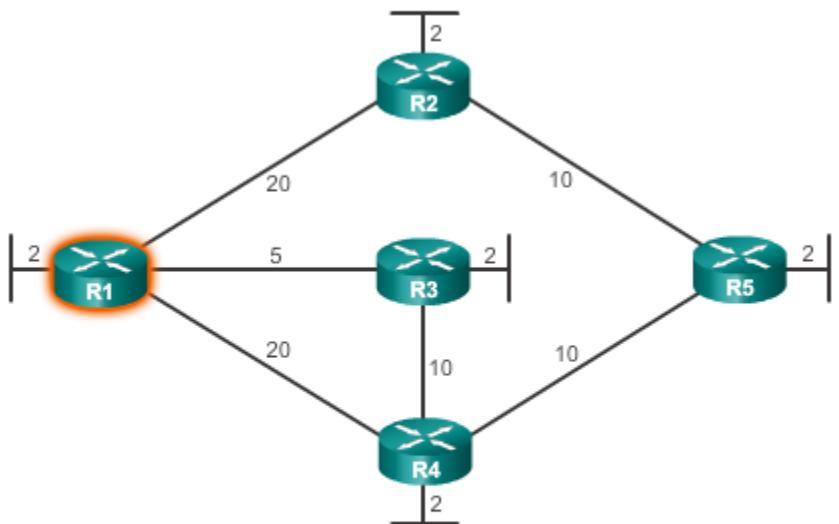


En la tabla de la figura 1, se muestra la ruta más corta y el costo acumulado para llegar a las redes de destino identificadas desde la perspectiva del R1.

La ruta más corta no es necesariamente la ruta con la menor cantidad de saltos. Por ejemplo, observe la ruta hacia la LAN R5. Podría suponerse que el R1 realizaría el envío directamente al R4 en lugar de al R3. Sin embargo, el costo para llegar a R4 directamente (22) es más alto que el costo para llegar a R4 a través de R3 (17).

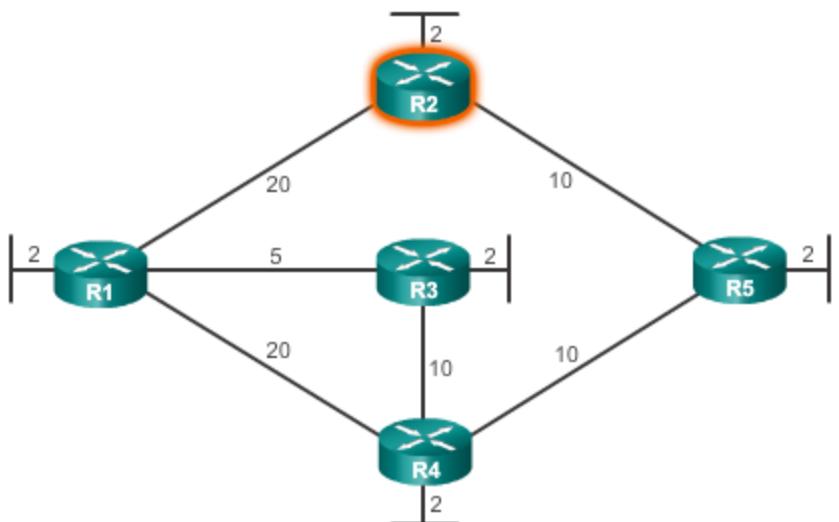
Observe la ruta más corta para que cada router llegue a cada una de las LAN, como se muestra en las figuras 2 a 5.

Árbol SPF del R1



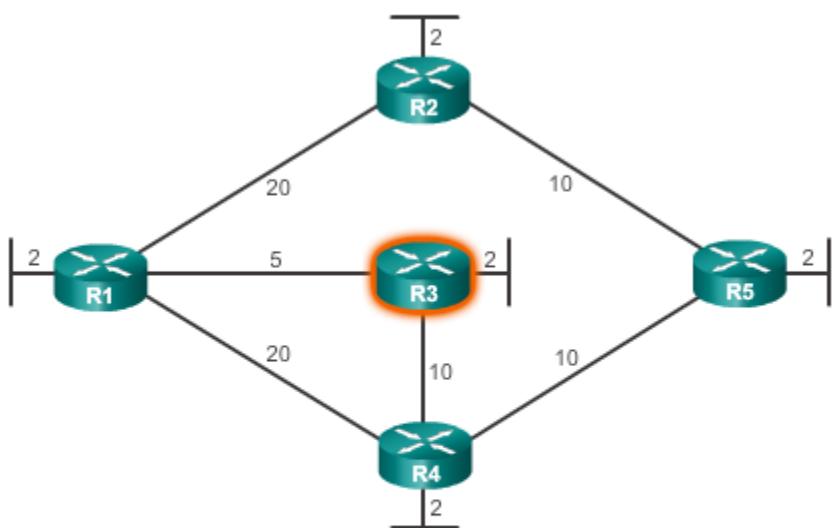
Destino	Ruta más corta	Costo
LAN del R2	R1 a R2	22
LAN del R3	R1 a R3	7
LAN del R4	Del R1 al R3 al R4	17
LAN del R5	Del R1 al R3 al R4 al R5	27

Árbol SPF del R2



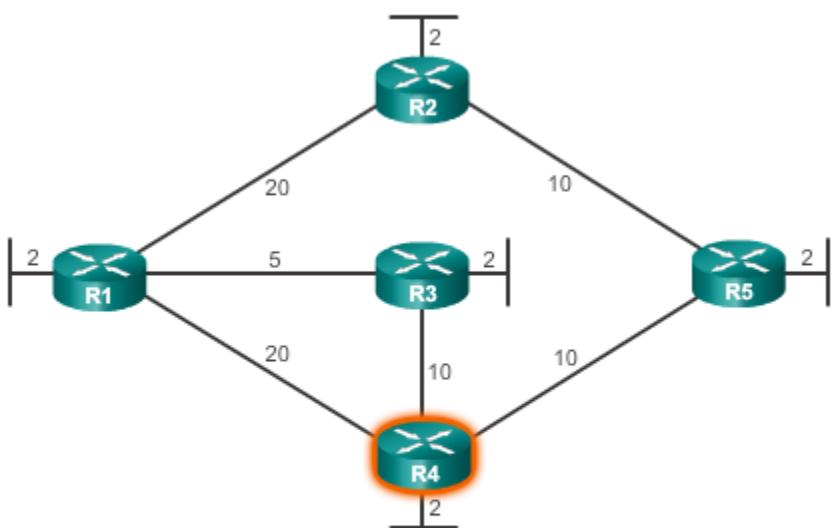
Destino	Ruta más corta	Costo
LAN de R1	Del R2 al R1	22
LAN del R3	Del R2 al R1 al R3	27
LAN del R4	Del R2 al R5 al R4	22
LAN del R5	Del R2 al R5	12

Árbol SPF del R3

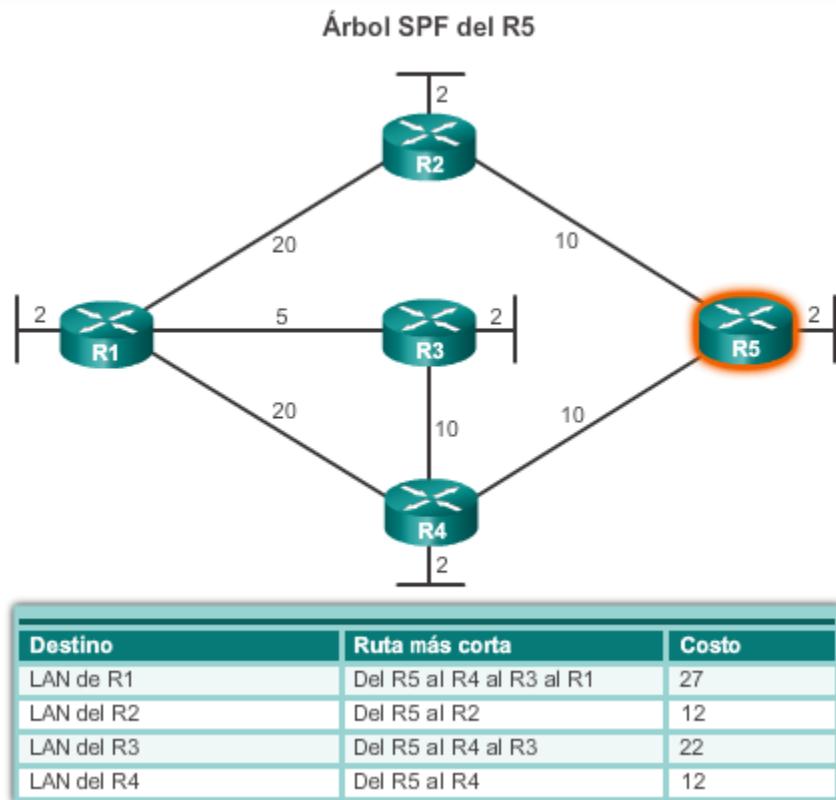


Destino	Ruta más corta	Costo
LAN de R1	Del R3 al R1	7
LAN del R2	Del R3 al R1 al R2	27
LAN del R4	R3 a R4	12
LAN del R5	Del R3 al R4 al R5	22

Árbol SPF del R4



Destino	Ruta más corta	Costo
LAN de R1	Del R4 al R3 al R1	17
LAN del R2	Del R4 al R5 al R2	22
LAN del R3	Del R4 al R3	12
LAN del R5	Del R4 al R5	12



7.5.2 Actualizaciones de estado de enlace

Por lo tanto, ¿de qué manera exactamente funciona un protocolo de enrutamiento de link-state? Con los protocolos de enrutamiento de link-state, un enlace es una interfaz en un router. La información acerca del estado de dichos enlaces se conoce como estados de enlace.

Analice la topología en la ilustración. Todos los routers de la topología realizarán el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia:

1. Cada router obtiene información acerca de sus propios enlaces y sus propias redes conectadas directamente. Esto se realiza al detectar que una interfaz se encuentra en el estado activado.
2. Cada router es responsable de reunirse con sus vecinos en redes conectadas directamente. Los routers de estado de enlace lo hacen mediante el intercambio paquetes de salud con otros routers de estado de enlace en redes conectadas directamente.
3. Cada router crea un Paquete de link-state (LSP) que incluye el estado de cada enlace directamente conectado. Esto se realiza registrando toda la información pertinente acerca de cada vecino, que incluye el ID de vecino, el tipo de enlace y el ancho de banda.
4. Cada router satura a todos los vecinos con el LSP. Estos vecinos almacenan todos los LSP recibidos en una base de datos. A continuación, saturan a sus vecinos con los LSP hasta que todos los routers del área hayan recibido los LSP. Cada router almacena una copia de cada LSP recibido por parte de sus vecinos en una base de datos local.

5. Cada router utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino. En forma similar a tener un mapa de carretera, el router tiene ahora un mapa completo de todos los destinos de la topología y las rutas para alcanzarlos. El algoritmo SPF se utiliza para construir el mapa de la topología y determinar el mejor camino hacia cada red.

Nota: este proceso es el mismo para OSPF para IPv4 e IPv6. En los ejemplos de esta sección, se hará referencia a OSPF para IPv4.

Proceso del enrutamiento de link-state

Proceso del enrutamiento de link-state

- Cada router obtiene información sobre cada una de sus propias redes conectadas directamente.
- Cada router tiene la responsabilidad de "saludar" a sus vecinos en redes conectadas directamente.
- Cada router crea un Paquete de link-state (LSP) que incluye el estado de cada enlace directamente conectado.
- Cada router satura con el LSP a todos los vecinos, que luego almacenan todos los LSP recibidos en una base de datos.
- Cada router utiliza la base de datos para construir un mapa completo de la topología y calcula el mejor camino hacia cada red de destino.

El primer paso en el proceso de routing de estado de enlace es que cada router descubra sus propios enlaces y sus propias redes conectadas directamente. Cuando se configura una interfaz de router con una dirección IP y una máscara de subred, la interfaz se vuelve parte de esa red.

Consulte la topología en la figura 1. A los fines de este análisis, suponga que el R1 se configuró previamente y que tenía plena conectividad a todos los vecinos. Sin embargo, se cortó la alimentación del R1 brevemente y tuvo que reiniciarse.

Durante el arranque, el R1 carga el archivo de configuración de inicio guardado. A medida que se activan las interfaces configuradas anteriormente, el R1 obtiene información sobre sus propias redes conectadas directamente. Más allá de los protocolos de routing utilizados, dichas redes conectadas directamente ahora constituyen entradas en la tabla de routing.

Como ocurre con los protocolos vector distancia y las rutas estáticas, la interfaz debe configurarse de manera adecuada con una dirección IPv4 y una máscara de subred, y el enlace debe encontrarse en estado activo antes de que el protocolo de routing de estado de enlace pueda obtener información sobre un enlace. Asimismo, como ocurre con los protocolos vector distancia, la interfaz debe incluirse en una de las instrucciones **network** de configuración del router para que pueda participar en el proceso de routing de estado de enlace.

En la figura 1, se muestra el R1 enlazado a cuatro redes conectadas directamente:

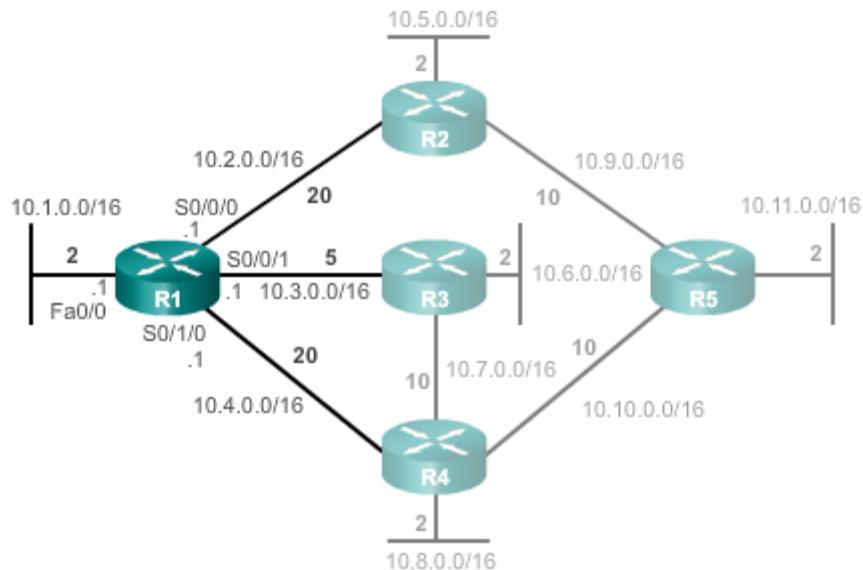
- FastEthernet 0/0, 10.1.0.0/16
- Serial 0/0/0, 10.2.0.0/16
- Serial 0/0/1, 10.3.0.0/16
- Serial 0/1/0, 10.4.0.0/16

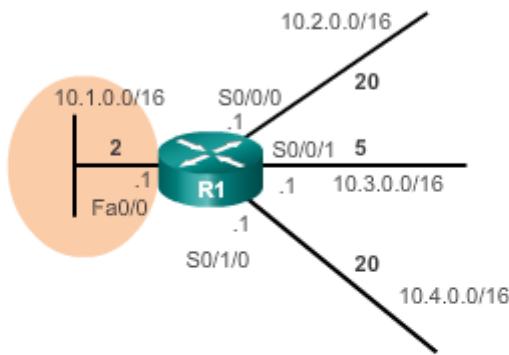
Como se muestra en las figuras 2 a 5, la información de estado de enlace incluye lo siguiente:

- La dirección IPv4 y la máscara de subred de la interfaz
- El tipo de red, como Ethernet (difusión) o enlace serial punto a punto
- El costo de dicho enlace
- Cualquier router vecino en dicho enlace

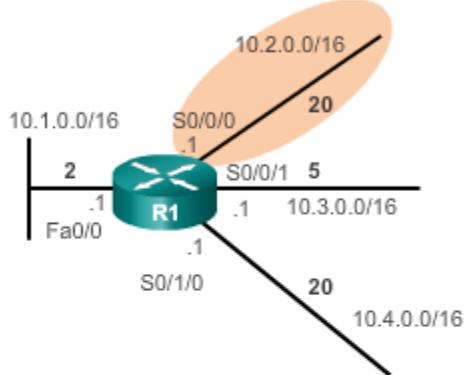
Nota: la implementación de OSPF de Cisco especifica la métrica de routing OSPF como el costo del enlace sobre la base del ancho de banda de la interfaz de salida. A los fines de este capítulo, utilizamos valores de costo arbitrarios para simplificar la demostración.

Enlaces del R1

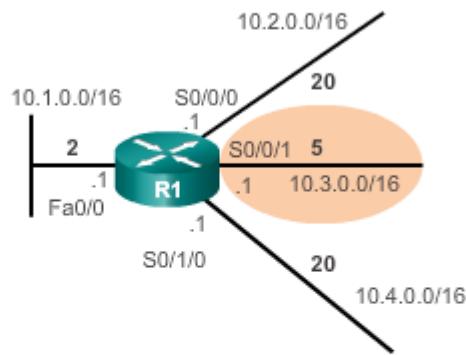


Estado de enlace de la interfaz Fa0/0**Enlace 1**

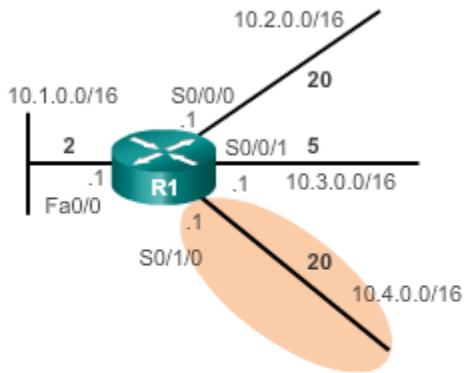
- Red: **10.1.0.0/16**
- Dirección IP: **10.1.0.1**
- Tipo de red: **Ethernet**
- Costo del enlace: **2**
- Vecinos: **ninguno**

Estado de enlace de la interfaz S0/0/0**Enlace 2**

- Red: **10.2.0.0/16**
- Dirección IP: **10.2.0.1**
- Tipo de red: **serial**
- Costo del enlace: **20**
- Vecinos: **R2**

Estado de enlace de la interfaz S0/0/1**Enlace 3**

- Red: **10.3.0.0/16**
- Dirección IP: **10.3.0.1**
- Tipo de red: **serial**
- Costo del enlace: **5**
- Vecinos: **R3**

Estado de enlace de la interfaz S0/1/0**Enlace 4**

- Red: **10.4.0.0/16**
- Dirección IP: **10.4.0.1**
- Tipo de red: **serial**
- Costo del enlace: **20**
- Vecinos: **R4**

El segundo paso en el proceso de routing de estado de enlace es que cada router asume la responsabilidad de encontrarse con sus vecinos en redes conectadas directamente.

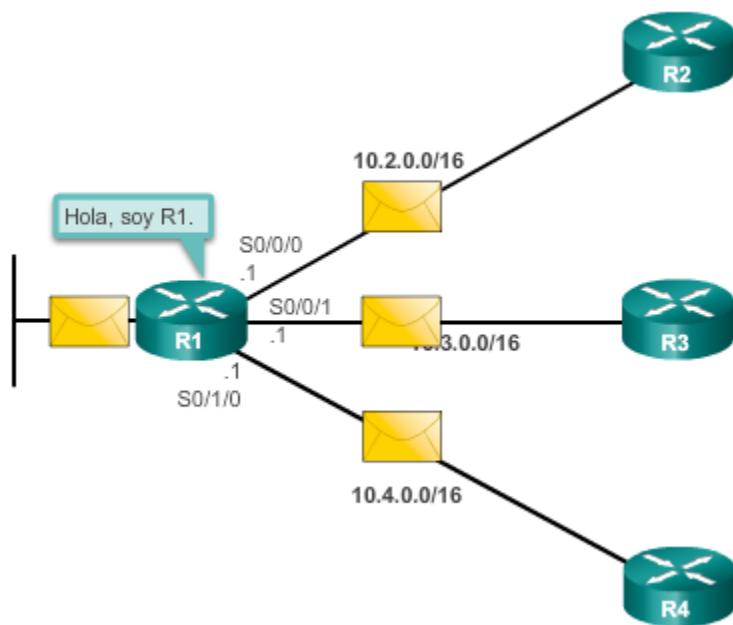
Los routers con protocolos de enrutamiento de link-state utilizan un protocolo de saludo para descubrir cualquier vecino en sus enlaces. Un vecino es cualquier otro router habilitado con el mismo protocolo de enrutamiento de link-state.

Haga clic en Reproducir en la ilustración para ver una animación sobre el proceso de descubrimiento de vecinos de estado de enlace con paquetes de saludo.

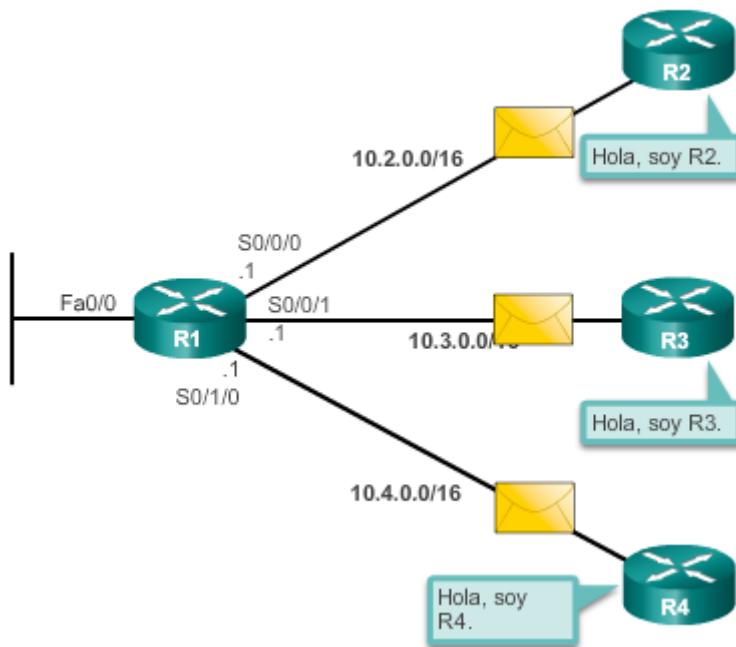
En la animación, el R1 envía paquetes de saludo por sus enlaces (interfaces) para detectar la presencia de vecinos. R2, R3 y R4 responden al paquete de saludo con sus propios paquetes de saludo debido a que dichos routers están configurados con el mismo protocolo de enrutamiento de link-state. No hay vecinos fuera de la interfaz FastEthernet 0/0. Debido a que el R1 no recibe un saludo en esta interfaz, no continúa con los pasos del proceso de routing de estado de enlace para el enlace FastEthernet 0/0.

Cuando dos routers de estado de enlace descubren que son vecinos, forman una adyacencia. Dichos pequeños paquetes de saludo continúan intercambiándose entre dos vecinos adyacentes y cumplen la función de keepalive para monitorear el estado del vecino. Si un router deja de recibir paquetes de saludo por parte de un vecino, dicho vecino se considera inalcanzable y se rompe la adyacencia.

Descubrimiento de vecinos - paquetes de saludo



Descubrimiento de vecinos - paquetes de saludo

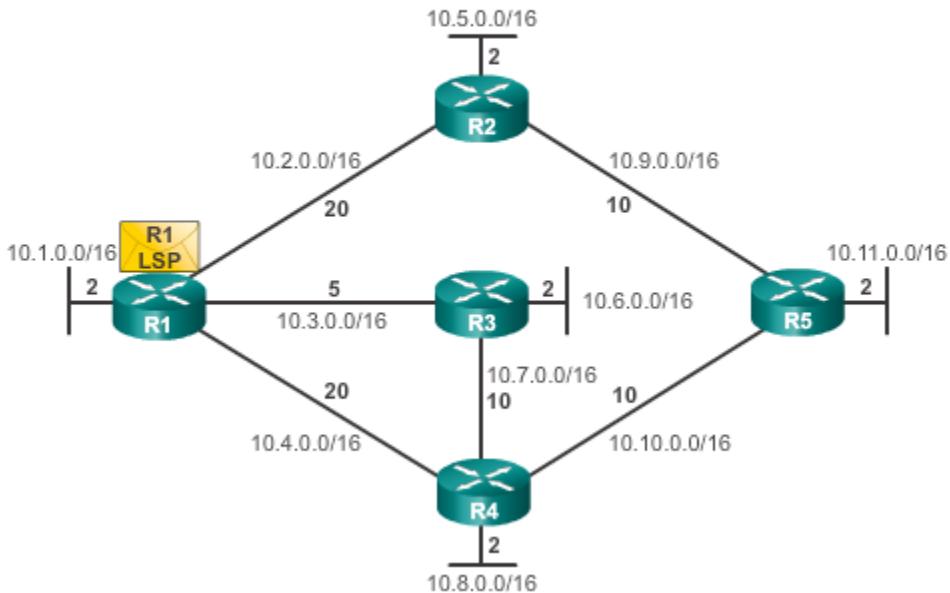


El tercer paso en el proceso de routing de estado de enlace es que cada router cree un paquete de estado de enlace (LSP) que contiene el estado de cada enlace conectado directamente.

Una vez que un router establece sus adyacencias, puede armar LSP que contienen la información de estado de enlace de sus enlaces. Una versión simplificada de LSP del R1, que se muestra en la ilustración, contendría lo siguiente:

1. R1; Red Ethernet 10.1.0.0/16; Costo 2
2. R1 -> R2; Red serial punto a punto; 10.2.0.0/16; Costo 20
3. R1 -> R3; Red serial punto a punto; 10.3.0.0/16; Costo 5
4. R1 -> R4; Red serial punto a punto; 10.4.0.0/16; Costo 20

Armado de LSP



El cuarto paso en el proceso de routing de estado de enlace es que cada router satura con LSP a todos los vecinos, quienes luego almacenan todos los LSP recibidos en una base de datos.

Cada router inunda con su información de link-state a todos los demás routers de link-state en el área de enrutamiento. Siempre que un router recibe un LSP de un router vecino, envía de inmediato dicho LSP a todas las demás interfaces, excepto la interfaz que recibió el LSP. Este proceso crea un efecto de saturación de los LSP desde todos los routers a través del área de enrutamiento.

Haga clic en Reproducir en la ilustración para ver una animación de la saturación con LSP.

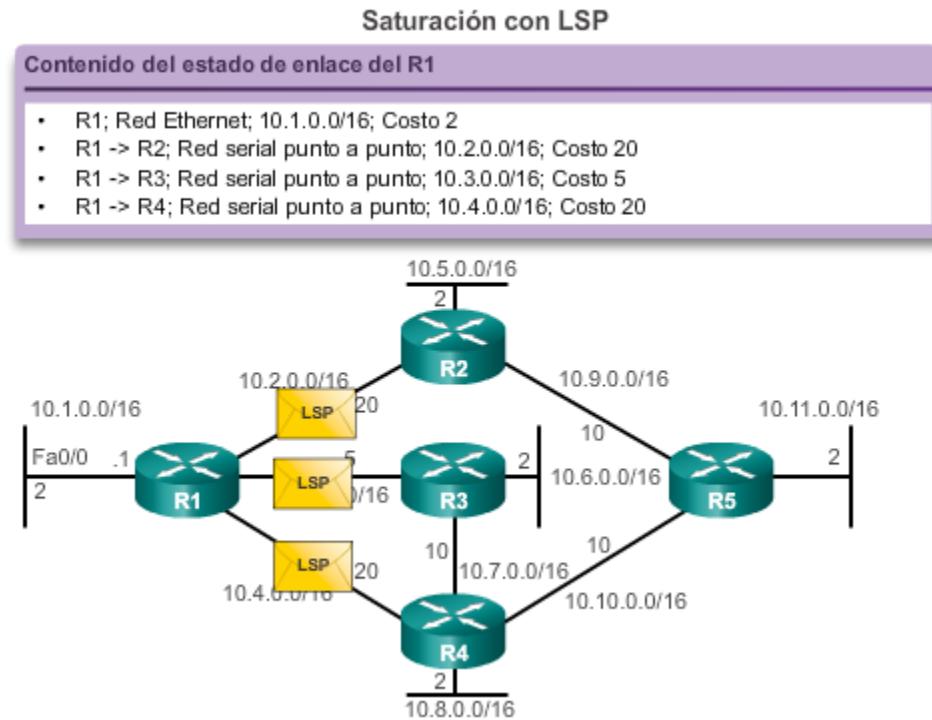
En la animación, observe cómo se lleva a cabo la saturación con LSP de forma casi inmediata después de ser recibidos sin ningún cálculo intermedio. Los protocolos de routing de estado de enlace calculan el algoritmo SPF una vez que finaliza la saturación. Como resultado, los protocolos de routing de estado de enlace logran la convergencia muy rápidamente.

Recuerde que los LSP no necesitan enviarse periódicamente. Un LSP sólo necesita enviarse:

- Durante el arranque inicial del proceso del protocolo de routing (por ejemplo, en el reinicio del router)
- Cuando hay un cambio en la topología (por ejemplo, un enlace que se desactiva o activa, o una adyacencia de vecinos que se establece o se rompe)

Además de la información de estado de enlace, se incluye información adicional en el LSP, como los números de secuencia y la información de vencimiento, para ayudar a administrar el proceso de saturación. Cada router utiliza esta información para determinar si ya recibió el LSP de otro router o si el LSP tiene información más nueva que la contenida en la base de datos de link-state. Este

Este proceso permite que un router conserve sólo la información más actual en su base de datos de link-state.



El paso final en el proceso de routing de estado de enlace es que cada router utiliza la base de datos para construir un mapa completo de la topología y calcula la mejor ruta para cada red de destino.

Finalmente, todos los routers reciben un LSP de todos los demás routers de estado de enlace en el área de routing. Dichos LSP se almacenan en la base de datos de link-state.

En el ejemplo en la ilustración, se muestra el contenido de la base de datos de estado de enlace del R1.

Como resultado del proceso de saturación, el R1 obtuvo la información de estado de enlace para cada router de su área de routing. Observe que R1 también incluye su propia información de link-state en la base de datos de link-state.

Con una base de datos de estado de enlace completa, el R1 ahora puede utilizar la base de datos y el algoritmo SPF (Shortest Path First) para calcular la ruta preferida o la ruta más corta a cada red, lo que da como resultado el árbol SPF.

Contenido de la base de datos de estado de enlace

Base de datos de Link-State de R1	
Estados de enlace del R1:	<ul style="list-style-type: none"> • Conectado a la red 10.1.0.0/16, costo=2 • Conectado al R2 en la red 10.2.0.0/16, costo=20 • Conectado al R3 en la red 10.3.0.0/16, costo=5 • Conectado al R4 en la red 10.4.0.0/16, costo=20
Estados de enlace del R2:	<ul style="list-style-type: none"> • Conectado a la red 10.5.0.0/16, costo=2 • Conectado al R1 en la red 10.2.0.0/16, costo=20 • Conectado al R5 en la red 10.9.0.0/16, costo=10
Estados de enlace del R3:	<ul style="list-style-type: none"> • Conectado a la red 10.6.0.0/16, costo=2 • Conectado al R1 en la red 10.3.0.0/16, costo=5 • Conectado al R4 en la red 10.7.0.0/16, costo=10
Estados de enlace del R4:	<ul style="list-style-type: none"> • Conectado a la red 10.8.0.0/16, costo=2 • Conectado al R1 en la red 10.4.0.0/16, costo=20 • Conectado al R3 en la red 10.7.0.0/16, costo=10 • Conectado al R5 en la red 10.10.0.0/16, costo=10
Estados de enlace del R5:	<ul style="list-style-type: none"> • Conectado a la red 10.11.0.0/16, costo=2 • Conectado al R2 en la red 10.9.0.0/16, costo=10 • Conectado al R4 en la red 10.10.0.0/16, costo=10

Cada router en el área de routing utiliza la base de datos de estado de enlace y el algoritmo SPF para armar el árbol SPF.

Por ejemplo, utilizando la información de estado de enlace de todos los demás routers, el R1 ahora puede comenzar a armar un árbol SPF de la red. Para comenzar, el algoritmo SPF interpreta el LSP de cada router para identificar las redes y los costos asociados.

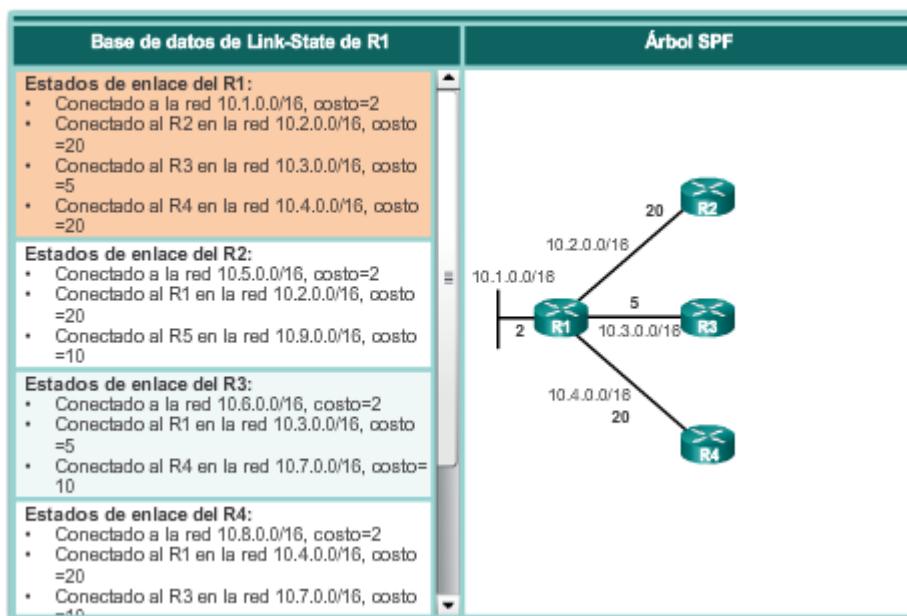
En la figura 1, el R1 identifica sus redes conectadas directamente y los costos.

En las figuras 2 a 5, el R1 continúa agregando toda red desconocida y sus costos asociados al árbol SPF. Observe que el R1 ignora cualquier red que ya haya identificado.

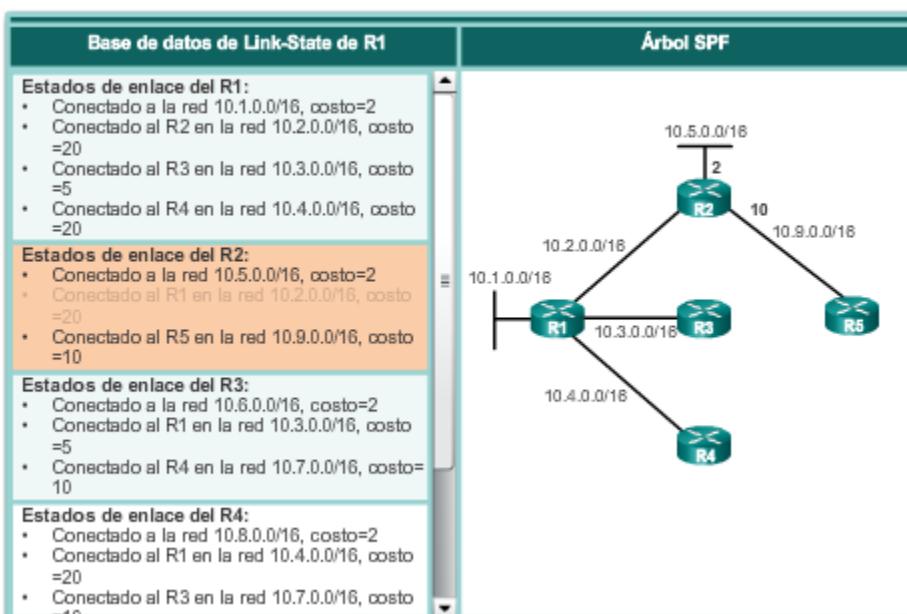
A continuación, el algoritmo SPF calcula las rutas más cortas para llegar a cada red individual, lo que da como resultado el árbol SPF como se muestra en la figura 6. El R1 ahora tiene una vista de topología completa del área de estado de enlace.

Cada router construye su propio árbol SPF independientemente de los otros routers. Para garantizar el enrutamiento adecuado, las bases de datos de link-state utilizadas para construir dichos árboles deben ser idénticas en todos los routers.

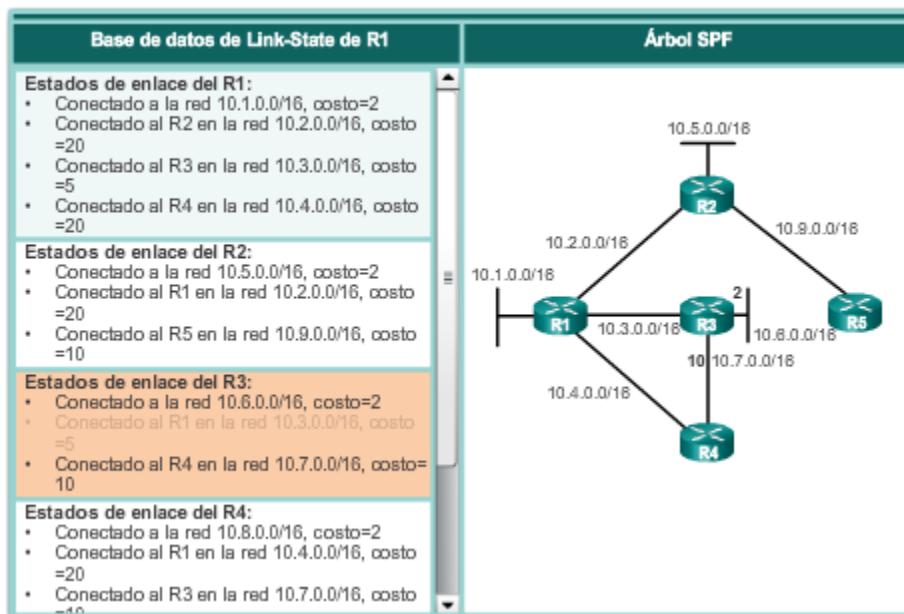
Identificación de las rutas conectadas directamente



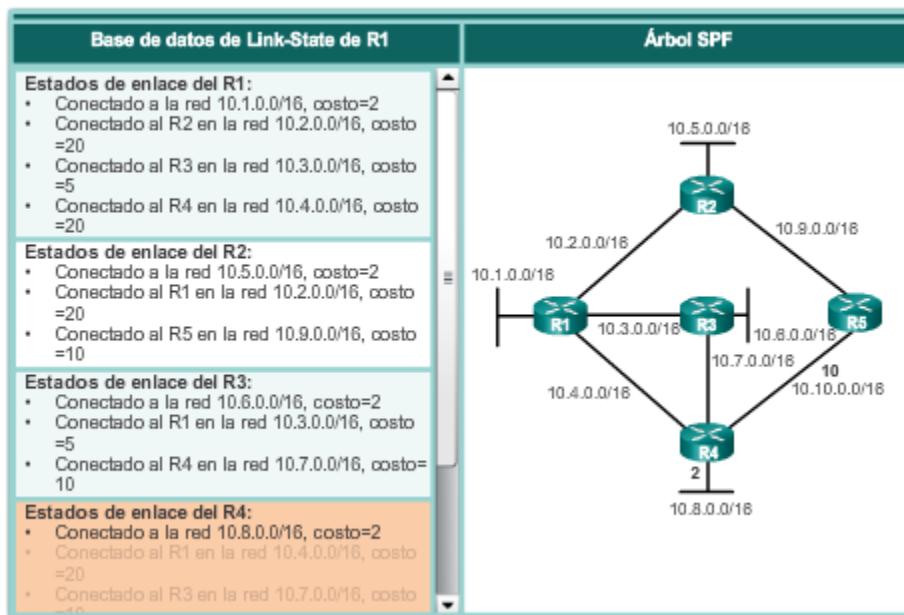
Identificación de las redes desconocidas y los costos del R2



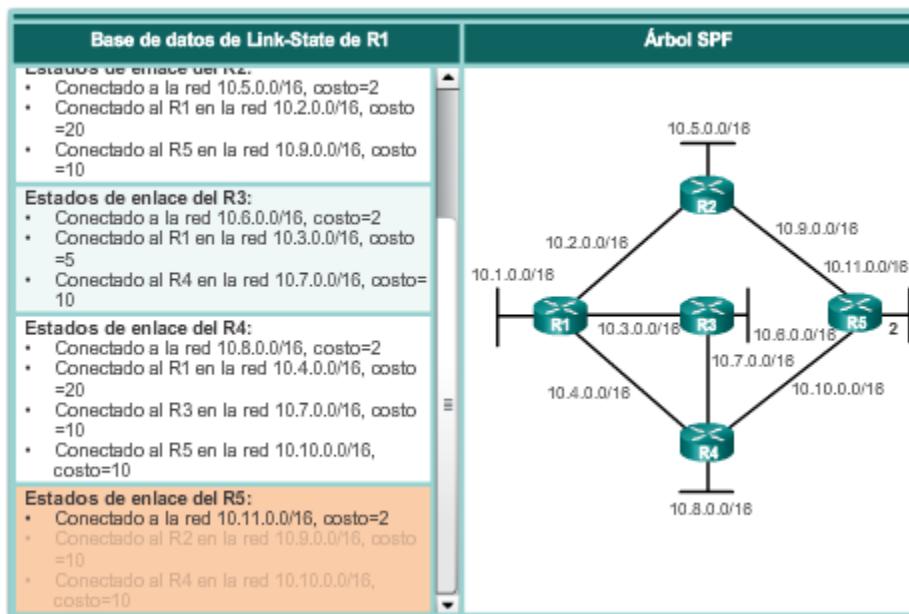
Identificación de las redes desconocidas y los costos del R3



Identificación de las redes desconocidas y los costos del R4

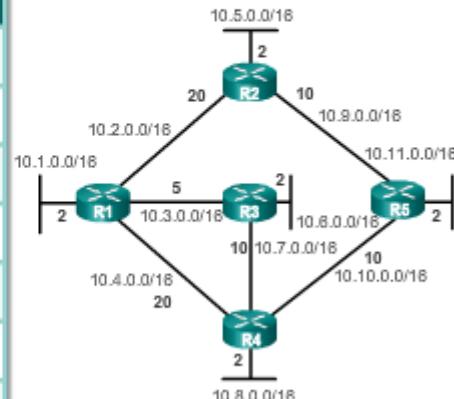


Identificación de las redes desconocidas y los costos del R5



Árbol SPF resultante del R1

Destino	Ruta más corta	Costo
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3→ R4→ R5	27



Al utilizar la información de la ruta más corta determinada por el algoritmo SPF, dichas rutas ahora pueden agregarse a la tabla de enrutamiento. En la ilustración, se muestran las rutas que se agregaron a la tabla de routing IPv4 del R1.

La tabla de routing también incluye todas las redes conectadas directamente y las rutas provenientes de cualquier otro origen, tales como las rutas estáticas. Los paquetes ahora se reenvían según dichas entradas en la tabla de routing.

Completar la tabla de routing

Destino	Ruta más corta	Costo
10.5.0.0/16	R1 → R2	22
10.6.0.0/16	R1 → R3	7
10.7.0.0/16	R1 → R3	15
10.8.0.0/16	R1 → R3 → R4	17
10.9.0.0/16	R1 → R2	30
10.10.0.0/16	R1 → R3 → R4	25
10.11.0.0/16	R1 → R3 → R4 → R5	27

Tabla de enrutamiento de R1

Redes conectadas directamente

- 10.1.0.0/16, red conectada directamente
- 10.2.0.0/16, red conectada directamente
- 10.3.0.0/16, red conectada directamente
- 10.4.0.0/16, red conectada directamente

Redes remotas

- 10.5.0.0/16 mediante Serial 0/0/0 del R2, costo = 22
- 10.6.0.0/16 mediante Serial 0/0/1 del R3, costo = 7
- 10.7.0.0/16 mediante Serial 0/0/1 del R3, costo = 15
- 10.8.0.0/16 mediante Serial 0/0/1 del R3, costo = 17
- 10.9.0.0/16 mediante Serial 0/0/0 del R2, costo = 30
- 10.10.0.0/16 mediante Serial 0/0/1 del R3, costo = 25
- 10.11.0.0/16 mediante Serial 0/0/1 del R3, costo = 27

7.5.3 Razones para utilizar protocolos de routing de estado de enlace

Como se muestra en la ilustración, los protocolos de routing de estado de enlace presentan varias ventajas en comparación con los protocolos de routing vector distancia.

- **Armado de un mapa topológico:** los protocolos de routing de estado de enlace crean un mapa topológico o árbol SPF de la topología de la red. Debido a que los protocolos de enrutamiento de link-state intercambian estados de enlace, el algoritmo SPF puede crear un árbol SPF de la red. Al utilizar el árbol SPF, cada router puede determinar en forma independiente la ruta más corta a cada red.
- **Convergencia rápida:** cuando reciben un LSP, los protocolos de routing de estado de enlace saturan de inmediato todas las interfaces con el LSP, excepto la interfaz desde la que se lo recibió. En cambio, el protocolo RIP necesita procesar cada actualización de routing y actualizar su tabla de routing antes de saturar otras interfaces.
- **Actualizaciones desencadenadas por eventos:** después de la saturación inicial con LSP, los protocolos de routing de estado de enlace solo envían un LSP cuando se produce un cambio en la topología. El LSP sólo incluye la información relacionada con el enlace afectado. A diferencia de algunos protocolos de enrutamiento vector distancia, los protocolos de enrutamiento de link-state no envían actualizaciones periódicas.
- **Diseño jerárquico:** los protocolos de routing de estado de enlace utilizan el concepto de áreas. Las áreas múltiples crean un diseño jerárquico para redes y permiten un mejor agregado de rutas (sumarización) y el aislamiento de los problemas de enrutamiento dentro del área.

Los protocolos de estado de enlace también tienen algunas desventajas en comparación con los protocolos de routing vector distancia:

- **Requisitos de memoria:** los protocolos de estado de enlace requieren memoria adicional para crear y mantener la base de datos de estado de enlace y el árbol SPF.
- **Requisitos de procesamiento:** los protocolos de estado de enlace también pueden requerir un mayor procesamiento de CPU que los protocolos de routing vector distancia. El algoritmo SPF requiere un mayor tiempo de CPU que los algoritmos vector distancia, como Bellman-Ford, ya que los protocolos de estado de enlace arman un mapa completo de la topología.
- **Requisitos de ancho de banda:** la saturación de paquetes de estado de enlace puede ejercer un impacto negativo en el ancho de banda disponible en una red. Si bien esto sólo debería ocurrir durante la puesta en marcha inicial de los routers, también podría ser un problema en redes inestables.

Ventajas de los protocolos de routing de estado de enlace

- Cada router arma su propio mapa topológico de la red para determinar la ruta más corta.
- Se logra una convergencia más rápida mediante la saturación inmediata con LSP.
- Los LSP se envían solo cuando hay un cambio en la topología y contienen únicamente información relacionada con ese cambio.
- Se utiliza diseño jerárquico al implementar varias áreas.

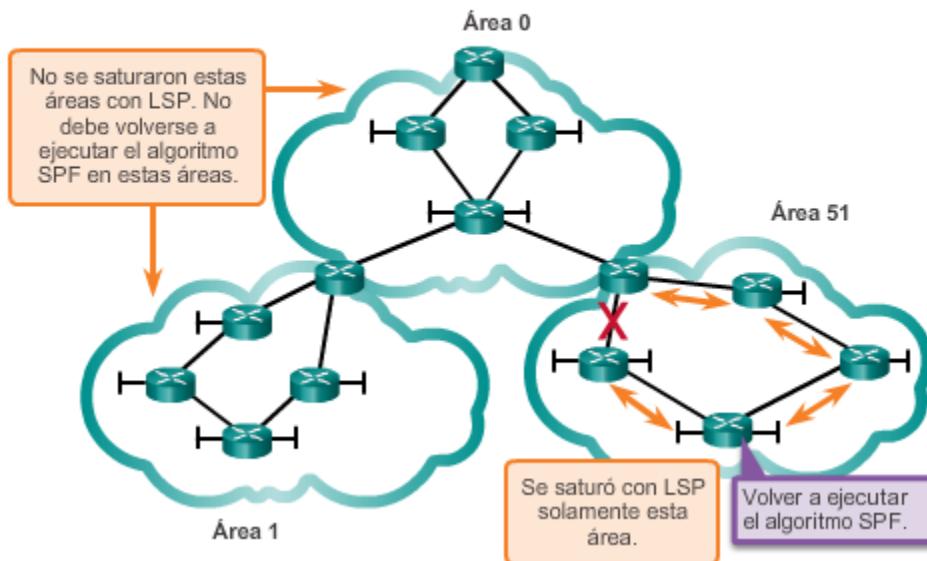
Desventajas de los protocolos de routing de estado de enlace

- El mantenimiento de una base de datos de estado de enlace y un árbol SPF requiere memoria adicional.
- El cálculo del algoritmo SPF también requiere mayor procesamiento de CPU.
- La saturación de paquetes de estado de enlace puede afectar de manera negativa el ancho de banda.

Los protocolos de enrutamiento de link-state modernos están diseñados para minimizar los efectos en la memoria, el CPU y el ancho de banda. La utilización y configuración de áreas múltiples puede reducir el tamaño de las bases de datos de link-state. Las áreas múltiples también pueden limitar el grado de saturación de información de link-state en un dominio de enrutamiento y enviar los LSP sólo a aquellos routers que los necesitan. Cuando hay un cambio en la topología, solo los routers del área afectada reciben el LSP y ejecutan el algoritmo SPF. Esto puede ayudar a aislar un enlace inestable en un área específica en el dominio de enrutamiento.

Por ejemplo, en la ilustración hay tres dominios de routing independientes: área 1, área 0 y área 51. Si una red en el área 51 deja de funcionar, solo los routers en esa área se saturan con el LSP que contiene la información sobre dicho enlace fuera de servicio. Únicamente los routers del área 51 necesitan actualizar sus bases de datos de estado de enlace, volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar sus tablas de routing. Los routers de otras áreas descubren que esta ruta no funciona, pero esto se realiza con un tipo de LSP que no los obliga a volver a ejecutar su algoritmo SPF. Los routers de otras áreas pueden actualizar sus tablas de enrutamiento directamente.

Creación de áreas para minimizar el uso de recursos del router



Existen solamente dos protocolos de routing de estado de enlace: OSPF e IS-IS.

El protocolo OSPF (Open Shortest Path First) es la implementación más popular. Fue diseñado por el grupo de trabajo de OSPF del Grupo de trabajo de ingeniería de Internet (IETF). El desarrollo de OSPF comenzó en 1987 y actualmente hay dos versiones en uso:

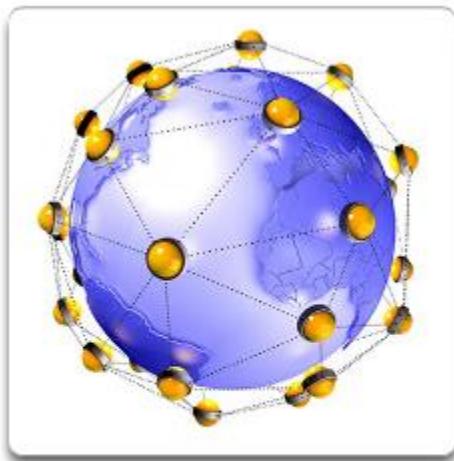
- OSPFv2: OSPF para redes IPv4 (RFC 1247 y RFC 2328)
- OSPFv3: OSPF para redes IPv6 (RFC 2740)

Nota: con la característica de familias de direcciones de OSPFv3, esta versión del protocolo es compatible con IPv4 e IPv6.

El protocolo IS-IS fue diseñado por la Organización Internacional para la Estandarización (ISO) y se describe en ISO 10589. La primera versión de este protocolo de routing se desarrolló en la Digital Equipment Corporation (DEC) y se conoce como "DECnet fase V". Radia Perlman fue la principal diseñadora del protocolo de routing IS-IS.

IS-IS se diseñó originalmente para el suite de protocolos de OSI y no para el suites de protocolo de TCP/IP. Más adelante, IS-IS integrado, o IS-IS doble, incluyó la compatibilidad con redes IP. Si bien se conoció a IS-IS como el protocolo de enruteamiento más utilizado por proveedores e ISP, se están comenzando a utilizar más redes IS-IS corporativas.

OSPF e IS-IS presentan varias similitudes y diferencias. Existen diversas posturas a favor de OSPF y a favor de IS-IS que analizan y debaten las ventajas de un protocolo de enruteamiento frente al otro. Ambos protocolos de routing proporcionan la funcionalidad de routing necesaria.



IS-IS

- ISO 10589.
- IS-IS integrado (IS-IS doble) admite redes IP.
- Utilizado principalmente por los ISP y por las empresas prestadoras de servicios.

7.6 La tabla de routing

7.6.1 Partes de una entrada de ruta IPv4

La topología que se muestra en la figura 1 se utiliza como la topología de referencia para esta sección. Observe lo siguiente en la topología:

El R1 es el router perimetral que se conecta a Internet. Por lo tanto, propaga una ruta estática predeterminada al R2 y al R3.

El R1, el R2 y el R3 contienen redes no contiguas separadas por otra red con clase.

El R3 también introduce una ruta de superred 192.168.0.0/16.

En la figura 2, se muestra la tabla de routing IPv4 del R1 con las rutas dinámicas, estáticas y conectadas directamente.

Nota: en los inicios, la jerarquía de la tabla de routing en el IOS de Cisco se implementó con el esquema de routing con clase. Si bien la tabla de enrutamiento incorpora el direccionamiento con clase y sin clase, la estructura general aún se construye en base a este esquema con clase.

Topología de referencia

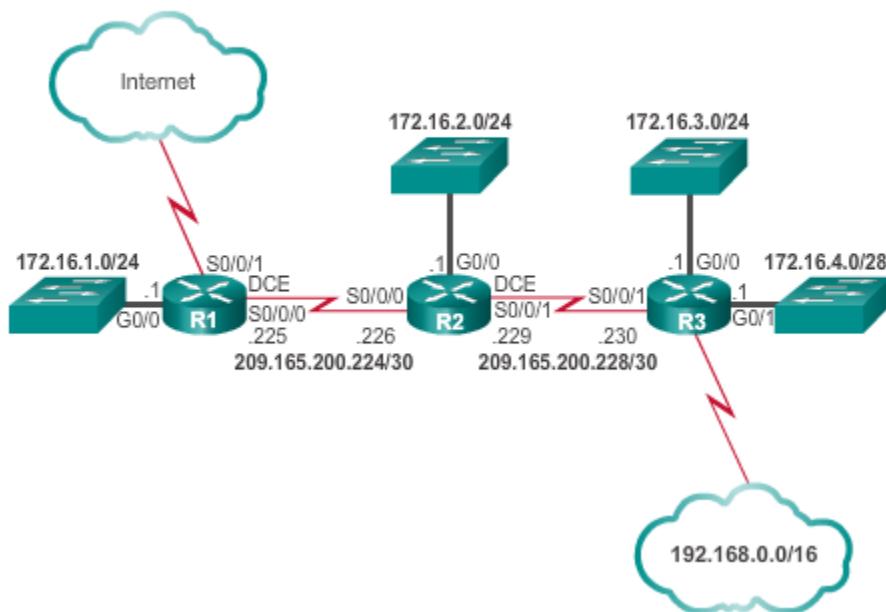


Tabla de routing del R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, serial0/0/1
    is directly connected, Serial0/0/1
C   172.16.0.0/16 is variably subnetted, 5 subnets, 3 masks
L     172.16.1.0/24 is directly connected, GigabitEthernet0/0
L     172.16.1.1/32 is directly connected, GigabitEthernet0/0
R     172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R     192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C     209.165.200.224/30 is directly connected, Serial0/0/0
L     209.165.200.225/32 is directly connected, Serial0/0/0
R     209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
        Serial0/0/0
C     209.165.200.232/30 is directly connected, Serial0/0/1
L     209.165.200.233/30 is directly connected, Serial0/0/1
R1#
```

Como se destaca en la figura 1, la tabla de routing del R1 contiene tres redes conectadas directamente. Observe que cuando se configura una interfaz del router activa con una dirección IP y una máscara de subred, automáticamente se crean dos entradas en la tabla de routing.

En la figura 2, se muestra una de las entradas de la tabla de routing en el R1 para la red conectada directamente 172.16.1.0. Estas entradas se agregaron de forma automática a la tabla de enrutamiento cuando se configuró y se activó la interfaz GigabitEthernet 0/0. Las entradas contienen la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta. **C** identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa. **L** identifica que la ruta es local. Las rutas locales se crean de forma automática cada vez que se configura una interfaz con una dirección IP y se activa.
- **Red de destino:** la dirección de la red remota y la forma en que se conecta esa red.
- **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

Nota: antes del IOS versión 15, las entradas de la tabla de routing local no aparecían en las tablas de routing.

En general, los routers tienen varias interfaces configuradas. En la tabla de routing se almacena información acerca de las rutas conectadas directamente y de las rutas remotas. Tal como ocurre con las redes conectadas directamente, el origen de la ruta identifica cómo se descubrió la ruta. Por ejemplo, los códigos frecuentes para las redes remotas incluyen los siguientes:

- **S:** indica que un administrador creó la ruta manualmente para llegar a una red específica. Esto se conoce como “ruta estática”.
- **D:** indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing EIGRP.
- **O:** indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing OSPF.
- **R:** indica que la ruta se descubrió de forma dinámica de otro router mediante el protocolo de routing RIP.

Interfaces del R1 conectadas directamente

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 209.165.200.234, serial0/0/1
    is directly connected, Serial0/0/1
    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
R   172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
R   172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R   172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12, Serial0/0/0
R   192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03, Serial0/0/0
    209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C   209.165.200.224/30 is directly connected, Serial0/0/0
L   209.165.200.225/32 is directly connected, Serial0/0/0
R   209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12, Serial0/0/0
C   209.165.200.232/30 is directly connected, Serial0/0/1
L   209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Rutas conectadas directamente en el R1

Origen de la ruta	Red destino	Interfaz de salida
C	172.16.1.0/24 is directly connected, GigabitEthernet0/0	
L	172.16.1.1/32 is directly connected, GigabitEthernet0/0	

Leyenda

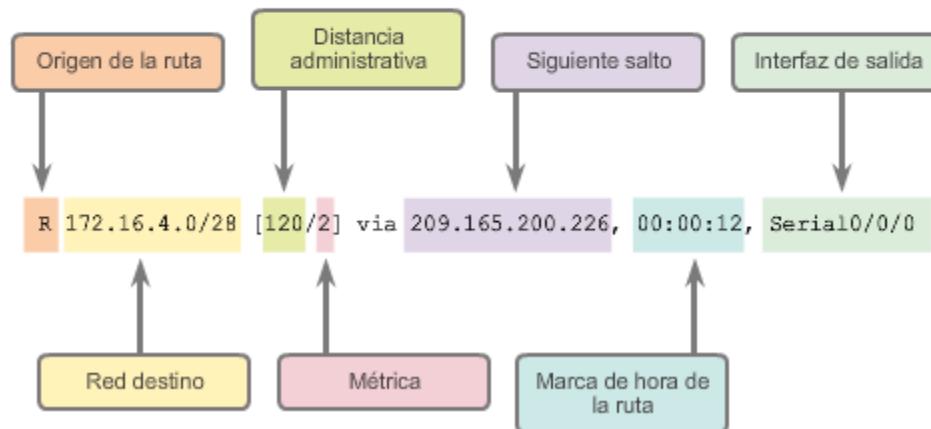
- Identifica de qué manera el router identificó la red.
- Identifica la red de destino y cómo está conectada.
- Identifica la interfaz en el router conectado a la red de destino.

En la ilustración, se muestra una entrada de la tabla de routing IPv4 en el R1 para la ruta hacia la red remota 172.16.4.0 en el R3. La entrada indica la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta.
- **Red de destino:** identifica la dirección de la red remota.
- **Distancia administrativa:** identifica la confiabilidad del origen de la ruta.

- **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Siguiente salto:** identifica la dirección IPv4 del router siguiente al que se debe reenviar el paquete.
- **Marca de hora de la ruta:** identifica cuándo fue la última comunicación con la ruta.
- **Interfaz de salida:** identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Entrada de ruta de red remota en el R1



Gateway of last resort is not set

```

S 10.0.0.0/16 is subnetted, 1 subnets
  S 10.4.0.0 is directly connected, Serial0/0/0
    172.16.0.0/24 is subnetted, 3 subnets
      C 172.16.1.0 is directly connected, FastEthernet0/0
      C 172.16.2.0 is directly connected, Serial0/0/0
      D 172.16.3.0 [90/2172416] via 172.16.2.1, 00:00:18, Serial0/0/0
      C 192.168.1.0/24 is directly connected, Serial0/0/1
      O 192.168.100.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0/0
      O 192.168.110.0/24 [110/65] via 172.16.2.1, 00:00:03, Serial0/0/0
      R 192.168.120.0/24 [120/1] via 172.16.2.1, 00:00:18, Serial0/0/0

```

Ruta	Origen de la ruta	AD	Métrica
10.4.0.0/16	Estática	1	0
172.16.2.0/24	Conectada	0	0
172.16.3.0/24	EIGRP	90	2172416
192.168.110.0/24	OSPF	110	65
192.168.120.0/24	RIP	120	1

7.6.2 Rutas IPv4 descubiertas en forma dinámica

Una tabla de routing armada dinámicamente proporciona mucha información, como se muestra en la ilustración. Por lo tanto, es de vital importancia comprender el resultado generado por la tabla de routing. Al analizar el contenido de una tabla de routing, se utilizan términos especiales.

La tabla de enrutamiento IP de Cisco no es una base de datos plana. La tabla de enrutamiento, en realidad, es una estructura jerárquica que se usa para acelerar el proceso de búsqueda cuando se ubican rutas y se reenvían paquetes. Dentro de esta estructura, la jerarquía incluye varios niveles.

Las rutas se analizan en términos de lo siguiente:

- Ruta final
- Ruta de Nivel 1
- Ruta principal de nivel 1
- Rutas secundarias de nivel 2

Tabla de routing del R1

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
      is directly connected, Serial0/0/1
      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
R      172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
      Serial0/0/0
R      172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
      Serial0/0/0
R      172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
      Serial0/0/0
R      192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
      Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C      209.165.200.224/30 is directly connected, Serial0/0/0
L      209.165.200.225/32 is directly connected, Serial0/0/0
R      209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
      Serial0/0/0
C      209.165.200.232/30 is directly connected, Serial0/0/1
L      209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Una ruta final es una entrada de la tabla de routing que contiene una dirección IPv4 del siguiente salto o una interfaz de salida. Las rutas conectadas directamente, las rutas descubiertas dinámicamente y las rutas locales son rutas finales.

En la ilustración, las áreas resaltadas son ejemplos de rutas finales. Observe que todas estas rutas especifican una dirección IPv4 del siguiente salto o una interfaz de salida.

Rutas finales del R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
      is directly connected, Serial0/0/1
      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
R      172.16.2.0/24 [120/1] via 209.165.200.226, 00:00:12,
      Serial0/0/0
R      172.16.3.0/24 [120/2] via 209.165.200.226, 00:00:12,
      Serial0/0/0
R      172.16.4.0/28 [120/2] via 209.165.200.226, 00:00:12,
      Serial0/0/0
R      192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
      Serial0/0/0
      209.165.200.0/24 is variably subnetted, 5 subnets, 2 masks
C      209.165.200.224/30 is directly connected, Serial0/0/0
L      209.165.200.225/32 is directly connected, Serial0/0/0
R      209.165.200.228/30 [120/1] via 209.165.200.226, 00:00:12,
      Serial0/0/0
C      209.165.200.232/30 is directly connected, Serial0/0/1
L      209.165.200.233/32 is directly connected, Serial0/0/1
R1#
```

Una ruta de nivel 1 con una máscara de subred igual o inferior a la máscara con clase de la dirección de red. Por lo tanto, una ruta de nivel 1 puede ser cualquiera de las siguientes:

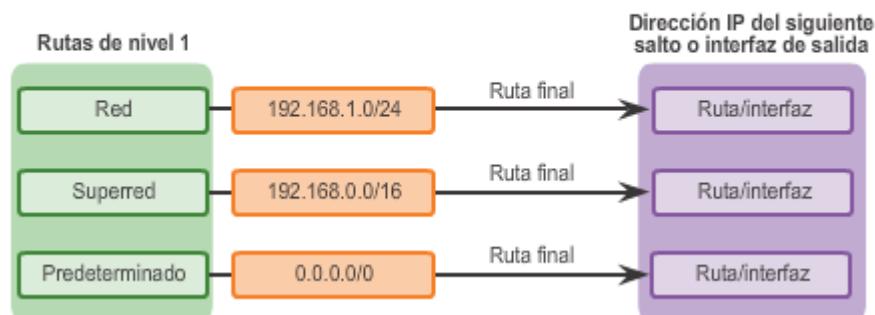
- **Ruta de red:** una ruta de red que tiene una máscara de subred igual a la de la máscara con clase.
- **Ruta de superred:** una dirección de red con una máscara menor que la máscara con clase, por ejemplo, una dirección de resumen.
- **Ruta predeterminada:** una ruta estática con la dirección 0.0.0.0/0.

El origen de la ruta de nivel 1 puede ser una red conectada directamente, una ruta estática o un protocolo de enrutamiento dinámico.

En la figura 1, se destaca la forma en que las rutas de nivel 1 también son rutas finales.

En la figura 2, se destacan las rutas de nivel 1.

Orígenes de las rutas de nivel 1



Ejemplo de rutas de nivel 1

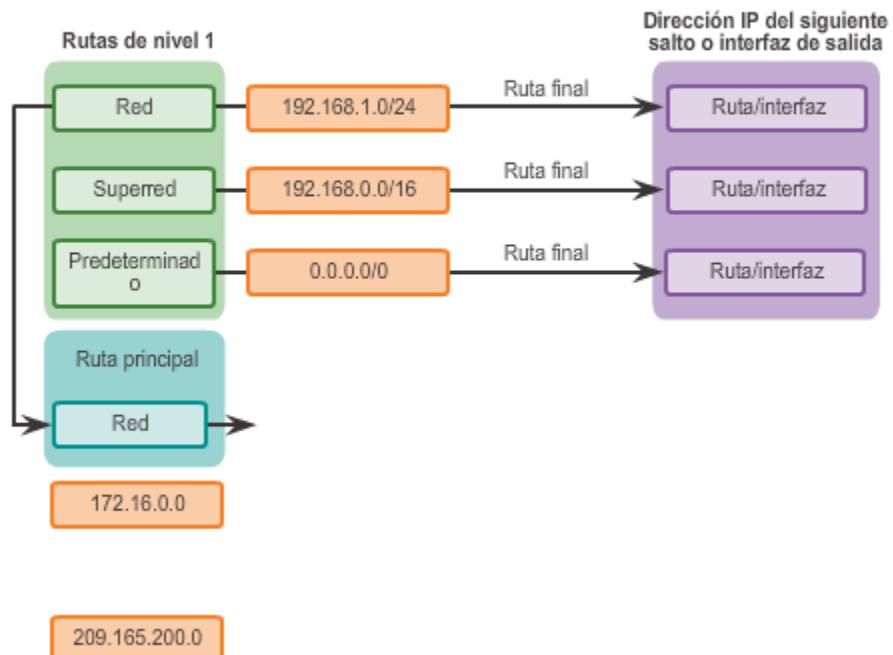
```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*      0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
          is directly connected, Serial0/0/1
          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
R          172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R          172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R          172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R          192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
          209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C          209.165.200.224/30 is directly connected,
Serial0/0/0
```

Como se ilustra en la figura 1, una ruta principal de nivel 1 es una ruta de red de nivel 1 que está dividida en subredes. Una ruta principal nunca puede ser una ruta final.

En la figura 2, se destacan las rutas principales de nivel 1 en la tabla de routing del R1. En la tabla de routing, básicamente se proporciona un encabezado para las subredes específicas que contiene. Cada entrada muestra la dirección de red con clase, la cantidad de subredes y la cantidad de máscaras de subred diferentes en las que se subdividió la dirección con clase.

Ruta primaria de nivel 1



Rutas principales de nivel 1 del R1

```
R1# show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

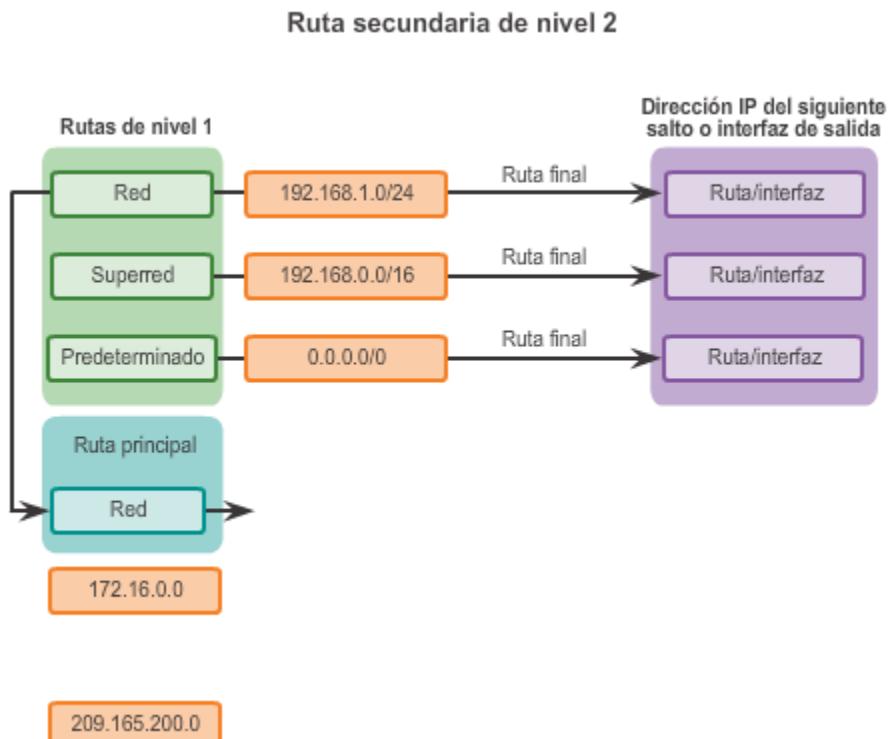
S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
          is directly connected, Serial0/0/1
        172.16.0.0/16 is variably subnetted, 5 subnets, 3
masks
C        172.16.1.0/24 is directly connected,
GigabitEthernet0/0
L        172.16.1.1/32 is directly connected,
GigabitEthernet0/0
R        172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R        172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R        192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
          209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C        209.165.200.224/30 is directly connected,
Serial0/0/0
```

Una ruta secundaria de nivel 2 es una ruta que constituye una subred de una dirección de red con clase. Como se ilustra en la figura 1, una ruta principal de nivel 1 es una ruta de red de nivel 1 que está dividida en subredes. Las rutas principales de nivel 1 contienen rutas secundarias de nivel 2, como se muestra en la figura 2.

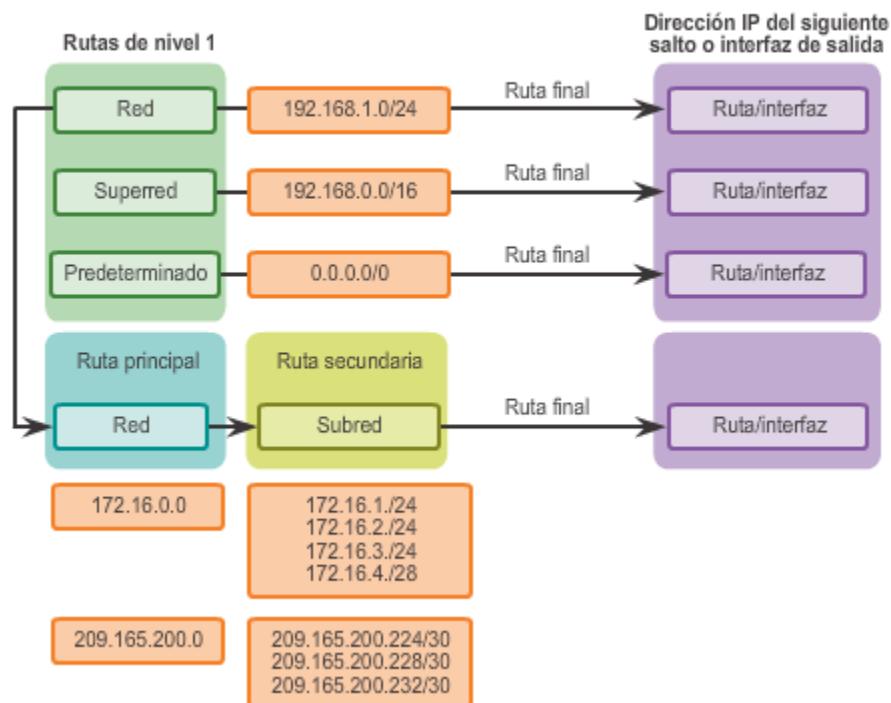
Al igual que en las rutas de nivel 1, el origen de una ruta de nivel 2 puede ser una red conectada directamente, una ruta estática o una ruta descubierta en forma dinámica. Las rutas secundarias de nivel 2 también son rutas finales.

Nota: la jerarquía de la tabla de routing en el IOS de Cisco tiene un esquema de routing con clase. Una ruta principal de nivel 1 es la dirección de red con clase de la ruta de subred. Esto es así incluso si un protocolo de enrutamiento sin clase es el origen de la ruta de subred.

En la figura 3, se destacan las rutas secundarias en la tabla de routing del R1.



Las rutas secundarias son rutas finales



Ejemplo de rutas secundarias de nivel 2

```
R1#show ip route | begin Gateway
Gateway of last resort is 209.165.200.234 to network
0.0.0.0

S*    0.0.0.0/0 [1/0] via 209.165.200.234, Serial0/0/1
          is directly connected, Serial0/0/1
          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
R      172.16.2.0/24 [120/1] via 209.165.200.226,
00:00:12, Serial0/0/0
R      172.16.3.0/24 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R      172.16.4.0/28 [120/2] via 209.165.200.226,
00:00:12, Serial0/0/0
R      192.168.0.0/16 [120/2] via 209.165.200.226, 00:00:03,
Serial0/0/0
          209.165.200.0/24 is variably subnetted, 5 subnets, 2
masks
C      209.165.200.224/30 is directly connected,
Serial0/0/0
```

7.6.3 Proceso de búsqueda de rutas IPv4

Cuando un paquete llega a una interfaz del router, el router analiza el encabezado de IPv4, identifica la dirección IPv4 de destino y continúa a través del proceso de búsqueda del router.

En la figura 1, el router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv4.

1. Si la mejor coincidencia es una ruta final de nivel 1, se utiliza esa ruta para reenviar el paquete.
2. Si la mejor coincidencia es una ruta principal de nivel 1, se continúa con el siguiente paso.

En la figura 2, el router examina las rutas secundarias (las rutas de subred) de la ruta principal en busca de la mejor coincidencia.

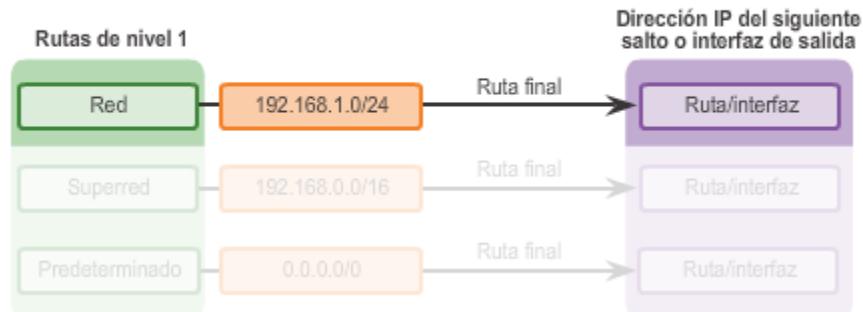
3. Si hay una coincidencia con una ruta secundaria de nivel 2, se utiliza esa subred para reenviar el paquete.
4. Si no hay una coincidencia con ninguna de las rutas secundarias de nivel 2, se continúa con el paso siguiente.

En la figura 3, el router continúa buscando rutas de superred de nivel 1 en la tabla de routing para detectar una coincidencia, incluida la ruta predeterminada, si la hubiera.

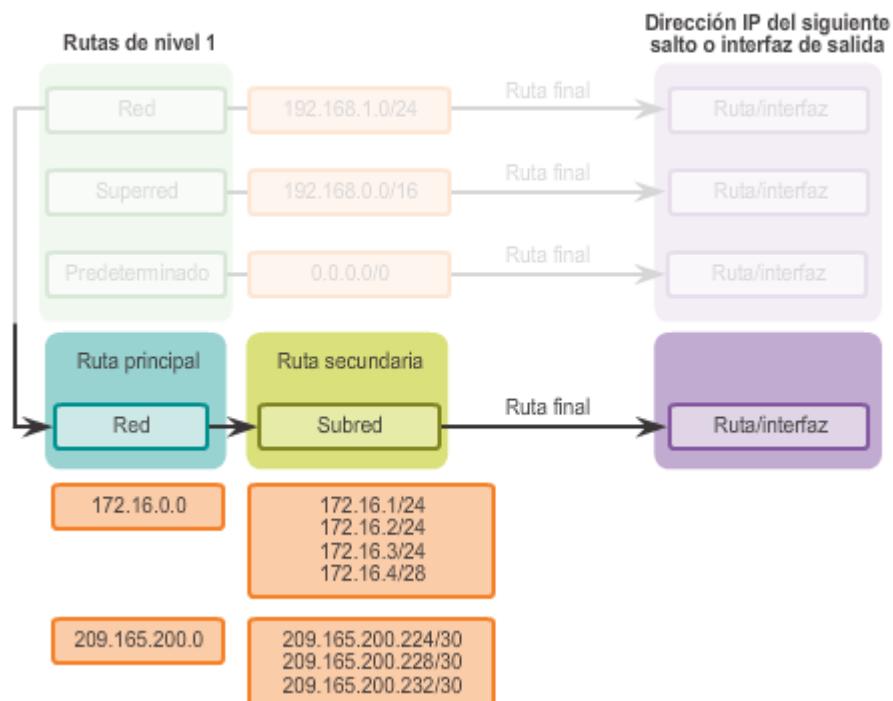
5. Si ahora hay una coincidencia menor con las rutas predeterminadas o de superred de nivel 1, el router usa esa ruta para reenviar el paquete.
6. Si no hay coincidencia con ninguna ruta de la tabla de enrutamiento, el router descarta el paquete.

Nota: una ruta que solo hace referencia a una dirección IP del siguiente salto y no a una interfaz de salida debe resolverse a una ruta con una interfaz de salida. Se realiza una búsqueda recurrente en la dirección IP del siguiente salto hasta que la ruta se resuelva con una interfaz de salida.

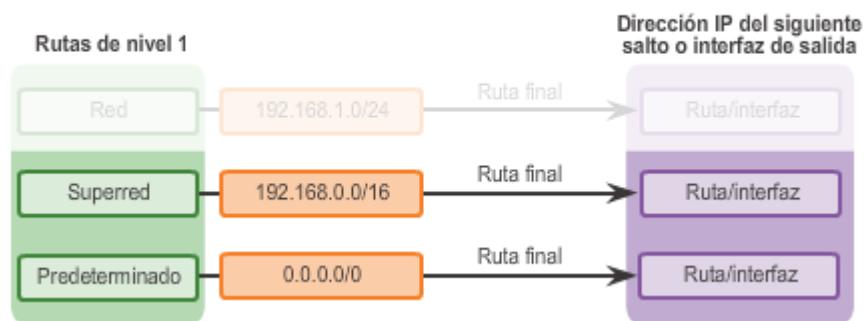
Coincidencia de rutas de nivel 1



Coincidencia de rutas secundarias de nivel 2



Coincidencia de superred y, luego, de ruta predeterminada



¿Qué significa que el router deba encontrar la mejor coincidencia en la tabla de routing? La mejor coincidencia es la coincidencia más larga.

Para que haya una coincidencia entre la dirección IPv4 de destino de un paquete y una ruta en la tabla de routing, una cantidad mínima de los bits del extremo izquierdo deben coincidir entre la dirección IPv4 del paquete y la ruta en la tabla de routing. La máscara de subred de la ruta en la tabla de routing se utiliza para determinar la cantidad mínima de bits del extremo izquierdo que deben coincidir. Recuerde que un paquete IPv4 solo contiene la dirección IPv4 y no la máscara de subred.

La mejor coincidencia es la ruta de la tabla de routing que contiene la mayor cantidad de bits del extremo izquierdo coincidentes con la dirección IPv4 de destino del paquete. La ruta con la mayor cantidad de bits del extremo izquierdo equivalentes, o la coincidencia más larga, es siempre la ruta preferida.

En la ilustración, el destino de un paquete es 172.16.0.10. El router tiene tres rutas posibles que coinciden con este paquete: 172.16.0.0/12, 172.16.0.0/18 y 172.16.0.0/26. De las tres rutas, 172.16.0.0/26 tiene la coincidencia más larga y, por lo tanto, se elige para reenviar el paquete. Recuerde que para que cualquiera de estas rutas se considere una coincidencia debe tener al menos la cantidad de bits coincidentes que se indica en la máscara de subred de la ruta.

Coincidencias para el paquete destinado a 172.16.0.10

Destino del paquete IP	172.16.0.10	10101100.00010000.00000000.00001010
Ruta 1	172.16.0.0/12	10101100.00010000.00000000.00000000
Ruta 2	172.16.0.0/18	10101100.00010000.00000000.00000000
Ruta 3	172.16.0.0/26	10101100.00010000.00000000.00000000

↑
Coincidencia más larga con el destino del paquete IP

7.6.4 Análisis de una tabla de routing IPv6

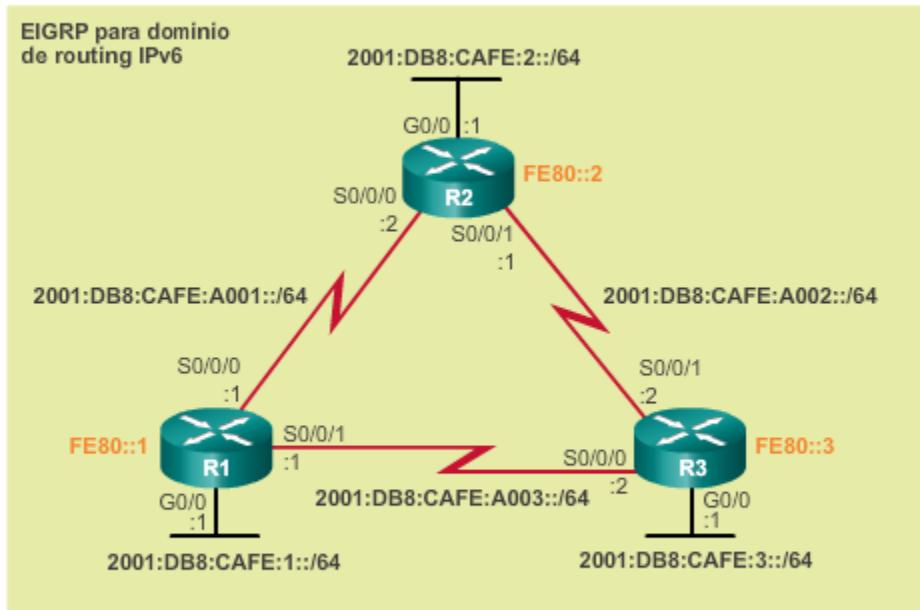
Los componentes de la tabla de routing IPv6 son muy similares a los de la tabla de routing IPv4. Por ejemplo, se completa con las interfaces conectadas directamente, con las rutas estáticas y con las rutas descubiertas de forma dinámica.

Dado que IPv6 fue diseñado como un protocolo sin clase, todas las rutas son en realidad rutas finales de nivel 1. No hay rutas principales de nivel 1 para rutas secundarias de nivel 2.

La topología que se muestra en la ilustración se utiliza como la topología de referencia para esta sección. Observe lo siguiente en la topología:

- El R1, el R2 y el R3 están configurados en una topología de malla completa. Todos los routers tienen rutas redundantes hacia diversas redes.
- El R2 es el router perimetral y se conecta con el ISP. Sin embargo, no se anuncia una ruta estática predeterminada.
- Se configuró EIGRP para IPv6 en los tres routers.

Topología de IPv6 de referencia



La dirección FE80 representa la dirección link-local asignada a cada router.

En la figura 1, se muestra la tabla de routing del R1 mediante el comando **show ipv6 route**. Si bien el resultado del comando se muestra de manera levemente distinta de como se muestra en la versión IPv4, aún contiene la información importante de la ruta.

En la figura 2, se destacan la red conectada y las entradas en la tabla de routing local de las interfaces conectadas directamente. Las tres entradas se agregaron cuando las interfaces se configuraron y activaron.

Como se muestra en la figura 3, en las entradas de las rutas conectadas directamente se muestra la siguiente información:

- **Origen de la ruta:** identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de ruta ("C" identifica una red conectada directamente, mientras que "L" identifica que esta es una ruta local).
- **Red conectada directamente:** la dirección IPv6 de la red conectada directamente.
- **Distancia administrativa:** identifica la confiabilidad del origen de la ruta. IPv6 utiliza las mismas distancias que IPv4. El valor 0 indica el mejor origen y el más confiable.
- **Métrica:** identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Interfaz de salida:** identifica la interfaz de salida que se utiliza para reenviar paquetes a la red de destino.

Nota: los enlaces seriales tienen anchos de banda de referencia configurados para observar la forma en que las métricas de EIGRP seleccionan la mejor ruta. El ancho de banda de referencia no es una representación realista de las redes modernas. Se utiliza solamente para proporcionar una idea visual de la velocidad del enlace.

Tabla de routing IPv6 del R1

```
R1# show ipv6 route
<resultado omitido>

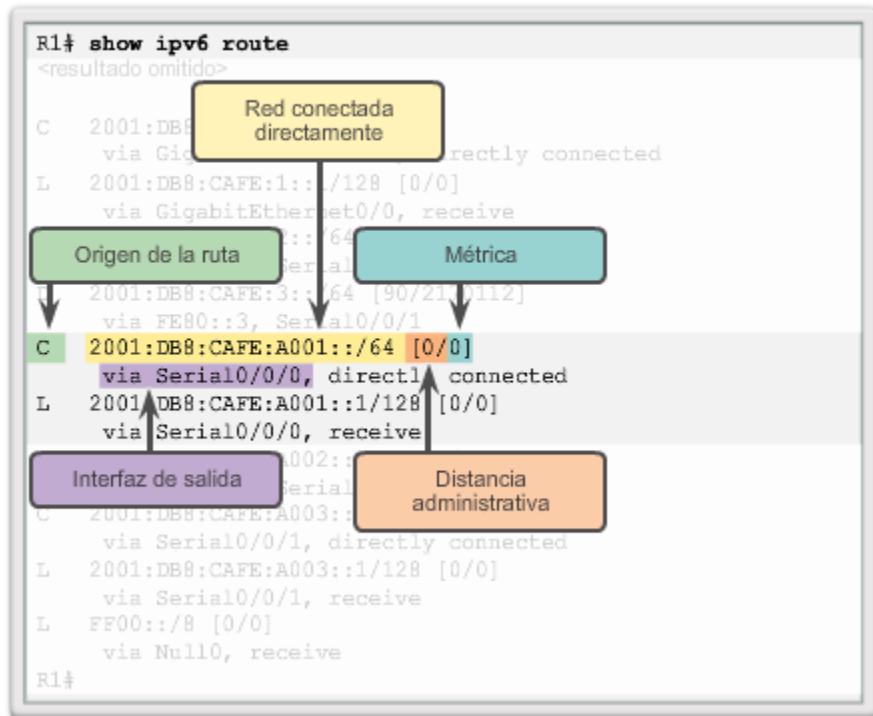
C 2001:DB8:CAFE:1::/64 [0/0]
    via GigabitEthernet0/0, directly connected
L 2001:DB8:CAFE:1::1/128 [0/0]
    via GigabitEthernet0/0, receive
D 2001:DB8:CAFE:2::/64 [90/3524096]
    via FE80::3, Serial0/0/1
D 2001:DB8:CAFE:3::/64 [90/2170112]
    via FE80::3, Serial0/0/1
C 2001:DB8:CAFE:A001::/64 [0/0]
    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#
```

Rutas conectadas directamente en el 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#
```

Rutas conectadas directamente en el R1



En la figura 1, se destacan las entradas de la tabla de routing para las tres redes remotas (es decir, la LAN del R2, la LAN del R3 y el enlace entre el R2 y el R3). Las tres entradas se agregaron mediante EIGRP.

En la figura 2, se muestra una entrada de la tabla de routing en el R1 para la ruta hacia la red remota 2001:DB8:CAFE:3::/64 en el R3. La entrada indica la siguiente información:

- **Origen de la ruta**: identifica el modo en que se descubrió la ruta. Los códigos comunes incluyen O (OSPF), D (EIGRP), R (RIP) y S (ruta estática).
- **Red de destino**: identifica la dirección de la red IPv6 remota.
- **Distancia administrativa**: identifica cuán confiable es el origen de la ruta. IPv6 utiliza las mismas distancias que IPv4.
- **Métrica**: identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- **Siguiente salto**: identifica la dirección IPv6 del router siguiente al que se debe reenviar el paquete.
- **Interfaz de salida**: identifica la interfaz de salida que se debe utilizar para reenviar un paquete hacia el destino final.

Cuando un paquete IPv6 llega a una interfaz del router, el router analiza el encabezado de IPv6 e identifica la dirección IPv6 de destino. A continuación, el router continúa con el proceso de búsqueda del siguiente router.

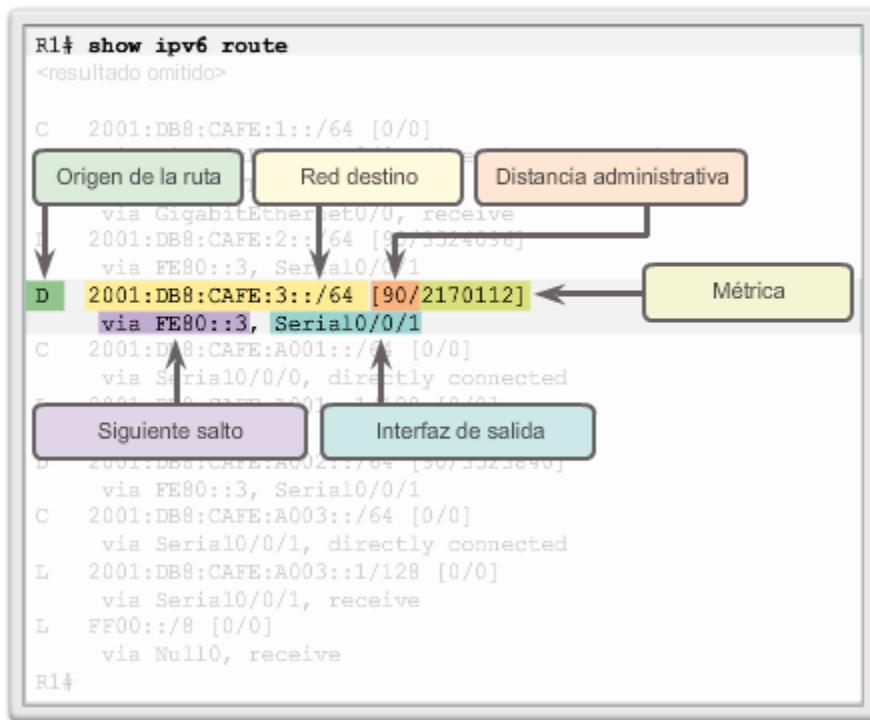
El router examina las rutas de red de nivel 1 en busca de la mejor coincidencia con la dirección de destino del paquete IPv6. Al igual que en IPv4, la coincidencia más larga es la mejor coincidencia. Por ejemplo, si hay varias coincidencias en la tabla de routing, el router elige la ruta con la coincidencia más larga. La coincidencia se encuentra entre los bits del extremo izquierdo de la dirección IPv6 de destino del paquete y el prefijo IPv6 y la duración de prefijo en la tabla de routing IPv6.

Entradas de redes remotas en el 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#
```

Entradas de redes remotas en el R1



7.7 Resumen

Los routers utilizan protocolos de routing dinámico para facilitar el intercambio de información de routing entre ellos. El propósito de los protocolos de routing dinámico incluye lo siguiente: detección de redes remotas, mantenimiento de información de routing actualizada, selección de la mejor ruta hacia las redes de destino y capacidad para encontrar una mejor ruta nueva si la ruta actual deja de estar disponible. Si bien los protocolos de routing dinámico requieren menos sobrecarga administrativa que el routing estático, requieren 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.

Las redes generalmente utilizan una combinación de routing estático y dinámico. El routing dinámico es la mejor opción para las redes grandes, y el routing estático es más adecuado para las redes de rutas internas.

Los protocolos de routing se encargan de detectar redes remotas y de mantener información de red precisa. Cuando se produce un cambio en la topología, los protocolos de routing propagan esa información por todo el dominio de routing. El proceso para lograr que todas las tablas de routing alcancen un estado de coherencia, en el cual todos los routers en el mismo dominio o área de routing tienen información completa y precisa acerca de la red, se denomina "convergencia". Algunos protocolos de routing convergen más rápido que otros.

Los protocolos de routing pueden clasificarse como con clase o sin clase, vector distancia o estado de enlace, y protocolo de gateway interior o protocolo de gateway exterior.

Los protocolos vector distancia utilizan routers como "letreros" a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para

llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento vector distancia no tienen un mapa en sí de la topología de la red.

Un router configurado con un protocolo de routing de estado de enlace puede crear una “vista completa” o una topología de la red al reunir información proveniente de todos los demás routers.

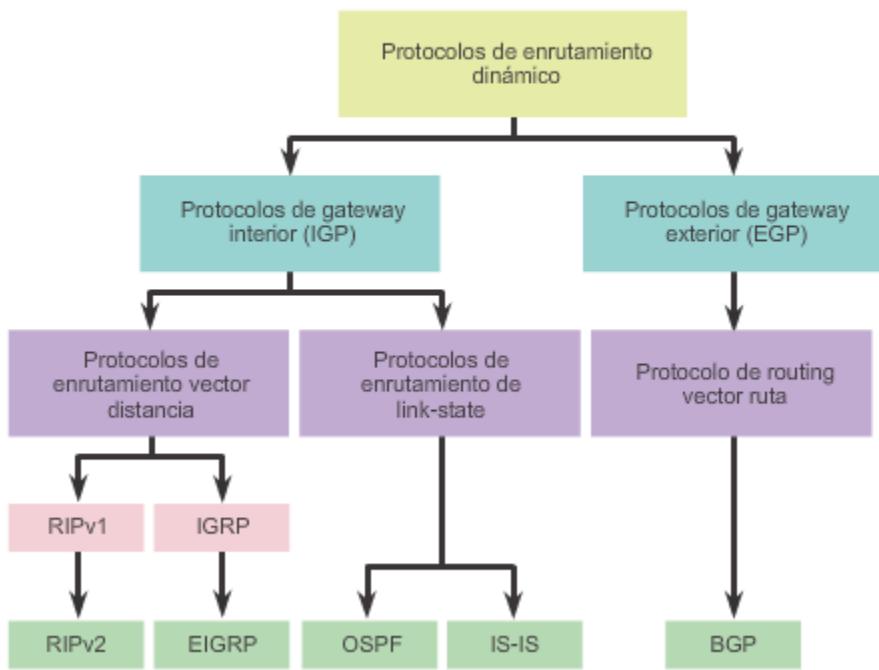
Los protocolos de enrutamiento usan métricas para determinar el mejor camino o la ruta más corta para llegar a una red de destino. Diferentes protocolos de enrutamiento pueden usar diferentes métricas. Por lo general, una métrica inferior indica un mejor camino. Las métricas se pueden determinar mediante los saltos, el ancho de banda, el retraso, la confiabilidad y la carga.

Los routers a veces obtienen información sobre múltiples rutas hacia la misma red a partir de rutas estáticas como de protocolos de enrutamiento dinámico. Cuando un router aprende sobre una red de destino desde más de un origen de enrutamiento, los routers Cisco usan el valor de distancia administrativa para determinar qué origen usar. Cada protocolo de enrutamiento dinámico tiene un valor administrativo único junto con las rutas estáticas y las redes conectadas directamente. Cuanto menor es el valor administrativo, mayor es la preferencia del origen de ruta. Una red conectada directamente es siempre el origen preferido, seguido de las rutas estáticas y luego los diversos protocolos de enrutamiento dinámico.

El comando **show ip protocols** muestra los parámetros del protocolo de routing IPv4 configurados actualmente en el router. Para IPv6, utilice **show ipv6 protocols**.

En los protocolos de routing de estado de enlace, como OSPF, un enlace es una interfaz en un router. La información acerca del estado de dichos enlaces se conoce como estados de enlace. Todos los protocolos de routing de estado de enlace aplican el algoritmo de Dijkstra para calcular la mejor ruta. A este algoritmo se le llama comúnmente “algoritmo SPF” (Shortest Path First). Para determinar el costo total de una ruta, este algoritmo utiliza costos acumulados a lo largo de cada ruta, de origen a destino.

Clasificación de los protocolos de routing



8 OSPF de área única

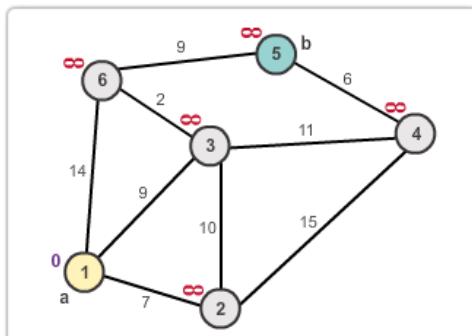
8.1 Introducción

El protocolo OSPF (Open Shortest Path First) es un protocolo de routing de estado de enlace desarrollado como reemplazo del protocolo de routing vector distancia RIP. Durante los comienzos de la tecnología de redes y de Internet, RIP era un protocolo de routing aceptable. Sin embargo, el hecho de que RIP dependiera del conteo de saltos como única métrica para determinar la mejor ruta rápidamente se volvió problemático. El uso del conteo de saltos no escala bien en redes más grandes con varias rutas de distintas velocidades. OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.

OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad. En este capítulo, se abordan las implementaciones y configuraciones básicas de OSPF de área única.

Después de completar este capítulo, podrá hacer lo siguiente:

- Explicar el proceso mediante el cual los routers de estado de enlace descubren otras redes.
- Describir los tipos de paquetes que usan los routers IOS de Cisco para establecer y mantener una red OSPF.
- Explicar la forma en que los routers IOS de Cisco logran la convergencia en una red OSPF.
- Configurar una ID de router OSPF.
- Configurar OSPFv2 de área única en una red IPv4 enrutada pequeña.
- Explicar la forma en que OSPF usa el costo para determinar la mejor ruta.
- Verificar OSPFv2 de área única en una red enrutada pequeña.
- Comparar las características y las operaciones de OSPFv2 y OSPFv3.
- Configurar OSPFv3 de área única en una red enrutada pequeña.
- Verificar OSPFv3 de área única en una red enrutada pequeña.



OSPF es un protocolo que utiliza el costo como métrica.

8.2 Características de OSPF

8.2.1 Open Shortest Path First

Como se muestra en la figura 1, OSPF versión 2 (OSPFv2) se encuentra disponible para IPv4, mientras que OSPF versión 3 (OSPFv3) se encuentra disponible para IPv6.

El desarrollo inicial de OSPF comenzó en 1987 por parte del grupo de trabajo de OSPF, el Grupo de trabajo de ingeniería de Internet (IETF). En aquel momento, Internet era fundamentalmente una red académica y de investigación financiada por el gobierno de los EE. UU .

En 1989, se publicó la especificación para OSPFv1 en RFC 1131. Se escribieron dos implementaciones. Una implementación se desarrolló para ejecutarse en routers, y la otra se desarrolló para ejecutarse en estaciones de trabajo UNIX. Esta última implementación se convirtió en un proceso UNIX generalizado que se conoce como GATED. OSPFv1 era un protocolo de routing experimental y nunca se implementó.

En 1991, John Moy introdujo OSPFv2 en RFC 1247. OSPFv2 ofrecía significativas mejoras técnicas con respecto a OSPFv1. Por su diseño, es un protocolo sin clase, de modo que admite VLSM y CIDR.

Al mismo tiempo que se presentó OSPF, ISO trabajaba en un protocolo de routing de estado de enlace propio, Intermediate System-to-Intermediate System (IS-IS). El IETF eligió OSPF como protocolo de gateway interior (IGP) recomendado.

En 1998, se actualizó la especificación OSPFv2 en RFC 2328, que en la actualidad sigue siendo la RFC para OSPF.

En 1999, OSPFv3 para IPv6 se publicó en RFC 2740. OSPF para IPv6, creado por John Moy, Rob Coltun y Dennis Ferguson, no solo es una nueva implementación de protocolo para IPv6, sino también una importante reforma del funcionamiento del protocolo.

En 2008, se actualizó OSPFv3 en RFC 5340 como OSPF para IPv6.

Nota: en este capítulo, a menos que se identifique explícitamente como OSPFv2 u OSPFv3, el término OSPF se utiliza para indicar conceptos que comparten ambas versiones.

Protocolos de routing de gateway interior

	Protocolos de gateway interior				Protocolos de gateway exterior
	Vector distancia		Estado de enlace	Vector ruta	
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP para IPv6	OSPFv3	IS-IS para IPv6	BGP-MP

Las características de OSPF, las cuales se muestran en la figura 1, incluyen lo siguiente:

- **Sin clase:** por su diseño, es un protocolo sin clase, de modo que admite VLSM y CIDR.
- **Eficaz:** los cambios de routing dirigen 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 tamaños de redes pequeños 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.

La distancia administrativa (AD) es la confiabilidad (o preferencia) del origen de la ruta. OSPF tiene una distancia administrativa predeterminada de 110. Como se muestra en la figura 2, se prefiere OSPF a IS-IS y RIP.



Distancia administrativa de OSPF

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

Todos los protocolos de routing comparten componentes similares. Todos usan mensajes de protocolo de routing para intercambiar información de la ruta. Los mensajes contribuyen a armar estructuras de datos, que luego se procesan con un algoritmo de routing.

Los tres componentes principales del protocolo de routing OSPF incluyen lo siguiente:

Estructuras de datos

OSPF crea y mantiene tres bases de datos (consulte la figura 1):

- **Base de datos de adyacencia:** crea la tabla de vecinos.
- **Base de datos de estado de enlace (LSDB):** crea la tabla de topología.
- **Base de datos de reenvío:** crea la tabla de routing.

Estas tablas contienen una lista de routers vecinos para intercambiar información de routing, y se guardan y mantienen en la RAM.

Mensajes de protocolo de routing

OSPF intercambia mensajes para transmitir información de routing mediante cinco tipos de paquetes. Estos paquetes, los cuales se muestran en la figura 2, son los siguientes:

- Paquete de saludo
- Paquete de descripción de la base de datos
- Paquete de solicitud de estado de enlace
- Paquete de actualización de estado de enlace
- Paquete de acuse de recibo de estado de enlace

Estos paquetes se usan para descubrir routers vecinos y también para intercambiar información de routing a fin de mantener información precisa acerca de la red.

Algoritmo

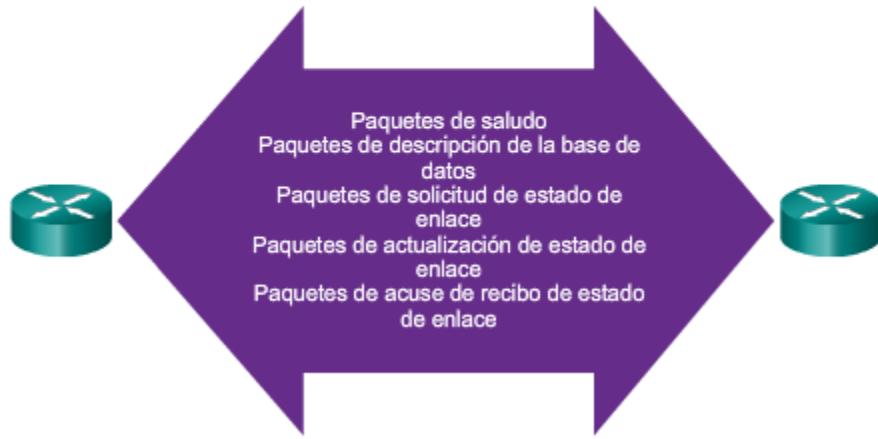
La CPU procesa las tablas de vecinos y de topología mediante el algoritmo SPF de Dijkstra. El algoritmo SPF se basa en el costo acumulado para llegar a un destino.

El algoritmo SPF crea un árbol SPF posicionando cada router en la raíz del árbol y calculando la ruta más corta hacia cada nodo. Luego, el árbol SPF se usa para calcular las mejores rutas. OSPF coloca las mejores rutas en la base de datos de reenvío, que se usa para crear la tabla de routing.

Estructuras de datos OSPF

Base de datos	Tabla	Descripción
Base de datos de adyacencia	Tabla de vecinos	<ul style="list-style-type: none"> Lista de todos los routers vecinos con los que un router estableció comunicación bidireccional. Esta tabla es única para cada router. Se puede ver con el comando <code>show ip ospf neighbor</code>.
Base de datos de estado de enlace (LSDB)	Tabla de topología	<ul style="list-style-type: none"> Muestra información sobre todos los otros routers en la red. Esta base de datos representa la topología de la red. Todos los routers dentro de un área tienen LSDB idénticas. Se puede ver con el comando <code>show ip ospf database</code>.
Base de datos de reenvío	Tabla de enrutamiento	<ul style="list-style-type: none"> Lista de rutas generada cuando se ejecuta un algoritmo en la base de datos de estado de enlace. La tabla de routing de cada router es única y contiene información sobre cómo y dónde enviar paquetes para otros routers. Se puede ver con el comando <code>show ip route</code>.

Los routers OSPF intercambian paquetes



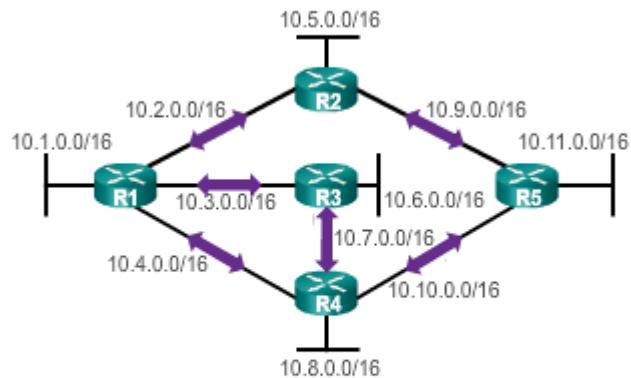
A fin de mantener la información de routing, los routers OSPF realizan el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia:

1. Establecimiento de las adyacencias de vecinos (figura 1): los routers con OSPF habilitado deben reconocerse entre sí en la red antes de poder compartir información. Los routers con OSPF habilitado envían paquetes de saludo por todas las interfaces con OSPF habilitado para determinar si hay vecinos presentes en esos enlaces. Si se detecta un vecino, el router con OSPF habilitado intenta establecer una adyacencia de vecino con ese vecino.
2. Intercambio de notificaciones de estado de enlace (figura 2): una vez que se establecen las adyacencias, los routers intercambian notificaciones de estado de enlace (LSA). Las LSA contienen el estado y el costo de cada enlace conectado directamente. Los routers saturan a los vecinos adyacentes con sus LSA. Los vecinos adyacentes que reciben las LSA saturan de inmediato a otros vecinos conectados directamente, hasta que todos los routers en el área tengan todas las LSA.
3. Creación de la tabla de topología (figura 3): una vez que se reciben las LSA, los routers con OSPF habilitado crean la tabla de topología (LSDB) sobre la base de las LSA recibidas. Finalmente, esta base de datos contiene toda la información sobre la topología de la red.
4. Ejecución del algoritmo SPF (figuras 4 y 5): a continuación, los routers ejecutan el algoritmo SPF. Los engranajes que se muestran en la ilustración se utilizan para indicar la ejecución del algoritmo SPF. El algoritmo SPF crea el árbol SPF.

En la figura 6, se muestra el contenido del árbol SPF del R1.

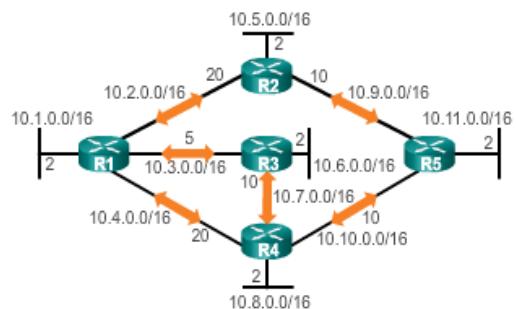
Las mejores rutas del árbol SPF se insertan en la tabla de routing. Las decisiones de routing se toman sobre la base de las entradas de la tabla de routing.

Los routers intercambian paquetes de saludo



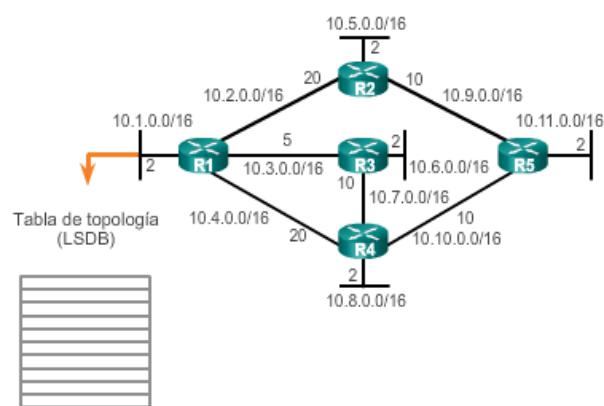
Paquetes de saludo

Los routers intercambian LSA

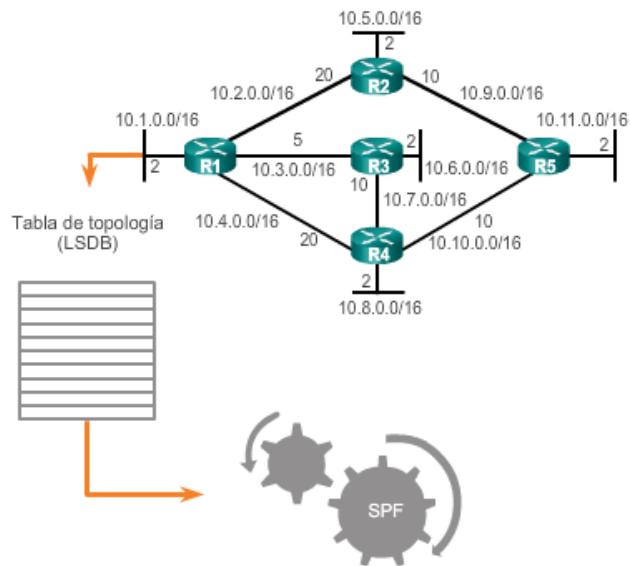


LSA

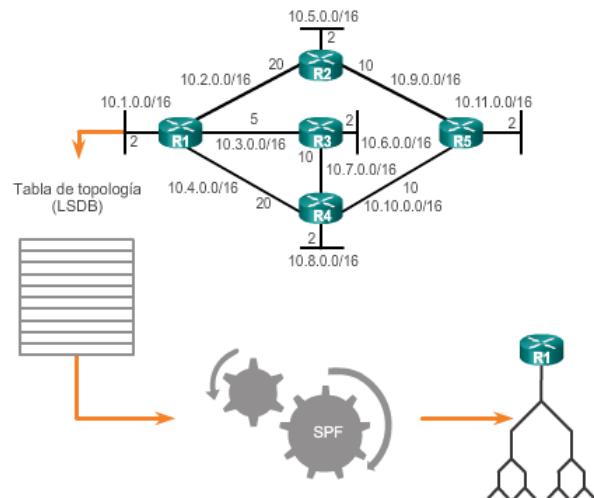
El R1 crea su base de datos topológica

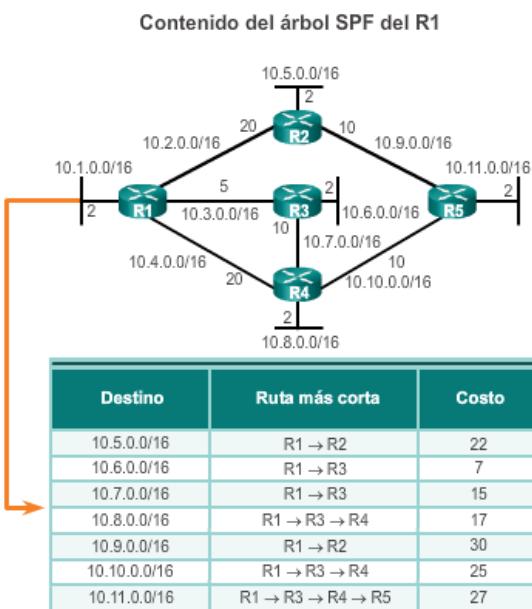


El R1 ejecuta el algoritmo SPF



El R1 crea el árbol SPF





Para que OSPF sea más eficaz y escalable, este protocolo admite el routing jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB.

OSPF se puede implementar de dos maneras:

- **OSPF de área única:** en la figura 1, todos los routers se encuentran en un área llamada “área backbone” (área 0).
- **OSPF multiárea:** en la figura 2, OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área backbone (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR).

Con OSPF multiárea, OSPF puede dividir un sistema autónomo (AS) grande en áreas más pequeñas, a fin de admitir el routing jerárquico. Con el routing jerárquico, se sigue produciendo el routing entre áreas, y muchas de las operaciones de routing que implican una gran exigencia para el procesador, como volver a calcular la base de datos, se guardan en un área.

Por ejemplo, cada vez que un router recibe información nueva acerca de un cambio de topología dentro del área (como el agregado, 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.

Nota: los cambios de topología se distribuyen a los routers de otras áreas en formato vector distancia. En otras palabras, estos routers solo actualizan sus tablas de routing y no necesitan volver a ejecutar el algoritmo SPF.

Si hubiera demasiados routers en un área, la LSDB sería muy 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.

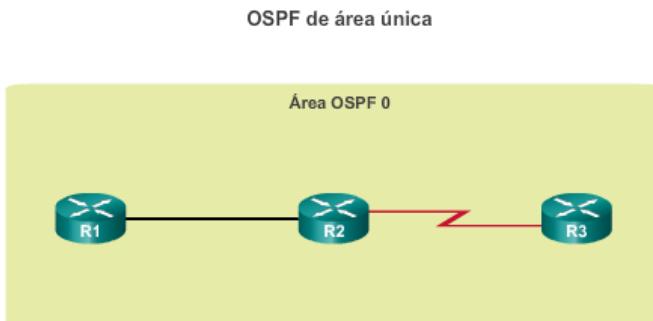
Las posibilidades de topología jerárquica de OSPF multiárea presentan las siguientes ventajas:

- **Tablas de routing más pequeñas:** se crean menos entradas de tabla de routing, ya que las direcciones de red pueden resumirse entre áreas. La sumarización de ruta no está habilitada de manera predeterminada.
- **Menor sobrecarga de actualización de estado de enlace:** minimiza los requisitos de procesamiento y memoria.
- **Menor frecuencia de cálculos de SPF:** localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de las actualizaciones de routing debido a que la saturación con LSA se detiene en el límite del área.

En la figura 3, se ilustran estas ventajas.

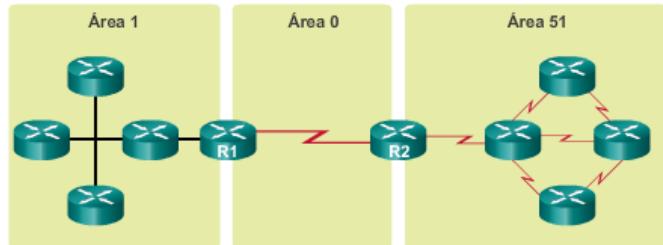
Por ejemplo, el R2 es un ABR para el área 51. Como ABR, resumiría las rutas del área 51 en el área 0. Cuando uno de los enlaces resumidos falla, las LSA se intercambian solo dentro del área 51. Los routers del área 51 deben volver a ejecutar el algoritmo SPF para identificar las mejores rutas. Sin embargo, los routers del área 0 y el área 1 no reciben ninguna actualización, motivo por el cual no ejecutan el algoritmo SPF.

Este capítulo se centra en OSPF de área única.



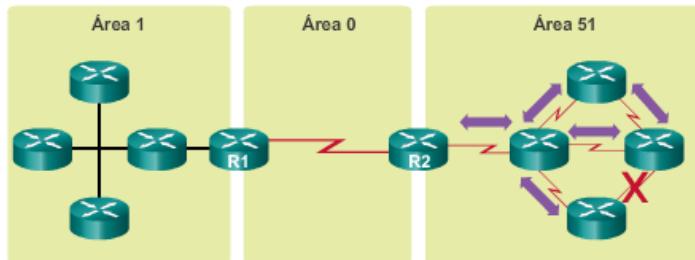
- El área 0 también se denomina "área backbone".
- OSPF de área única es útil en redes más pequeñas con pocos routers.

OSPF multiárea



- Implementado mediante una jerarquía de área de dos capas, dado que todas las áreas se deben conectar al área backbone (área 0).
- Los routers que interconectan áreas se denominan "routers fronterizos de área" (ABR).
- Útil en implementaciones de redes más grandes para reducir la sobrecarga de procesamiento y memoria.

El cambio de enlace afecta solo el área local



- La falla del enlace afecta solo el área local (área 51).
- El ABR (R2) aísla la falla solo al área 51.
- Los routers en las áreas 0 y 1 no necesitan ejecutar el algoritmo SPF.

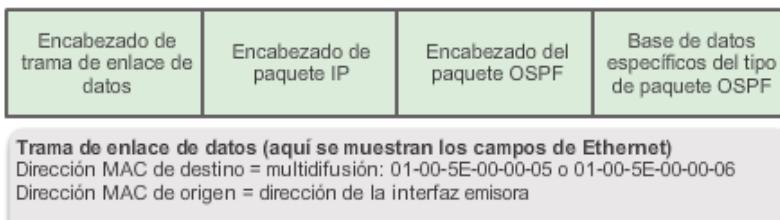
Características de OSPF	Función/descripción
✓ Convergencia rápida	Propaga rápidamente los cambios que se producen en la red.
✓ Sin clase	Admite VLSM y CIDR.
✓ Asegurar	Admite la autenticación MD5.

8.2.2 Mensajes OSPF

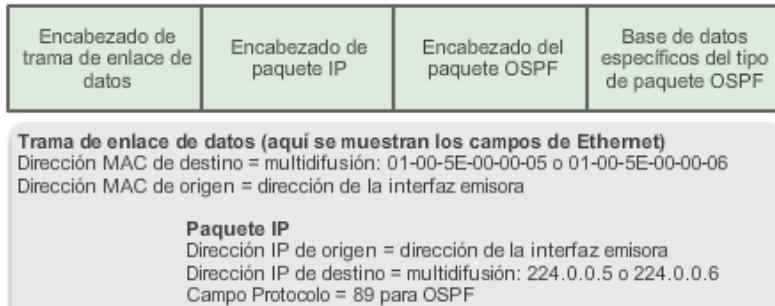
Los mensajes OSPF que se transmiten a través de un enlace Ethernet contienen la siguiente información:

- **Encabezado de la trama de Ethernet de enlace de datos:** identifica las direcciones MAC de multidifusión de destino 01-00-5E-00-00-05 o 01-00-5E-00-00-06. (figura 1)
- **Encabezado del paquete IP:** identifica el campo 89 del protocolo IPv4, que indica que se trata de un paquete OSPF. También identifica una de dos direcciones OSPF de multidifusión, 224.0.0.5 o 224.0.0.6. (Figura 2)
- **Encabezado del paquete OSPF:** identifica el tipo de paquete OSPF, la ID del router y la ID del área. (Figura 3)
- **Datos específicos del tipo de paquete OSPF:** contiene información del tipo de paquete OSPF. El contenido varía según el tipo de paquete. En este caso, se trata de un encabezado de IPv4. (figura 4)

Encabezado de la trama de Ethernet de enlace de datos



Encabezado de paquete IP



Encabezado del paquete OSPF

Encabezado de trama de enlace de datos	Encabezado de paquete IP	Encabezado del paquete OSPF	Base de datos específicos del tipo de paquete OSPF
--	--------------------------	-----------------------------	--

Trama de enlace de datos (aquí se muestran los campos de Ethernet)

Dirección MAC de destino = multidifusión: 01-00-5E-00-00-05 o 01-00-5E-00-00-06

Dirección MAC de origen = dirección de la interfaz emisora

Paquete IP

Dirección IP de origen = dirección de la interfaz emisora

Dirección IP de destino = multidifusión: 224.0.0.5 o 224.0.0.6

Campo Protocolo = 89 para OSPF

Encabezado del paquete OSPF

Código de tipo para el tipo de paquete OSPF

ID del router e ID del área

Campos del encabezado de IPv4 OSPF

Encabezado de trama de enlace de datos	Encabezado de paquete IP	Encabezado del paquete OSPF	Base de datos específicos del tipo de paquete OSPF
--	--------------------------	-----------------------------	--

Trama de enlace de datos (aquí se muestran los campos de Ethernet)

Dirección MAC de destino = multidifusión: 01-00-5E-00-00-05 o 01-00-5E-00-00-06

Dirección MAC de origen = dirección de la interfaz emisora

Paquete IP

Dirección IP de origen = dirección de la interfaz emisora

Dirección IP de destino = multidifusión: 224.0.0.5 o 224.0.0.6

Campo Protocolo = 89 para OSPF

Encabezado del paquete OSPF

Código de tipo para el tipo de paquete OSPF

ID del router e ID del área

Tipos de paquetes OSPF

0x01 Saludo

0x02 Descripción de la base de datos (DD)

0X03 Solicitud de estado de enlace

0X04 Actualización de estado de enlace

0X05 Acuse de recibo de estado de enlace

OSPF utiliza paquetes de estado de enlace (LSP) para establecer y mantener adyacencias de vecinos, así como para intercambiar actualizaciones de routing.

En la ilustración, se muestran los cinco tipos de LSP que usa OSPF. Cada paquete cumple una función específica en el proceso de enrutamiento de OSPF:

- **Tipo 1, paquete de saludo:** se usa para establecer y mantener la adyacencia con otros routers OSPF.
- **Tipo 2, paquete de descripción de base de datos (DBD):** contiene una lista abreviada de la LSDB del router emisor, y los routers receptores la usan para compararla con la LSDB local. Para crear un árbol SPF preciso, la LSDB debe ser idéntica en todos los routers de estado de enlace dentro de un área.
- **Tipo 3, paquete de solicitud de estado de enlace (LSR):** los routers receptores pueden requerir más información sobre cualquier entrada de la DBD mediante el envío de un LSR.

- **Tipo 4, paquete de actualización de estado de enlace (LSU):** se utiliza para responder a los LSR y anunciar la nueva información. Los LSU contienen siete tipos de LSA.
- **Tipo 5, paquete de acuse de recibo de estado de enlace (LSAck):** cuando se recibe una LSU, el router envía un LSAck para confirmar la recepción de la LSU. El campo de datos del LSAck está vacío.

Descripciones de los paquetes OSPF

Tipo	Nombre del paquete	Descripción
1	Hola	Descubre los vecinos y construye adyacencias entre ellos
2	Descriptores de bases de datos (DBD)	Controla la sincronización de bases de datos entre routers.
3	solicitud de link-state (LSR)	Solicita registros específicos de estado de enlace de router a router
4	Actualización de link-state (LSU)	Envía los registros de estado de enlace específicamente solicitados
5	Acuse de recibo de estado de enlace (LSAck)	Reconoce los demás tipos de paquetes

Paquete de saludo

El paquete OSPF de tipo 1 es el paquete de saludo. Los paquetes de saludo se utilizan para:

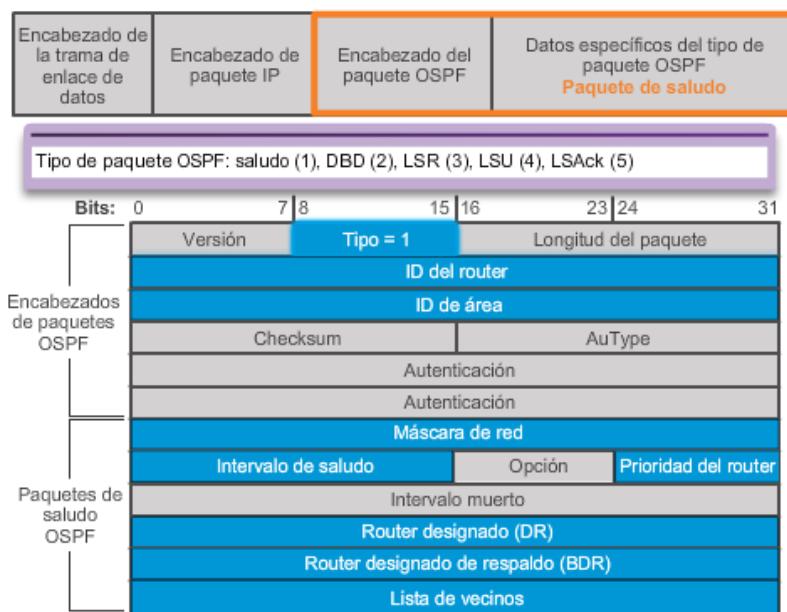
- Descubrir vecinos OSPF y establecer adyacencias de vecinos.
- Publicar parámetros en los que dos routers deben acordar convertirse en vecinos.
- Elegir el Router designado (DR) y el Router designado de respaldo (BDR) en redes de accesos múltiples, como Ethernet y Frame Relay. Los enlaces punto a punto no requieren DR o BDR.

En la ilustración, se muestran los campos contenidos en el paquete de tipo 1, el paquete de saludo. Los campos importantes que se muestran en la figura incluyen:

- **Tipo:** identifica el tipo de paquete. Un uno (1) indica un paquete de saludo. Un valor de 2 identifica un paquete DBD, un valor de 3 identifica un paquete LSR, un valor de 4 identifica un paquete LSU, y un valor de 5 identifica un paquete LSAck.
- **ID del router:** un valor de 32 bits expresado en notación decimal con puntos (una dirección IPv4) que se utiliza para identificar exclusivamente el router de origen.
- **ID de área:** el área en la cual se originó el paquete.
- **Máscara de red:** la máscara de subred asociada a la interfaz emisora.
- **Intervalo de saludo:** especifica la frecuencia, en segundos, a la que un router envía paquetes de saludo. El intervalo de saludo predeterminado en redes de accesos múltiples es de 10 segundos. Este temporizador debe ser el mismo en los routers vecinos; de lo contrario, no se establece ninguna adyacencia.

- **Prioridad del router:** se utiliza en una elección de DR/BDR. La prioridad predeterminada para todos los routers OSPF es 1, pero se puede modificar manualmente desde 0 hasta 255. Cuanto mayor es el valor, mayor es la probabilidad de que el router sea el DR en el enlace.
- **Intervalo muerto:** es el tiempo en segundos que espera un router para establecer comunicación con un vecino antes de declarar que el router vecino no funciona. De manera predeterminada, el intervalo muerto del router es cuatro veces el intervalo de saludo. Este temporizador debe ser el mismo en los routers vecinos; de lo contrario, no se establece ninguna adyacencia.
- **Router designado (DR):** la ID del router del DR.
- **Router designado de respaldo (BDR):** la ID del router del BDR.
- **Lista de vecinos:** la lista en la que se identifican las ID del router de todos los routers adyacentes.

Contenido del paquete de saludo OSPF



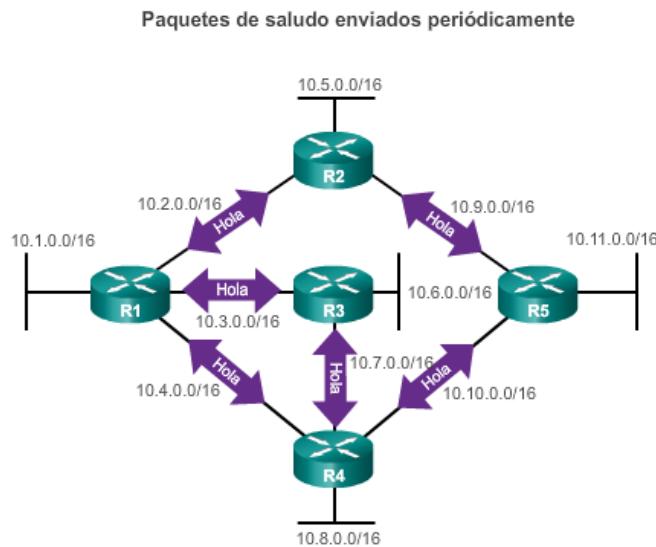
Como se muestra en la ilustración, los paquetes de saludo OSPF se transmiten a la dirección de multidifusión 224.0.0.5 en IPv4 y FF02::5 en IPv6 (todos los routers OSPF) cada:

- 10 segundos (intervalo predeterminado en redes de accesos múltiples y punto a punto)
- 30 segundos (intervalo predeterminado en redes multiacceso sin difusión [NBMA], por ejemplo, Frame Relay)

El intervalo muerto es el período que el router espera para recibir un paquete de saludo antes de declarar al vecino como inactivo. Si el intervalo muerto caduca antes de que los routers reciban un paquete de saludo, OSPF elimina ese vecino de su LSDB. El router satura la LSDB con información acerca del vecino inactivo por todas las interfaces con OSPF habilitado.

Cisco utiliza un intervalo predeterminado de cuatro veces el intervalo de saludo:

- 40 segundos (intervalo predeterminado en redes de accesos múltiples y punto a punto)
- 120 segundos (intervalo predeterminado en redes NBMA, por ejemplo, Frame Relay).



Los routers inicialmente intercambian paquetes DBD de tipo 2, que son una lista abreviada de la LSDB del router emisor que los routers receptores usan para compararla con la LSDB local.

Los routers receptores usan paquetes LSR de tipo 3 para solicitar más información acerca de una entrada de la DBD.

El paquete LSU de tipo 4 se utiliza para responder a un paquete LSR.

Los paquetes LSU también se usan para reenviar actualizaciones de routing OSPF, como cambios de enlace. Específicamente, un paquete LSU puede contener 11 tipos de LSA OSPFv2, como se muestra en la ilustración. OSPFv3 cambió el nombre de varias de estas LSA y también contiene dos LSA adicionales.

Nota: en ocasiones, la diferencia entre los términos LSU y LSA puede resultar confusa, ya que estos términos a menudo se usan de manera indistinta. Sin embargo, una LSU contiene una o más LSA.

Las LSU contienen LSA

Tipo	Nombre del paquete	Descripción
1	Hola	Descubre los vecinos y construye adyacencias entre ellos
2	DBD	Controla la sincronización de bases de datos entre routers.
3	LSR	Solicita registros específicos de estado de enlace de router a router
4	LSU	Envía los registros de estado de enlace específicamente solicitados
5	LSAck	Reconoce los demás tipos de paquetes

- Una LSU contiene uno o más LSA.
- Los LSA contienen información de la ruta para las redes de destino.

Tipo de LSA	Descripción
1	LSA de router
2	LSA de red
3 o 4	LSA de resumen
5	LSA externos del sistema autónomo
6	LSA de OSPF multicast
7	Definido para áreas no tan llenas
8	LSA de atributos externos para el protocolo de gateway fronterizo (BGP)
9, 10, 11	LSA opacas

Solicita registros específicos de estado de enlace de router a router.

✓ solicitud de link-state (LSR)

Envía los registros de estado de enlace específicamente solicitados

✓ Actualización de link-state (LSU)

Descubre los vecinos y construye adyacencias entre ellos

✓ Hola

8.2.3 Funcionamiento de OSPF

Cuando un router OSPF se conecta inicialmente a una red, intenta hacer lo siguiente:

- Crear adyacencias con los vecinos
- Intercambiar información de routing
- Calcular las mejores rutas
- Lograr la convergencia

Al intentar lograr la convergencia, OSPF atraviesa varios estados:

- Estado Down
- Estado Init
- Estado Two-Way
- Estado ExStart

- Estado Exchange
- Estado Loading
- Estado Full



Cuando se habilita OSPF en una interfaz, el router debe determinar si existe otro vecino OSPF en el enlace. Para hacerlo, el router reenvía un paquete de saludo con la ID del router por todas las interfaces con OSPF habilitado. El proceso OSPF utiliza la ID del router OSPF para identificar cada router en el área OSPF de manera exclusiva. Una ID de router es una dirección IP asignada para identificar un router específico entre peers OSPF.

Cuando un router vecino con OSPF habilitado recibe un paquete de saludo con una ID de router que no figura en su lista de vecinos, el router receptor intenta establecer una adyacencia con el router que inició la comunicación.

Consulte el R1 de la figura 1. Cuando se habilita OSPF, la interfaz Gigabit Ethernet 0/0 habilitada pasa del estado Down al estado Init. El R1 comienza a enviar paquetes de saludo por todas las interfaces con OSPF habilitado para descubrir vecinos OSPF a fin de desarrollar adyacencias con ellos.

En la figura 2, el R2 recibe el paquete de saludo del R1 y agrega la ID del router R1 a su lista de vecinos. A continuación, el R2 envía un paquete de saludo al R1. El paquete contiene la ID del router R2 y la ID del router R1 en la lista de vecinos de la misma interfaz.

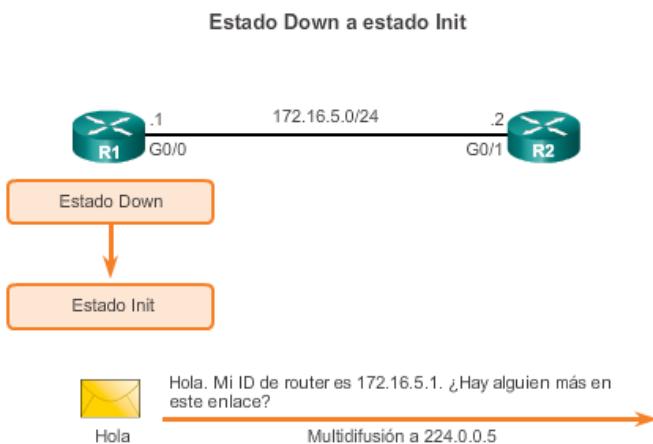
En la figura 3, el R1 recibe el saludo y agrega la ID del router R2 a su lista de vecinos OSPF. También advierte su propia ID de router en la lista de vecinos del paquete de saludo. Cuando un router recibe un paquete de saludo en el que se indica su ID de router en la lista de vecinos, el router pasa del estado Init al estado Two-Way.

La acción realizada en el estado Two-Way depende del tipo de interconexión de los routers adyacentes:

- Si los dos vecinos adyacentes se interconectan a través de un enlace punto a punto, pasan de inmediato del estado Two-Way a la fase de sincronización de bases de datos.
- Si los routers se interconectan a través de una red Ethernet común, se debe elegir un router designado DR y un BDR.

Debido a que el R1 y el R2 se interconectan a través de una red Ethernet, se elige un DR y un BDR. Como se muestra en la figura 4, el R2 se convierte en el DR, y el R1 es el BDR. Este proceso tiene lugar solo en las redes de accesos múltiples, como las LAN Ethernet.

Los paquetes de saludo se intercambian de manera continua para mantener la información del router.



¿Por qué se necesita elegir un DR y un BDR?

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 LSA cada vez que se inicializa OSPF o cuando se produce un cambio en la topología. Esta saturación puede llegar a ser excesiva.

Para comprender el problema de las adyacencias múltiples, se debe estudiar una fórmula:

Para cualquier cantidad de routers (designada como n) en una red de accesos múltiples, hay $n(n - 1) / 2$ adyacencias.

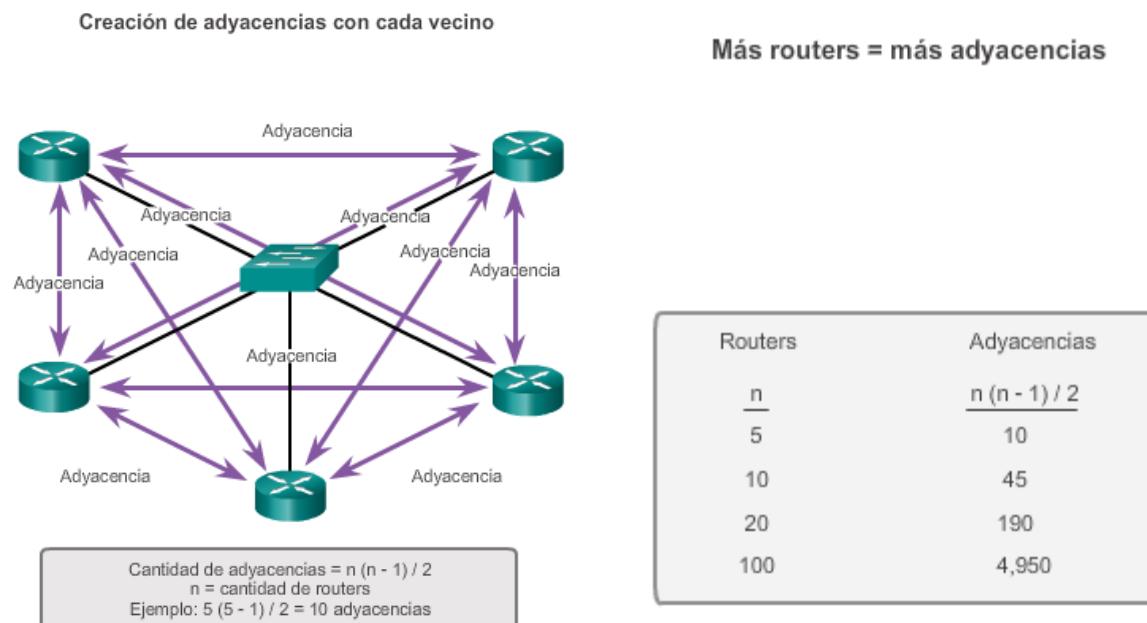
En la figura 1, se muestra una topología simple de cinco routers, los cuales están conectados a la misma red Ethernet de accesos múltiples. Sin ningún tipo de mecanismo para reducir la cantidad de adyacencias, estos routers en forma colectiva formarán 10 adyacencias:

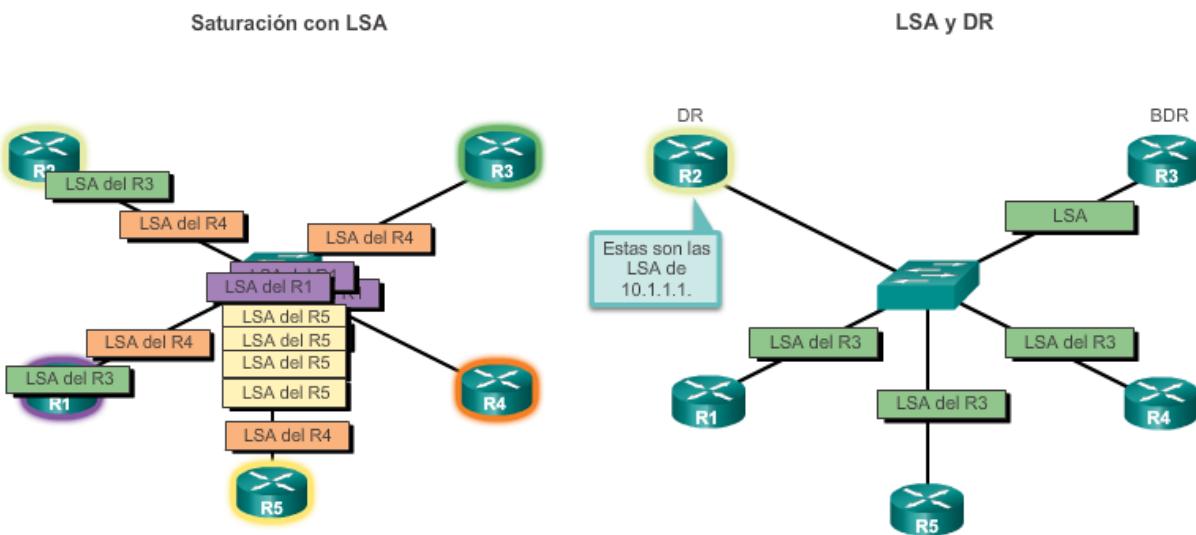
$$5 (5 - 1) / 2 = 10$$

Puede parecer poco, pero a medida que se agregan routers a la red, la cantidad de adyacencias aumenta notablemente, como se muestra en la figura 2.

Para comprender el problema de la saturación intensa con LSA, reproduzca la animación de la figura 3. En la animación, el R2 envía una LSA. Este evento hace que cada router también envíe una LSA. Los acuses de recibo requeridos que se envían por cada LSA recibida no se muestran en la animación. Si cada router en una red de accesos múltiples tuviera que saturar y reconocer todas las LSA recibidas a todos los demás routers en la misma red de accesos múltiples, el tráfico de la red se volvería bastante caótico.

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. Todos los otros routers se convierten en DROTHER. Un DROTHER es un router que no funciona como DR ni como BDR.





Después del estado Two-Way, los routers pasan a los estados de sincronización de bases de datos. Mientras que el paquete de saludo se utilizó para establecer adyacencias de vecinos, los otros cuatro tipos de paquetes OSPF se utilizan durante el proceso de intercambio y sincronización de LSDB.

En el estado ExStart, se crea una relación de maestro y esclavo entre cada router y su DR y su BDR adyacentes. El router con la mayor ID de router funciona como maestro para el estado Exchange. En la figura 1, el R2 se convierte en maestro.

En el estado Exchange, los routers maestros y esclavos intercambian uno o más paquetes DBD. Un paquete DBD incluye información acerca del encabezado de la entrada de LSA que aparece en la LSDB del router. Las entradas pueden hacer referencia a un enlace o a una red. Cada encabezado de entrada de LSA incluye información acerca del tipo de estado de enlace, la dirección del router que realiza el anuncio, el costo del enlace y el número de secuencia. El router usa el número de secuencia para determinar qué tan nueva es la información de estado de enlace recibida.

En la figura 2, el R2 envía un paquete DBD al R1. Cuando el R1 recibe la DBD, realiza las siguientes acciones:

1. Confirma la recepción de la DBD con el paquete LSAck.
2. A continuación, el R1 envía paquetes DBD al R2.
3. El R2 acusa recibo al R1.

El R1 compara la información recibida con la información que tiene en su propia LSDB. Si el paquete DBD tiene una entrada de estado de enlace más actual, el router pasa al estado Loading.

Por ejemplo, en la figura 3, el R1 envía una LSR con respecto a la red 172.16.6.0 al R2. El R2 responde con la información completa sobre 172.16.6.0 en un paquete LSU. Una vez más, cuando

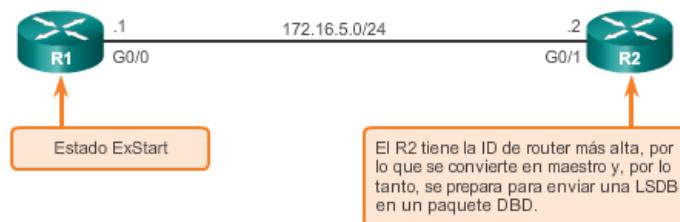
el R1 recibe una LSU, envía un LSAck. A continuación, el R1 agrega las nuevas entradas de estado de enlace a su LSDB.

Después de cumplir con todas las LSR para un router determinado, los routers adyacentes se consideran sincronizados y en estado Full.

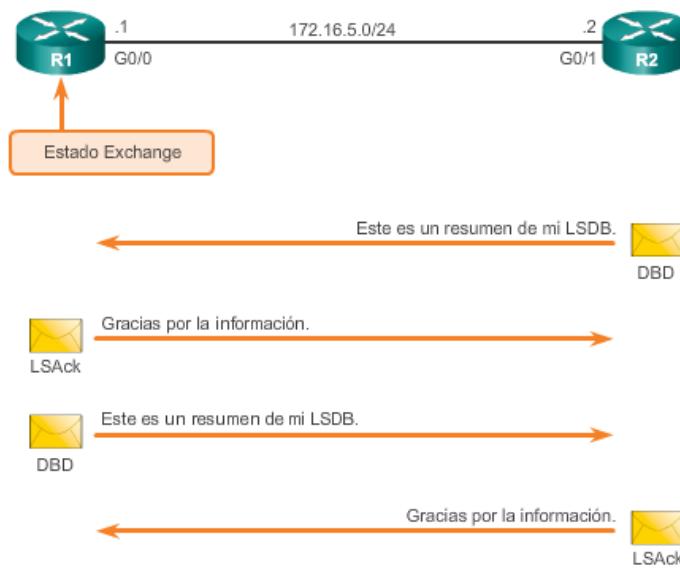
En la medida en que los routers vecinos sigan recibiendo paquetes de saludo, la red en las LSA transmitidas permanece en la base de datos de topología. Una vez que se sincronizan las bases de datos topológicas, se envían actualizaciones (LSU) a los vecinos solo en las siguientes circunstancias:

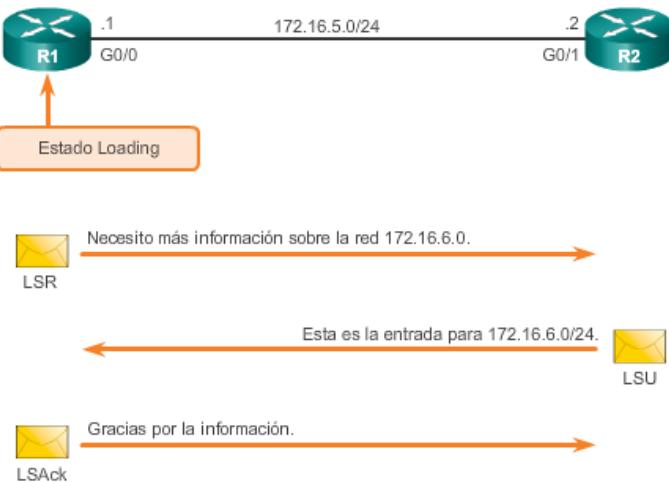
- Cuando se percibe un cambio (actualizaciones incrementales).
- Cada 30 minutos.

Decisión sobre qué router envía la primera DBD



Intercambio de paquetes DBD



Obtención de información adicional de la ruta**Instrucciones de adyacencia OSPF**

- ✓ Estado Two-Way** En los enlaces Ethernet, se elige un router designado (DR) y un router designado de respaldo (BDR).
- ✓ Estado Exchange** Los routers intercambian paquetes DBD.
- ✓ Estado Init** Se reciben los paquetes de saludo de los vecinos con la ID del router emisor.
- ✓ Estado Ex-Start** Se inicia el intercambio de paquetes DBD.

Instrucciones de adyacencia OSPF

- ✓ Estado Full** Los routers convergieron.
- ✓ Estado Down** No se recibió ningún paquete de saludo.
- ✓ Estado Ex-Start** Se negocia la relación de maestro/esclavo y el número de secuencia del paquete DBD..
- ✓ Estado Loading** Las rutas se procesan mediante el algoritmo SPF.

8.3 Configuración de OSPFv2 de área única

8.3.1 ID del router OSPF

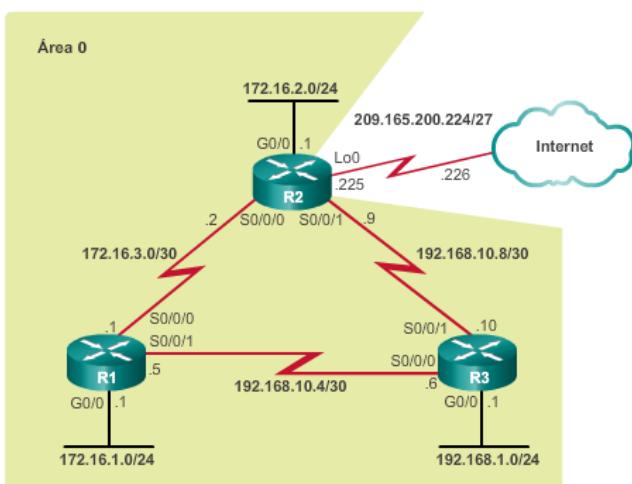
OSPFv2 es un protocolo de routing de estado de enlace para IPv4 que se presentó en 1991. OSPF se diseñó como alternativa a otro protocolo de routing IPv4, RIP.

En la ilustración, se muestra la topología que se usa para configurar OSPFv2 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. 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, incluidas las direcciones de interfaz. 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 backbone de OSPF. El router ISP se usa como gateway del dominio de routing a Internet.

Nota: en esta topología, la interfaz loopback se usa para simular el enlace WAN a Internet.

Topología OSPF de referencia

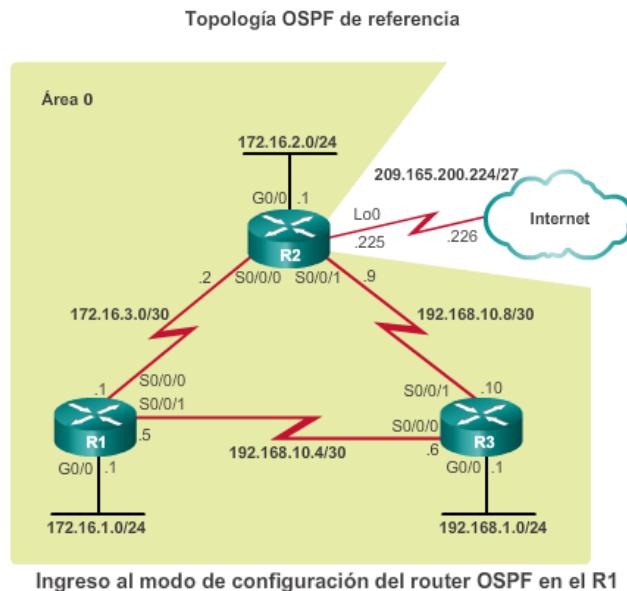


En la figura 1, se muestra la topología de referencia para este tema. OSPFv2 se habilita con el comando **router ospf id-proceso** del modo de configuración global. El valor *id-proceso* representa un número entre 1 y 65 535, y lo elige el administrador de red. El valor *id-proceso* tiene importancia en el ámbito local, lo que significa que no necesita ser el mismo valor en los demás routers OSPF para establecer adyacencias con esos vecinos.

En la figura 2, se proporciona un ejemplo del ingreso al modo de configuración de OSPF del router en el R1.

Nota: la lista de comandos se modificó para que se muestren solo los comandos que se utilizan en este capítulo. Para obtener una lista completa de comandos, utilice los verificadores de sintaxis de la figura 3.

Utilice el verificador de sintaxis de la figura 3 para ingresar al modo de configuración de router OSPF en el R2 y enumerar los comandos disponibles en la petición de entrada.



```
R1(config)# router ospf 10
R1(config-router)# ?
Router configuration commands:
  auto-cost          Calculate OSPF interface cost
                     according to bandwidth
  network            Enable routing on an IP network
  no                Negate a command or set its defaults
  passive-interface Suppress routing updates on an
                     interface
  priority           OSPF topology priority
  router-id          router-id for this OSPF process
```

Nota: se modificó el resultado a fin de mostrar solo los comandos que se utilizarán en este capítulo.

Para participar en un dominio OSPF, cada router requiere una ID de router. La ID del router puede estar definida por un administrador o puede ser asignada en forma automática por el router. El router con OSPF habilitado usa la ID del router para realizar lo siguiente:

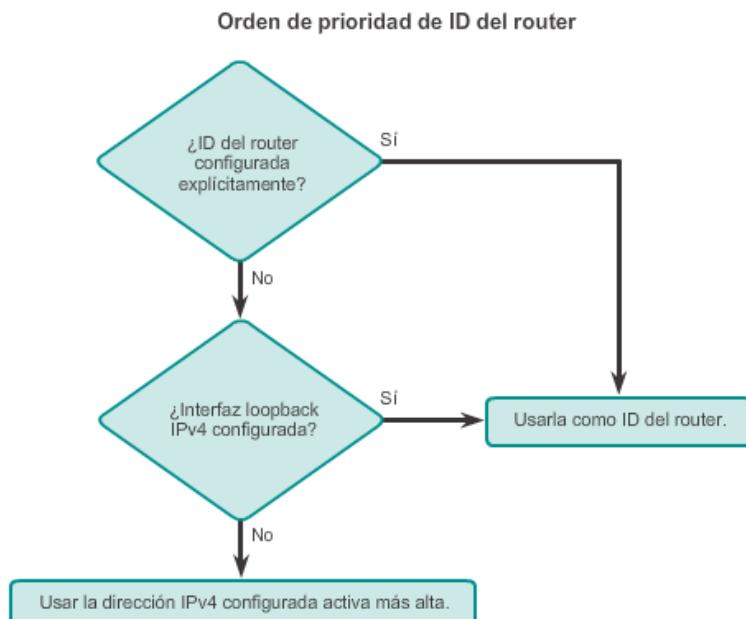
- **Identificar el router de manera exclusiva:** otros routers usan la ID del router para identificar de forma exclusiva cada router dentro del dominio OSPF y todos los paquetes que se originan en ellos.
- **Participar en la elección del DR:** en un entorno LAN de accesos múltiples, la elección del DR se lleva a cabo durante el establecimiento inicial de la red OSPF. Cuando se activan los enlaces OSPF, el dispositivo de routing configurado con la prioridad más alta se elige como DR. Si se parte de la suposición de que no hay ninguna prioridad configurada o de que hay un empate, se elige como DR el router con la mayor ID de router. El dispositivo de routing con la segunda ID de router más alta se elige como BDR.

¿Pero de qué manera el router determina la ID de router? Como se muestra en la ilustración, los routers Cisco derivan la ID del router sobre la base de uno de tres criterios, en el siguiente orden de preferencia:

- La ID del router se configura explícitamente con el comando **router-id id-router** del modo de configuración de OSPF del router. El valor *id-router* es cualquier valor de 32 bits expresado como dirección IPv4. Este es el método recomendado para asignar una ID de router.
- Si la ID del router no se configura explícitamente, el router elige la dirección IPv4 más alta de cualquiera de las interfaces loopback configuradas. Esta constituye la segunda mejor opción para asignar una ID de router.
- Si no se configuró ninguna interfaz loopback, el router elige la dirección IPv4 activa más alta de cualquiera de sus interfaces físicas. Este es el método menos recomendado, ya que hace que a los administradores les resulte más difícil diferenciar entre routers específicos.

Si el router usa la dirección IPv4 más alta para la ID del router, la interfaz no necesita tener OSPF habilitado. Esto significa que no se necesita incluir la dirección de interfaz en uno de los comandos **network** de OSPF para que el router use esa dirección IP como ID del router. El único requisito es que la interfaz esté activa y en estado up (activo).

Nota: la ID del router parece una dirección IP, pero no es enrutable y, por lo tanto, no se incluye en la tabla de routing, a menos que el proceso de routing de OSPF elija una interfaz (física o loopback) que esté definida en forma adecuada por un comando **network**.



Utilice el comando **router-id id-router** del modo de configuración del router para asignar manualmente un valor de 32 bits expresado como dirección IPv4 a un router. Un router OSPF se identifica ante otros routers mediante esta ID del router.

Como se muestra en la figura 1, se configuró una ID de router 1.1.1.1 en el R1, una ID 2.2.2.2 en el R2 y una ID 3.3.3.3 en el R3.

En la figura 2, se asigna la ID de router 1.1.1.1 al R1. Utilice el comando **show ip protocols** para verificar la ID del router.

Nota: el R1 nunca se había configurado con una ID de router OSPF. De haber sido así, se debería modificar la ID del router.

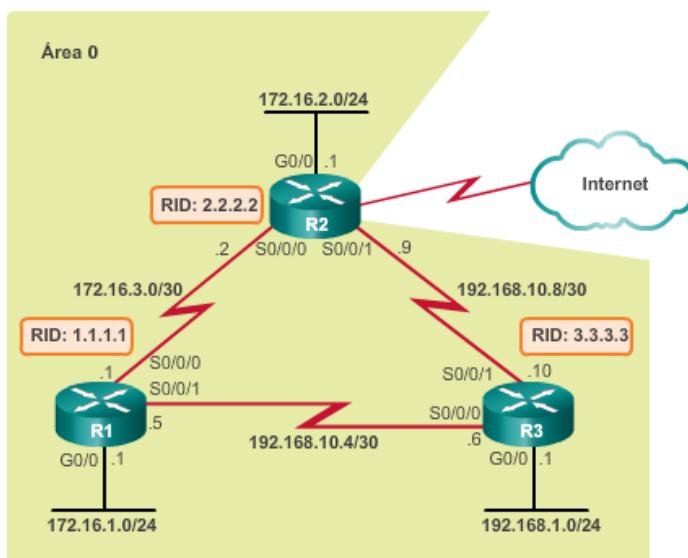
Si la ID del router es la misma en dos routers vecinos, el router muestra un mensaje de error similar al siguiente:

%OSPF-4-DUP_RTRID1: Detected router with duplicate router ID (Se detectó un router con una ID de router duplicada).

Para corregir este problema, configure todos los routers para que tengan una ID del router OSPF única.

Utilice el verificador de sintaxis de la figura 3 para asignar la ID del router al R2 y al R3.

Topología OSPF de referencia



Asignación de una ID de router al R1

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
R1#
*Mar 25 19:50:36.595: %SYS-5-CONFIG_I: Configured from
console by console
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 0. 0 normal 0 stub 0
      nssa
        Maximum path: 4
        Routing for Networks:
          Routing Information Sources:
            Gateway          Distance      Last Update
            Distance: (default is 110)

R1#
```

En ocasiones, es necesario modificar una ID de router, por ejemplo, cuando un administrador de red establece un nuevo esquema de ID de router para la red. Sin embargo, una vez que un router selecciona una ID de router, un router OSPF activo no permite que se modifique la ID del router hasta que se vuelva a cargar el router o se borre el proceso OSPF.

En la figura 1, observe que la ID del router actual es 192.168.10.5. La ID del router debería ser 1.1.1.1.

En la figura 2, se asigna la ID de router 1.1.1.1 al R1. Observe que aparece un mensaje informativo que indica que se debe borrar el proceso OSPF o se debe volver a cargar el router. Esto ocurre debido a que el R1 ya tiene adyacencias con otros vecinos que utilizan la ID de router 192.168.10.5. Se deben volver a negociar esas adyacencias utilizando la nueva IP de router 1.1.1.1.

El método preferido para restablecer la ID del router es borrar el proceso OSPF.

En la figura 3, se borra el proceso de routing de OSPF con el comando **clear ip ospf process** del modo EXEC privilegiado. Esto obliga al protocolo OSPF en el R1 a pasar a los estados Down e Init. Observe los mensajes de cambio de adyacencia de Full a Down y de Loading a Full. El comando **show ip protocols** verifica que se haya cambiado la ID del router.

Utilice el verificador de sintaxis de la figura 4 para modificar la ID del router para el R1.

Verificación del ID del router

```
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 192.168.10.5
  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
    209.165.200.225      110          00:07:02
    192.168.10.10       110          00:07:02
  Distance: (default is 110)

R1#
```

Modificación de la ID del router en el R1

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for
this to take effect
R1(config-router)# end
R1#
*Mar 25 19:46:09.711: %SYS-5-CONFIG_I: Configured from
console by console
```

Eliminación del proceso OSPF

```
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1#
*Mar 25 19:46:22.423: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on Serial0/0/1 from FULL to DOWN, Neighbor Down:
Interface down or detached
*Mar 25 19:46:22.423: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from FULL to DOWN, Neighbor Down:
Interface down or detached
*Mar 25 19:46:22.475: %OSPF-5-ADJCHG: Process 10, Nbr
3.3.3.3 on Serial0/0/1 from LOADING to FULL, Loading Done
*Mar 25 19:46:22.475: %OSPF-5-ADJCHG: Process 10, Nbr
2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done
R1#
R1# show ip protocols | section Router ID
  Router ID 1.1.1.1
R1#
```

Una ID de router también se puede asignar mediante una interfaz loopback.

La dirección IPv4 de la interfaz loopback se debe configurar con una máscara de subred de 32 bits (255.255.255.255). Esto crea una ruta de host. Una ruta de host de 32 bits no se anuncia como ruta a otros routers OSPF.

En el ejemplo de la ilustración, se muestra cómo configurar una interfaz loopback con una ruta de host en el R1. El R1 usa la ruta de host como ID del router, suponiendo que no se configuró ninguna ID de router de manera explícita o que no se obtuvo anteriormente.

Nota: algunas versiones anteriores de IOS no reconocen el comando **router-id**; por lo tanto, la mejor forma de establecer la ID del router en esos routers es mediante una interfaz loopback.

Configuración de una interfaz loopback para utilizarla como ID del router

```
R1(config)# interface loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
R1#
```

8.3.2 Configuración de OSPFv2 de área única

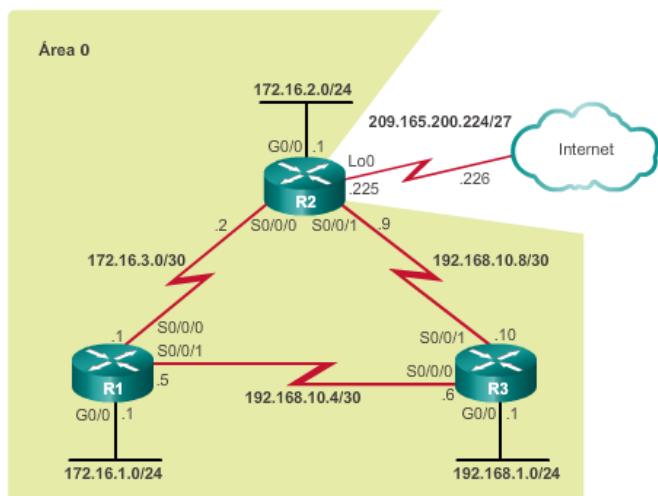
El comando **network** determina qué interfaces participan en el proceso de routing para un área OSPF. Cualquier interfaz de un router que coincide con la dirección de red en el comando **network** está habilitada para enviar y recibir paquetes OSPF. Como consecuencia, se incluye la dirección de red (o de subred) para la interfaz en las actualizaciones de routing OSPF.

La sintaxis básica del comando es **network dirección-red máscara-wildcard área id-área**.

La sintaxis **area id-área** se refiere al área OSPF. Al configurar OSPF de área única, se debe configurar el comando **network** con el mismo valor *id-área* en todos los routers. Si bien se puede usar cualquier ID de área, es aconsejable utilizar una ID de área 0 con OSPF de área única. Esta convención facilita la tarea si posteriormente se modifica la red para admitir OSPF multiárea.

En la ilustración, se muestra la topología de referencia.

Topología OSPF de referencia



OSPFv2 usa la combinación de argumentos *dirección-red máscara-wildcard* para habilitar OSPF en las interfaces. Por su diseño, OSPF es un protocolo sin clase; por lo tanto, siempre se requiere la máscara wildcard. Al identificar las interfaces que participan en un proceso de routing, la máscara wildcard generalmente es el valor inverso a la máscara de subred configurada en esa interfaz.

Una máscara wildcard es una cadena de 32 dígitos binarios que el router utiliza para determinar qué bits de la dirección debe examinar para obtener una coincidencia. En una máscara de subred, un 1 binario equivale a una coincidencia, y un 0 binario no es una coincidencia. En una máscara wildcard, sucede lo contrario:

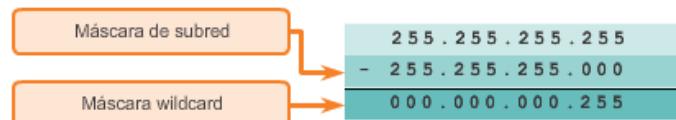
- **Bit 0 de máscara wildcard:** coincide con el valor de bit correspondiente en la dirección.
- **Bit 1 de máscara wildcard:** omite el valor del bit correspondiente en la dirección.

El método más sencillo para calcular una máscara wildcard es restar la máscara de subred de la red a 255.255.255.255.

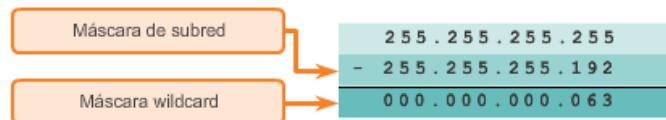
En el ejemplo de la figura 1, se calcula la máscara wildcard a partir de la dirección de red 192.168.10.0/24. Para hacerlo, se resta la máscara de subred 255.255.255.0 a 255.255.255.255, cuyo resultado es 0.0.0.255. Por lo tanto, 192.168.10.0/24 es 192.168.10.0 con una máscara wildcard 0.0.0.255.

En el ejemplo de la figura 2, se calcula la máscara wildcard a partir de la dirección de red 192.168.10.64/26. Para hacerlo, se resta la máscara de subred 255.255.255.192 a 255.255.255.255, cuyo resultado es 0.0.0.63. Por lo tanto, 192.168.10.0/26 es 192.168.10.0 con una máscara wildcard 0.0.0.63.

Cálculo de una máscara wildcard para /24



Cálculo de una máscara wildcard para /26



Existen varias maneras de identificar las interfaces que participan en el proceso de routing OSPFv2.

En la figura 1, se muestran los comandos requeridos para determinar qué interfaces del R1 participan en el proceso de routing OSPFv2 para un área. Observe el uso de las máscaras wildcard para identificar las respectivas interfaces sobre la base de sus direcciones de red. Dado que se trata de una red OSPF de área única, todas las ID de área se establecen en 0.

Como alternativa, se puede habilitar OSPFv2 con el comando **network dirección-ip-interfaz 0.0.0.0area id-área** del modo de configuración del router.

En la figura 2, se proporciona un ejemplo de cómo especificar la dirección IPv4 de interfaz con una máscara wildcard de cuádruple cero. La introducción de **network 172.16.3.1 0.0.0.0 area 0** en el R1 le indica al router que habilite la interfaz Serial0/0/0 para el proceso de routing. Como resultado, el proceso OSPFv2 anuncia la red que se encuentra en esta interfaz (172.16.3.0/30).

La ventaja de especificar la interfaz es que no se necesita calcular la máscara wildcard. OSPFv2 usa la dirección y máscara de subred de la interfaz para determinar qué red debe anunciar.

Algunas versiones de IOS permiten introducir la máscara de subred en lugar de la máscara wildcard. Luego, IOS convierte la máscara de subred al formato de la máscara wildcard.

Utilice el verificador de sintaxis de la figura 3 para anunciar las redes conectadas al R2.

Nota: mientras completa el verificador de sintaxis, observe los mensajes informativos que describen la adyacencia entre el R1 (1.1.1.1) y el R2 (2.2.2.2). El esquema de direccionamiento IPv4 utilizado para la ID del router facilita la identificación del vecino.

Asignación de interfaces a un área OSPF

```
R1(config)# router ospf 10
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)#

```

Asignación de interfaces a un área OSPF con cuádruple cero

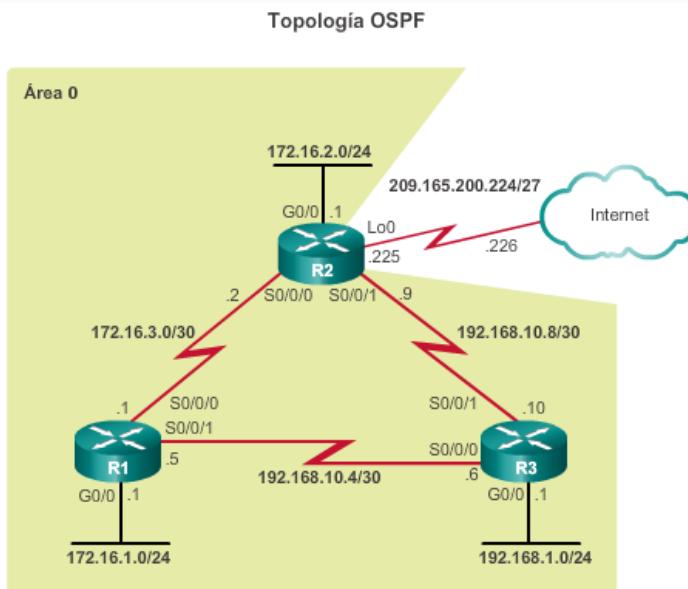
```
R1(config)# router ospf 10
R1(config-router)# network 172.16.1.1 0.0.0.0 area 0
R1(config-router)# network 172.16.3.1 0.0.0.0 area 0
R1(config-router)# network 192.168.10.5 0.0.0.0 area 0
R1(config-router)#

```

De manera predeterminada, los mensajes OSPF se reenvían por todas las interfaces con OSPF habilitado. Sin embargo, estos mensajes solo necesitan enviarse por las interfaces que se conectan a otros routers con OSPF habilitado.

Consulte la topología de la ilustración. Los mensajes OSPF se reenvían por la interfaz G0/0 de los tres routers, aunque no existe ningún vecino OSPF en esa LAN. El envío de mensajes innecesarios en una LAN afecta la red de tres maneras:

- **Uso ineficaz del ancho de banda:** se consume el ancho de banda disponible con el transporte de mensajes innecesarios. Los mensajes se transmiten por multidifusión; por lo tanto, los switches también reenvían los mensajes por todos los puertos.
- **Uso ineficaz de los recursos:** todos los dispositivos en la LAN deben procesar el mensaje y, finalmente, descartarlo.
- **Mayor riesgo de seguridad:** anunciar actualizaciones en una red de difusión constituye un riesgo de seguridad. Los mensajes OSPF se pueden interceptar con software de detección de paquetes. Las actualizaciones de enrutamiento se pueden modificar y enviar de regreso al router, y dañar la tabla de enrutamiento con métricas falsas que desorientan el tráfico.



Utilice el comando **passive-interface** del modo de configuración del router para evitar la transmisión de mensajes de routing a través de una interfaz del router, pero sin dejar de permitir que se anuncie esa red a otros routers, como se muestra en la figura 1. Concretamente, el comando evita que se envíen los mensajes de routing por la interfaz especificada. Sin embargo, la red a la que pertenece la interfaz especificada se sigue anunciando en los mensajes de routing que se envían por otras interfaces.

Por ejemplo, no es necesario que el R1, el R2 y el R3 reenvíen mensajes OSPF por sus interfaces LAN. La configuración identifica la interfaz G0/0 del R1 como pasiva.

Es importante saber que no se puede formar una adyacencia de vecino a través de una interfaz pasiva. Esto se debe a que los paquetes de estado de enlace no se pueden enviar ni confirmar.

A continuación, se usa el comando **show ip protocols** para verificar que la interfaz Gigabit Ethernet sea pasiva, como se muestra en la figura 2. Observe que la interfaz G0/0 ahora figura en la sección Passive Interface(s) (Interfaces pasivas). La red 172.16.1.0 aún figura en Routing for

Networks (Routing para redes), lo que significa que esta red aún se incluye como entrada de ruta en las actualizaciones OSPF que se envían al R2 y al R3.

Nota: OSPFv2 y OSPFv3 admiten el comando **passive-interface**.

Utilice el verificador de sintaxis de la figura 3 para configurar la interfaz LAN como interfaz pasiva en el R2.

Como alternativa, todas las interfaces se pueden convertir en pasivas con el comando **passive-interface default**. Las interfaces que no deben ser pasivas se pueden volver a habilitar con el comando **no passive-interface**.

Continúe utilizando el verificador de sintaxis de la figura 3 para configurar la interfaz LAN como interfaz pasiva en el R3.

Nota: mientras completa el verificador de sintaxis, observe los mensajes informativos de estado de OSPF a medida que todas las interfaces se hacen pasivas y las dos interfaces seriales se hacen no pasivas.

Configuración de una interfaz pasiva en el R1

```
R1(config)# router ospf 10
R1(config-router)# passive-interface GigabitEthernet 0/0
R1(config-router)# end
R1#
```

Verificación de una ruta predeterminada 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#
```

8.3.3 Costo OSPF

Recuerde que un protocolo de routing utiliza una métrica para determinar la mejor ruta de un paquete a través de una red. Una métrica indica la sobrecarga que se requiere para enviar paquetes a través de una interfaz determinada. OSPF utiliza el costo como métrica. Cuando el costo es menor, la ruta es mejor que una con un costo mayor.

El costo de una interfaz es inversamente proporcional al ancho de banda de la interfaz. Por lo tanto, cuanto mayor es el ancho de banda, menor es el costo. Cuanto más sobrecarga y retraso, mayor es el costo. Por lo tanto, una línea Ethernet de 10 Mb/s tiene un costo mayor que una línea Ethernet de 100 Mb/s.

La fórmula que se usa para calcular el costo de OSPF es la siguiente:

- **Costo** = ancho de banda de referencia / ancho de banda de la interfaz

El ancho de banda de referencia predeterminado es 10^8 (100 000 000); por lo tanto, la fórmula es la siguiente:

- **Costo** = 100 000 000 bps / ancho de banda de la interfaz en bps

Consulte la tabla de la ilustración para obtener un desglose del cálculo del costo. Observe que las interfaces FastEthernet, Gigabit Ethernet y 10 GigE comparten el mismo costo, debido a que el valor del costo de OSPF debe ser un número entero. En consecuencia, dado que el ancho de banda de referencia predeterminado se establece en 100 Mb/s, todos los enlaces que son más rápidos que Fast Ethernet también tienen un costo de 1.

Valores de costo de OSPF predeterminados de Cisco

Tipo de interfaz	Ancho de banda de referencia en bps	Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	100,000,000	\div 10,000,000,000	1
Gigabit Ethernet 1 Gbps	100,000,000	\div 1,000,000,000	1
Fast Ethernet 100 Mbps	100,000,000	\div 100,000,000	1
Ethernet 10 Mbps	100,000,000	\div 10,000,000	10
Serial 1,544 Mbps	100,000,000	\div 1,544,000	64
Serial 128 kbps	100,000,000	\div 128,000	781
Serial 64 kbps	100,000,000	\div 64,000	1562

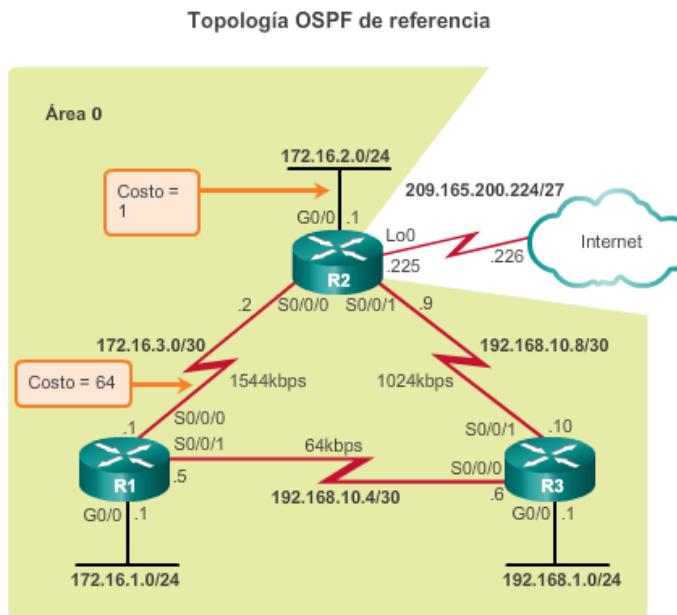
El mismo costo debido al ancho de banda de referencia

El costo de una ruta OSPF es el valor acumulado desde un router hasta la red de destino.

Por ejemplo, en la figura 1, el costo para llegar desde el R1 hasta la LAN 172.16.2.0/24 del R2 debe ser el siguiente:

- Costo del enlace serial del R1 al R2 = 64
- Costo del enlace Gigabit Ethernet en el R2 = 1
- Costo total para llegar a 172.16.2.0/24=65

En la tabla de routing del R1 de la figura 2, se confirma que la métrica para llegar a la LAN del R2 equivale a un costo de 65.



Verificación del costo para la LAN del R2

```
R1# show ip route | include 172.16.2.0
O      172.16.2.0/24 [110/65] via 172.16.3.2, 03:39:07,
      Serial0/0/0
R1#
R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "ospf 10", distance 110, metric 65, type intra
  area
  Last update from 172.16.3.2 on Serial0/0/0, 03:39:15 ago
  Routing Descriptor Blocks:
    * 172.16.3.2, from 2.2.2.2, 03:39:15 ago, via Serial0/0/0
      Route metric is 65, traffic share count is 1
R1#
```

OSPF utiliza un ancho de banda de referencia de 100 Mb/s para todos los enlaces que sean iguales o más rápidos que una conexión Fast Ethernet. Por lo tanto, el costo asignado a una interfaz Fast Ethernet con un ancho de banda de interfaz de 100 Mb/s sería igual a 1.

Costo = $100\ 000\ 000\ bps / 100\ 000\ 000 = 1$

Si bien este cálculo funciona para las interfaces Fast Ethernet, es problemático para los enlaces que son más rápidos que 100 Mb/s, debido a que la métrica de OSPF solo utiliza números enteros como costo final de un enlace. Si se calcula un valor menor que un número entero, OSPF redondea al número entero más cercano. Por este motivo, desde la perspectiva de OSPF, una interfaz con un ancho de banda de interfaz de 100 Mb/s (un costo de 1) tiene el mismo costo que una interfaz con un ancho de banda de 100 Gb/s (un costo de 1).

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.

Ajuste del ancho de banda de referencia

El cambio del ancho de banda de referencia en realidad no afecta la capacidad de ancho de banda en el enlace, sino que simplemente afecta el cálculo utilizado para determinar la métrica. Para ajustar el ancho de banda de referencia, use el comando de configuración del router **auto-cost reference-bandwidth Mb/s**. Se debe configurar este comando en cada router en el dominio OSPF. Observe que el valor se expresa en Mb/s; por lo tanto, a fin de ajustar los costos para estas interfaces, utilice los siguientes comandos:

- **Gigabit Ethernet: auto-cost reference-bandwidth 1000**
- **10 Gigabit Ethernet: auto-cost reference-bandwidth 10000**

Para volver al ancho de banda de referencia predeterminado, use el comando **auto-cost reference-bandwidth 100**.

En la tabla de la figura 1, se muestra el costo de OSPF si el ancho de banda de referencia se establece en Gigabit Ethernet. Si bien los valores de métrica aumentan, OSPF toma mejores decisiones debido a que ahora puede diferenciar entre enlaces FastEthernet y enlaces Gigabit Ethernet.

En la figura 2, se muestra el costo de OSPF si se ajusta el ancho de banda de referencia para admitir 10 enlaces Gigabit Ethernet. Se debe ajustar el ancho de banda de referencia cada vez que haya enlaces más rápidos que FastEthernet (100 Mb/s).

Nota: los costos representan números enteros que se redondearon hacia abajo.

En la figura 3, todos los routers se configuraron para admitir el enlace Gigabit Ethernet con el comando de configuración del router **auto-cost reference-bandwidth 1000**. El nuevo costo acumulado para llegar desde el R1 hasta la LAN 172.16.2.0/24 del R2 es el siguiente:

- Costo del enlace serial del R1 al R2 = 647
- Costo del enlace Gigabit Ethernet en el R2 = 1
- Costo total para llegar a 172.16.2.0/24=648

Utilice el comando **show ip ospf interface s0/0/0** para verificar el costo de OSPF actual asignado a la interfaz Serial 0/0/0 del R1, como se muestra en la figura 4. Observe que se muestra un costo de 647.

En la tabla de routing del R1 de la figura 5, se confirma que la métrica para llegar a la LAN del R2 equivale a un costo de 648.

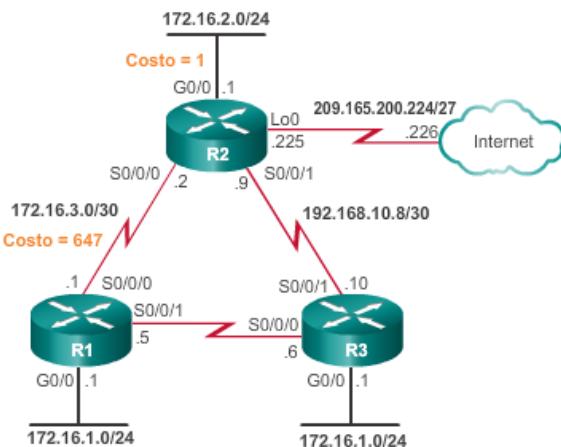
auto-cost reference-bandwidth 1000

Tipo de interfaz	Ancho de banda de referencia en bps	Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	1,000,000,000	÷ 10,000,000,000	1
Gigabit Ethernet 1 Gbps	1,000,000,000	÷ 1,000,000,000	1
Fast Ethernet 100 Mbps	1,000,000,000	÷ 100,000,000	10
Ethernet 10 Mbps	1,000,000,000	÷ 10,000,000	100
Serial 1,544 Mbps	1,000,000,000	÷ 1,544,000	647
Serial 128 kbps	1,000,000,000	÷ 128,000	7812
Serial 64 kbps	1,000,000,000	÷ 64,000	15625

auto-cost reference-bandwidth 10000

Tipo de interfaz	Ancho de banda de referencia en bps	Ancho de banda predeterminado en bps	Costo
10 Gigabit Ethernet 10 Gbps	10,000,000,000	÷ 10,000,000,000	1
Gigabit Ethernet 1 Gbps	10,000,000,000	÷ 1,000,000,000	10
Fast Ethernet 100 Mbps	10,000,000,000	÷ 100,000,000	100
Ethernet 10 Mbps	10,000,000,000	÷ 10,000,000	1000
Serial 1,544 Mbps	10,000,000,000	÷ 1,544,000	6477
Serial 128 kbps	10,000,000,000	÷ 128,000	78125
Serial 64 kbps	10,000,000,000	÷ 64,000	156250

Topología OSPF de referencia



Verificación del costo del enlace S0/0/0

```
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:647
  Topology-MTID    Cost      Disabled     Shutdown     Topology Name
    0          647        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 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, 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 la métrica para la LAN del R2

```
R1# show ip route | include 172.16.2.0
O      172.16.2.0/24 [110/648] via 172.16.3.2, 00:06:03, Serial0/0/0
R1#
R1# show ip route 172.16.2.0
Routing entry for 172.16.2.0/24
  Known via "ospf 10", distance 110, metric 648, type intra area
  Last update from 172.16.3.2 on Serial0/0/0, 00:06:17 ago
  Routing Descriptor Blocks:
    * 172.16.3.2, from 2.2.2.2, 00:06:17 ago, via Serial0/0/0
      Route metric is 648, traffic share count is 1
R1#
```

Todas las interfaces tienen asignados valores de ancho de banda predeterminados. Al igual que el ancho de banda de referencia, los valores del ancho de banda de interfaz en realidad no afectan la velocidad o la capacidad del enlace. En cambio, OSPF los utiliza para calcular la métrica de routing. Por lo tanto, es importante que el valor del ancho de banda refleje la velocidad real del enlace para que la tabla de routing tenga información precisa acerca de la mejor ruta.

Si bien los valores de ancho de banda de las interfaces Ethernet suelen coincidir con la velocidad del enlace, es posible que en otras interfaces no lo hagan. Por ejemplo, la velocidad real de las interfaces seriales a menudo es distinta del ancho de banda predeterminado. En los routers Cisco, el ancho de banda predeterminado en la mayoría de las interfaces seriales se establece en 1,544 Mb/s.

Nota: es posible que las interfaces seriales antiguas tengan un valor predeterminado de 128 kb/s.

Consulte el ejemplo de la figura 1. Observe lo siguiente:

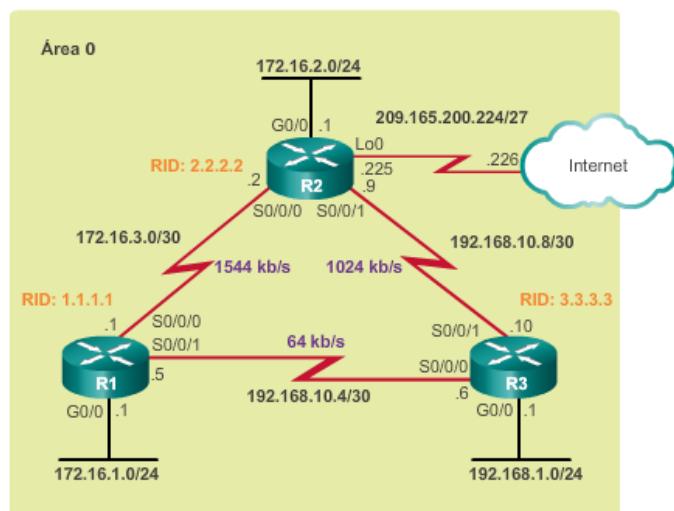
- El enlace entre el R1 y el R2 se debe establecer en 1544 kb/s (valor predeterminado).
- El enlace entre el R2 y el R3 se debe establecer en 1024 kb/s.
- El enlace entre el R1 y el R3 se debe establecer en 64 kb/s.

Utilice el comando **show interfaces** para ver la configuración del ancho de banda de interfaz. En la figura 2, se muestra la configuración de la interfaz serial 0/0/0 para el R1. La configuración del ancho de banda es precisa y, por lo tanto, no es necesario ajustar la interfaz serial.

En la figura 3, se muestra la configuración de la interfaz serial 0/0/1 para el R1. También se confirma que la interfaz usa el ancho de banda de interfaz predeterminado de 1544 kb/s. Según la topología de referencia, este se debe establecer en 64 kb/s. Por lo tanto, se debe ajustar la interfaz serial 0/0/1 del R1.

En la figura 4, se muestra la métrica de costo resultante de 647, que se basa en el ancho de banda de referencia establecido en 1 000 000 000 bps y en el ancho de banda de interfaz predeterminado de 1544 kb/s (1 000 000 000 / 1 544 000).

Topología OSPF de referencia



Verificación de la configuración del ancho de banda predeterminado de la interfaz Serial 0/0/0 del R1

```
R1# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is WIC MBRD Serial
  Description: Link to R2
  Internet address is 172.16.3.1/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DL 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:03, 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
    215 packets input, 17786 bytes, 0 no buffer
    Received 109 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored,
    0 abort
    216 packets output, 17712 bytes, 0 underruns
    0 output errors, 0 collisions, 5 interface resets
```

Configuración de Serial 0/0/1 del R1

```
R1# show interfaces serial 0/0/1 | include BW
  MTU 1500 bytes, BW 1544 Kbit/sec, DL 20000 usec,
```

Configuración de Serial 0/0/1 del R1

```
R1# show ip ospf interface serial 0/0/1
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
  Topology-MTID  Cost  Disabled Shutdown  Topology Name
    0      647    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 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 3/3, 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 3.3.3.3
  Suppress hello for 0 neighbor(s)
R1#
```

Ajuste del ancho de banda de interfaz

Para ajustar el ancho de banda de la interfaz, utilice el comando de configuración de interfaz **bandwidth kilobits**. Utilice el comando **no bandwidth** para restaurar el valor predeterminado.

En el ejemplo de la figura 1, se ajusta el ancho de banda de la interfaz Serial 0/0/1 del R1 a 64 kb/s. Una verificación rápida confirma que la configuración del ancho de banda de la interfaz ahora es de 64 kb/s.

Se debe ajustar el ancho de banda en cada extremo de los enlaces seriales, de lo cual se deriva lo siguiente:

- El R2 requiere que su interfaz S0/0/1 se ajuste a 1024 kb/s.
- El R3 requiere que su interfaz serial 0/0/0 se ajuste a 64 kb/s y que su interfaz serial 0/0/1 se ajuste a 1024 kb/s.

Utilice el verificador de sintaxis de la figura 2 para ajustar la interfaz serial del R2 y del R3.

Nota: un concepto erróneo habitual de los estudiantes nuevos en la tecnología de redes y en IOS de Cisco es suponer que el comando **bandwidth** cambia el ancho de banda físico del enlace. Este comando solo modifica la métrica de ancho de banda que usan EIGRP y OSPF. El comando no modifica el ancho de banda real en el enlace.

Ajuste de la interfaz Serial 0/0/1 del R1

```
R1(config)# int s0/0/1
R1(config-if)# bandwidth 64
R1(config-if)# end
R1#
*Mar 27 10:10:07.735: %SYS-5-CONFIG_I: Configured from console by c
R1#
R1# show interfaces serial 0/0/1 | include BW
    MTU 1500 bytes, BW 64 Kbit/sec, DLY 20000 usec,
R1#
R1# show ip ospf interface serial 0/0/1 | include Cost:
    Process ID 10, Router ID 1.1.1.1, Network Type
    POINT_TO_POINT, Cost: 15625
R1#
```

Como alternativa a la configuración del ancho de banda de interfaz predeterminado, es posible configurar el costo de forma manual en una interfaz con el comando de configuración de interfaz **ip ospf cost valor**.

Una ventaja de configurar un costo en lugar del ancho de banda de la interfaz es que, cuando se configura el costo manualmente, el router no necesita calcular la métrica. En cambio, cuando se configura el ancho de banda de la interfaz, el router debe calcular el costo de OSPF sobre la base del ancho de banda. El comando **ip ospf cost** es útil en entornos de varios proveedores, donde los routers que no son de Cisco pueden usar una métrica distinta del ancho de banda para calcular los costos de OSPF.

Con los comandos de interfaz **bandwidth** e **ip ospf cost** se logra el mismo resultado, que es proporcionar a OSPF un valor preciso para determinar la mejor ruta.

Por ejemplo, en la figura 1, el ancho de banda de interfaz de serial 0/0/1 se restablece al valor predeterminado, y el costo de OSPF se establece de forma manual en 15 625. Si bien el ancho de banda de interfaz se restablece al valor predeterminado, el costo de OSPF se establece como si aún se calculara el ancho de banda.

En la figura 2, se muestran las dos alternativas que se pueden utilizar para modificar los costos de los enlaces seriales en la topología. En el lado derecho de la ilustración, se muestran los comandos **ip ospf cost** equivalentes a los comandos **bandwidth** de la izquierda.

Ajuste de la interfaz Serial 0/0/1 del R1

```
R1(config)# int s0/0/1
R1(config-if)# no bandwidth 64
R1(config-if)# ip ospf cost 15625
R1(config-if)# end
R1#
R1# show interface serial 0/0/1 | include BW
    MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
R1#
R1# show ip ospf interface serial 0/0/1 | include Cost:
    Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT,
    Cost: 15625
R1#
```

Comandos bandwidth e ip ospf cost

Ajuste del ancho de banda de interfaz	=	Configuración manual del costo de OSPF
R1(config)# interface S0/0/1 R1(config-if)# bandwidth 64	=	R1(config)# interface S0/0/1 R1(config-if)# ip ospf cost 15625
R2(config)# interface S0/0/1 R2(config-if)# bandwidth 1024	=	R2(config)# interface S0/0/1 R2(config-if)# bandwidth 976
R3(config)# interface S0/0/0 R3(config-if)# bandwidth 64	=	R3(config)# interface S0/0/0 R3(config-if)# ip ospf cost 15625
R3(config)# interface S0/0/1 R3(config-if)# bandwidth 1024	=	R3(config)# interface S0/0/1 R3(config-if)# ip ospf cost 976

En la figura 1, se muestra la topología de referencia.

Utilice el comando **show ip ospf neighbor** para verificar que el router haya formado 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.

Si dos routers no establecen una adyacencia, no se intercambia la información de estado de enlace. Las LSDB incompletas pueden producir imprecisiones en los árboles SPF y en las tablas de routing. Es posible que no existan rutas hacia las redes de destino o que estas no representen la ruta más óptima.

En la figura 2, se muestra la adyacencia de vecino del R1. Este comando muestra el siguiente resultado para cada vecino:

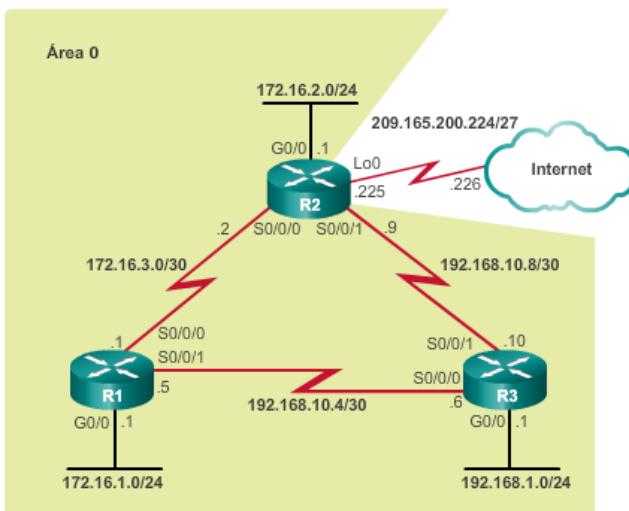
- **Neighbor ID:** la ID del router vecino.
- **Pri:** la prioridad OSPF de la interfaz. Este valor se utiliza en la elección del DR y del BDR.
- **State:** el estado de OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen LSDB de OSPF idénticas. En las redes de accesos múltiples, como Ethernet, dos routers adyacentes pueden mostrar sus estados como 2WAY. El guion indica que no se requiere ningún DR o BDR debido al tipo de red.
- **Dead Time:** la cantidad de tiempo restante que el router espera para recibir un paquete de saludo OSPF del vecino antes de declararlo inactivo. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
- **Address:** la dirección IPv4 de la interfaz del vecino a la que el router está conectado directamente.
- **Interface:** la interfaz en la que este router formó adyacencia con el vecino.

Utilice el verificador de sintaxis de la figura 3 para verificar los vecinos del R2 y del R3 con el comando **show ip ospf neighbor**.

Dos routers pueden no formar una adyacencia OSPF si:

- Las máscaras de subred no coinciden, esto hace que los routers se encuentren en redes separadas.
- Los temporizadores muerto y de saludo de OSPF no coinciden.
- Los tipos de redes OSPF no coinciden.
- Falta un comando **network** de OSPF o este es incorrecto.

Topología OSPF de referencia



Verificación de los vecinos OSPF del 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
2.2.2.2       0    FULL/-   00:00:30  172.16.3.2    Serial0/0/0
R1#
```

Como se muestra en la figura 1, el comando **show ip protocols** es una manera rápida de verificar la información fundamental de configuración 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.

Utilice el verificador de sintaxis de la figura 2 para verificar la configuración del protocolo OSPF del R2 y el R3 con el comando **show ip protocols**.

Verificación de los vecinos OSPF del 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
  Routing Information Sources:
    Gateway          Distance      Last Update
    2.2.2.2           110          00:17:18
    3.3.3.3           110          00:14:49
  Distance: (default is 110)

R1#
```

El comando **show ip ospf** también se puede usar para examinar la ID del proceso OSPF y la ID del router, como se muestra en la figura 1. Este comando muestra información del área OSPF y la última vez que se calculó el algoritmo SPF.

Utilice el verificador de sintaxis de la figura 2 para verificar el proceso OSPF del R2 y el R3 con el comando **show ip ospf**.

Verificación del proceso OSPF del R1

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
Start time: 01:37:15.156, Time elapsed: 01:32:57.776
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 0. Checksum Sum 0x000000
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
```

La forma más rápida de verificar la configuración de interfaz OSPF es utilizar el comando **show ip ospf interface**. Este comando proporciona una lista detallada para cada interfaz con OSPF habilitado. El comando es útil para determinar si se compusieron correctamente las instrucciones del comando **network**.

Para obtener un resumen de las interfaces con OSPF habilitado, utilice el comando **show ip ospf interface brief**, como se muestra en la figura 1.

Utilice el verificador de sintaxis de la figura 2 para recuperar y ver un resumen de las interfaces con OSPF habilitado en el R2 mediante el comando **show ip ospf interface brief**. Observe que especificar el nombre de la interfaz como se hace en el comando **show ip ospf interface serial 0/0/1** proporciona información detallada de OSPF.

Continúe utilizando el verificador de sintaxis de la figura 2 para obtener un resumen de las interfaces con OSPF habilitado en el R3 mediante el comando **show ip ospf interface brief**. Recupere y vea información adicional de la interfaz Serial 0/0/0 con el comando **show ip ospf interface serial 0/0/0**.

Verificación de las interfaces OSPF del R1

```
R1# show ip ospf interface brief
Interface    PID  Area   IP Address/Mask Cost  State   Nbrs F/C
Se0/0/1      10   0      192.168.10.5/30 15625 P2P    1/1
Se0/0/0      10   0      172.16.3.1/30   647   P2P    1/1
Gi0/0        10   0      172.16.1.1/24   1      DR     0/0
R1#
```

8.4 Configuración de OSPFv3 de área única

8.4.1 Comparación de los protocolos OSPFv2 y OSPFv3

OSPFv3 es el equivalente a OSPFv2 para intercambiar prefijos IPv6. Recuerde que, en IPv6, la dirección de red se denomina “prefijo” y la máscara de subred se denomina “longitud de prefijo”.

De manera similar a su equivalente de IPv4, OSPFv3 intercambia la información de routing para completar la tabla de routing IPv6 con prefijos remotos, como se muestra en la ilustración.

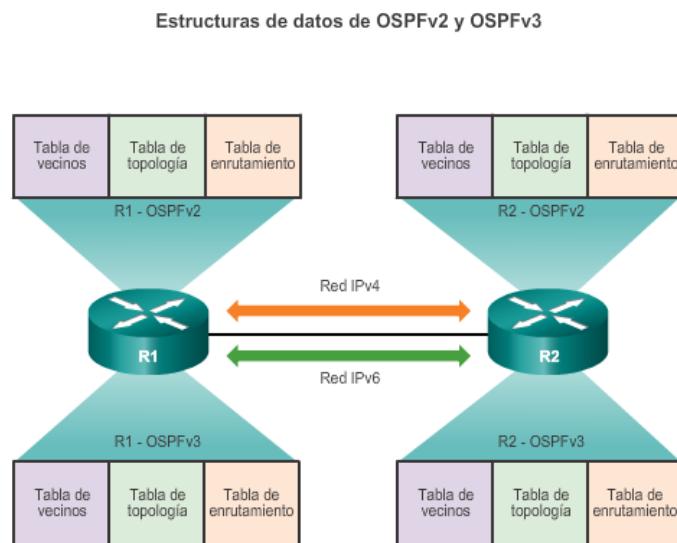
Nota: con la característica de familias de direcciones de OSPFv3, esta versión del protocolo es compatible con IPv4 e IPv6.

OSPFv2 se ejecuta a través de la capa de red IPv4, por lo que se comunica con otros peers IPv4 OSPF y solo anuncia rutas IPv4.

OSPFv3 tiene la misma funcionalidad que OSPFv2, pero utiliza IPv6 como transporte de la capa de red, por lo que se comunica con peers OSPFv3 y anuncia rutas IPv6. OSPFv3 también utiliza el algoritmo SPF como motor de cálculo para determinar las mejores rutas a lo largo del dominio de routing.

Al igual que con todos los protocolos de routing IPv6, OSPFv3 tiene procesos diferentes de los de su equivalente de IPv4. Los procesos y las operaciones son básicamente los mismos que en el protocolo de routing IPv4, pero se ejecutan de forma independiente. OSPFv2 y OSPFv3 tienen tablas de adyacencia, tablas de topología OSPF y tablas de routing IP independientes, como se muestra en la ilustración.

Los comandos de configuración y verificación de OSPFv3 son similares a los que se utilizan en OSPFv2.



Como se muestra en la ilustración, las similitudes entre OSPFv2 y OSPFv3 son las siguientes:

- **Estado de enlace:** OSPFv2 y OSPFv3 son protocolos de routing de estado de enlace sin clase.
- **Algoritmo de routing:** OSPFv2 y OSPFv3 usan el algoritmo SPF para tomar decisiones de routing.
- **Métrica:** las RFC para OSPFv2 y OSPFv3 definen la métrica como el costo del envío de paquetes por la interfaz. OSPFv2 y OSPFv3 pueden modificarse mediante el comando del modo de configuración del router **auto-cost reference-bandwidth ancho-banda-referencia**. El comando solo afecta la métrica de OSPF donde se configuró. Por ejemplo, si se introdujo este comando para OSPFv3, no afecta las métricas de routing de OSPFv2.
- **Áreas:** el concepto de varias áreas en OSPFv3 es el mismo que en OSPFv2. Varias áreas que minimizan la saturación de estado de enlace y proporcionan mejor estabilidad con el dominio OSPF.
- **Tipos de paquetes OSPF:** OSPFv3 usa los mismos cinco tipos de paquetes básicos que OSPFv2 (saludo, DBD, LSR, LSU y LSAck).
- **Mecanismo de descubrimiento de vecinos:** la máquina de estado de vecinos, incluida la lista de estados y eventos de vecinos OSPF, no se modifica. OSPFv2 y OSPFv3 utilizan el mecanismo de saludo para obtener información sobre los routers vecinos y formar adyacencias. Sin embargo, en OSPFv3, no existe ningún requisito con respecto a la coincidencia de subredes para formar adyacencias de vecinos. Esto se debe a que las adyacencias de vecinos se forman mediante direcciones link-local, no direcciones de unidifusión global.

- **Proceso de elección del DR/BDR:** el proceso de elección del DR/BDR no se modifica en OSPFv3.
- **ID del router:** tanto OSPFv2 como OSPFv3 usan un número de 32 bits para la ID del router representada en notación decimal con puntos. Por lo general, se trata de una dirección IPv4. Se debe utilizar el comando de OSPF **router-id** para configurar la ID del router. El proceso para determinar la ID del router de 32 bits es el mismo en ambos protocolos. Utilice una ID de router configurada explícitamente; de lo contrario, la dirección IPv4 de loopback más alta se convierte en la ID del router.

Similitudes entre OSPFv2 y OSPFv3

OSPFv2 y OSPFv3	
Estado de enlace	Sí
Algoritmo de routing	SPF
Métrica	Costo
Áreas	Admite la misma jerarquía de dos niveles.
Tipos de paquetes	Mismos paquetes de saludo, DBD, LSR, LSU y LSAck.
Descubrimiento de vecinos	Transiciones a través de los mismos estados mediante los paquetes de saludo.
DR y BDR	La función y el proceso de elección son los mismos.
ID del router	ID del router de 32bits: determinada mediante el mismo proceso en ambos protocolos.

En la ilustración, se muestran las diferencias entre OSPFv2 y OSPFv3:

- **Anuncios:** OSPFv2 anuncia rutas IPv4, mientras que OSPFv3 anuncia rutas para IPv6.
- **Dirección de origen:** los mensajes OSPFv2 se originan en la dirección IPv4 de la interfaz de salida. En OSPFv3, los mensajes OSPF se originan con la dirección link-local de la interfaz de salida.
- **Dirección de multidifusión de todos los routers OSPF:** OSPFv2 utiliza la dirección 224.0.0.5, mientras que OSPFv3 utiliza la dirección FF02::5.
- **Dirección de multidifusión de DR/BDR:** OSPFv2 utiliza la dirección 224.0.0.6, mientras que OSPFv3 utiliza la dirección FF02::6.
- **Anuncio de redes:** OSPFv2 anuncia las redes mediante el comando de configuración del router **network**, mientras que OSPFv3 utiliza el comando de configuración de interfaz **ipv6 ospf id-proceso areaid-área**.
- **Routing de unidifusión IP:** habilitado de manera predeterminada en IPv4; en cambio, el comando de configuración global **ipv6 unicast-routing** se debe configurar.
- **Autenticación:** OSPFv2 utiliza autenticación de texto no cifrado o autenticación MD5. OSPFv3 utiliza autenticación IPv6.

Diferencias entre OSPFv2 y OSPFv3

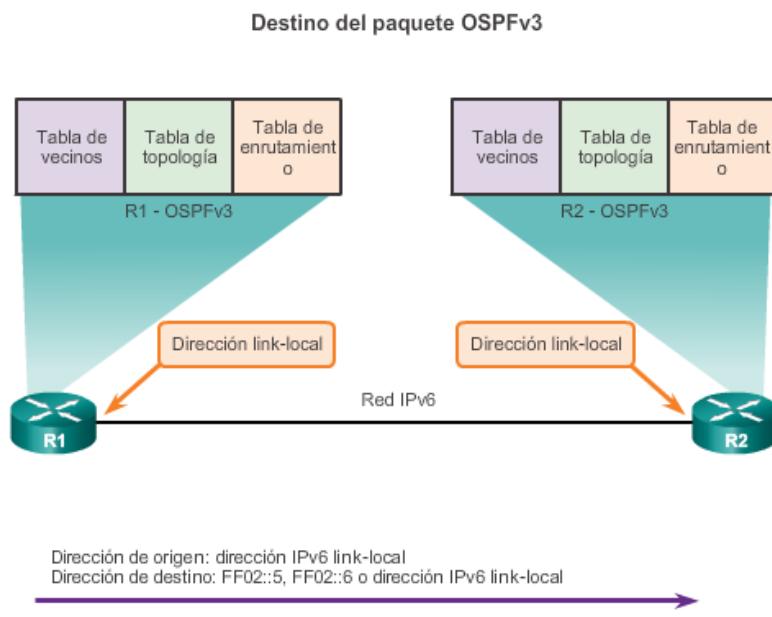
	OSPFv2	OSPFv3
Anuncios	Redes IPv4	Prefijos IPv6
Dirección de origen	Dirección IPv4 de origen	Dirección IPv6 link-local
Dirección de destino	Opción de: ▪ Dirección IPv4 de unidifusión de vecino ▪ Dirección de multidifusión 224.0.0.5 de todos los routers OSPF ▪ Dirección de multidifusión 224.0.0.6 del DR/BDR	Opción de: ▪ Dirección IPv6 link-local de vecino ▪ Dirección de multidifusión FF02::5 de todos los routers OSPFv3 ▪ Dirección de multidifusión FF02::6 del DR/BDR
Anuncio de redes	Configurado con el comando de configuración de router network	Configurado con el comando de configuración de interfaz ipv6 ospf id-proceso area id-área
Routing de unidifusión IP	El routing de unidifusión IPv4 está habilitado de manera predeterminada.	El reenvío de unidifusión IPv6 no está habilitado de manera predeterminada. Se debe configurar el comando de configuración global ipv6 unicast-routing .
Autenticación	Texto no cifrado y MD5	Autenticación IPv6

Los routers que ejecutan un protocolo de routing dinámico, como OSPF, 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 IPv4 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.

Como se muestra en la ilustración, los mensajes OSPFv3 se envían utilizando lo siguiente:

- **Dirección IPv6 de origen:** esta es la dirección IPv6 link-local de la interfaz de salida.
- **Dirección IPv6 de destino:** se pueden enviar los paquetes OSPFv3 a una dirección de unidifusión mediante la dirección IPv6 link-local del vecino. También es posible enviarlos utilizando una dirección de multidifusión. La dirección FF02::5 es la dirección de todos los routers OSPF, mientras que FF02::6 es la dirección de multidifusión del DR/BDR.



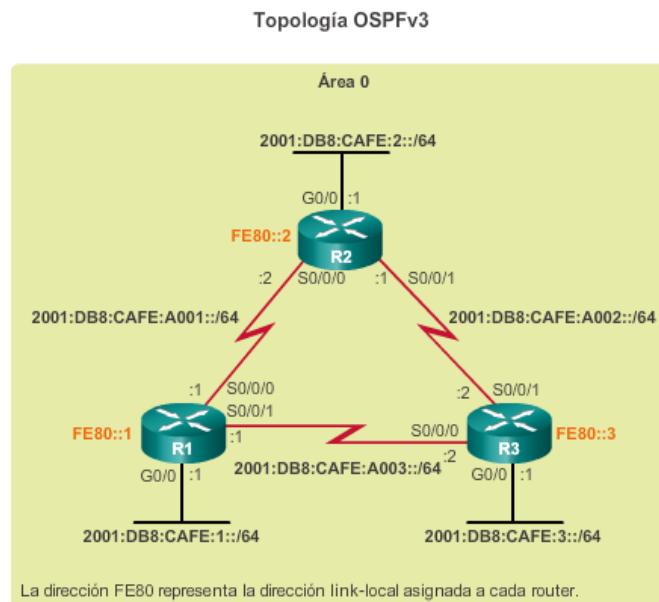
8.4.2 Configuración de OSPFv3

En la figura 1, se muestra la topología de la red que se utiliza para configurar OSPFv3.

En la figura 2, se muestra el routing de unidifusión IPv6 y la configuración de las direcciones de unidifusión global del R1, como se identifican en la topología de referencia. Suponga que las interfaces del R2 y el R3 también se configuraron con sus direcciones de unidifusión global, como se identifica en la topología mencionada.

En esta topología, ninguno de los routers tiene direcciones IPv4 configuradas. Una red con las interfaces del router configuradas con direcciones IPv4 e IPv6 se denomina “dual-stack”. Una red dual-stack puede tener OSPFv2 y OSPFv3 habilitados de manera simultánea.

En la figura 3, se muestran los pasos para configurar OSPFv3 básico en un área única.



Configuración de direcciones de unidifusión global en el R1

```
R1(config)# ipv6 unicast-routing
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# description R1 LAN
R1(config-if)# ipv6 address 2001:DB8:CAFE:1::1/64
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ipv6 address 2001:DB8:CAFE:A001::1/64
R1(config-if)# clock rate 128000
R1(config-if)# no shut
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# description Link to R3
R1(config-if)# ipv6 address 2001:DB8:CAFE:A003::1/64
R1(config-if)# no shut
R1(config-if)# end
R1#
```

Pasos para configurar OSPFv3

- Paso 1:** habilitar el routing de unidifusión IPv6 (`ipv6 unicast-routing`).
- Paso 2:** (opcional) configurar las direcciones link-local.
- Paso 3:** configurar una ID del router de 32 bits en el modo de configuración del router OSPFv3 con el comando `router-id id-router`.
- Paso 4:** configurar detalles de routing optativos, como ajustar el ancho de banda de referencia.
- Paso 5:** (opcional) configurar parámetros específicos de interfaz OSPFv3. Por ejemplo, ajustar el ancho de banda de la interfaz.
- Paso 6:** habilitar el routing IPv6 con el comando `ipv6 ospf area`.

En la ilustración, el resultado del comando `show ipv6 interface brief` confirma que se configuraron correctamente las direcciones IPv6 globales y que se habilitaron las interfaces. Además, observe que cada interfaz generó automáticamente una dirección link-local, como se destaca en la ilustración.

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 configure manualmente, los routers Cisco crean la dirección link-local utilizando el prefijo FE80::/10 y el proceso EUI-64. 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. Observe en la ilustración que las tres interfaces usan la misma dirección link-local.

Verificación de las interfaces con IPv6 habilitado en el R1

```
R1# show ipv6 interface brief
Em0/0 [administratively down/down]
    unassigned
GigabitEthernet0/0 [up/up]
    FE80::32F7:DEF:FEA3:DAO
    2001:DB8:CAFE:1::1
GigabitEthernet0/1 [administratively down/down]
    unassigned
Serial0/0/0 [up/up]
    FE80::32F7:DFF:FEA3:DAO
    2001:DB8:CAFE:A001::1
Serial0/0/1 [up/up]
    FE80::32F7:DFF:FEA3:DAO
    2001:DB8:CAFE:A003::1
R1#
```

Las direcciones link-local creadas con el formato EUI-64 o, en algunos casos, con ID de interfaz 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, es habitual hacer que sea una dirección fácil de reconocer.

Configurar la dirección link-local de forma manual permite crear una dirección reconocible y más fácil de recordar. Además, un router con varias interfaces puede asignar la misma dirección link-local a cada interfaz IPv6. Esto se debe a que la dirección link-local solo se requiere para las comunicaciones locales.

Las direcciones link-local pueden configurarse de forma manual con el mismo comando de interfaz que se usa para crear direcciones IPv6 de unidifusión global, pero agregando la palabra clave **link-local** al comando **ipv6 address**.

Una dirección link-local tiene un prefijo dentro del rango FE80 a FEBF. Cuando una dirección comienza con este hexteto (segmento de 16 bits), la palabra clave **link-local** debe seguir la dirección.

En el ejemplo de la figura 1, se configura la misma dirección link-local FE80::1 en las tres interfaces del R1. Se eligió FE80::1 para que las direcciones link-local del R1 sean fáciles de recordar.

Con una vista rápida de las interfaces como se muestran en la figura 2, se confirma que las direcciones link-local de las interfaces del R1 se cambiaron a FE80::1.

Utilice el verificador de sintaxis de la figura 3 para configurar y verificar la dirección link-local FE80::2 en el R2 y la dirección link-local FE80::3 en el R3.

Configuración de direcciones link-local en el R1

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# exit
R1(config)# interface Serial0/0/1
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)#

```

Verificación de las direcciones link-local en el R1

```
R1# show ipv6 interface brief
Em0/0                  [administratively down/down]
    unassigned
GigabitEthernet0/0      [up/up]
    FE80::1
    2001:DB8:CAFE:1::1
GigabitEthernet0/1      [administratively down/down]
    unassigned
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#

```

Utilice el comando **ipv6 router ospf *id-proceso*** del modo de configuración global para ingresar al modo de configuración del router. La petición de entrada del modo de configuración del router IPv6 es distinta de la petición de entrada del modo de configuración del router IPv4. Utilice el modo de confirmación del router IPv6 para configurar los parámetros globales de OSPFv3, como la asignación de la ID del router OSPF de 32 bits y del ancho de banda de referencia.

Los protocolos de routing IPv6 se habilitan en una interfaz, no desde el modo de configuración del router, como sus equivalentes de IPv4. El comando **network** del modo de configuración del router IPv4 no existe en IPv6.

Al igual que en OSPFv2, el valor *id-proceso* es un número entre 1 y 65 535, y lo elige el administrador de red. El valor *id-proceso* tiene importancia en el ámbito local, lo que significa que no hace falta que coincida con otros routers OSPF para establecer adyacencias con esos vecinos.

OSPFv3 requiere que se asigne una ID de router de 32 bits antes de que se pueda habilitar OSPF en una interfaz. En el diagrama de lógica de la figura 1, se muestra cómo se elige una ID de router. Al igual que OSPFv2, OSPFv3 utiliza lo siguiente:

- En primer lugar, una ID de router configurada explícitamente.
- Si no se configuró ninguna, el router usa la dirección IPv4 configurada más alta de una interfaz loopback.
- Si no se configuró ninguna, el router usa la dirección IPv4 configurada más alta de una interfaz activa.
- Si un router no tiene ningún origen de direcciones IPv4, este muestra un mensaje de consola para configurar la ID del router de forma manual.

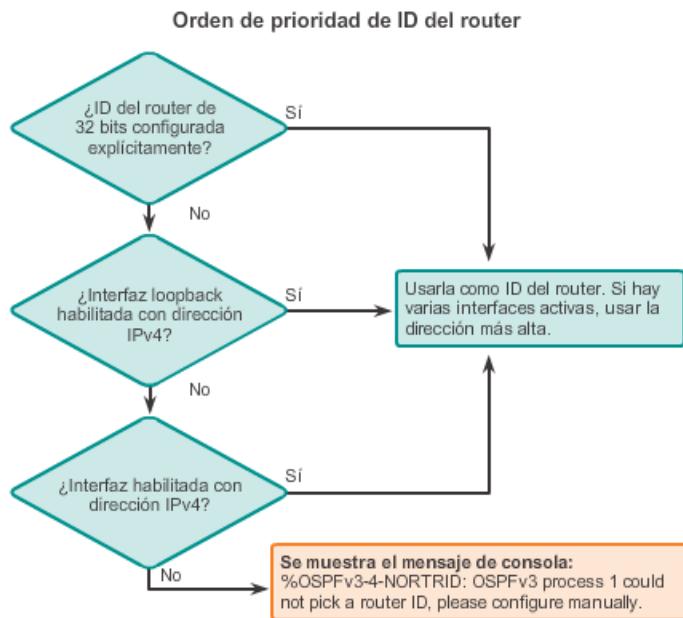
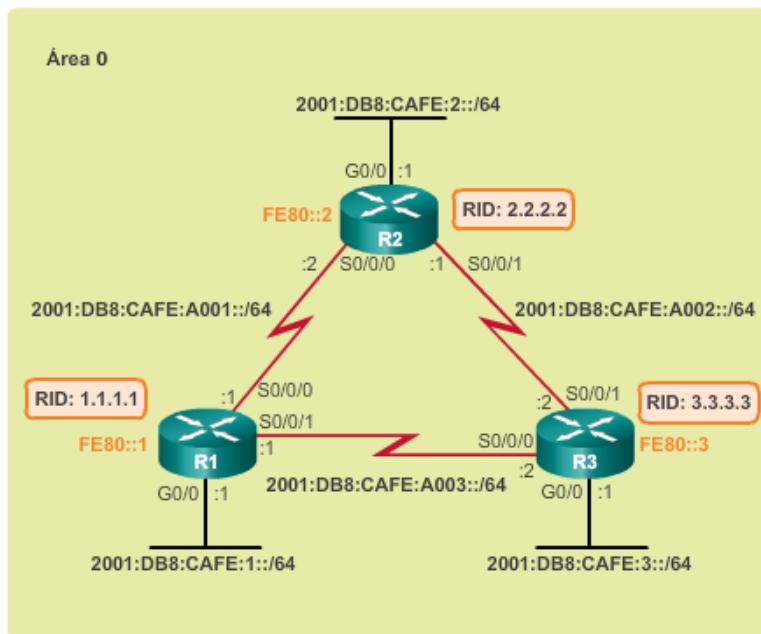
Nota: para mantener la coherencia, los tres routers usan la ID de proceso 10.

Como se muestra en la topología de la figura 2, se deben asignar las ID de router indicadas a los routers R1, R2 y R3. El comando **router-id id-router** utilizado para asignar una ID de router en OSPFv2 es el mismo comando que se utiliza en OSPFv3.

En el ejemplo de la figura 3, se realiza lo siguiente:

- Se ingresa al modo de configuración de OSPFv3 del router. Observe que la petición de entrada del router es distinta de la petición de entrada predeterminada del router del modo de protocolo de routing IPv4. Además, observe que apareció un mensaje informativo de consola cuando se accedió al modo de configuración de router OSPFv3.
- Se asigna la ID de router 1.1.1.1.
- Se ajusta el ancho de banda de referencia a 1 000 000 000 bps (1 Gb/s), debido a que hay enlaces Gigabit Ethernet en la red. Observe el mensaje informativo de consola que indica que se debe configurar este comando en todos los routers en el dominio de routing.
- El comando **show ipv6 protocols** se usa para verificar que la ID de proceso OSPFv3 10 utiliza la ID de router 1.1.1.1.

Utilice el verificador de sintaxis de la figura 4 para configurar los parámetros globales de OSPFv3 en el R2 y el R3.

**Topología OSPFv3**

Asignación de una ID de router al R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)#
*Mar 29 11:21:53.739: %OSPFv3-4-NORTRID: Process OSPFv3-1-
IPv6 could not pick a router-id, please configure manually
R1(config-rtr)#
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)#
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-1-IPv6: Reference bandwidth is changed. Please
ensure reference bandwidth is consistent across all routers.
R1(config-rtr)#
R1(config-rtr)# end
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: 0 normal, 0 stub, 0 nssa
      Redistribution:
        None
R1#
```

En ocasiones, se deben cambiar las ID de router, por ejemplo, si el administrador de red estableció un nuevo esquema de identificación de ID de router. Sin embargo, después de que un router OSPFv3 establece una ID de router, esta no se puede cambiar hasta que se vuelva a cargar el router o se borre el proceso OSPF.

En la figura 1, observe que la ID del router actual es 10.1.1.1. La ID del router OSPFv3 debería ser 1.1.1.1.

En la figura 2, se asigna la ID de router 1.1.1.1 al R1.

Nota: el método preferido para restablecer la ID del router es borrar el proceso OSPF.

En la figura 3, se borra el proceso de routing de OSPF con el comando **clear ipv6 ospf process** del modo EXEC privilegiado. Hacer esto obliga al protocolo OSPF en el R1 a volver a negociar las adyacencias de vecinos con la nueva ID del router.

El comando **show ipv6 protocols** verifica que se haya cambiado la ID del router.

Utilice el verificador de sintaxis de la figura 4 para modificar la ID del router para el R1.

Verificación del ID del router

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
Router ID 10.1.1.1
Number of areas: 0 normal, 0 stub, 0 nssa
Redistribution:
None
R1#
```

Modificación de la ID del router en el R1

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# end
R1#
```

Eliminación del proceso OSPF

```
R1# clear ipv6 ospf process
Reset selected OSPFv3 processes? [no]: y
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: 0 normal, 0 stub, 0 nssa
Redistribution:
None
R1#
```

OSPFv3 utiliza un método diferente para habilitar una interfaz para OSPF. En lugar de usar el comando **network** del modo de configuración del router para especificar las direcciones de interfaz que coinciden, OSPFv3 se configura directamente en la interfaz.

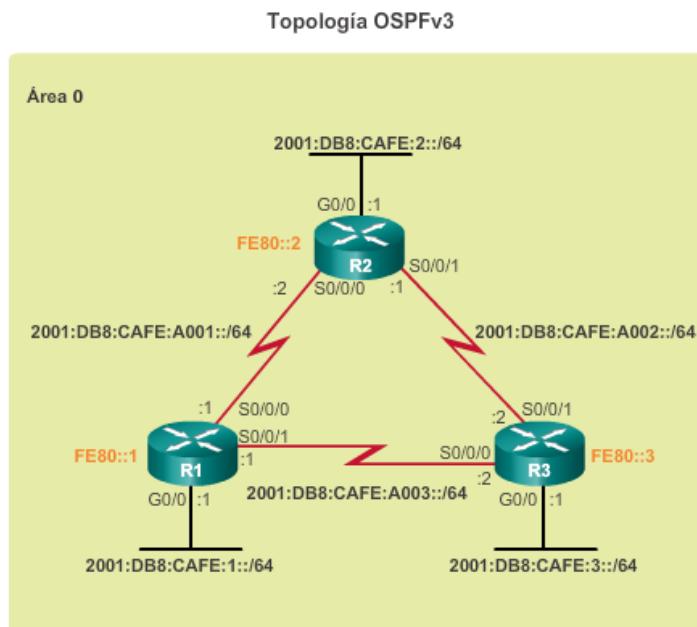
Para habilitar OSPFv3 en una interfaz, utilice el comando **ipv6 ospf id-proceso area id-área** del modo de configuración de interfaz.

El valor *id-proceso* identifica el proceso de routing específico y debe coincidir con la ID de proceso utilizada para crear el proceso de routing en el comando **ipv6 router ospf id-proceso**.

El valor *id-área* es el área que se debe asociar a la interfaz OSPFv3. Aunque pudo haberse configurado cualquier valor para el área, se seleccionó 0 debido a que el área 0 es el área backbone a la que se deben conectar todas las demás áreas, como se muestra en la figura 1. Esto contribuye a la migración a OSPF multiárea, si surge la necesidad.

En la figura 2, se habilita OSPFv3 en las interfaces del R1 con el comando **ipv6 ospf 10 area 0**. El comando **show ipv6 ospf interface brief** muestra las interfaces OSPFv3 activas.

Utilice el verificador de sintaxis de la figura 3 para habilitar OSPFv3 en las interfaces del R2 y el R3.



Habilitación de OSPFv3 en las interfaces del R1

```
R1(config)# interface GigabitEthernet 0/0
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)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface PID Area Intf ID Cost State Nbrs F/C
Se0/0/1 10 0 7 15625 P2P 0/0
Se0/0/0 10 0 6 647 P2P 0/0
Gi0/0 10 0 3 1 WAIT 0/0
R1#
```

8.4.3 Verificación de OSPFv3

Utilice el comando **show ipv6 ospf neighbor** para verificar que el router haya formado 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.

Si dos routers no establecen una adyacencia de vecino, no se intercambia la información de estado de enlace. Las LSDB incompletas pueden producir imprecisiones en los árboles SPF y en las tablas de routing. Es posible que no existan rutas hacia las redes de destino o que estas no representen la ruta más óptima.

En la figura 1, se muestra la adyacencia de vecino del R1. Este comando muestra el siguiente resultado para cada vecino:

- **Neighbor ID:** la ID del router vecino.
- **Pri:** la prioridad OSPF de la interfaz. El valor se utiliza en la elección del DR y del BDR.
- **State:** el estado de OSPF de la interfaz. El estado FULL significa que el router y su vecino poseen LSDB de OSPF idénticas. En el caso de redes de accesos múltiples como Ethernet, dos routers adyacentes pueden mostrar sus estados como 2WAY. El guion indica que no se requiere ningún DR o BDR debido al tipo de red.
- **Dead Time:** la cantidad de tiempo restante que el router espera para recibir un paquete de saludo OSPF del vecino antes de declararlo inactivo. Este valor se reestablece cuando la interfaz recibe un paquete de saludo.
- **Interface ID:** la ID de interfaz o de enlace.
- **Interface:** la interfaz en la que este router formó adyacencia con el vecino.

Utilice el verificador de sintaxis de la figura 2 para verificar los vecinos del R2 y el R3 con el comando **show ipv6 ospf neighbor**.

Verificación de los vecinos OSPFv3 para el R1

```
R1# show ipv6 ospf neighbor
OSPFv3 Router with ID {1.1.1.1} (Process ID 10)
Neighbro ID Pri State Dead Time Interface ID Interface
3.3.3.3 0 FULL/ - 00:00:39 6 Serial0/0/1
2.2.2.2 0 FULL/ - 00:00:36 6 Serial0/0/0
R1#
```

Como se muestra en la figura 1, el comando **show ipv6 protocols** es una manera rápida de verificar la información fundamental de configuración OSPFv3, incluidas la ID del proceso OSPF, la ID del router y las interfaces habilitadas para OSPFv3.

Utilice el verificador de sintaxis de la figura 2 para verificar la configuración del protocolo OSPF del R2 y el R3 con el comando **show ipv6 protocols**.

Además, utilice el comando **show ipv6 ospf** para examinar la ID del proceso OSPFv3 y la ID del router. Este comando muestra información del área OSPF y la última vez que se calculó el algoritmo SPF.

Verificación de la configuración del protocolo OSPFv3 para 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#
```

La forma más rápida de verificar la configuración de interfaz OSPF es utilizar el comando **show ipv6 ospf interface**. Este comando proporciona una lista detallada para cada interfaz con OSPF habilitado.

Para recuperar y ver un resumen de las interfaces con OSPFv3 habilitado en el R1, utilice el comando **show ipv6 ospf interface brief**, como se muestra en la figura 1.

Utilice el verificador de sintaxis de la figura 2 para ver un resumen de las interfaces con OSPF habilitado en el R2 mediante el comando **show ipv6 ospf interface brief**. Observe que especificar el nombre de la interfaz como se hace en el comando **show ipv6 ospf interface serial 0/0/1** proporciona información detallada de OSPF.

Continúe utilizando el verificador de sintaxis de la figura 2 para obtener un resumen de las interfaces con OSPF habilitado en el R3 mediante el comando **show ipv6 ospf interface brief**. Recupere y vea información adicional de la interfaz Serial 0/0/0 con el comando **show ipv6 ospf interface serial 0/0/0**.

Verificación de las interfaces OSPFv3 del R1

```
R1# show ipv6 ospf interface brief
Interface   PID  Area           Intf ID   Cost  State Nbrs F/C
Se0/0/1     10   0              7         15625 P2P   1/1
Se0/0/0     10   0              6         647    P2P   1/1
Gi0/0       10   0              3         1       DR    0/0
R1#
```

En la figura 1, el comando **show ipv6 route ospf** proporciona datos específicos sobre las rutas OSPF en la tabla de routing.

Utilice el verificador de sintaxis de la figura 2 para verificar la tabla de routing OSPFv3 del R2 y el R3; use el comando **show ipv6 route ospf**.

Verificación de la tabla de routing IPv6 del 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, 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
    NDx - 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 [110/657]
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:3::/64 [110/1304]
    via FE80::2, Serial0/0/0
O  2001:DB8:CAFE:A002::/64 [110/1294]
    via FE80::2, Serial0/0/0
R1#
```

8.5 Resumen

La versión actual de OSPF para IPv4 es OSPFv2, introducida en RFC 1247 y actualizada en RFC 2328 por John Moy. En 1999, OSPFv3 para IPv6 se publicó en RFC 2740.

OSPF es un protocolo de routing de estado de enlace sin clase con una distancia administrativa predeterminada de 110 y se indica en la tabla de routing con el código de origen de ruta **O**.

OSPF se habilita con el comando **router ospf id**-proceso del modo de configuración global. El valor *id*-proceso tiene importancia en el ámbito local, lo que significa que no necesita coincidir con otros routers OSPF para establecer adyacencias con esos vecinos.

El comando **network** utilizado con OSPF cumple la misma función que cuando se lo utiliza con otros protocolos de routing IGP, pero con una sintaxis ligeramente diferente. El valor **máscara-wildcard** es el valor inverso a la máscara de subred, y el valor **id-área** se debe establecer en **0**.

De manera predeterminada, los paquetes de saludo OSPF se envían cada 10 segundos en segmentos de accesos múltiples y punto a punto, y cada 30 segundos en los segmentos NBMA (Frame Relay, X.25, ATM), y OSPF los usa para establecer adyacencias de vecinos. De manera predeterminada, el intervalo muerto es equivalente a cuatro veces el valor del intervalo de saludo.

Para que los routers establezcan una adyacencia, sus intervalos de saludo, intervalos muertos, tipos de red y máscaras de subred deben coincidir. Use el comando **show ip ospf neighbors** para verificar las adyacencias OSPF.

En una red de accesos múltiples, OSPF elige un DR para que funcione como punto de recopilación y distribución de las LSA enviadas y recibidas. Un BDR se elige para cumplir la función del DR en caso de que este falle. Todos los demás routers se conocen como DROTHER. Todos los routers envían sus LSA al DR, que luego satura con la LSA todos los demás routers en la red de accesos múltiples.

El comando **show ip protocols** se utiliza para verificar la información importante de configuración OSPF, incluidas la ID del proceso OSPF, la ID del router y las redes que anuncia el router.

OSPFv3 se habilita en una interfaz, no en el modo de configuración del router. OSPFv3 necesita que se configuren direcciones link-local. Se debe habilitar el routing de unidifusión IPv6 para OSPFv3. Para habilitar una interfaz para OSPFv3, antes se requiere una ID de router de 32 bits.

9 Listas de control de acceso

La seguridad de red es un tema muy amplio, y gran parte de este tema se encuentra más allá del ámbito de este curso. Sin embargo, una de las habilidades más importantes que necesita un administrador de red es el dominio de las listas de control de acceso (ACL).

Los diseñadores de red utilizan firewalls para proteger las redes del uso no autorizado. Los firewalls son soluciones de hardware o de software que aplican las políticas de seguridad de la red. Imagine una cerradura en la puerta de una habitación dentro de un edificio. La cerradura permite que solo los usuarios autorizados que poseen una llave o una tarjeta de acceso puedan entrar. De igual forma, un firewall filtra los paquetes no autorizados o potencialmente peligrosos e impide que ingresen a la red. En un router Cisco, puede configurar un firewall simple que proporcione capacidades básicas de filtrado de tráfico mediante ACL. Los administradores utilizan las ACL para detener el tráfico o para permitir solamente tráfico específico en sus redes.

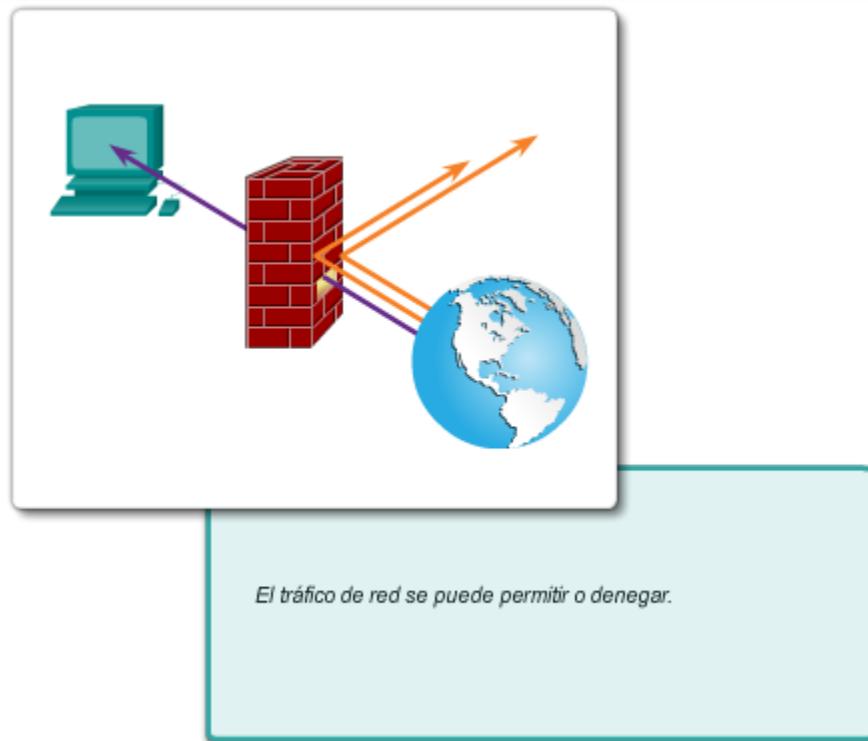
Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar) que se aplican a los protocolos de capa superior o a las direcciones. Las ACL son una herramienta potente para controlar el tráfico hacia y desde la red. Se pueden configurar ACL para todos los protocolos de red enrutada.

El motivo más importante para configurar ACL es aportar seguridad a una red. En este capítulo, se explica cómo utilizar las ACL estándar y extendidas en un router Cisco como parte de una solución de seguridad. Se incluyen consejos, consideraciones, recomendaciones y pautas generales sobre cómo utilizar las ACL.

En este capítulo, se ofrece la oportunidad de desarrollar su dominio de las ACL con una serie de lecciones, actividades y ejercicios de práctica de laboratorio.

Después de completar este capítulo, podrá hacer lo siguiente:

- Explicar la forma en que se utilizan las ACL para filtrar el tráfico.
- Comparar las ACL de IPv4 estándar y extendidas.
- Explicar la forma en que las ACL utilizan máscaras wildcard.
- Explicar las pautas para la creación de ACL.
- Explicar las pautas para la colocación de ACL.
- Configurar ACL de IPv4 estándar para filtrar el tráfico según los requisitos de red.
- Modificar una ACL de IPv4 estándar mediante los números de secuencia.
- Configurar una ACL estándar para proteger el acceso a VTY.
- Explicar la estructura de una entrada de control de acceso (ACE) extendida.
- Configurar ACL de IPv4 extendidas para filtrar el tráfico según los requisitos de red.
- Configurar una ACL para que limite el resultado de depuración.
- Explicar la forma en que procesa los paquetes un router cuando se aplica una ACL.
- Resolver problemas comunes de ACL con los comandos de CLI.
- Comparar la creación de ACL de IPv4 y ACL de IPv6.
- Configurar ACL de IPv6 para filtrar el tráfico según los requisitos de red.



9.1 Funcionamiento de ACL de IP

9.1.1 Propósito de los ACLs

Una ACL es una serie de comandos del IOS que controlan si un router reenvía o descarta paquetes según la información que se encuentra en el encabezado del paquete. Las ACL son una de las características del software IOS de Cisco más utilizadas.

Cuando se las configura, las ACL realizan las siguientes tareas:

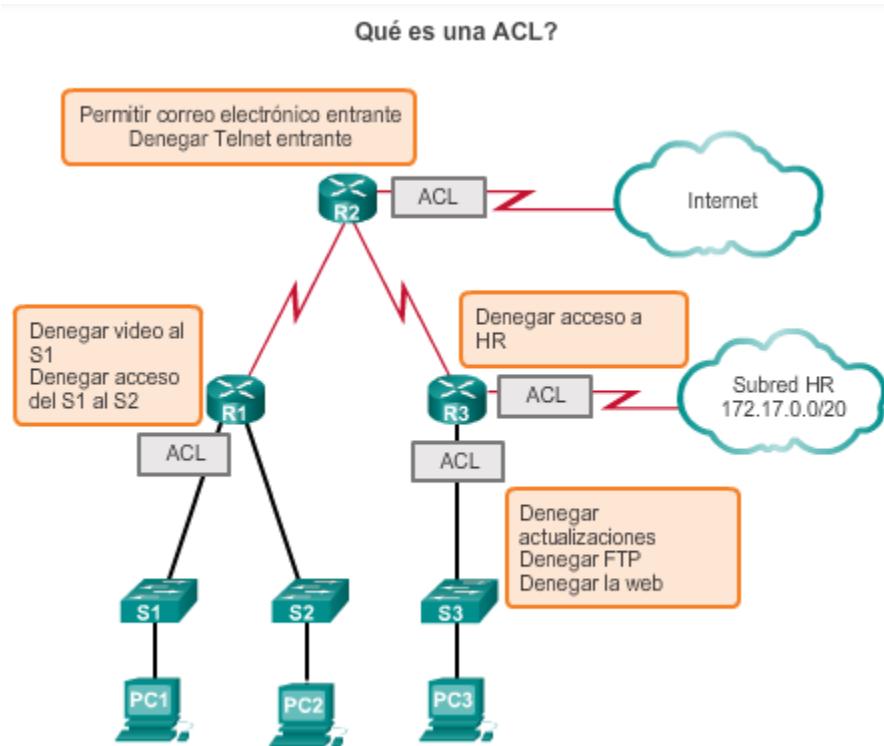
- Limitan el tráfico de la red para aumentar su rendimiento. Por ejemplo, si la política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que bloquen el tráfico de video. Esto reduciría considerablemente la carga de la red y aumentaría su rendimiento.
- Proporcionan control del flujo de tráfico. Las ACL pueden restringir la entrega de actualizaciones de routing. Si no se requieren actualizaciones debido a las condiciones de la red, se preserva ancho de banda.
- Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro host acceda a la misma área. Por ejemplo, se puede restringir el acceso a la red de Recursos Humanos a los usuarios autorizados.
- Filtran el tráfico según el tipo de tráfico. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de Telnet.

- Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos, como FTP o HTTP.

Los routers no tienen ACL configuradas de manera predeterminada, por lo que no filtran el tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing. Sin embargo, cuando se aplica una ACL a una interfaz, el router realiza la tarea adicional de evaluar todos los paquetes de red a medida que pasan a través de la interfaz para determinar si el paquete se puede reenviar.

Además de permitir o denegar tráfico, las ACL se pueden utilizar para seleccionar tipos de tráfico para analizar, reenviar o procesar de otras formas. Por ejemplo, se pueden utilizar ACL para clasificar el tráfico a fin de permitir el procesamiento por prioridad. Esta capacidad es similar a tener un pase vip para un concierto o un evento deportivo. El pase vip brinda a ciertos invitados privilegios que no se ofrecen a los asistentes que poseen entradas de admisión general, como prioridad de entrada o el ingreso a un área restringida.

En la ilustración, se muestra una topología de ejemplo a la que se le aplicaron ACL.



Las ACL permiten a los administradores controlar el tráfico hacia y desde la red. Este control puede ser tan simple como permitir o denegar el tráfico según las direcciones de red o tan complejo como controlar el tráfico de la red según el puerto TCP solicitado. Es más fácil comprender cómo filtra el tráfico una ACL si se examina el diálogo que se produce durante una conversación TCP, por ejemplo, cuando se solicita una página web.

Comunicación TCP

Cuando un cliente solicita datos a un servidor web, IP administra la comunicación entre la computadora (origen) y el servidor (destino). TCP administra la comunicación entre el navegador web (aplicación) y el software del servidor de red.

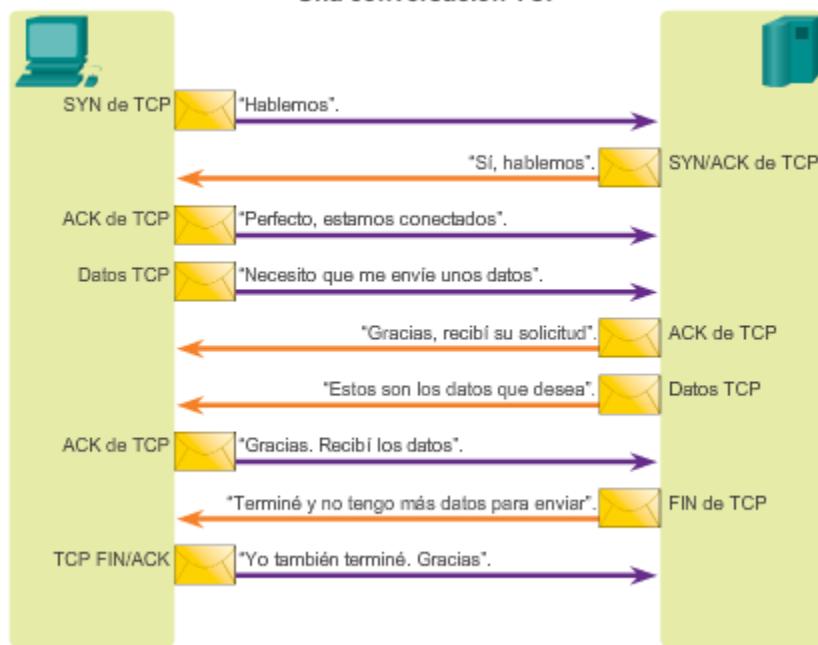
Cuando envía un correo electrónico, observa una página web o descarga un archivo, TCP se encarga de descomponer los datos en segmentos para IP antes de que se envíen. TCP también administra el montaje de los datos de los segmentos cuando estos llegan. El proceso de TCP es muy similar a una conversación en la que dos nodos en una red acuerdan transmitirse datos entre sí.

TCP proporciona un servicio de flujo de bytes confiable y orientado a la conexión. Que sea orientado a la conexión significa que las dos aplicaciones deben establecer una conexión TCP antes de intercambiar datos. TCP es un protocolo full-duplex, lo que significa que cada conexión TCP admite un par de flujos de bytes, y cada flujo fluye en una sentido. TCP incluye un mecanismo de control del flujo para cada flujo de bytes que permite que el receptor limite la cantidad de datos que puede transmitir el emisor. TCP también implementa un mecanismo de control de la congestión.

En la animación que se muestra en la figura 1, se ilustra cómo se lleva a cabo una conversación TCP/IP. Los segmentos TCP se marcan con indicadores que denotan su objetivo: la sesión comienza (se sincroniza) con un indicador SYN, el indicador ACK es un acuse de recibo de un segmento esperado, y un indicador FIN finaliza la sesión. Un indicador SYN/ACK confirma que la transferencia está sincronizada. Los segmentos de datos TCP incluyen el protocolo del nivel más alto necesario para dirigir los datos de aplicación a la aplicación correcta.

Los segmentos de datos TCP también identifican el puerto que coincide con el servicio solicitado. Por ejemplo, para HTTP es el puerto 80, para SMTP es el puerto 25 y para FTP son los puertos 20 y 21. En la figura 2, se muestran los rangos de puertos UDP y TCP.

En las figuras 3 a 5, se exploran los puertos TCP/UDP.

Una conversación TCP**Números de puerto**

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Puertos TCP

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Leyenda

Puertos TCP registrados:

- 1863 MSN Messenger
- 2000 Cisco SCCP (VoIP)
- 8008 HTTP alternativo
- 8080 HTTP alternativo

Puertos TCP bien conocidos:

- 21 FTP
- 23 Telnet
- 25 SMTP
- 80 HTTP
- 143 IMAP
- 194 Internet Relay Chat (IRC)
- 443 HTTP seguro (HTTPS)

Puertos UDP

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Leyenda

Puertos UDP registrados:

- 1812 Protocolo de autenticación RADIUS
- 5004 RTP (protocolo de transporte de voz y video)
- 5040 SIP (VoIP)

Puertos UDP bien conocidos:

- 69 TFTP
- 520 RIP

Puertos TCP/UDP comunes

Rango de números de puerto	Grupo de puertos
De 0 a 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Leyenda

Puertos TCP/UDP registrados comunes:

- 1433 MS SQL
- 2948 WAP (MMS)

Puertos TCP/UDP bien conocidos comunes:

- 53 DNS
- 161 SNMP
- 531 AOL Instant Messenger, IRC

Entonces, ¿cómo es que una ACL utiliza la información transferida durante una conversación TCP/IP para filtrar tráfico?

El filtrado de paquetes, a veces denominado “filtrado de paquetes estático”, controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según determinados criterios, como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete.

Cuando reenvía o deniega los paquetes según las reglas de filtrado, un router funciona como filtro de paquetes. Cuando llega un paquete a un router que filtra paquetes, el router extrae cierta información del encabezado. Con esta información, el router decide si el paquete puede pasar o si se debe descartar, según las reglas de los filtros configurados. Como se muestra en la ilustración, el filtrado de paquetes puede operar en diversas capas del modelo OSI o en la capa de Internet de TCP/IP.

Un router que filtra paquetes utiliza reglas para determinar si permite o deniega el tráfico. Un router también puede realizar el filtrado de paquetes en la capa 4, la capa de transporte. El router puede filtrar paquetes según el puerto de origen y de destino del segmento TCP o UDP. Estas reglas se definen mediante el uso de ACL.

Una ACL es una lista secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso” (ACE). Las ACE también se denominan comúnmente “instrucciones de ACL”. Las ACE se pueden crear para filtrar tráfico según ciertos criterios, como la dirección de origen, la dirección de destino, el protocolo y los números de puerto. Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada ACE, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda. De esta manera, se pueden configurar ACL para controlar el acceso a una red o a una subred.

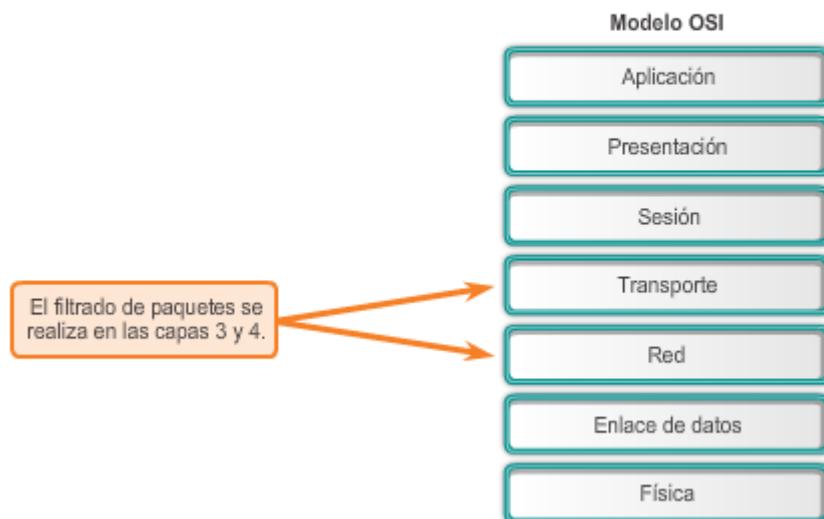
Para evaluar el tráfico de la red, la ACL extrae la siguiente información del encabezado de capa 3 del paquete:

- Dirección IP de origen
- Dirección IP de destino
- Tipo de mensaje ICMP

La ACL también puede extraer información de capa superior del encabezado de capa 4, incluido lo siguiente:

- Puerto de origen TCP/UDP
- Puerto de destino TCP/UDP

Filtrado de paquetes



Ejemplo del filtrado de paquetes

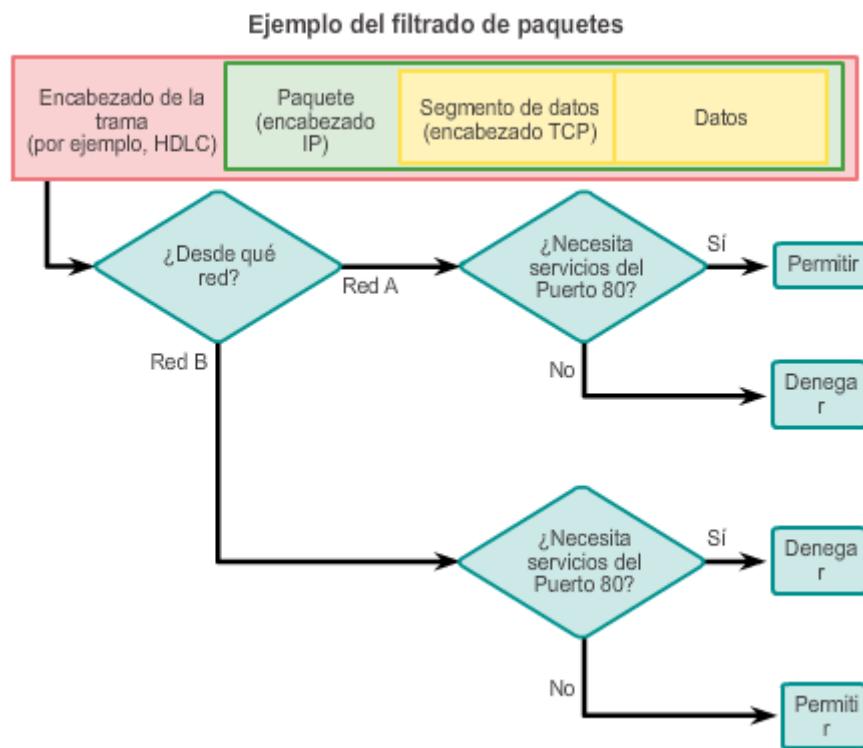
Para entender el concepto de cómo utiliza el router el filtrado de paquetes, imagine que se coloca un guarda en una puerta cerrada con llave. Las instrucciones del guarda son que solo permita el acceso por esa puerta a aquellas personas cuyos nombres aparecen en una lista. El guarda filtra las personas según el criterio de que los nombres aparezcan en la lista autorizada. Las ACL funcionan de manera similar: toman decisiones sobre la base de criterios establecidos.

Por ejemplo, una ACL se puede configurar para “permitir el acceso web a los usuarios de la red A, pero denegar el resto de los servicios a los usuarios de esa red. Denegar el acceso HTTP a los usuarios de la red B, pero permitir que los usuarios de esa red tengan todos los otros tipos de acceso”, de manera lógica. Consulte la ilustración para examinar la ruta de decisión que utiliza el filtro de paquetes para llevar a cabo esta tarea.

Para esta situación, el filtro de paquetes examina cada paquete de la siguiente manera:

- Si el paquete es un SYN de TCP de la red A que utiliza el puerto 80, tiene permiso para pasar. El resto de los tipos de acceso se deniega a esos usuarios.
- Si el paquete es un SYN de TCP de la red B que utiliza el puerto 80, se bloquea. Sin embargo, se permite el resto de los tipos de acceso.

Este es solo un ejemplo sencillo. Se pueden configurar varias reglas para permitir o denegar otros servicios a usuarios específicos.



Las ACL definen el conjunto de reglas que proporcionan un control adicional para los paquetes que ingresan por las interfaces de entrada, para los que retransmiten a través del router y para los que salen por las interfaces de salida del router. Las ACL no operan sobre paquetes que se originan en el router mismo.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente, como se muestra en la ilustración.

- **ACL de entrada:** los paquetes entrantes se procesan antes de enrutararse a la interfaz de salida. Las ACL de entrada son eficaces, porque ahoran la sobrecarga de enrutar búsquedas si el paquete se descarta. Si las pruebas permiten el paquete, este se procesa para el routing. Las ACL de entrada son ideales para filtrar los paquetes cuando la red conectada a una interfaz de entrada es el único origen de los paquetes que se deben examinar.
- **ACL de salida:** los paquetes entrantes se enrutan a la interfaz de salida y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica el mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

La última sentencia de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esta denegación implícita, una ACL que no tiene, por lo menos, una instrucción permit bloqueará todo el tráfico.



9.1.2 Comparación entre ACL de IPv4 estándar y extendidas

Los dos tipos de ACL de IPv4 de Cisco son estándar y extendida.

Nota: las ACL de IPv6 de Cisco son similares a las ACL de IPv4 extendidas y se abordarán en una sección posterior.

ACL estándar

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. En el ejemplo de la figura 1, se permite todo el tráfico de la red 192.168.30.0/24. Debido al “deny any” (denegar todo) implícito al final, todo el resto del tráfico se bloquea con esta ACL. Las ACL estándar se crean en el modo de configuración global.

ACL extendidas

Las ACL extendidas filtran paquetes IPv4 según varios atributos:

- Tipo de protocolo
- Dirección IPv4 de origen
- Dirección IPv4 de destino
- Puertos TCP o UDP de origen
- Puertos TCP o UDP de destino
- Información optativa de tipo de protocolo para un control más preciso

En la figura 2, la ACL 103 permite el tráfico que se origina desde cualquier dirección en la red 192.168.30.0/24 hasta cualquier red IPv4 si el puerto de host de destino es 80 (HTTP). Las ACL extendidas se crean en el modo de configuración global.

Los comandos para las ACL se abordan en los siguientes temas.

Nota: las ACL estándar y extendidas se analizarán en mayor detalle más adelante en este capítulo.

ACL estándar

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Las ACL estándar filtran paquetes IP solamente según la dirección de origen.

ACL extendidas

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Las ACL extendidas filtran paquetes IP según varios atributos, incluidos los siguientes:

- Las direcciones IP de origen y destino
- Los puertos TCP y UDP de origen y destino
- El tipo y número de protocolo (por ejemplo: IP, ICMP, UDP, TCP, etc.)

Las ACL estándar y extendidas se pueden crear con un número o un nombre para identificar la ACL y su lista de instrucciones.

El uso de ACL numeradas es un método eficaz para determinar el tipo de ACL en redes más pequeñas con tráfico definido de forma más homogénea. Sin embargo, un número no proporciona información sobre el propósito de la ACL. Por este motivo, a partir de la versión 11.2 del IOS de Cisco, se puede utilizar un nombre para identificar una ACL de Cisco.

En la ilustración, se resumen las reglas que se deben seguir para designar las ACL numeradas y con nombre.

En relación con las ACL numeradas, se omiten los números del 200 al 1299 debido a que esos números los utilizan otros protocolos, muchos de los cuales son antiguos u obsoletos. Este curso se centra solamente en las ACL de IP. Algunos ejemplos de números de protocolos ACL antiguos van del 600 al 699, utilizados por AppleTalk y del 800 al 899, utilizados por IPX.

Numeración y denominación de las ACL

ACL numerada:

Asignar un número según el protocolo que se debe filtrar.

- (1 a 99) y (1300 y 1999): ACL de IP estándar
- (100 a 199) y (2000 a 2699): ACL de IP extendida

ACL con nombre:

Asignar un nombre para identificar la ACL.

- Los nombres pueden contener caracteres alfanuméricos.
- Se sugiere escribir el nombre en MAYÚSCULAS.
- Los nombres no pueden contener espacios ni signos de puntuación.
- Se pueden agregar o eliminar entradas dentro de la ACL.

9.1.3 Máscaras wildcard en ACL

Máscara wildcard

Las ACE de IPv4 incluyen el uso de máscaras wildcard. Una máscara wildcard es una cadena de 32 dígitos binarios que el router utiliza para determinar los bits de la dirección que debe examinar para encontrar una coincidencia.

Nota: a diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir. Las ACL de IPv6 se analizan más adelante en este capítulo.

Como ocurre con las máscaras de subred, los números 1 y 0 en la máscara wildcard identifican lo que hay que hacer con los bits de dirección IP correspondientes. Sin embargo, en una máscara wildcard, estos bits se utilizan para fines diferentes y siguen diferentes reglas.

Las máscaras de subred utilizan unos y ceros binarios para identificar la red, la subred y la porción de host de una dirección IP. Las máscaras wildcard utilizan unos y ceros binarios para filtrar direcciones IP individuales o grupos de direcciones IP para permitir o denegar el acceso a los recursos.

Las máscaras wildcard y las máscaras de subred se diferencian en la forma en que establecen la coincidencia entre los unos y ceros binarios. Las máscaras wildcard utilizan las siguientes reglas para establecer la coincidencia entre los unos y ceros binarios:

- Bit 0 de máscara wildcard: se establece la coincidencia con el valor del bit correspondiente en la dirección.
- Bit 1 de máscara wildcard: se omite el valor del bit correspondiente en la dirección.

En la figura 1, se muestra cómo las diferentes máscaras wildcard filtran las direcciones IP. Recuerde que, en el ejemplo, el valor binario 0 indica un bit que debe coincidir y el valor binario 1 indica un bit que se puede ignorar.

Nota: a las máscaras wildcard a menudo se las denomina “máscaras inversas”. La razón es que, a diferencia de una máscara de subred en la que el 1 binario equivale a una coincidencia y el 0 binario no es una coincidencia, en las máscaras wildcard es al revés.

Uso de una máscara wildcard

En la tabla de la figura 2, se muestran los resultados de la aplicación de una máscara wildcard 0.0.255.255 a una dirección IPv4 de 32 bits. Recuerde que un 0 binario indica un valor con coincidencia.

Las máscaras wildcard también se utilizan para configurar algunos protocolos de routing IPv4, como OSPF, a fin de habilitar el protocolo en interfaces específicas.

Máscara wildcard									
Posición del bit de octeto y valor de dirección para el bit									
128	64	32	16	8	4	2	1		Ejemplos
0	0	0	0	0	0	0	0	0	= Hacer coincidir todos los bits de dirección (coincidir todos)
0	0	1	1	1	1	1	1	1	= Ignorar los últimos 6 bits de dirección
0	0	0	0	1	1	1	1	1	= Omitir los últimos 4 bits de la dirección
1	1	1	1	1	1	1	0	0	= Ignorar los primeros 6 bits de dirección
1	1	1	1	1	1	1	1	1	= Omitir todos los bits del octeto

0 significa hacer coincidir el valor del bit de dirección correspondiente
1 significa ignorar el valor del bit de dirección correspondiente

Ejemplo de máscara wildcard

	Dirección decimal	Dirección binaria
Dirección IP para procesar	192.168.10.0	11000000.10101000.00001010.00000000
Máscara wildcard	0.0.255.255	00000000.00000000.11111111.11111111
Dirección IP resultante	192.168.0.0	11000000.10101000.00000000.00000000

Máscaras wildcard para establecer coincidencias con subredes IPv4

Se necesita práctica para calcular la máscara wildcard. En la figura 1, se proporcionan tres ejemplos de máscara wildcard.

En el primer ejemplo, la máscara wildcard estipula que cada bit en la IPv4 192.168.1.1 debe coincidir con exactitud.

En el segundo ejemplo, la máscara wildcard estipula que no habrá coincidencias.

En el tercer ejemplo, la máscara wildcard estipula que cualquier host dentro de la red 192.168.1.0/24 tendrá una coincidencia.

Estos ejemplos son bastante simples y directos. Sin embargo, el cálculo de máscaras wildcard puede ser más complejo.

Máscaras wildcard para establecer coincidencias con rangos

Los dos ejemplos en la figura 2 son más complejos. En el ejemplo 1, los primeros dos octetos y los primeros cuatro bits del tercer octeto deben coincidir con exactitud. Los cuatro últimos bits del tercer octeto y el último octeto pueden ser cualquier número válido. Esto genera una máscara que verifica el rango de redes 192.168.16.0 a 192.168.31.0.

En el ejemplo 2, se muestra una máscara wildcard que coincide con los primeros dos octetos y el bit con menor importancia del tercer octeto. El último octeto y los primeros siete bits en el tercer octeto pueden ser cualquier número válido. Esto genera una máscara que permite o deniega todos los hosts de subredes impares de la red principal 192.168.0.0.

Máscaras wildcard para establecer coincidencias con hosts y subredes IPv4

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	0.0.0.0	00000000.00000000.00000000.00000000
Resultado	192.168.1.1	11000000.10101000.00000001.00000001

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	255.255.255.255	11111111.11111111.11111111.11111111
Resultado	0.0.0.0	00000000.00000000.00000000.00000000

Ejemplo 3

	Decimal	Binario
Dirección IP	192.168.1.1	11000000.10101000.00000001.00000001
Máscara wildcard	0.0.0.255	00000000.00000000.00000000.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000

Máscaras wildcard para establecer coincidencias con rangos

Ejemplo 1

	Decimal	Binario
Dirección IP	192.168.16.0	11000000.10101000.00010000.00000000
Máscara wildcard	0.0.15.255	00000000.00000000.00001111.11111111
Rango de resultados	De 192.168.16.0 a 192.168.31.255	De 11000000.10101000.00010000.00000000 a 11000000.10101000.00011111.11111111

Ejemplo 2

	Decimal	Binario
Dirección IP	192.168.1.0	11000000.10101000.00000001.00000000
Máscara wildcard	0.0.254.255	00000000.00000000.1111110.11111111
Resultado	192.168.1.0	11000000.10101000.00000001.00000000
	Todas las subredes con número impar en la red principal 192.168.0.0	

El cálculo de máscaras wildcard puede ser difícil. Un método abreviado es restar la máscara de subred a 255.255.255.255.

Cálculo de máscara wildcard: ejemplo 1

En el primer ejemplo en la ilustración, suponga que desea permitir el acceso a todos los usuarios en la red 192.168.3.0. Dado que la máscara de subred es 255.255.255.0, podría tomar 255.255.255.255 y restarle la máscara de subred 255.255.255.0. El resultado genera la máscara wildcard 0.0.0.255.

Cálculo de máscara wildcard: ejemplo 2

En el segundo ejemplo en la ilustración, suponga que desea permitir el acceso a la red a los 14 usuarios en la subred 192.168.3.32/28. La máscara de subred para la subred IP es 255.255.255.240; por lo tanto, tome 255.255.255.255 y réstale la máscara de subred 255.255.255.240. Esta vez, el resultado genera la máscara wildcard 0.0.0.15.

Cálculo de máscara wildcard: ejemplo 3

En el tercer ejemplo en la ilustración, suponga que solo quiere establecer la coincidencia con las redes 192.168.10.0 y 192.168.11.0. Una vez más, tome 255.255.255.255 y reste la máscara de subred regular que, en este caso, es 255.255.252.0. El resultado es 0.0.3.255.

Puede lograr el mismo resultado con instrucciones como las dos que se muestran a continuación:

```
R1(config)# access-list 10 permit 192.168.10.0
```

```
R1(config)# access-list 10 permit 192.168.11.0
```

Resulta mucho más eficaz configurar la máscara wildcard de la siguiente manera:

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.3.255
```

Tenga en cuenta la configuración que se indica a continuación para establecer coincidencias con las redes en el rango entre 192.168.16.0 y 192.168.31.0:

```
R1(config)# access-list 10 permit 192.168.16.0
```

```
R1(config)# access-list 10 permit 192.168.17.0
```

```
R1(config)# access-list 10 permit 192.168.18.0
```

```
R1(config)# access-list 10 permit 192.168.19.0
```

```
R1(config)# access-list 10 permit 192.168.20.0
```

```
R1(config)# access-list 10 permit 192.168.21.0
```

```
R1(config)# access-list 10 permit 192.168.22.0
```

```
R1(config)# access-list 10 permit 192.168.23.0
```

```
R1(config)# access-list 10 permit 192.168.24.0
```

```
R1(config)# access-list 10 permit 192.168.25.0
```

```
R1(config)# access-list 10 permit 192.168.26.0
```

```
R1(config)# access-list 10 permit 192.168.27.0
```

```
R1(config)# access-list 10 permit 192.168.28.0
```

```
R1(config)# access-list 10 permit 192.168.29.0
```

```
R1(config)# access-list 10 permit 192.168.30.0
```

```
R1(config)# access-list 10 permit 192.168.31.0
```

Las 16 instrucciones de configuración indicadas anteriormente se pueden reducir a una sola instrucción con la máscara wildcard correcta, como se muestra a continuación:

```
R1(config)# access-list 10 permit 192.168.16.0 0.0.15.255
```

Cálculo de máscara wildcard

Ejemplo 1

255.	255.	255.	255.	255
-	255.	255.	255.	000
				000.000.000.255

Ejemplo 2

255.	255.	255.	255.	255
-	255.	255.	255.	240
				000.000.000.015

Ejemplo 3

255.	255.	255.	255.	255
-	255.	255.	254.	000
				000.000.001.255

Palabras clave de la máscara de bits wildcard

Trabajar con representaciones decimales de los bits binarios de máscaras wildcard puede ser tedioso. Para simplificar esta tarea, las palabras clave **host** y **any** ayudan a identificar los usos más comunes de las máscaras wildcard. Estas palabras clave eliminan la necesidad de introducir máscaras wildcard para identificar un host específico o toda una red. También facilitan la lectura de una ACL, ya que proporcionan pistas visuales en cuanto al origen o el destino de los criterios.

La palabra clave **host** reemplaza la máscara 0.0.0.0. Esta máscara indica que todos los bits de direcciones IPv4 deben coincidir o que solo un host coincide.

La opción **any** sustituye la dirección IP y la máscara 255.255.255.255. Esta máscara establece que se omita la dirección IPv4 completa o que se acepte cualquier dirección.

Ejemplo 1: proceso de máscara wildcard con una única dirección IP

En el ejemplo 1 en la ilustración, en vez de introducir **192.168.10.10 0.0.0.0**, puede utilizar **host 192.168.10.10**.

Ejemplo 2: proceso de máscara wildcard con coincidencia con cualquier dirección IP

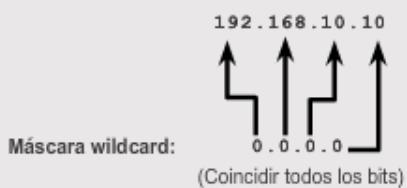
En el ejemplo 2 en la ilustración, en vez de introducir **0.0.0.0 255.255.255.255**, puede utilizar la palabra clave **any(cualquier)** sola.

Nota: Las palabras clave **host** y **any** solo se pueden utilizar al configurar una ACL de IPv6.

Abreviaturas de la máscara de bits wildcard

Ejemplo 1

- 192.168.10.10 0.0.0.0 coincide con todos los bits de la dirección.
- Abrevie esta máscara wildcard con la dirección IP precedida por la palabra clave **host** (**host** 192.168.10.10).



Ejemplo 2

- 0.0.0.0 255.255.255.255 omite todos los bits de la dirección.
- Abrevie la expresión con la palabra clave **any**.

Las palabras clave **any** y **host**

En el ejemplo 1 en la ilustración, se muestra cómo utilizar la palabra clave **any** para sustituir la dirección IPv4 0.0.0.0 por una máscara wildcard 255.255.255.255.

En el ejemplo 2, se muestra cómo utilizar la palabra clave **host** para sustituir la máscara wildcard para identificar un único host.

Las palabras clave **any** y **host**

Ejemplo 1:

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Ejemplo 2:

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

Este es el formato de las palabras clave optativas **host** y **any** en una instrucción de ACL.

Máscara wildcard	Instrucción de ACL
✓ 0.0.0.255	Denegar todos los hosts de la red 10.10.10.0/24.
✓ 0.0.0.0	Denegar el host 192.168.5.7.
✓ 0.0.0.255	Permitir todos los hosts de la subred 172.18.15.0/24.
✓ 0.0.0.0	Permitir el host 10.10.10.1.
✓ 0.255.255.255	Permitir todos los hosts de la red 10.0.0.0/8.
✓ 0.0.0.0	Denegar el host 172.18.33.1.
✓ 0.0.0.31	Permitir todos los hosts de la subred 192.168.5.0/27.
✓ 0.0.255.255	Denegar todos los hosts de la red 172.18.0.0/16.

Instrucción de ACL	Dirección de comparación	Permitir o denegar
access-list 50 permit 192.168.122.128 0.0.0.63	192.168.122.195	✓ Denegar
access-list 20 permit 192.168.223.64 0.0.0.15	192.168.223.72	✓ Permitir
access-list 30 permit 192.168.223.32 0.0.0.31	192.168.223.60	✓ Permitir
access-list 1 permit 192.168.155.0 0.0.0.255	192.168.155.245	✓ Permitir
access-list 33 permit 198.51.100.58 0.0.0.63	198.51.100.3	✓ Permitir
access-list 21 permit 192.0.2.11 0.0.0.15	192.0.2.17	✓ Denegar
access-list 50 permit 192.168.155.0 0.0.0.255	192.168.156.245	✓ Denegar

9.1.4 Pautas para la creación de ACL

La composición de ACL puede ser una tarea compleja. Para cada interfaz, puede haber varias políticas necesarias para administrar el tipo de tráfico que tiene permitido ingresar a la interfaz o salir de ella. El router en la ilustración tiene dos interfaces configuradas para IPv4 e IPv6. Si necesitáramos ACL para ambos protocolos, en ambas interfaces y en ambos sentidos, esto requeriría ocho ACL diferentes. Cada interfaz tendría cuatro ACL: dos ACL para IPv4 y dos ACL para IPv6. Para cada protocolo, una ACL es para el tráfico entrante y otra para el tráfico saliente.

Nota: las ACL no deben configurarse en ambos sentidos. La cantidad de ACL y el sentido aplicado a la interfaz dependen de los requisitos que se implementen.

Las siguientes son algunas pautas para el uso de ACL:

- Utilice las ACL en los routers de firewall ubicados entre su red interna y una red externa, como Internet.
- Utilice las ACL en un router ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de su red interna o que sale de esta.
- Configure las ACL en los routers de frontera, es decir, los routers ubicados en los límites de las redes. Esto proporciona una separación muy básica de la red externa o entre un área menos controlada y un área más importante de su propia red.
- Configure las ACL para cada protocolo de red configurado en las interfaces del router de frontera.

Las tres P

Para recordar una regla general de aplicación de ACL en un router, puede pensar en “las tres P”. Se puede configurar una ACL por protocolo, por sentido y por interfaz:

- **Una ACL por protocolo:** para controlar el flujo de tráfico en una interfaz, se debe definir una ACL para cada protocolo habilitado en la interfaz.
- **Una ACL por sentido:** las ACL controlan el tráfico en una interfaz de a un sentido por vez. Se deben crear dos ACL diferentes para controlar el tráfico entrante y saliente.
- **Una ACL por interfaz:** las ACL controlan el tráfico para una interfaz, por ejemplo, GigabitEthernet 0/0.

Filtrado de tráfico en un router mediante ACL



Con dos interfaces y dos protocolos en ejecución, este router podría tener un total de ocho ACL distintas aplicadas.

Las tres P para utilizar ACL

Solo se puede tener una ACL por protocolo, por interfaz y por sentido:

- Una ACL por protocolo (p. ej., IPv4 o IPv6)
- Una ACL por sentido (es decir, de entrada o de salida)
- Una ACL por interfaz (p. ej., FastEthernet0/0)

El uso de las ACL requiere prestar atención a los detalles y un extremo cuidado. Los errores pueden ser costosos en términos de tiempo de inactividad, esfuerzos de resolución de problemas y servicio de red deficiente. Antes de configurar una ACL, se requiere una planificación básica. En la ilustración, se presentan pautas que constituyen la base de una lista de prácticas recomendadas para ACL.

Optimizaciones de las ACL

Pautas	Beneficios
Fundamente sus ACL según las políticas de seguridad de la organización.	Esto asegurará la implementación de las pautas de seguridad de la organización.
Prepare una descripción de lo que desea que realicen las ACL.	Esto lo ayudará a evitar posibles problemas de acceso generados de manera inadvertida.
Utilice un editor de texto para crear, editar y guardar las ACL.	Esto lo ayudará a crear una biblioteca de ACL reutilizables.
Pruebe sus ACL en una red de desarrollo antes de implementarlas en una red de producción.	Esto lo ayudará a evitar errores costosos.

Finalización	Funcionamiento de las ACL
✓ Permitir	Una lista de control de acceso (ACL) controla si el router _____ o _____ el tráfico de paquetes según los criterios del encabezado del paquete.
✓ Denegar	
✓ Firewall	Las ACL suelen utilizarse en routers entre las redes internas y externas para proporcionar _____.
✓ Dose	Un router con tres interfaces y dos protocolos de red (IPv4 e IPv6) puede tener un máximo de _____ ACL activas.
✓ Antes	Para las ACL de entrada, los paquetes entrantes se procesan _____ se envían a la interfaz de salida.
✓ Después	Para las ACL de salida, los paquetes entrantes se procesan _____ se envían a la interfaz de salida.
✓ Descartado	Para cada ACL, hay una instrucción deny implícita. Si un paquete no coincide con los criterios de ACL, será _____.
✓ Interfaz	Las ACL pueden filtrar el tráfico de datos por protocolo, por sentido y por _____.
✓ Protocolo	Las ACL pueden filtrar el tráfico según la dirección de origen/destino, _____ y los números de puerto.

9.1.5 Pautas para la colocación de ACL

La correcta colocación de las ACL puede contribuir a que la red funcione de forma más eficaz. Se puede colocar una ACL para reducir el tráfico innecesario. Por ejemplo, el tráfico que se denegará en un destino remoto no se debe reenviar mediante recursos de red por la ruta hacia ese destino.

Cada ACL se debe colocar donde tenga más impacto en la eficiencia. Como se muestra en la ilustración, las reglas básicas son las siguientes:

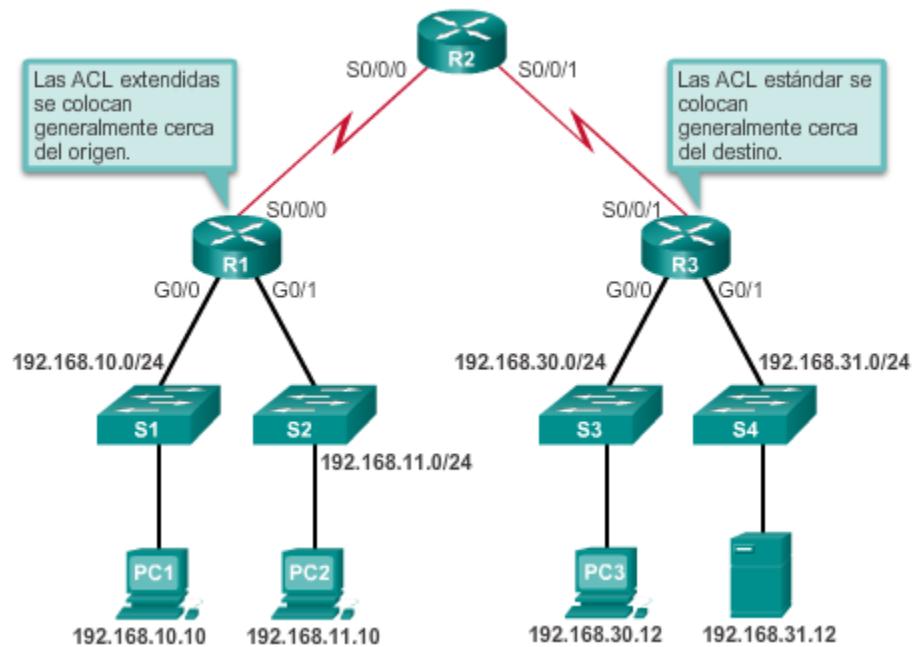
- **ACL extendidas:** coloque las ACL extendidas lo más cerca posible del origen del tráfico que se filtrará. De esta manera, el tráfico no deseado se deniega cerca de la red de origen, sin que cruce la infraestructura de red.
- **ACL estándar:** debido a que en las ACL estándar no se especifican las direcciones de destino, colóquelas tan cerca del destino como sea posible. Si coloca una ACL estándar en el origen del tráfico, evitará de forma eficaz que ese tráfico llegue a cualquier otra red a través de la interfaz a la que se aplica la ACL.

La colocación de la ACL y, por lo tanto, el tipo de ACL que se utiliza también puede depender de lo siguiente:

- **Alcance del control del administrador de la red:** la colocación de la ACL puede depender de si el administrador de red controla tanto la red de origen como la de destino o no.
- **Ancho de banda de las redes involucradas:** el filtrado del tráfico no deseado en el origen impide la transmisión de ese tráfico antes de que consuma ancho de banda en la ruta hacia un destino. Esto es de especial importancia en redes con un ancho de banda bajo.
- **Facilidad de configuración:** si un administrador de red desea denegar el tráfico proveniente de varias redes, una opción es utilizar una única ACL estándar en el router más cercano al destino. La desventaja es que el tráfico de dichas redes utilizará ancho de banda de manera innecesaria. Se puede utilizar una ACL extendida en cada router donde se origina tráfico. Esto ahorra ancho de banda, ya que el tráfico se filtra en el origen, pero requiere la creación de ACL extendidas en varios routers.

Nota: para la certificación CCNA, la regla general es que las ACL extendidas se coloquen lo más cerca posible del origen y que las ACL estándar se coloquen lo más cerca posible del destino.

Colocación de ACL



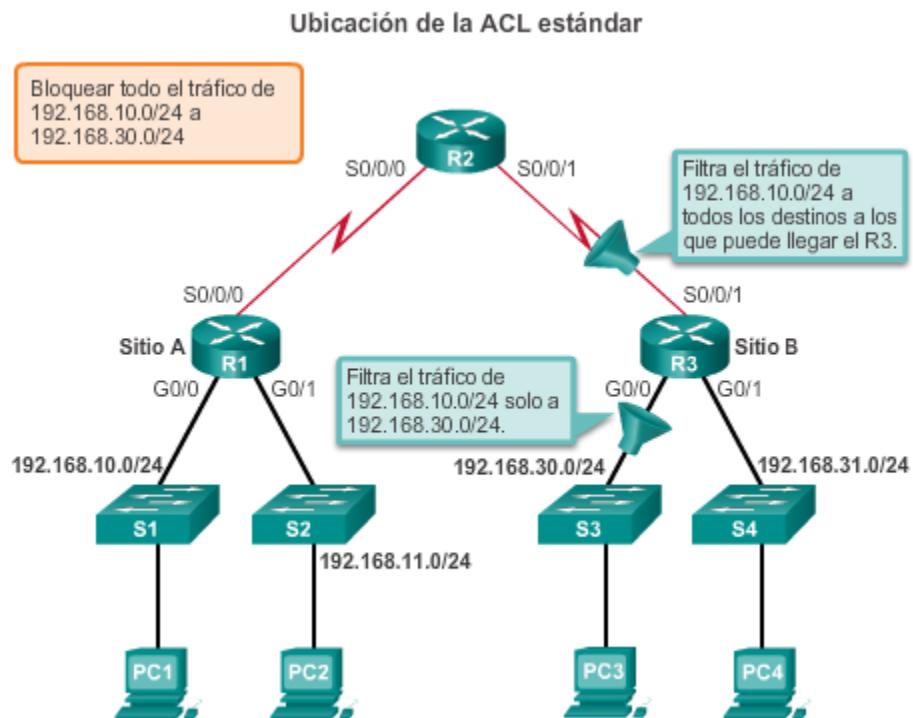
Las ACL estándar solo pueden filtrar tráfico según la dirección de origen. La regla básica para la colocación de una ACL estándar es colocar la ACL lo más cerca posible de la red de destino. Esto permite que el tráfico llegue a todas las demás redes, excepto la red que filtra los paquetes.

En la ilustración, el administrador desea impedir que el tráfico que se origina en la red 192.168.10.0/24 llegue a la red 192.168.30.0/24.

Si la ACL estándar se coloca en la interfaz de salida del R1, eso evitaría que el tráfico de la red 192.168.10.0/24 alcance cualquier red a la que se pueda llegar a través de la interfaz Serial 0/0/0 del R1.

De acuerdo con las pautas básicas de colocación de ACL estándar cerca del destino, en la ilustración se muestran dos interfaces posibles del R3 a las que aplicar la ACL estándar:

- **Interfaz S0/0/1 del R3:** la aplicación de una ACL estándar para impedir que el tráfico de 192.168.10.0/24 ingrese a la interfaz S0/0/1 evita que dicho tráfico llegue a 192.168.30.0/24 y al resto de las redes a las que puede llegar el R3. Esto incluye la red 192.168.31.0/24. Dado que el objetivo de la ACL es filtrar el tráfico destinado solo a 192.168.30.0/24, no se debe aplicar una ACL estándar a esta interfaz.
- **Interfaz G0/0 del R3:** al aplicar una ACL estándar al tráfico que sale por la interfaz G0/0, se filtran los paquetes que van de 192.168.10.0/24 a 192.168.30.0/24. Esto no afecta a las otras redes a las que puede llegar el R3. Los paquetes de 192.168.10.0/24 aún pueden llegar a 192.168.31.0/24.



Al igual que las ACL estándar, las ACL extendidas pueden filtrar el tráfico según la dirección de origen. Sin embargo, las ACL extendidas también pueden filtrar el tráfico según la dirección de destino, el protocolo y el número de puerto. Esto permite que los administradores de red tengan más flexibilidad en cuanto al tipo de tráfico que se puede filtrar y dónde colocar la ACL. La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen. Esto evita que el tráfico no deseado se envíe a través de varias redes y luego sea denegado cuando llegue a destino.

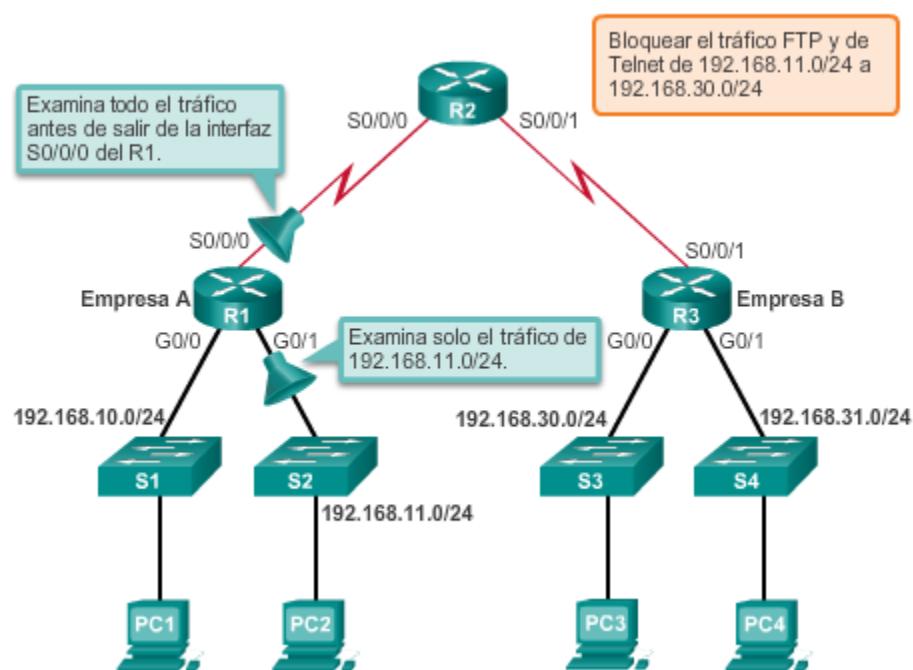
Los administradores de red solo pueden colocar ACL en los dispositivos que controlan. Por lo tanto, la colocación se debe determinar en el contexto de hasta dónde se extiende el control del administrador de red. En la ilustración, se muestra que el administrador de la empresa A, que incluye las redes 192.168.10.0/24 y 192.168.11.0/24 (denominadas .10 y .11 en este ejemplo), desea controlar el tráfico a la empresa B. Lo que el administrador desea específicamente es denegar el tráfico de Telnet y FTP de la red .11 a la red 192.168.30.0/24 de la empresa B (.30 en este ejemplo). Al mismo tiempo, se debe permitir que el resto del tráfico de la red .11 salga de la empresa A sin restricciones.

Existen varias formas de lograr estos objetivos. Una ACL extendida en el R3 que bloquee Telnet y FTP de la red .11 cumpliría el objetivo, pero el administrador no controla el R3. Además, esta solución también permite que el tráfico no deseado cruce toda la red y luego sea bloqueado en el destino. Esto afecta la eficacia general de la red.

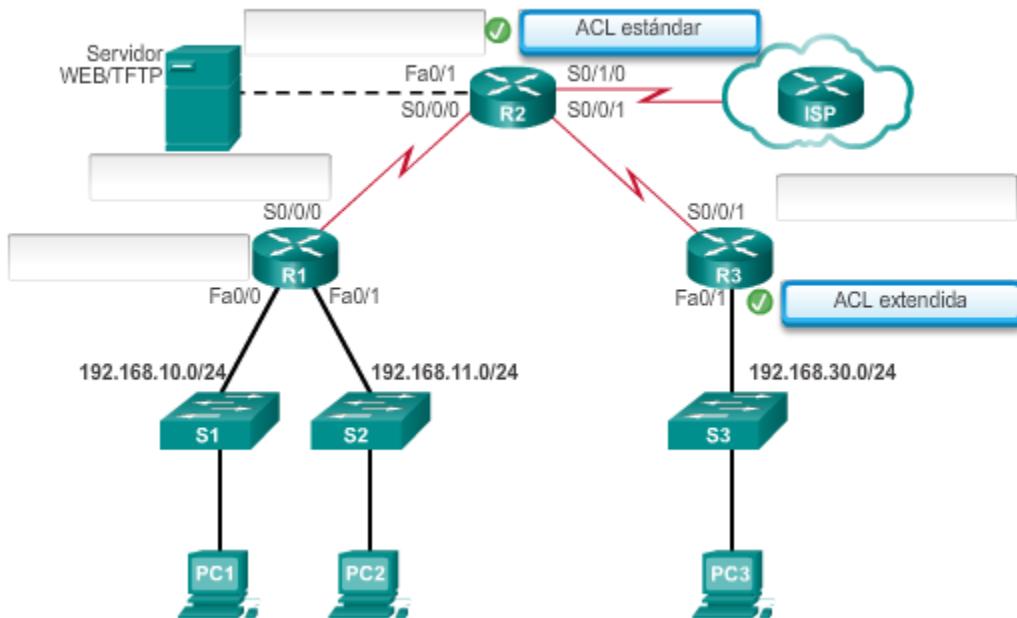
Una mejor solución es colocar una ACL extendida en el R1 que especifique tanto las direcciones de origen como las de destino (redes .11 y .30, respectivamente) y que aplique la regla “no se permite que el tráfico de Telnet y FTP de la red .11 vaya a la red .30”. En la ilustración, se muestran dos interfaces posibles en el R1 para aplicar la ACL extendida:

- **Interfaz S0/0/0 del R1 (de salida):** una de las posibilidades es aplicar una ACL extendida de salida en la interfaz S0/0/0. Debido a que la ACL extendida puede examinar tanto la dirección de origen como la de destino, solo se deniegan los paquetes FTP y Telnet de 192.168.11.0/24, y el R1 reenvía el resto del tráfico de 192.168.11.0/24 y de otras redes. La desventaja de colocar la ACL extendida en esta interfaz es que la ACL debe procesar todo el tráfico que sale de S0/0/0, incluidos los paquetes de 192.168.10.0/24.
- **Interfaz G0/1 del R1 (de entrada):** la aplicación de una ACL extendida al tráfico que ingresa a la interfaz G0/1 implica que solamente los paquetes de la red 192.168.11.0/24 están sujetos al procesamiento de la ACL en el R1. Debido a que el filtro se debe limitar solo a aquellos paquetes que salen de la red 192.168.11.0/24, la aplicación de una ACL extendida a G0/1 es la mejor solución.

Ubicación de la ACL extendida



Actividad: colocar ACL estándar y extendidas



9.2 ACL de IPv4 estándar

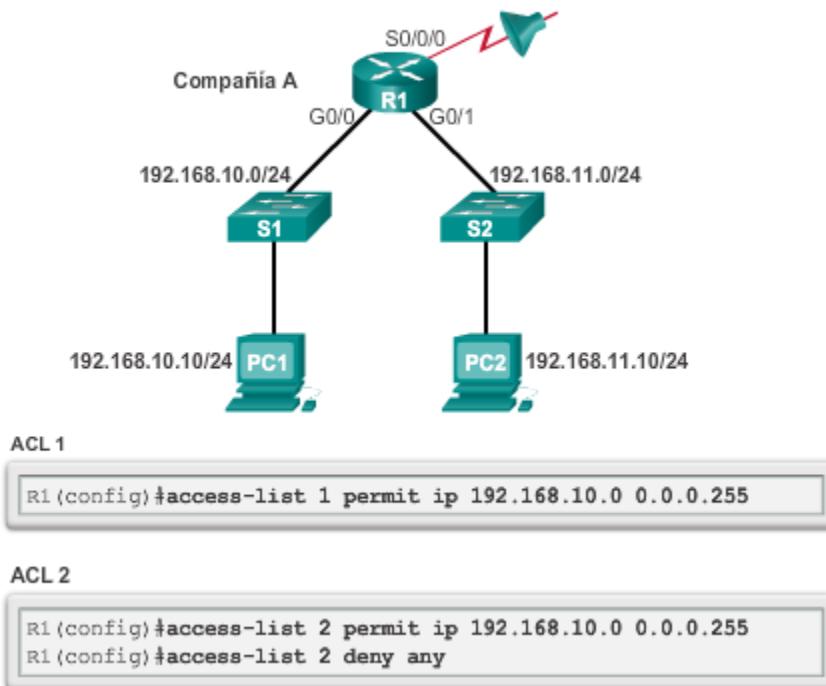
9.2.1 Configuración de ACL de IPv4 estándar

Cuando el tráfico ingresa al router, se compara con todas las ACE en el orden en que las entradas se encuentran en la ACL. El router continúa procesando las ACE hasta que encuentra una coincidencia. El router procesa el paquete según la primera coincidencia y no se examinan más ACE.

Si no se encuentran coincidencias cuando el router llega al final de la lista, se deniega el tráfico. Esto se debe a que, de manera predeterminada, hay una denegación implícita al final de todas las ACL para el tráfico sin coincidencias con una entrada configurada. Una ACL de entrada única con solo una entrada de denegación tiene el efecto de denegar todo el tráfico. Se debe configurar al menos una ACE permit en una ACL. En caso contrario, se bloquea todo el tráfico.

Para la red en la ilustración, si se aplica la ACL 1 o la ACL 2 a la interfaz S0/0/0 del R1 en el sentido de salida, se obtiene el mismo resultado. A la red 192.168.10.0 se le permite acceder a las redes a las que puede llegar mediante S0/0/0, mientras que a 192.168.11.0 no se le permite acceder a esas redes.

Cómo ingresar sentencias de criterios

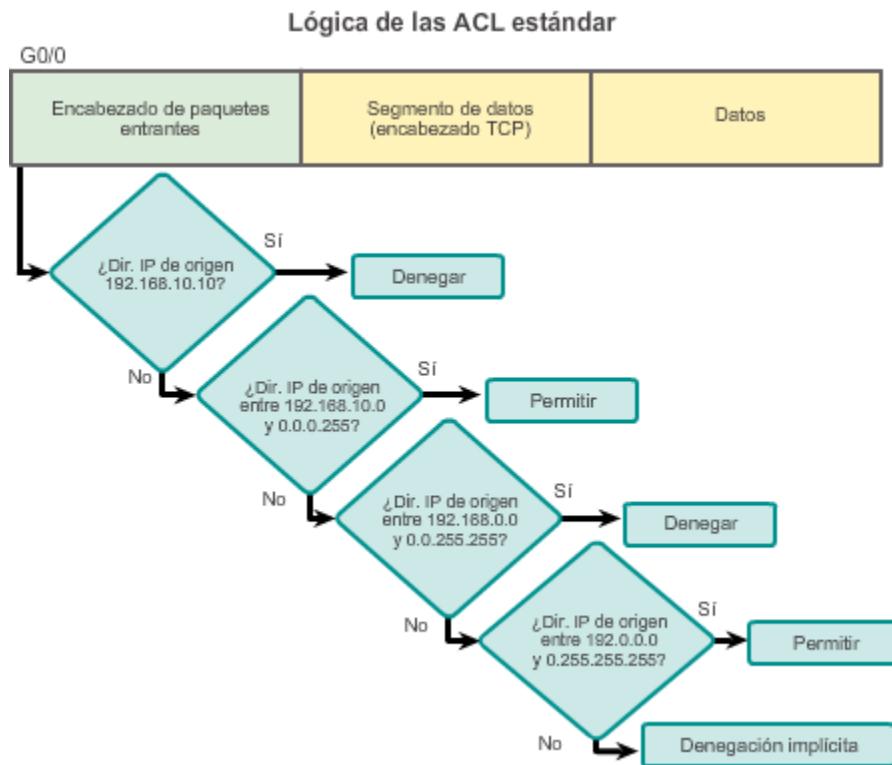


Lógica de las ACL estándar

En la ilustración, se revisa la dirección de origen de los paquetes que ingresan al router a través de la interfaz G0/0 según las siguientes entradas:

```
access-list 2 deny 192.168.10.10
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 0.255.255.255
```

Si se permiten los paquetes, se enrutan a través del router hacia una interfaz de salida. Si se niegan los paquetes, se descartan en la interfaz de entrada.



Configurar las ACL estándar.

Para utilizar ACL estándar numeradas en un router Cisco, primero debe crear la ACL estándar y, a continuación, activarla en una interfaz.

El comando de configuración **global access-list** define una ACL estándar con un número entre 1 y 99. La versión 12.0.1 del software IOS de Cisco amplió ese intervalo y permite que se utilicen los números que van de 1300 a 1999 para las ACL estándar. Esto permite que se genere un máximo de 798 ACL estándar posibles. A estos números adicionales se los denomina “ACL de IP extendidas”.

La sintaxis completa del comando de ACL estándar es la siguiente:

```
Router(config)# access-list access-list-number { deny | permit | remark } Origen [source-wildcard] [log]
```

En la figura 1, se explica detalladamente la sintaxis para una ACL estándar.

Las ACE pueden permitir o denegar un solo host o un rango de direcciones host. Para crear una instrucción de host en la ACL numerada 10 que permita un host específico con la dirección IP 192.168.10.0, debe introducir lo siguiente:

```
R1(config)# access-list 10 permit host 192.168.10.10
```

Como se muestra en la figura 2, para crear una instrucción que permita un rango de direcciones IPv4 en una ACL numerada 10 que permite todas las direcciones IPv4 en la red 192.168.10.0/24, debe introducir lo siguiente:

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
```

Para eliminar la ACL, se utiliza el comando de configuración global `no access-list`. La ejecución del comando `show access-list` confirma que se eliminó la lista de acceso 10.

Por lo general, cuando un administrador crea una ACL, conoce y entiende el objetivo de cada instrucción. Sin embargo, para asegurar que el administrador y otras personas recuerden el propósito de las instrucciones, se deben incluir comentarios (remarks). La palabra clave `remark` se utiliza en los documentos y hace que sea mucho más fácil comprender las listas de acceso. El texto de cada comentario tiene un límite de 100 caracteres. La ACL que se muestra en la figura 3, que es bastante simple, se utiliza a modo de ejemplo. Cuando se revisa la ACL en la configuración mediante el comando `show running-config`, también se muestra el comentario.

Sintaxis de comando de la ACL estándar `access-list`

Parámetro	Descripción
<code>access-list-number</code>	Número de una ACL. Es un número decimal del 1 al 99 o del 1300 al 1999 (para las ACL estándar).
<code>deny</code>	Deniega el acceso si las condiciones concuerdan.
<code>permit</code>	Permite el acceso si las condiciones concuerdan.
<code>remark</code>	Agregue un comentario sobre las entradas en la lista de acceso IP para facilitar la comprensión y el análisis de la lista.
<code>origen</code>	Número de la red o del host desde el que se envía el paquete. Existen dos formas de especificar el <code>origen</code> : <ul style="list-style-type: none"> • Utilice una cantidad de 32bits en formato decimal punteado de cuatro partes. • Utilice la palabra clave <code>any</code> como abreviatura de <code>origen</code> y <code>wildcard-origen</code> de 0.0.0.0 255.255.255.255.
<code>source-wildcard</code>	(Opcional) Máscara wildcard de 32bits para aplicar al origen. Coloca unos en las posiciones de bits que desea omitir.
<code>log</code>	(Opcional) Genera un mensaje de registro informativo en la consola acerca del paquete que coincide con la entrada. (El nivel de mensajes registrados en la consola lo controla el comando <code>logging console</code>). El mensaje incluye el número de ACL, si el paquete fue permitido o denegado, la dirección de origen y la cantidad de paquetes. El mensaje se genera para el primer paquete que coincide y, luego, a intervalos de cinco minutos, incluida la cantidad de paquetes permitidos o denegados en el intervalo de cinco minutos anterior.

Eliminación de una ACL

```
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#exit
R1#show access-lists
Standard IP access list 10
    10 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#conf t
Enter configuration commands, one per line. End with
CTRL/Z.
R1(config)#no access-list 10
R1(config)#exit
R1#show access-lists
R1#
```

```
R1(config)#access-list 10 remark Permit hosts from the
192.168.10.0 LAN
R1(config)#access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#exit
R1#show running-config | include access-list 10
access-list 10 remark Permit hosts from the 192.168.10.0 LAN
access-list 10 permit 192.168.10.0 0.0.0.255
R1#
```

El IOS de Cisco aplica una lógica interna al aceptar y procesar las ACE estándar. Como se mencionó anteriormente, las ACE se procesan en forma secuencial, por lo que el orden en que se introducen es importante.

Por ejemplo, en la figura 1, la ACL 3 contiene dos ACE. La primera ACE utiliza una máscara wildcard para denegar un rango de direcciones que incluye todos los hosts en la red 192.168.10.0/24. La segunda ACE es una instrucción de host que examina un host específico: 192.168.10.10. Este es un host dentro del rango de hosts que se configuró en la instrucción anterior. Es decir, 192.168.10.10 es un host en la red 192.168.10.0/24. La lógica interna del IOS para las listas de acceso estándar rechaza la segunda instrucción y envía un mensaje de error, porque es un subconjunto de la instrucción anterior. Observe que, en la ilustración, el router asigna automáticamente el número de secuencia 10 como número de secuencia asignado a la primera instrucción introducida en este ejemplo. El resultado del router incluye el mensaje “part of the existing rule at sequence num 10” en referencia a la regla (“parte de la regla existente en el número de secuencia 10”) y no acepta la instrucción.

Nota: actualmente, las ACL extendidas no producen errores similares.

La configuración en la figura 2 de la ACL 4 tiene las mismas dos instrucciones, pero en orden inverso. Esta es una secuencia válida de instrucciones, porque la primera instrucción se refiere a un host específico, no a un rango de hosts.

En la figura 3, la ACL 5 muestra que se puede configurar una instrucción de host después de una instrucción que denota un rango de hosts. El host no debe estar dentro del rango que abarca una instrucción anterior. La dirección host 192.168.11.10 no forma parte de la red 192.168.10.0/24, por lo que se trata de una instrucción válida.

Nota: es posible que el orden en que se introducen las ACE estándar no sea el orden en que se almacenen, se muestren o se procesen en el router. Esto se analizará en una sección posterior.

Conflictos con las instrucciones

```
R1(config)#access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#End
```

ACL 3: la instrucción de host entra en conflicto con la instrucción de rango anterior.

Instrucción de host introducida antes que la instrucción de rango

```
R1(config)#access-list 4 permit host 192.168.10.10
R1(config)#access-list 4 deny 192.168.10.0 0.0.0.255
R1(config)#End
```

ACL 4: la instrucción de host siempre puede configurarse antes que las instrucciones de rango.

Host configurado después del rango sin conflictos

```
R1(config)#access-list 5 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 5 permit host 192.168.11.10
R1(config)#End
```

ACL 5: si no existen conflictos, la instrucción de host se puede configurar después que la instrucción de rango.

Procedimientos de configuración de ACL estándar

Después de que se configura una ACL estándar, se vincula a una interfaz mediante el comando **ip access-group** del modo de configuración de interfaz:

```
Router(config-if)# ip      access-group { access-list-number | nombre-lista-
acceso } { pre | out}
```

Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** en la interfaz y, a continuación, introduzca el comando global **no access-list** para eliminar la ACL completa.

En la figura 1, se enumeran los pasos y la sintaxis para configurar y aplicar una ACL estándar numerada en un router.

En la figura 2, se muestra un ejemplo de una ACL para permitir una sola red.

Esta ACL solo permite que se reenvíe mediante la interfaz S0/0/0 el tráfico de la red de origen 192.168.10.0. El tráfico proveniente de redes distintas de la red 192.168.10.0 se bloquea.

En la primera línea, se identifica la ACL como lista de acceso 1. Esta lista permite el tráfico que coincide con los parámetros seleccionados. En este caso, la dirección IPv4 y la máscara wildcard que identifican a la red de origen son 192.168.10.0 0.0.0.255. Recuerde que existe una denegación implícita de todas las instrucciones que equivale a agregar la línea **access-list 1 deny 0.0.0.0 255.255.255.255**.

El comando de configuración de interfaz **ip access-group 1 out** vincula la ACL 1 a la interfaz Serial 0/0/0 como filtro de salida.

Por lo tanto, la ACL 1 solo permite que los hosts de la red 192.168.10.0/24 salgan por el router R1. Esta lista deniega cualquier otra red, incluida la red 192.168.11.0.

Procedimiento para la configuración de ACL estándar

Paso 1: utilice el comando de configuración global **access-list** para crear una entrada en una ACL de IPv4 estándar.

```
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
```

La sentencia del ejemplo coincide con cualquier dirección que comience con 192.168.10.x. Utilice la opción **comentario** para agregar una descripción a su ACL.

Paso 2: utilice el comando de configuración **interface** para seleccionar una interfaz a la cual aplicarle la ACL.

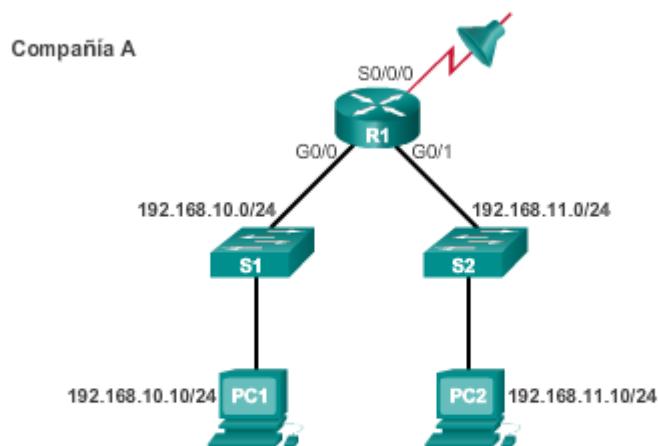
```
R1(config)#interface serial 0/0/0
```

Paso 3: utilice el comando de configuración de interfaz **ip access-group** para activar la ACL actual en una interfaz.

```
R1(config-if)#ip access-group 1 out
```

Este ejemplo activa la ACL estándar IPv4 1 en la interfaz como filtro de salida.

Admisión de una subred específica



```
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 1 out
```

En la figura 1, se muestra un ejemplo de una ACL que permite una subred específica, a excepción de un host específico en esa subred.

Esta ACL reemplaza el ejemplo anterior, pero también bloquea el tráfico de una dirección específica. El primer comando elimina la versión anterior de la ACL 1. La siguiente instrucción de ACL deniega el host de la PC1 ubicado en 192.168.10.10. Todos los demás hosts en la red

192.168.10.0/24 se permiten. En este caso, la instrucción deny implícita también coincide con todas las demás redes.

La ACL se vuelve a aplicar a la interfaz S0/0/0 en sentido de salida.

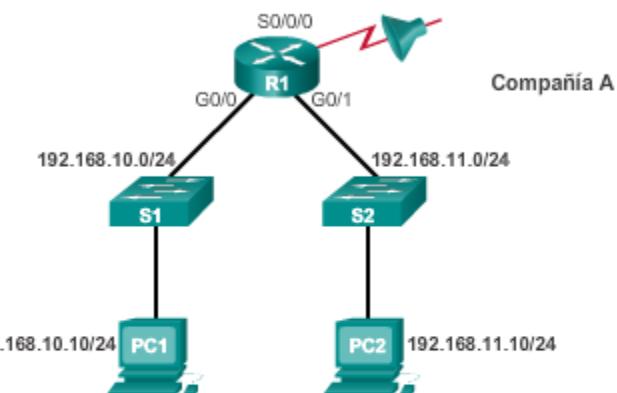
En la figura 2, se muestra un ejemplo de una ACL que deniega un host específico. Esta ACL reemplaza el ejemplo anterior. En este ejemplo, se sigue bloqueando el tráfico del host PC1, pero se permite el resto del tráfico.

Los primeros dos comandos son los mismos que en el ejemplo anterior. El primer comando elimina la versión anterior de la ACL 1, y la siguiente instrucción de ACL deniega el host PC1 que está ubicado en 192.168.10.10.

La tercera línea es nueva y permite el resto de los hosts. Esto significa que se permiten todos los hosts de la red 192.168.10.0/24, excepto PC1, que se denegó en la instrucción anterior.

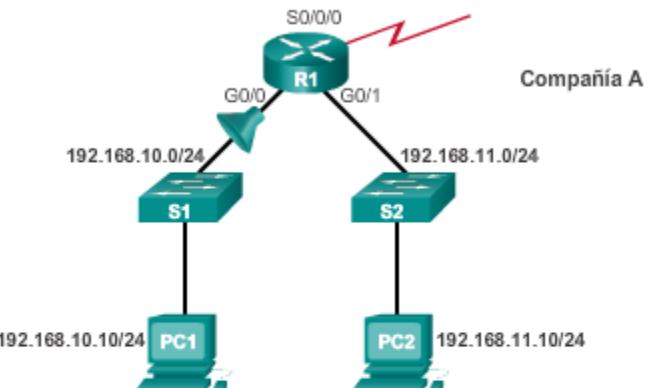
Esta ACL se aplica a la interfaz G0/0 en sentido de entrada. Debido a que el filtro afecta únicamente a la LAN 192.168.10.0/24 en G0/0, es más eficaz aplicar la ACL a la interfaz de entrada. Se puede aplicar la ACL a s0/0/0 en sentido de salida, pero entonces el R1 tendría que examinar los paquetes de todas las redes, incluida 192.168.11.0/24.

Denegación de un host específico y admisión de una subred específica



```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#interface s0/0/0
R1(config-if)#ip access-group 1 out
```

Denegación de un host específico



```
R1(config)#no access-list 1
R1(config)#access-list 1 deny host 192.168.10.10
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
```

La asignación de nombres a las ACL hace más fácil comprender su función. Por ejemplo, una ACL configurada para denegar el tráfico FTP se podría llamar NO_FTP. Cuando se identifica la ACL con un nombre en lugar de un número, el modo de configuración y la sintaxis de los comandos son sutilmente diferentes.

En la figura 1, se muestran los pasos necesarios para crear una ACL estándar con nombre.

Paso 1. En el modo de configuración global, utilice el comando **ip access-list** para crear una ACL con nombre. Los nombres de las ACL son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. El comando **ip access-list standard nombre** se utiliza para crear una ACL estándar con nombre, mientras que el comando **ip access-list extended nombre** se utiliza para una lista de acceso extendida. Después de introducir el comando, el router se encuentra en el modo de configuración de ACL estándar con nombre, según lo que indica la petición de entrada.

Nota: las ACL numeradas utilizan el comando de configuración global **access-list**, mientras que las ACL de IPv4 con nombre utilizan el comando **ip access-list**.

Paso 2. En el modo de configuración de ACL con nombre, utilice las instrucciones **permit** o **deny** a fin de especificar una o más condiciones para determinar si un paquete se reenvía o se descarta.

Paso 3. Aplique la ACL a una interfaz con el comando **ip access-group**. Especifique si la ACL se debe aplicar a los paquetes cuando ingresan por la interfaz (**in**) o cuando salen de la interfaz (**out**).

En la figura 2, se muestran los comandos que se utilizan para configurar una ACL estándar con nombre en el router R1, en la que la interfaz G0/0 deniega el acceso del host 192.168.11.10 a la red 192.168.10.0. La ACL se llama NO_ACCESS.

No es necesario que los nombres de las ACL comiencen con mayúscula, pero esto los hace destacarse cuando se observa el resultado de show running-config. También hace que sea menos probable que cree accidentalmente dos ACL diferentes con el mismo nombre pero con distinto uso de mayúsculas.

Ejemplo de ACL con nombre

```
Router(config)# ip access-list [standard | extended] name
```

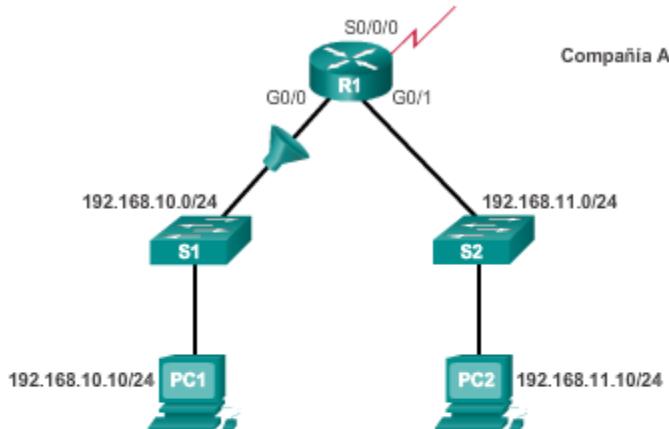
La cadena de nombres alfanuméricos debe ser única y no puede comenzar con un número.

```
Router(config-std-nacl)# [permit | deny | remark] {source  
[source-wildcard]} [log]
```

```
Router(config-if)# ip access-group name [in | out]
```

Activa la ACL de IP con nombre en una interfaz.

Ejemplo de ACL con nombre



```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

Puede utilizar la palabra clave **remark** para incluir comentarios (remarks) sobre entradas en cualquier ACL de IP estándar o extendida. Estos comentarios facilitan la comprensión y la revisión de las ACL. Cada línea de comentarios tiene un límite de 100 caracteres.

El comentario puede ir antes o después de una instrucción **permit** o **deny**. Debe ser coherente en cuanto a la ubicación del comentario, de manera que quede claro qué comentario describe cuál de las instrucciones **permit** o **deny**. Por ejemplo, sería confuso colocar algunos comentarios antes de las instrucciones **permit** o **deny** correspondientes y otros después de estas.

Para incluir un comentario para las ACL de IPv4 estándar o extendidas numeradas, utilice el comando de configuración global **access-list lista-acceso_número remark comentario**. Para eliminar el comentario, utilice la versión **no** de este comando.

En el primer ejemplo, se muestra que la ACL numerada deniega la salida de la estación de trabajo de invitado 192.168.10.10 por S0/0/0, pero permite el resto de los dispositivos de 192.168.0.0/16.

Para crear una entrada en una ACL estándar o extendida con nombre, utilice el comando de configuración de lista de acceso **remark**. Para eliminar el comentario, utilice la versión **no** de este comando. En el ejemplo 2, se muestra una ACL estándar con nombre. En este ejemplo, las instrucciones **remark** indican que se deniega la estación de trabajo de laboratorio con la dirección host 192.168.11.10, pero que los dispositivos de las demás redes están permitidos.

Comentarios sobre las ACL

Ejemplo 1: comentario sobre una ACL numerada

```
R1(config)# access-list 1 remark Do not allow Guest workstation
through
R1(config)# access-list 1 deny host 192.168.10.10
R1(config)# access-list 1 remark Allow devices from all other
192.168.x.x subnets
R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 1 out
R1(config-if)#End
```

Ejemplo 2: comentario sobre una ACL con nombre

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# remark Do not allow access from Lab
workstation
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# remark Allow access from all other networks
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config-std-nacl)# interface G0/0
R1(config-if)# ip access-group NO_ACCESS out
R1(config-if)#End
```

9.2.2 Modificación de ACL de IPv4

Edición de ACL numeradas

Cuando se configura una ACL estándar, las instrucciones se agregan a la configuración en ejecución. Sin embargo, no hay una característica de edición incorporada que permita realizar cambios en una ACL.

Existen dos maneras de editar una ACL estándar numerada.

Método 1: uso de un editor de texto

Después de familiarizarse con el proceso de creación y edición de ACL, puede ser más fácil generar la ACL mediante un editor de texto como el Bloc de notas de Microsoft. Esto permite crear o editar la ACL y luego pegarla en el router. Para una ACL existente, puede utilizar el comando `show running-config` para mostrar la ACL, copiarla y pegarla en el editor de texto, realizar los cambios necesarios y pegarla nuevamente en el router.

Configuración. Suponga, por ejemplo, que la dirección host IPv4 de la ilustración se introdujo incorrectamente. En lugar del host 192.168.10.99, debería ser el host 192.168.10.10. Los pasos para editar y corregir la ACL 1 son los siguientes:

Paso 1. Muestre la ACL mediante el comando `show running-config`. En el ejemplo de la ilustración, se utiliza la palabra clave `include` para mostrar solamente las ACE.

Paso 2. Seleccione la ACL, cópiela y, luego, péguela en el Bloc de notas de Microsoft. Edite la lista según sea necesario. Una vez que la ACL se muestre correctamente en el Bloc de notas de Microsoft, selecciónela y cópiela.

Paso 3. En el modo de configuración global, elimine la lista de acceso con el comando `no access-list 1`. De lo contrario, las nuevas instrucciones se agregarán a la ACL existente. A continuación, pegue la nueva ACL en la configuración del router.

Paso 4. Verifique los cambios mediante el comando `show running-config`.

Es necesario recordar que, al utilizar el comando `no access-list`, las distintas versiones del software IOS actúan de forma diferente. Si la ACL que se eliminó sigue estando aplicada a una interfaz, algunas versiones del IOS actúan como si no hubiera ninguna ACL que proteja la red, mientras que otras deniegan todo el tráfico. Por esta razón, es aconsejable eliminar la referencia a la lista de acceso de la interfaz antes de modificar la lista. Además, tenga en cuenta que si hay un error en la nueva lista, debe deshabilitarla y solucionar el problema. En ese caso, la red no tiene ninguna ACL durante el proceso de corrección.

Edición de ACL numeradas mediante un editor de texto

Configuración	<pre>R1(config)# access-list 1 deny host 192.168.10.99 R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255</pre>
Paso 1	<pre>R1# show running-config include access-list 1 access-list 1 deny host 192.168.10.99 access-list 1 permit 192.168.0.0 0.0.255.255</pre>
Paso 2	<pre><Editor de texto> access-list 1 deny host 192.168.10.10 access-list 1 permit 192.168.0.0 0.0.255.255</pre>
Paso 3	<pre>R1# config t Enter configuration commands, one per line. End with CTRL/Z. R1(config)# no access-list 1 R1(config)# access-list 1 deny host 192.168.10.10 R1(config)# access-list 1 permit 192.168.0.0 0.0.255.255</pre>
Paso 4	<pre>R1# show running-config include access-list 1 access-list 1 deny host 192.168.10.10 access-list 1 permit 192.168.0.0 0.0.255.255</pre>

Método 2: uso del número de secuencia

Como se muestra en la ilustración, en la configuración inicial de la ACL 1 se incluyó una instrucción de host para el host 192.168.10.99, pero eso fue un error. Se debería haber configurado el host 192.168.10.10. Para editar la ACL con los números de secuencia, siga estos pasos:

Paso 1. Muestre la ACL actual mediante el comando **show access-lists 1**. El resultado de este comando se analizará en mayor detalle más adelante en esta sección. El número de secuencia se muestra al principio de cada instrucción. El número de secuencia se asignó automáticamente cuando se introdujo la instrucción de la lista de acceso. Observe que la instrucción que está mal configurada tiene el número de secuencia 10.

Paso 2. Introduzca el comando **ip access-lists standard** que se utiliza para configurar las ACL con nombre. El número de la ACL, 1, se utiliza como nombre. Primero, la instrucción mal configurada se debe eliminar con el comando **no 10**, donde “10” se refiere al número de secuencia. Luego, se agrega una nueva instrucción de número de secuencia 10 mediante el comando **10 deny host 192.168.10.10**.

Nota: las instrucciones no se pueden sobrescribir con el mismo número de secuencia que el de una instrucción existente. Primero se debe eliminar la instrucción actual y, luego, se puede agregar la nueva.

Paso 3. Verifique los cambios mediante el comando **show access-lists**.

Como se mencionó anteriormente, el IOS de Cisco implementa una lógica interna en las listas de acceso estándar. Es posible que el orden en que se introducen las ACE estándar no sea el orden en que se almacenen, se muestren o se procesen en el router. El comando **show access-lists** muestra las ACE con sus números de secuencia.

Edición de ACL numeradas mediante números de secuencia

Configuración	<pre>R1(config)#access-list 1 deny host 192.168.10.99 R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255</pre>
Paso 1	<pre>R1#show access-lists 1 Standard IP access list 1 10 deny 192.168.10.99 20 permit 192.168.0.0, wildcard bits 0.0.255.255 R1#</pre>
Paso 2	<pre>R1#conf t R1(config)#ip access-list standard 1 R1(config-std-nacl)#no 10 R1(config-std-nacl)#10 deny host 192.168.10.10 R1(config-std-nacl)#end R1#</pre>
Paso 3	<pre>R1#show access-lists Standard IP access list 1 10 deny 192.168.10.10 20 permit 192.168.0.0, wildcard bits 0.0.255.255 R1#</pre>

En un ejemplo anterior, se utilizaron los números de secuencia para editar una ACL estándar numerada. Mediante una referencia a los números de secuencia de la instrucción, se pueden insertar o eliminar fácilmente instrucciones individuales. Este método también se puede utilizar para editar las ACL estándar con nombre.

En la ilustración, se muestra un ejemplo de inserción de una línea en una ACL con nombre.

- En el primer resultado del comando **show**, se puede ver que la ACL con el nombre NO_ACCESS tiene dos líneas numeradas que indican las reglas de acceso para una estación de trabajo con la dirección IPv4 192.168.11.10.
- El comando **ip access-list standard** se utiliza para configurar las ACL con nombre. Se pueden insertar o eliminar instrucciones desde el modo de configuración de listas de acceso con nombre. El comando **no número-secuencia** se utiliza para eliminar instrucciones individuales.
- Para agregar una instrucción para denegar otra estación de trabajo, se debe insertar una línea numerada. En el ejemplo, se agrega la estación de trabajo con la dirección IPv4 192.168.11.11 mediante el nuevo número de secuencia 15.
- Mediante el último resultado del comando **show**, se verifica que la nueva estación de trabajo ahora tiene el acceso denegado.

Cómo agregar una línea a la ACL con nombre

```
R1# show access-lists
Standard IP access list NO_ACCESS
 10 deny 192.168.11.10
 20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# conf t
Enter configuration commands, one per line. End with
CNTL/Z.
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# 15 deny host 192.168.11.11
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list NO_ACCESS
 10 deny 192.168.11.10
 15 deny 192.168.11.11
 20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Nota: el comando `no` `número-de-secuencia` de ACL con nombre se usa para eliminar instrucciones individuales.

Como se muestra en la figura 1, el comando `show ip interface` se utiliza para verificar la ACL en la interfaz. El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL. El resultado muestra que la lista de acceso 1 se aplica a la interfaz de salida S0/0/0 del router R1 y que la lista de acceso NO_ACCESS se aplica a la interfaz 0/0/0, también en sentido de salida.

En el ejemplo de la figura 2, se muestra el resultado de emitir el comando `show access-lists` en el router R1. Para ver una lista de acceso individual, utilice el comando `show access-lists` seguido del número o el nombre de la lista de acceso. Es posible que las instrucciones de NO_ACCESS se vean extrañas. Observe que el número de secuencia 15 se muestra antes que el número de secuencia 10. Esto se debe al proceso interno del router y se analizará más adelante en esta sección.

Verificación de interfaces de ACL estándar

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
<resultado omitido>
  Outgoing access list is 1
  Inbound access list is not set
<resultado omitido>

R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<resultado omitido>
  Outgoing access list is NO_ACCESS
  Inbound access list is not set
<resultado omitido>
```

Una vez que la ACL se aplicó a una interfaz y se realizaron algunas pruebas, el comando **show access-lists** muestra las estadísticas para cada instrucción que tiene coincidencias. En el resultado que se muestra en la figura 1, observe que se encontraron coincidencias para algunas de las instrucciones. Cuando se genera tráfico que debe coincidir con una instrucción de ACL, las coincidencias que se muestran en el resultado del comando **show access-lists** deberían aumentar. Por ejemplo, en este caso, si se hace ping de la PC1 a la PC3 o la PC4, en el resultado se mostrará un aumento en las coincidencias para la instrucción deny de ACL 1.

Tanto las instrucciones permit como las deny realizan un seguimiento de las estadísticas de coincidencias; sin embargo, recuerde que cada ACL tiene una instrucción deny any implícita como última instrucción. Esta instrucción no aparece en el comando **show access-lists**, por lo que no se muestran estadísticas para esa instrucción. Para ver las estadísticas de la instrucción deny any implícita, la instrucción se puede configurar manualmente y aparecerá en el resultado. Se debe tener sumo cuidado cuando se configura manualmente la instrucción deny any, ya que coincidirá con todo el tráfico. Si esta instrucción no se configura como la última instrucción en la ACL, podría ocasionar resultados inesperados.

Durante la prueba de una ACL, se pueden borrar los contadores mediante el comando **clear access-list counters**. Este comando se puede utilizar solo o con el número o el nombre de una ACL específica. Como se muestra en la figura 2, este comando borra los contadores de estadísticas para una ACL.

Visualización de estadísticas de ACL

```
R1# show access-lists
Standard IP access list 1
    10 deny  192.168.10.10 (4 match(es))
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO ACCESS
    15 deny  192.168.11.11
    10 deny  192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Resultado después del ping de PC1 a PC3.

```
R1# show access-lists
Standard IP access list 1
    10 deny  192.168.10.10 (8 match(es)) Aumentaron las coincidencias.
    20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO ACCESS
    15 deny  192.168.11.11
    10 deny  192.168.11.10 (4 match(es))
    20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1#
```

Eliminación de estadísticas de ACL

```
R1# show access-lists
Standard IP access list 1
  10 deny  192.168.10.10 (8 match(es))
  20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO ACCESS
  15 deny  192.168.11.11
  10 deny  192.168.11.10 (4 match(es))
  20 permit 192.168.11.0, wildcard bits 0.0.0.255
R1# clear access-list counters 1
R1#
R1# show access-lists
Standard IP access list 1
  10 deny  192.168.10.10
  20 permit 192.168.0.0, wildcard bits 0.0.255.255
Standard IP access list NO ACCESS
  15 deny  192.168.11.11
  10 deny  192.168.11.10 (4 match(es))
  20 permit 192.168.11.0, wildcard bits 0.0.0.255
```

Se borraron las coincidencias.

El IOS de Cisco implementa una lógica interna en las ACL estándar. Como se mencionó anteriormente, una parte de esta lógica evita que las instrucciones de host se configuren después de una instrucción de rango si el host es parte de ese rango, como se muestra en la figura 1.

Otra parte de la lógica interna del IOS es responsable de la secuenciación interna de las ACE estándar. En la figura 2, se muestra la configuración de una lista de acceso estándar. Las instrucciones de rango que deniegan tres redes se configuran primero, y después se configuran cinco instrucciones de host. Las instrucciones de host son todas instrucciones válidas, porque sus direcciones IP host no forman parte de las instrucciones de rango introducidas previamente.

El comando **show running-config** se utiliza para verificar la configuración de la ACL. Observe que las instrucciones se enumeran en un orden distinto al orden en que se introdujeron. Utilizaremos el comando **show access-lists** para comprender la lógica detrás de esto.

Como se muestra en la figura 3, el comando **show access-lists** muestra las ACE junto con sus números de secuencia. Sería de esperar que el orden de las instrucciones en el resultado reflejara el orden en que se introdujeron. Sin embargo, el resultado de **show access-lists** muestra que este no es el caso.

El orden en que se enumeran las ACE estándar es la secuencia utilizada por el IOS para procesar la lista. Observe que las instrucciones se agrupan en dos secciones: las instrucciones de host seguidas por las instrucciones de rango. El número de secuencia indica el orden en que se introdujo la instrucción, no el orden en que se procesará.

Las instrucciones de host se enumeran primero, pero no necesariamente en el orden en que se introdujeron. El IOS ordena las instrucciones de host mediante una función de hash especial. El orden resultante optimiza la búsqueda de una entrada de ACL de host.

Las instrucciones de rango se muestran después de las instrucciones de host. Estas instrucciones se enumeran en el orden en que se introdujeron.

Recuerde que las ACL estándar y numeradas se pueden editar con números de secuencia. El número de secuencia que se muestra en el resultado del comando **show access-lists** es el

número utilizado para eliminar las instrucciones individuales de la lista. Cuando se introduce una nueva instrucción de ACL, el número de secuencia solo afecta a la ubicación de una instrucción de rango en la lista. Las instrucciones de host siempre se ordenan con la función de hash.

Siguiendo con el ejemplo, una vez que se guarda la configuración en ejecución, el router se vuelve a cargar (se reinicia). Como se muestra en la figura 3, el comando `show access-lists` muestra la ACL en el mismo orden, sin embargo, las instrucciones se volvieron a numerar. Los números de secuencia ahora están en orden numérico.

Nota: la función de hash se aplica solamente a las instrucciones de host en listas de acceso de IPv4 estándar. El algoritmo no se utiliza para las ACL de IPv4 extendidas ni las ACL de IPv6. Esto se debe a que las ACL extendidas e IPv6 filtran más de una sola dirección de origen. Los detalles de la función de hash exceden el ámbito de este curso.

```
R1(config)# access-list 3 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 3 permit host 192.168.10.10
% Access rule can't be configured at higher sequence num as
it is part of the existing rule at sequence num 10
R1(config)#

```

Consideraciones de secuenciación durante la configuración

```
R1(config)# access-list 1 deny 192.168.10.0 0.0.0.255
R1(config)# access-list 1 deny 192.168.20.0 0.0.0.255
R1(config)# access-list 1 deny 192.168.30.0 0.0.0.255
R1(config)# access-list 1 permit 10.0.0.1
R1(config)# access-list 1 permit 10.0.0.2
R1(config)# access-list 1 permit 10.0.0.3
R1(config)# access-list 1 permit 10.0.0.4
R1(config)# access-list 1 permit 10.0.0.5
R1(config)# end
R1# show running-config | include access-list 1
access-list 1 permit 10.0.0.2
access-list 1 permit 10.0.0.3
access-list 1 permit 10.0.0.1
access-list 1 permit 10.0.0.4
access-list 1 permit 10.0.0.5
access-list 1 deny 192.168.10.0 0.0.0.255
access-list 1 deny 192.168.20.0 0.0.0.255
access-list 1 deny 192.168.30.0 0.0.0.255
R1#

```

Números de secuencia después de la recarga

```
R1# show access-lists 1
Standard IP access list 1
 50 permit 10.0.0.2
 60 permit 10.0.0.3
 40 permit 10.0.0.1
 70 permit 10.0.0.4
 80 permit 10.0.0.5
 10 deny   192.168.10.0, wildcard bits 0.0.0.255
 20 deny   192.168.20.0, wildcard bits 0.0.0.255
 30 deny   192.168.30.0, wildcard bits 0.0.0.255
R1# copy running-config startup-config
R1# reload
R1# show access-lists 1
Standard IP access list 1
 10 permit 10.0.0.2
 20 permit 10.0.0.3
 30 permit 10.0.0.1
 40 permit 10.0.0.4
 50 permit 10.0.0.5
 60 deny   192.168.10.0, wildcard bits 0.0.0.255
 70 deny   192.168.20.0, wildcard bits 0.0.0.255
 80 deny   192.168.30.0, wildcard bits 0.0.0.255
```

Las instrucciones de host se enumeran primero en un orden que permita que IOS los procese de manera eficaz.

Las instrucciones de rango se enumeran después de las instrucciones de host, en el orden en que se introdujeron.

9.2.3 Protección de puertos VTY con una ACL de IPv4 estándar

Uso de una ACL para controlar el acceso a VTY

Cisco recomienda utilizar SSH para las conexiones administrativas a los routers y switches. Si la imagen del software IOS de Cisco en su router no admite SSH, puede mejorar la seguridad de las líneas administrativas mediante la restricción del acceso a VTY. La restricción del acceso a VTY es una técnica que permite definir las direcciones IP a las que se les permite acceder por Telnet al proceso de EXEC del router. Puede controlar qué estación de trabajo administrativa o qué red administra el router mediante la configuración de una ACL y una instrucción **access-class** en las líneas VTY. También puede utilizar esta técnica con SSH para mejorar aún más la seguridad de acceso administrativo.

El comando **access-class** configurado en el modo de configuración de línea restringe las conexiones de entrada y salida entre una VTY determinada (en un dispositivo de Cisco) y las direcciones en una lista de acceso.

Las listas de control de acceso estándar y extendidas se aplican a los paquetes que se transportan a través de un router, no están diseñadas para bloquear los paquetes que se originan en el router. Una ACL extendida para Telnet de salida no evita las sesiones de Telnet iniciadas por el router de manera predeterminada.

Por lo general, se considera que el filtrado del tráfico de Telnet o SSH es una función de una ACL de IP extendida, porque filtra un protocolo de nivel superior. Sin embargo, debido a que se utiliza el comando **access-class** para filtrar sesiones de Telnet/SSH entrantes o salientes por dirección de origen, se puede utilizar una ACL estándar.

La sintaxis del comando **access-classes** la siguiente:

```
Router          (config) # access-class número-lista-acceso { pre [ vrf-
also ] | out }
```

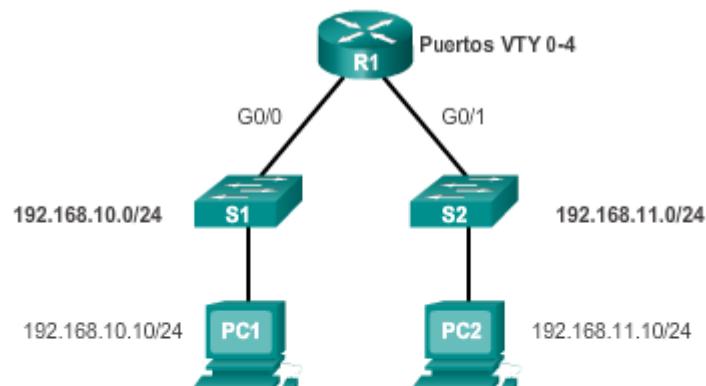
El parámetro **in** limita las conexiones de entrada entre las direcciones en la lista de acceso y el dispositivo de Cisco, mientras que el parámetro **out** limita las conexiones de salida entre un dispositivo de Cisco en particular y las direcciones en la lista de acceso.

En la figura 1, se muestra un ejemplo en el que se permite que un rango de direcciones acceda a las líneas VTY de 0 a 4. La ACL de la ilustración se configuró para permitir que la red 192.168.10.0 acceda a las líneas VTY de 0 a 4, pero para denegar las demás redes.

Para configurar listas de acceso en los VTY, se debe tener en cuenta lo siguiente:

- Solamente se pueden aplicar listas de acceso numeradas a los VTY.
- Se deben establecer restricciones idénticas en todos los VTY, porque un usuario puede intentar conectarse a cualquiera de ellos.

Utilice el verificador de sintaxis de la figura 2 para poner en práctica la protección del acceso a VTY.

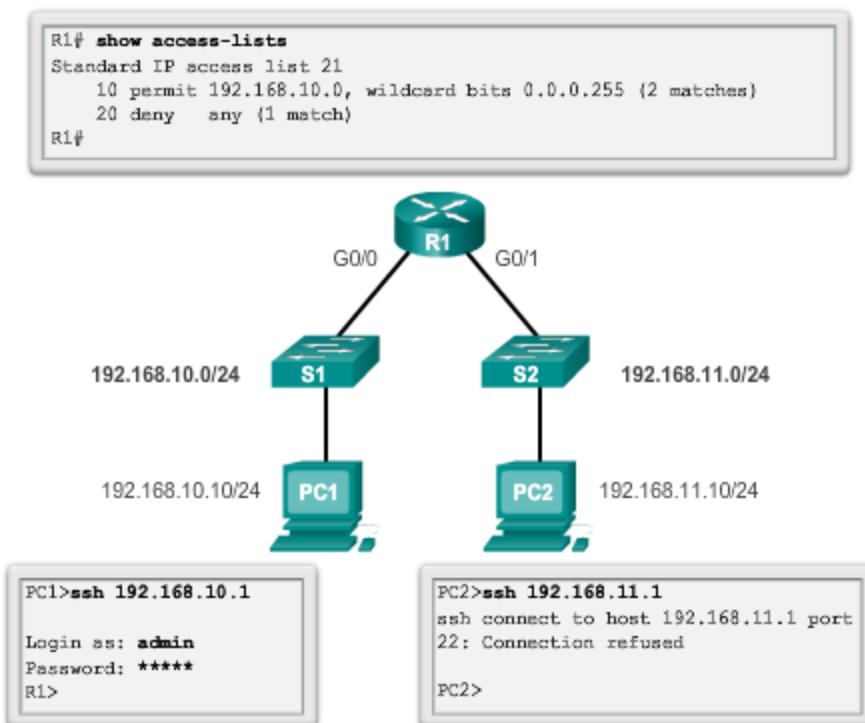


```
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#access-class 21 in
R1(config-line)#exit
R1(config)#access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 21 deny any
```

Después de configurar la ACL para restringir el acceso a las líneas VTY, es importante verificar que funcione correctamente. En la ilustración, se muestran dos dispositivos que intentan conectarse al R1 mediante SSH. Se configuró la lista de acceso 21 en las líneas VTY en el R1. La PC1 logra conectarse, mientras que la PC2 no puede establecer una conexión SSH. Este es el

comportamiento que se espera, ya que la lista de acceso configurada permite el acceso a VTY desde la red 192.168.10.0/24 y deniega al resto de los dispositivos.

El resultado del R1 muestra lo que se produce al emitir el comando `show access-lists` después de que la PC1 y la PC2 intentan conectarse mediante SSH. La coincidencia en la línea permit del resultado es producto de una conexión SSH correcta de la PC1. La coincidencia en la instrucción deny se debe al intento fallido de la PC2, un dispositivo en la red 192.168.11.0/24, de establecer una conexión SSH.



9.3 ACL de IPv4 extendidas

9.3.1 Estructura de una ACL de IPv4 extendida

Prueba de paquetes con ACL extendidas

Para un control más preciso del filtrado del tráfico, se pueden crear ACL de IPv4 extendidas. Las ACL extendidas se numeran del 100 al 199 y del 2000 a 2699, lo que da un total de 799 ACL extendidas numeradas posibles. Las ACL extendidas también pueden tener nombre.

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar, porque proporcionan un mayor grado de control. Como se muestra en la ilustración, al igual que las ACL estándar, las ACL extendidas revisan las direcciones de origen de los paquetes, pero también revisan la dirección de destino, los protocolos y los números de puerto (o de servicios). Esto proporciona una gama de criterios más amplia sobre la cual basar la ACL. Por ejemplo, una ACL extendida puede permitir el tráfico de correo electrónico de una red a un destino específico y, simultáneamente, denegar la transferencia de archivos y la navegación Web.



Prueba de puertos y servicios

La capacidad de filtrar por protocolos y números de puerto permite que los administradores de red creen ACL extendidas muy específicas. Se puede especificar una aplicación mediante la configuración del número o el nombre de un puerto bien conocido.

En la figura 1, se muestran algunos ejemplos de la forma en que un administrador especifica un número de puerto TCP o UDP colocándolo al final de la instrucción de la ACL extendida. Se pueden utilizar operaciones lógicas, por ejemplo, igual que (eq), distinto de (neq), mayor que (gt) y menor que (lt).

En la figura 2, se muestra cómo visualizar una lista de números de puerto y de palabras clave que pueden utilizarse al generar una ACL mediante el siguiente comando:

```
R1(config)# access-list 101 permit tcp any any eq?
```

Ejemplos de ACL extendidas

Uso de números de puerto

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

Uso de palabras clave

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

Generación de números de puerto

```
R1(config)# access-list 101 permit tcp any any eq ?
<0-65535>  Port number
bgp          Border Gateway Protocol (179)
chargen      Character generator (19)
cmd          Remote commands (rcmd, 514)
daytime     Daytime (13)
discard     Discard (9)
domain      Domain Name Service (53)
drip         Dynamic Routing Information Protocol (3949)
echo         Echo (7)
exec         Exec (rsh, 512)
finger       Finger (79)
ftp          File Transfer Protocol (21)
ftp-data    FTP data connections (20)
gopher      Gopher (70)
hostname    NIC hostname server (101)
ident        Ident Protocol (113)
irc          Internet Relay Chat (194)
klogin      Kerberos login (543)
kshell      Kerberos shell (544)
login       Login (rlogin, 513)
lpd          Printer service (515)
nntp        Network News Transport Protocol (119)
pim-auto-rp PIM Auto-RP (496)
pop2        Post Office Protocol v2 (109)
pop3        Post Office Protocol v3 (110)
```

9.3.2 Configuración de ACL de IPv4 extendidas

Los pasos del procedimiento para configurar ACL extendidas son los mismos que para las ACL estándar. Primero se configura la ACL extendida y, a continuación, se activa en una interfaz. Sin embargo, la sintaxis de los comandos y los parámetros son más complejos, a fin de admitir las funciones adicionales proporcionadas por las ACL extendidas.

Nota: la lógica interna aplicada al ordenamiento de las instrucciones de las ACL estándar no se aplica a las ACL extendidas. El orden en que se introducen las instrucciones durante la configuración es el orden en que se muestran y se procesan.

En la figura 1, se muestra la sintaxis frecuente de los comandos para las ACL de IPv4 extendidas. Observe que hay muchas palabras clave y parámetros para las ACL extendidas. No es necesario utilizar todas las palabras clave y todos los parámetros al configurar una ACL extendida. Recuerde que puede utilizar el símbolo? para obtener ayuda al introducir comandos complejos.

En la figura 2, se muestra un ejemplo de una ACL extendida. En este ejemplo, el administrador de red configuró las ACL para restringir el acceso de red a fin de permitir la navegación de sitios web solo desde la LAN conectada a la interfaz G0/0 a cualquier red externa. La ACL 103 permite que el tráfico proveniente de cualquier dirección en la red 192.168.10.0 vaya a cualquier destino, sujeto a la limitación de que el tráfico utilice solo los puertos 80 (HTTP) y 443 (HTTPS).

La naturaleza de HTTP requiere que el tráfico fluya nuevamente hacia la red desde los sitios web a los que se accede mediante clientes internos. El administrador de red desea restringir ese tráfico de retorno a los intercambios HTTP de los sitios web solicitados y denegar el resto del tráfico. La ACL 104 logra esto mediante el bloqueo de todo el tráfico entrante, excepto las conexiones establecidas previamente. La instrucción permit en la ACL 104 permite el tráfico entrante con el parámetro **established**.

El parámetro **established** permite que solo las respuestas al tráfico procedente de la red 192.168.10.0/24 vuelvan a esa red. Si el segmento TCP que regresa tiene los bits ACK o de restablecimiento (RST) establecidos, que indican que el paquete pertenece a una conexión existente, se produce una coincidencia. Sin el parámetro **established** en la instrucción de ACL, los clientes pueden enviar tráfico a un servidor web, pero no recibir el tráfico que vuelve de dicho servidor.

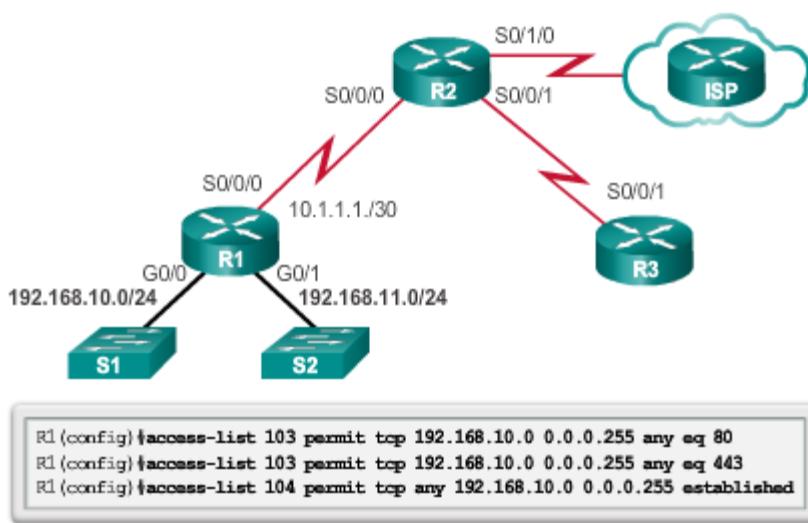
Configuring Extended ACLs

```
access-list access-list-number {deny | permit | remark}
protocol source [source-wildcard] [operator operand]
[port port-number or name] destination [destination-wildcard]
[operator operand] [port port-number or name] [established]
```

Parámetro	Descripción
access-list-number	Identifica la lista de acceso con un número en el rango entre 100 y 199 (para una ACL IP extendida) y entre 2000 y 2699 (para una ACL IP expandida).
deny	Deniega el acceso si las condiciones concuerdan.
permit	Permite el acceso si las condiciones concuerdan.
remark	Se utiliza para introducir comentarios.
protocol	Nombre o número de un protocolo de Internet. Algunas de las palabras clave más comunes son icmp , ip , tcp , o udp . Para que haya coincidencia con cualquier protocolo de Internet (como ICMP, TCP y UDP), se usa la palabra clave ip .
origen	Número de la red o del host desde el que se envía el paquete.
source-wildcard	Bits de wildcard para aplicar al origen.
destination	Número de la red o del host al que se envía un paquete.

destination-wildcard	Bits de wildcard para aplicar al destino.
operator	(Opcional) Compara los puertos de origen y de destino. Algunos de los operandos posibles son lt (menor que), gt (mayor que), eq (igual a), neq (distinto de), and range (rango inclusivo).
puerto	(Opcional) El número decimal o nombre de un puerto TCP o UDP.
established	(Optativo) Solo para el protocolo TCP: indica una conexión establecida.

Configurar las ACL extendidas



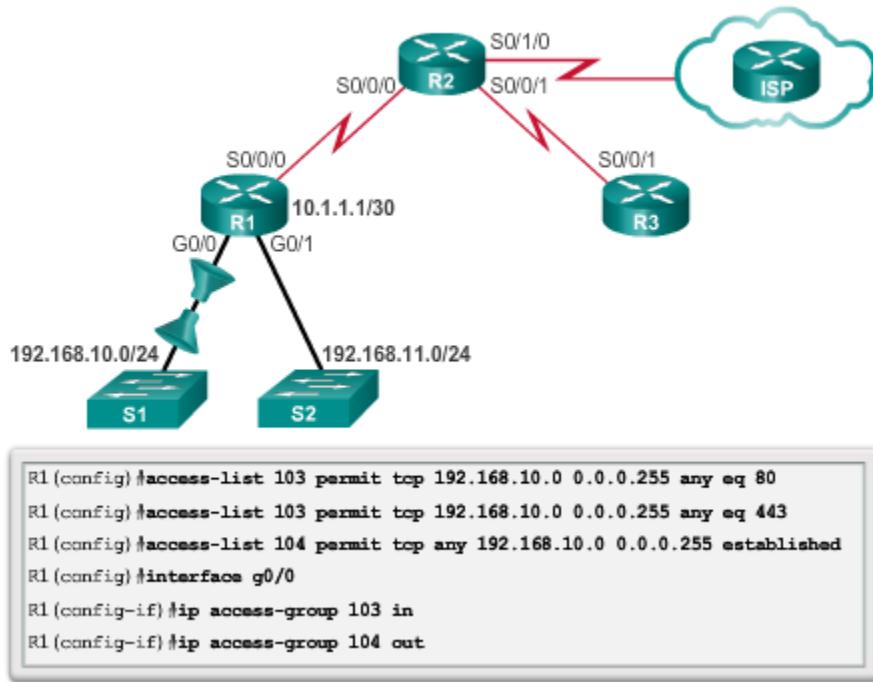
En el ejemplo anterior, el administrador de red configuró una ACL para permitir que los usuarios de la red 192.168.10.0/24 exploren sitios web seguros e inseguros. Aunque se configuró, la ACL no filtrará el tráfico hasta que se aplique a una interfaz. Para aplicar una ACL a una interfaz, primero debe considerar si el tráfico que se filtrará es entrante o saliente. Cuando un usuario de la LAN interna accede a un sitio web en Internet, hay tráfico que sale hacia Internet. Cuando un usuario interno recibe un correo electrónico de Internet, el tráfico ingresa al router local. Sin embargo, cuando se aplica una ACL a una interfaz, los términos “entrada” y “salida” tienen otros significados. Desde el punto de vista de una ACL, la entrada y salida son respecto de la interfaz del router.

En la topología de la ilustración, el R1 tiene tres interfaces: una interfaz serial, S0/0/0, y dos interfaces Gigabit Ethernet, G0/0 y G0/1. Recuerde que una ACL extendida comúnmente se debería aplicar cerca del origen. En esta topología, la interfaz más cercana al origen del tráfico de destino es la interfaz G0/0.

La solicitud de tráfico web de los usuarios en la LAN 192.168.10.0/24 entra a la interfaz G0/0. El tráfico de retorno de las conexiones establecidas a los usuarios en la LAN sale de la interfaz G0/0. En el ejemplo, se aplica la ACL a la interfaz G0/0 en ambos sentidos. La ACL de entrada, 103, revisa el tipo de tráfico. La ACL de salida, 104, revisa si hay tráfico de retorno de las conexiones establecidas. Esto restringe el acceso a Internet desde 192.168.10.0 para permitir solamente la navegación de sitios web.

Nota: las listas de acceso se podrían haber aplicado a la interfaz S0/0/0, pero en ese caso el proceso de ACL del router tendría que examinar todos los paquetes que ingresan al router y no solo el tráfico que va hacia 192.168.11.0 y que vuelve de esa red. Esto provocaría que el router realice un procesamiento innecesario.

Cómo aplicar una ACL a una interfaz



En el ejemplo que se muestra en la figura 1, se deniega el tráfico FTP de la subred 192.168.11.0 que va a la subred 192.168.10.0, pero se permite el resto del tráfico. Observe el uso de las máscaras wildcard y de la instrucción deny any explícita. Recuerde que FTP utiliza los puertos TCP 20 y 21, por lo tanto, la ACL requiere ambas palabras clave de nombre de puerto **ftp** y **ftp-data** o **eq 20** y **eq 21** para denegar el tráfico FTP.

Si se utilizan números de puerto en vez de nombres de puerto, los comandos se deben escribir de la siguiente forma:

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
```

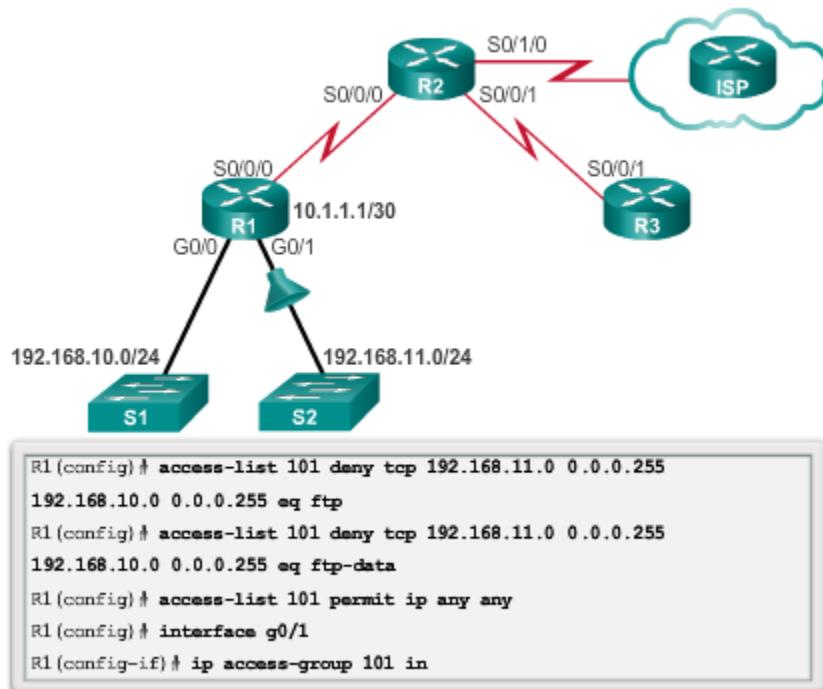
Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, se agrega la instrucción **permit ip any any**. Si no hay por lo menos una instrucción **permit** en una ACL, todo el tráfico en la interfaz donde se aplicó esa ACL se descarta. La ACL se debe aplicar en sentido de entrada en la interfaz G0/1 para filtrar el tráfico de la LAN 192.168.11.0/24 cuando ingresa a la interfaz del router.

En el ejemplo que se muestra en la figura 2, se deniega el tráfico de Telnet de cualquier origen a la LAN 192.168.11.0/24, pero se permite el resto del tráfico IP. Debido a que el tráfico destinado a la LAN 192.168.11.0/24 sale de la interfaz G0/1, la ACL se aplica a G0/1 con la palabra clave **out**.

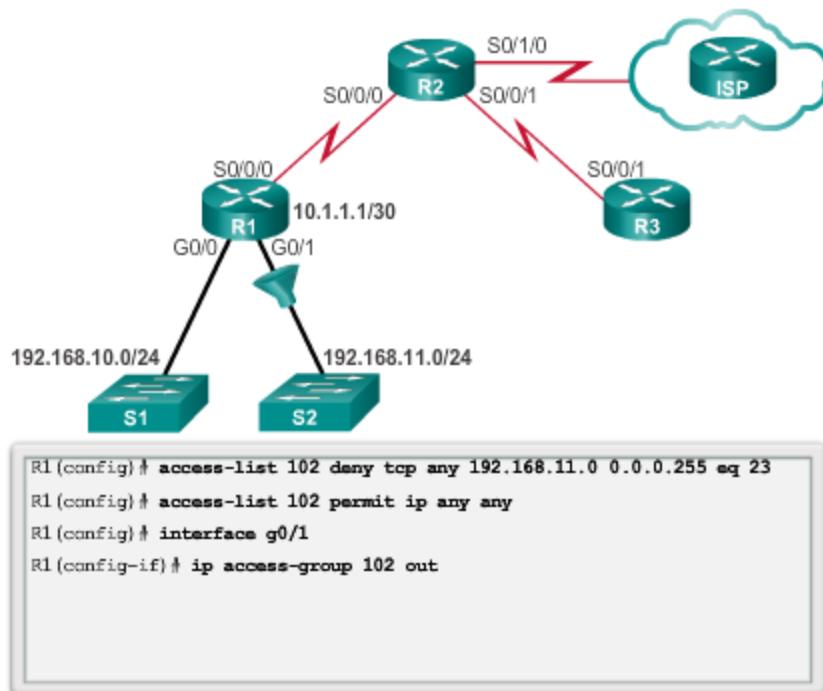
Observe el uso de las palabras clave **any** en la instrucción **permit**. Esta instrucción **permit** se agrega para asegurar que no se bloquee ningún otro tipo de tráfico.

Nota: en ambos ejemplos en las figuras 1 y 2, se utiliza la instrucción **permit ip any any** al final de la ACL. Para obtener mayor seguridad, se puede utilizar el comando **permit 192.168.11.0 0.0.0.255 any**.

ACL extendida para denegar FTP



ACL extendida para denegar Telnet



Las ACL extendidas con nombre se crean esencialmente de la misma forma que las ACL estándar con nombre. Para crear una ACL extendida con nombre, realice los siguientes pasos:

Paso 1. En el modo de configuración global, utilice el comando `ip access-list extended nombre` para definir un nombre para la ACL extendida.

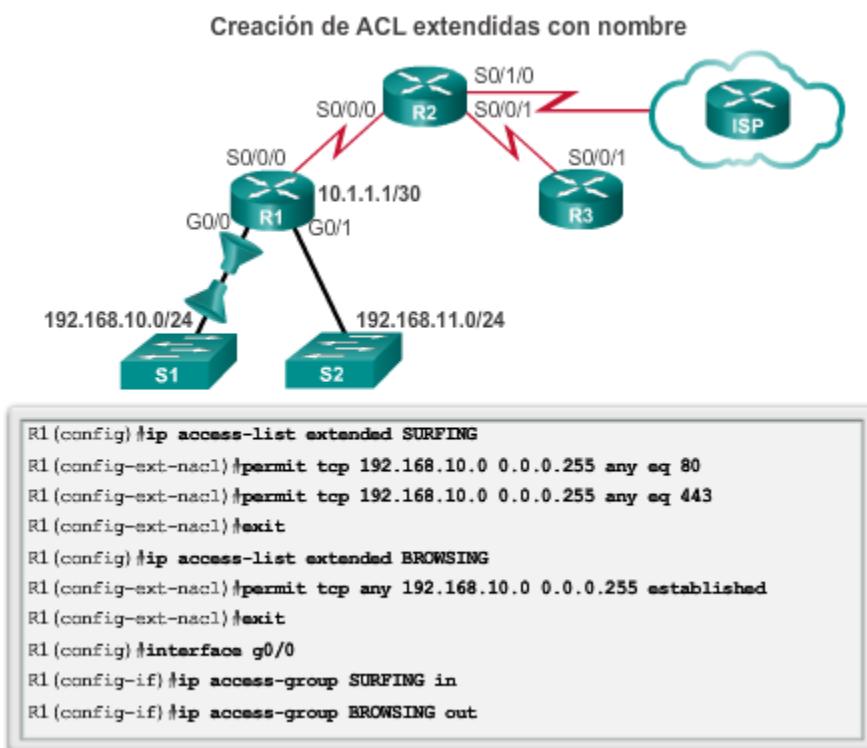
Paso 2. En el modo de configuración de ACL con nombre, especifique las condiciones para `permit` o `deny`.

Paso 3. Vuelva al modo EXEC privilegiado y verifique la ACL con el comando `show access-lists nombre`.

Paso 4. Guarde las entradas en el archivo de configuración mediante el comando `copy running-config startup-config`.

Para eliminar una ACL extendida con nombre, utilice el comando de configuración global `no ip access-list extended nombre`.

En la ilustración, se muestran las versiones con nombre de las ACL creadas en los ejemplos anteriores. La ACL con nombre SURFING permite que los usuarios en la LAN 192.168.10.0/24 accedan a sitios web. La ACL con nombre BROWSING permite el tráfico de retorno de las conexiones establecidas. Cuando se utilizan las ACL con nombre, las reglas se aplican en sentido de entrada y de salida en la interfaz G0/0.



Después de configurar una ACL y aplicarla a una interfaz, utilice los comandos `show` del IOS de Cisco para verificar la configuración. En la ilustración, en el ejemplo de arriba se muestra el comando del IOS de Cisco que se utiliza para mostrar el contenido de todas las ACL. En el ejemplo

de abajo, se muestra el resultado de emitir el comando `show ip interface g0/0` en el router R1.

A diferencia de las ACL estándar, las ACL extendidas no implementan la misma lógica interna ni la misma función de hash. El resultado y los números de secuencia que se muestran en el resultado del comando `show access-lists` están en el orden en que se introdujeron las instrucciones. Las entradas de host no se enumeran automáticamente antes de las entradas de rango.

El comando `show ip interface` se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó. El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL. Los nombres de las ACL BROWSING y SURFING en mayúscula se destacan en el resultado que se ve en la pantalla.

Después de verificar la configuración de una ACL, el siguiente paso es confirmar que la ACL funcione según lo esperado, es decir, que bloquee y permita el tráfico según se espera.

Las pautas analizadas anteriormente en esta sección sugieren que las ACL se configuren en una red de prueba y después se implementen en la red de producción.

Verificación de ACL extendidas

```
R1#show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1#show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
<resultado omitido por cuestiones de brevedad>
  Outgoing access list is BROWSING
  Inbound access list is SURFING
<resultado omitido por cuestiones de brevedad>
```

Se puede editar una ACL extendida mediante el mismo proceso que una ACL estándar, el cual se analizó en una sección anterior. Las ACL extendidas se pueden modificar mediante los métodos siguientes:

- **Método 1: editor de texto.** Con este método, la ACL se copia y pega en el editor de texto, donde se realizan los cambios. La lista de acceso actual se elimina mediante el comando `no access-list`. Luego, la ACL modificada se pega nuevamente en la configuración.
- **Método 2: números de secuencia.** Los números de secuencia se pueden utilizar para eliminar o para insertar una instrucción de ACL. El comando `ip access-list extended nombre` se utiliza para ingresar al modo de configuración de ACL con nombre. Si la ACL es numerada en vez de tener un nombre, se utiliza el número de la ACL en el parámetro `nombre`. Las ACE se pueden insertar o eliminar.

En la ilustración, se muestra que el administrador debe editar la ACL con nombre SURFING para corregir una errata en la instrucción de la red de origen. Para ver los números de secuencia actuales, se utiliza el comando `show access-lists`. La instrucción que se edita se identifica como instrucción 10. La instrucción original se elimina con el comando `no número_secuencia`. La instrucción corregida se agrega y se reemplaza la instrucción original.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.11.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq
www
R1(config-ext-nacl)# end
R1#
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
```

9.4 Resolución de problemas de ACL

9.4.1 Procesamiento de paquetes con ACL

Lógica de ACL de entrada

En la figura 1, se muestra la lógica para una ACL de entrada. Si hay una coincidencia entre la información en un encabezado de paquete y una instrucción de ACL, el resto de las instrucciones de la lista se omiten y se permite o se deniega el paquete según lo especificado por la instrucción de la coincidencia. Si no existe una coincidencia entre un encabezado de paquete y una instrucción de ACL, el paquete se prueba en relación con la siguiente instrucción de la lista. Este proceso de búsqueda de coincidencias continúa hasta que se llega al final de la lista.

Al final de cada ACL, hay una instrucción `deny any` implícita. Esta instrucción no se muestra en el resultado. Esta instrucción implícita final se aplica a todos los paquetes cuyas condiciones no se probaron como verdaderas. Esta condición de prueba final coincide con el resto de los paquetes y da como resultado una acción de denegación. En lugar de avanzar en el sentido de entrada o de salida de una interfaz, el router descarta todos los paquetes restantes. A esta instrucción final se la suele conocer como instrucción “`deny any` implícita” o “denegación de todo el tráfico”. Debido a esta instrucción, una ACL debería incluir, por lo menos, una instrucción `permit`. De lo contrario, la ACL bloquea todo el tráfico.

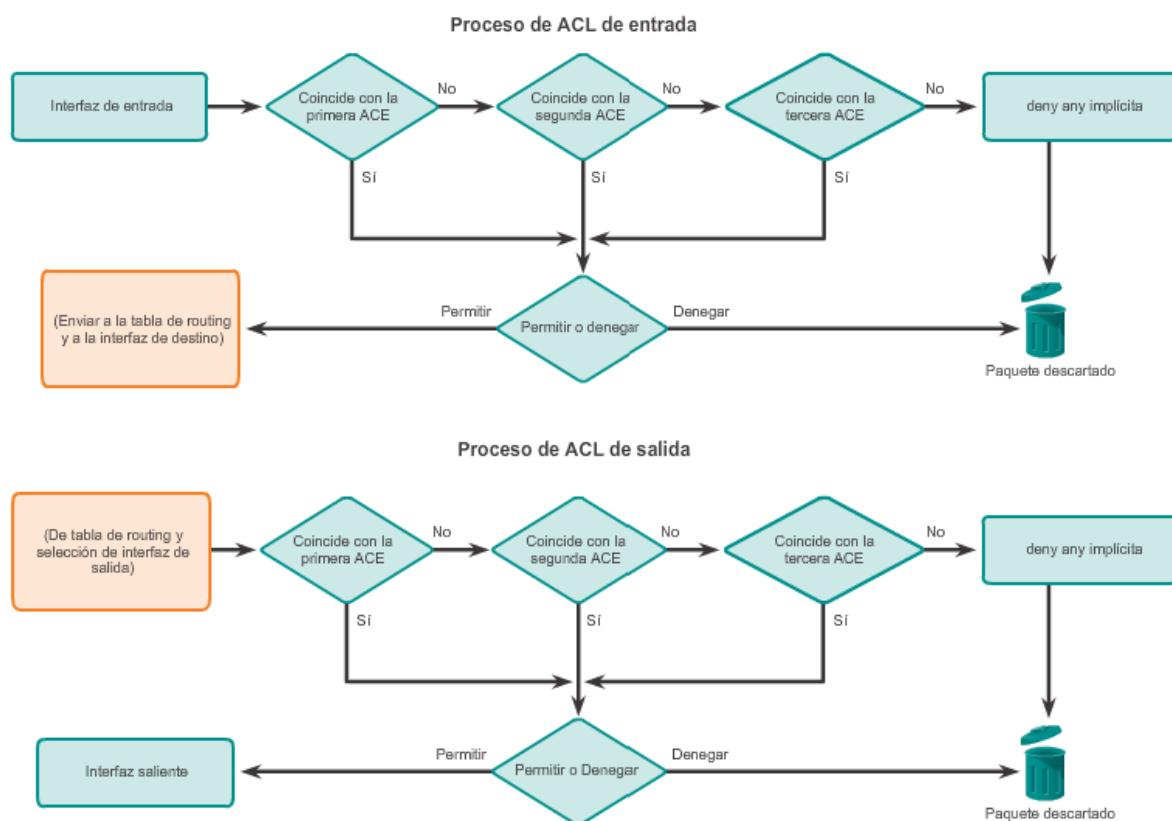
Lógica de ACL de salida

En la figura 2, se muestra la lógica para una ACL de salida. Antes de que se reenvíe un paquete a una interfaz de salida, el router revisa la tabla de routing para ver si el paquete es enrutable. Si no lo es, se descarta y no se prueba en relación con las ACE. A continuación, el router revisa si la

interfaz de salida está agrupada en una ACL. Si la interfaz de salida no está agrupada en una ACL, el paquete se puede enviar al búfer de salida. A continuación, se indican algunos ejemplos de la operación de la ACL de salida:

- **Ninguna ACL aplicada a la interfaz:** si la interfaz de salida no está agrupada en una ACL de salida, el paquete se envía directamente a la interfaz de salida.
- **ACL aplicada a la interfaz:** si la interfaz de salida está agrupada en una ACL de salida, el paquete no se envía por la interfaz de salida hasta que se lo prueba mediante la combinación de ACE relacionadas con esa interfaz. Según las pruebas de ACL, el paquete se permite o se deniega.

Para las listas de salida, “permit” (permitir) significa enviar el paquete al búfer de salida y “deny” (denegar) significa descartar el paquete.



ACL y routing, y procesos de ACL en un router

En la ilustración, se muestra la lógica de los procesos de routing y ACL. Cuando un paquete llega a una interfaz del router, el proceso del router es el mismo, ya sea si se utilizan ACL o no. Cuando una trama ingresa a una interfaz, el router revisa si la dirección de capa 2 de destino coincide con la dirección de capa 2 de la interfaz, o si dicha trama es una trama de difusión.

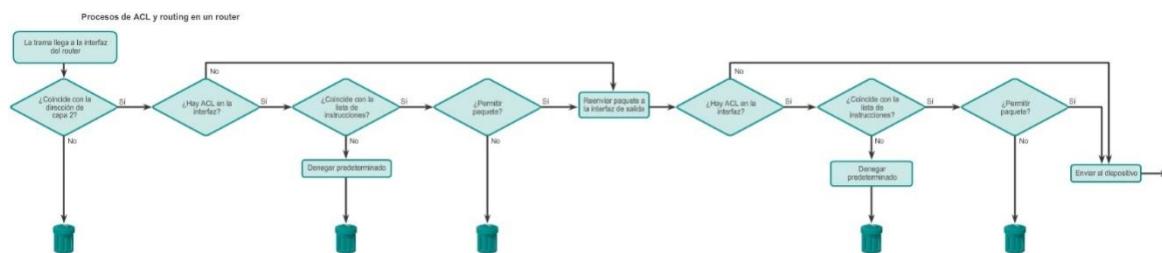
Si se acepta la dirección de la trama, se desmonta la información de la trama y el router revisa si hay una ACL en la interfaz de entrada. Si existe una ACL, el paquete se prueba en relación con las instrucciones de la lista.

Si el paquete coincide con una instrucción, se permite o se deniega. Si se acepta el paquete, se compara con las entradas en la tabla de routing para determinar la interfaz de destino. Si existe una entrada para el destino en la tabla de routing, el paquete se conmuta a la interfaz de salida. De lo contrario, se descarta.

A continuación, el router revisa si la interfaz de salida tiene una ACL. Si existe una ACL, el paquete se prueba en relación con las instrucciones de la lista.

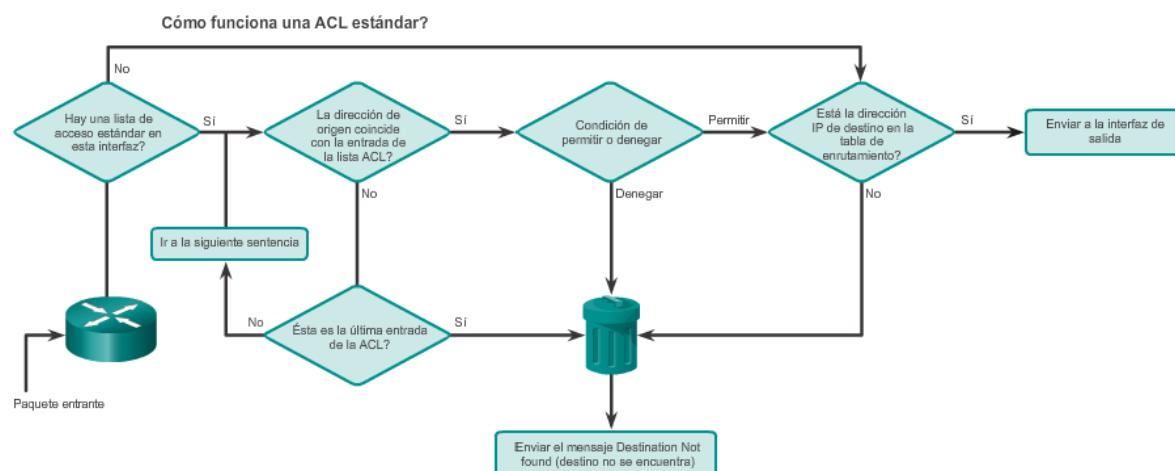
Si el paquete coincide con una instrucción, se permite o se deniega.

Si no hay una ACL o si se permite el paquete, este se encapsula en el nuevo protocolo de capa 2 y se reenvía por la interfaz al siguiente dispositivo.



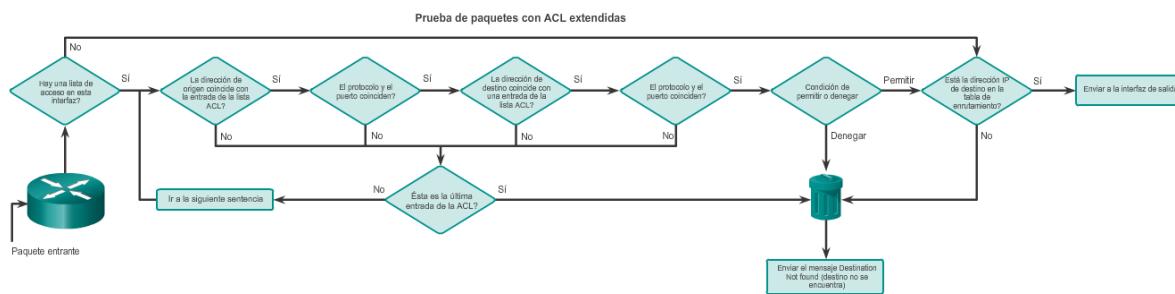
Las ACL estándar solo examinan la dirección IPv4 de origen. El destino del paquete y los puertos involucrados no se tienen en cuenta.

El proceso de decisión de una ACL estándar se detalla en la ilustración. El software IOS de Cisco prueba las direcciones en relación con cada una de las condiciones de la ACL. La primera coincidencia determina si el software acepta o rechaza la dirección. Dado que el software deja de probar las condiciones después de la primera coincidencia, el orden de las condiciones es fundamental. Si no coincide ninguna condición, la dirección se rechaza.



En la ilustración, se muestra la ruta de decisión lógica que utiliza una ACL extendida creada para filtrar direcciones de origen y destino, y números de protocolo y de puerto. En este ejemplo, la ACL primero filtra sobre la dirección de origen y, a continuación, sobre el puerto y el protocolo de origen. Luego, filtra sobre la dirección de destino y después sobre el puerto y el protocolo de destino, y toma la decisión final de permiso o denegación.

Recuerde que las entradas en las ACL se procesan una tras otra, de modo que una decisión negativa (“no”) no es necesariamente una decisión de denegación (“deny”). A medida que avanza a través de la ruta de decisión lógica, tenga en cuenta que un “no” significa que se debe pasar a la siguiente entrada hasta que se encuentre una coincidencia para una condición.



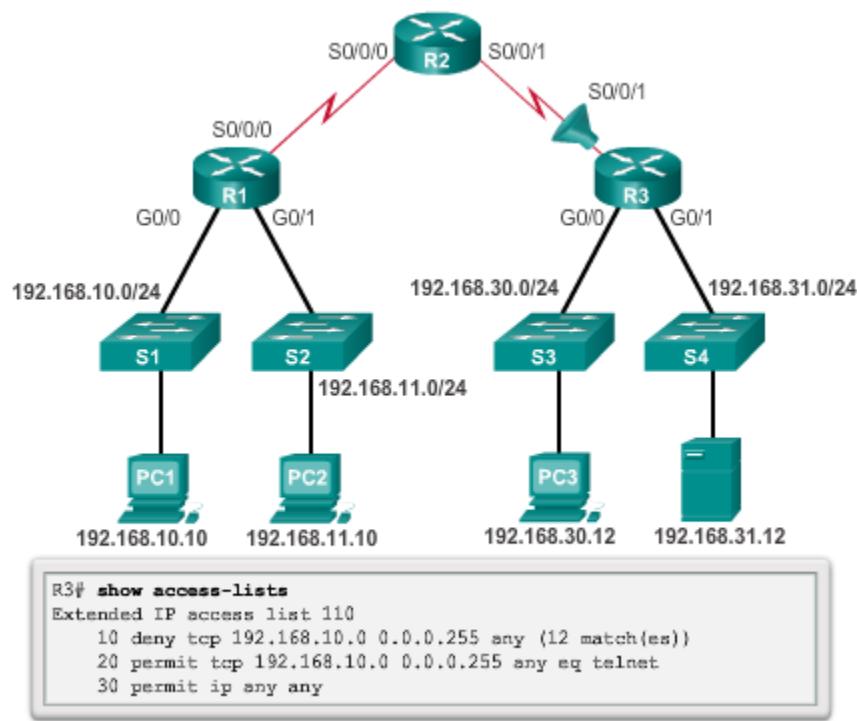
9.4.2 Errores comunes de ACL

Mediante los comandos `show` descritos anteriormente, se revela la mayoría de los errores más comunes de ACL. Los errores más comunes incluyen introducir las ACE en el orden incorrecto y no aplicar los criterios adecuados a las reglas de ACL.

Ejemplo de error 1

En la ilustración, el host 192.168.10.10 no tiene conectividad con 192.168.30.12. Al observar el resultado del comando `show access-lists`, se muestran las coincidencias para la primera instrucción deny. Esto indica que la instrucción coincidió con el tráfico.

Solución: mire el orden de las ACE. El host 192.168.10.10 no tiene conectividad con 192.168.30.12, debido al orden de la regla 10 en la lista de acceso. Dado que el router procesa las ACL en orden descendente, la instrucción 10 deniega el host 192.168.10.10, por lo que la instrucción 20 nunca puede tener una coincidencia. Las instrucciones 10 y 20 deben invertirse. La última línea permite el resto del tráfico que no es TCP y que se clasifica como IP (ICMP, UDP, etcétera).



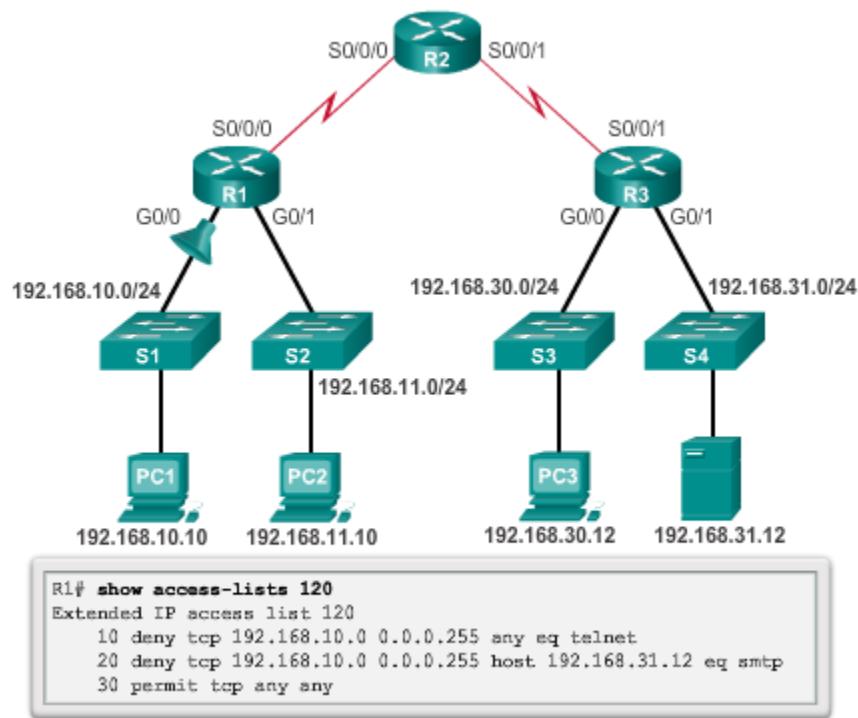
Ejemplo de error 2

En la ilustración, la red 192.168.10.0/24 no puede utilizar TFTP para conectarse a la red 192.168.30.0/24.

Solución: la red 192.168.10.0/24 no puede utilizar TFTP para conectarse a la red 192.168.30.0/24, porque TFTP utiliza el protocolo de transporte UDP. La instrucción 30 en la lista de acceso 120 permite todo el resto del tráfico TCP. Sin embargo, debido a que TFTP utiliza UDP en lugar de TCP, se deniega implícitamente. Recuerde que la instrucción deny any implícita no aparece en el resultado del comando `show access-lists` y, por lo tanto, las coincidencias no se muestran.

La instrucción 30 debería ser `ip any any`.

Esta ACL funciona si se aplica a G0/0 del R1, a S0/0/1 del R3 o a S0/0/0 del R2 en sentido de entrada. Sin embargo, según la regla que indica colocar las ACL extendidas más cerca del origen, la mejor opción es colocarla en sentido de entrada en G0/0 del R1, porque permite que el tráfico no deseado se filtre sin cruzar la infraestructura de la red.

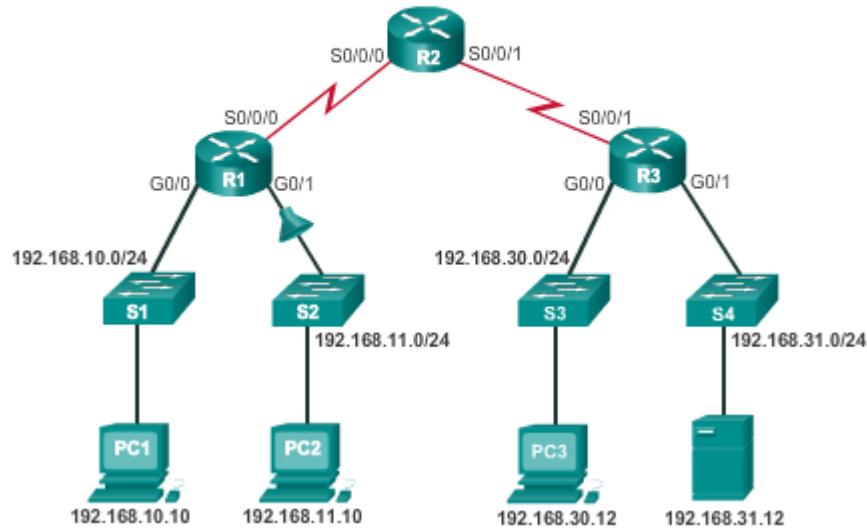


Ejemplo de error 3

En la ilustración, la red 192.168.11.0/24 puede utilizar Telnet para conectarse a 192.168.30.0/24, pero según la política de la empresa, esta conexión no debería permitirse. Los resultados del comando `show access-lists 130` indican que se encontró una coincidencia para la instrucción `permit`.

Solución: la red 192.168.11.0/24 puede utilizar Telnet para conectarse a la red 192.168.30.0/24, porque el número de puerto Telnet en la instrucción 10 de la lista de acceso 130 aparece en una posición incorrecta en la instrucción de ACL. Actualmente, la instrucción 10 deniega cualquier paquete de origen con un número de puerto que equivalga a Telnet. Para denegar el tráfico entrante de Telnet en G0/1, deniegue el número de puerto de destino que equivale a Telnet, por ejemplo, `deny tcp any any eq telnet`.

```
R1#show access-lists 130
Extended IP access list 130
  10 deny tcp any eq telnet any
  20 deny tcp 192.168.11.0 0.0.0.255 host 192.168.31.12 eq smtp
  30 permit tcp any any (12 match(es))
```

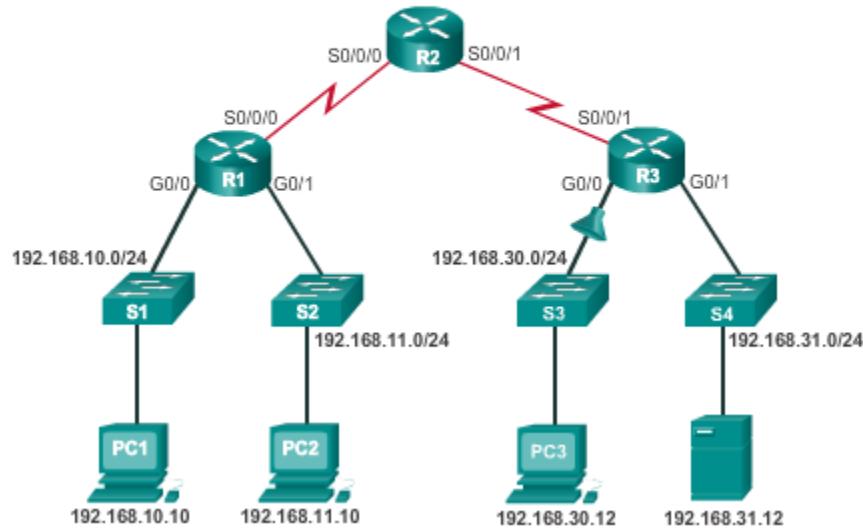


Ejemplo de error 4

En la ilustración, el host 192.168.30.12 puede conectarse a 192.168.31.12 mediante Telnet, pero la política de la empresa establece que esta conexión no debe permitirse. Los resultados del comando `show access-lists 140` indican que se encontró una coincidencia para la instrucción `permit`.

Solución: el host 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12 porque no hay reglas que denieguen el host 192.168.30.12 o su red como origen. La instrucción 10 de la lista de acceso 140 deniega la interfaz del router por la que el tráfico ingresa a este. La dirección host IPv4 en la instrucción 10 debería ser 192.168.30.12.

```
R3#show access-lists 140
Extended IP access list 140
  10 deny tcp host 192.168.30.1 any eq telnet
  20 permit ip any any (5 match(es))
```

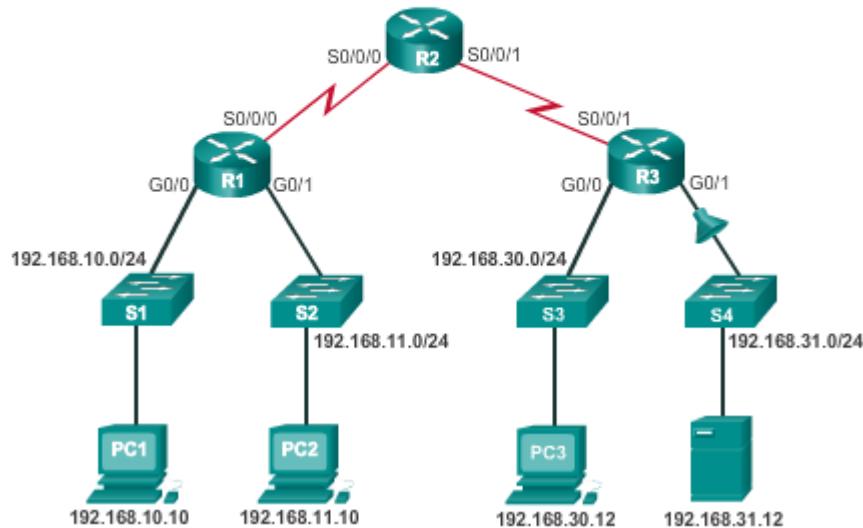


Ejemplo de error 5

En la ilustración, el host 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12, pero según la política de seguridad, esta conexión no debe permitirse. El resultado del comando `show access-lists 150` indica que no se encontraron coincidencias para la instrucción `deny` según se esperaba.

Solución: el host 192.168.30.12 puede utilizar Telnet para conectarse a 192.168.31.12, debido al sentido en el que se aplica la lista de acceso 150 a la interfaz G0/1. La instrucción 10 deniega que cualquier dirección de origen se conecte al host 192.168.31.12 mediante Telnet. Sin embargo, para un filtrado correcto, este filtro se debe aplicar en sentido de salida en G0/1.

```
R2#show access-lists 150
Extended IP access list 150
  10 deny tcp any host 192.168.31.12 eq telnet
  20 permit ip any any
```



9.5 ACL de IPv6

9.5.1 Creación de ACL de IPv6

Las ACL de IPv6 son similares a las ACL de IPv4 en cuanto a la configuración y el funcionamiento. Si ya está familiarizado con las listas de acceso de IPv4, las ACL de IPv6 serán fáciles de comprender y configurar.

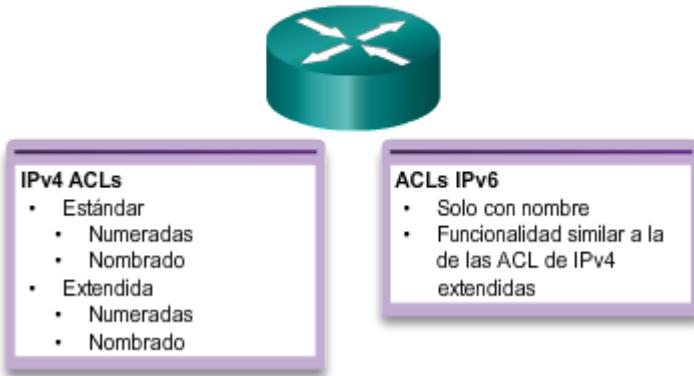
Existen dos tipos de ACL en IPv4: las estándar y las extendidas. Ambos tipos de ACL pueden ser numeradas o con nombre.

En cuanto a IPv6, hay solamente un tipo de ACL, que equivale a la ACL de IPv4 extendida con nombre. No existen ACL numeradas en IPv6. En resumen, las características de las ACL de IPv6 son las siguientes:

- Son ACL con nombre únicamente.
- Equivalen a la funcionalidad de una ACL de IPv4 extendida.

Una ACL de IPv4 y una ACL de IPv6 no pueden tener el mismo nombre.

ACL de IPv6



Aunque las ACL de IPv4 y de IPv6 son muy similares, hay tres diferencias fundamentales entre ellas.

- **Aplicación de una ACL de IPv6**

La primera diferencia es el comando que se utiliza para aplicar una ACL de IPv6 a una interfaz. IPv4 utiliza el comando `ip access-group` para aplicar una ACL de IPv4 a una interfaz IPv4. IPv6 utiliza el comando `ipv6 traffic-filter` para realizar la misma función para las interfaces IPv6.

- **Ausencia de máscaras wildcard**

A diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard. En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir.

- **Instrucciones predeterminadas adicionales**

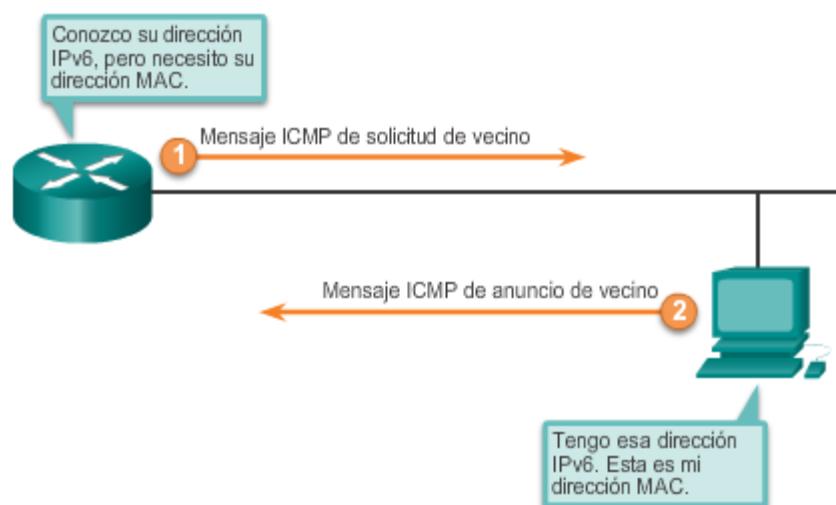
La última diferencia principal tiene que ver con la inclusión de dos instrucciones permit implícitas al final de cada lista de acceso de IPv6. Al final de todas las ACL de IPv4 estándar o extendidas, hay una instrucción `deny any` o `deny any any` implícita. En IPv6 se incluye una instrucción `deny ipv6 any any` similar al final de cada ACL de IPv6. La diferencia es que en IPv6 también se incluyen otras dos instrucciones implícitas de manera predeterminada:

- `permit icmp any any nd-na`
- `permit icmp any any nd-ns`

Estas dos instrucciones permiten que el router participe en el equivalente de ARP para IPv4 en IPv6. Recuerde que ARP se utiliza en IPv4 para resolver las direcciones de capa 3 a direcciones MAC de capa 2. Como se muestra en la ilustración, en IPv6 se utilizan mensajes ICMP de descubrimiento de vecinos (ND) para lograr el mismo propósito. ND utiliza mensajes de solicitud de vecino (NS) y de anuncio de vecino (NA).

Los mensajes ND se encapsulan en paquetes IPv6 y requieren los servicios de la capa de red IPv6, mientras que ARP para IPv4 no utiliza la capa 3. Dado que IPv6 utiliza el servicio de la capa 3 para el descubrimiento de vecinos, las ACL de IPv6 deben permitir implícitamente que los paquetes ND se envíen y reciban por una interfaz. Específicamente, se permiten tanto los mensajes de descubrimiento de vecinos-anuncio de vecino (nd-na) como los de descubrimiento de vecinos-solicitud de vecino (nd-ns).

Descubrimiento de vecinos IPv6

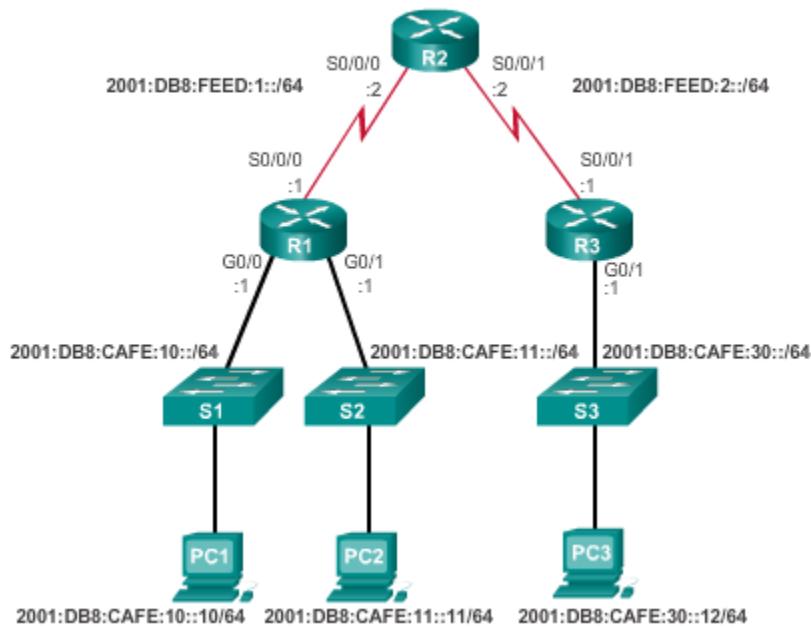


En la figura 1, se muestra la topología que se utilizará para configurar las ACL de IPv6. Esta es similar a la topología de IPv4 anterior, excepto por el esquema de direccionamiento IPv6. Hay tres subredes de 2001:DB8:CAFE::/64: 2001:DB8:CAFE:10::/64, 2001:DB8:CAFE:11::/64 y 2001:DB8:CAFE:30::/64. Hay dos redes seriales que conectan los tres routers: 2001:DB8:FEED:1::/64 y 2001:DB8:FEED:2::/64.

En las figuras 2, 3 y 4, se muestra la configuración de la dirección IPv6 para cada uno de los routers. El comando `show ipv6 interface brief` se utiliza para verificar la dirección y el estado de la interfaz.

Nota: el comando `no shutdown` y el comando `clock rate` no se muestran.

Topología IPv6



Configuración de R1

```

R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:cafe:10::1/64
R1(config-if)# exit
R1(config)# interface s0/0/0
R1(config-if)# ipv6 address 2001:db8:feed:1::1/64
R1(config-if)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:11::1/64
R1(config-if)# end
R1# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:CAFE:10::1
GigabitEthernet0/1      [up/up]
  FE80::FE99:47FF:FE75:C3E1
  2001:DB8:CAFE:11::1
Serial0/0/0             [up/up]
  FE80::FE99:47FF:FE75:C3E0
  2001:DB8:FEED:1::1
<resultado omitido>
R1#
    
```

Configuración de R2

```
R2(config)# interface s0/0/0
R2(config-if)# ipv6 address 2001:db8:feed:1::2/64
R2(config-if)# exit
R2(config)# interface s0/0/1
R2(config-if)# ipv6 address 2001:db8:feed:2::2/64
R2(config-if)# end
R2# show ipv6 interface brief
Serial0/0/0          [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:1::2
Serial0/0/1          [up/up]
    FE80::FE99:47FF:FE71:78A0
    2001:DB8:FEED:2::2
<resultado omitido>
R2#
```

Configuración de R3

```
R3(config)# interface s0/0/1
R3(config-if)# ipv6 address 2001:db8:feed:2::1/64
R3(config-if)# exit
R3(config)# interface g0/0
R3(config-if)# ipv6 address 2001:db8:cafe:30::1/64
R3(config-if)# end
R3# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:CAFE:30::1
Serial0/0/1            [up/up]
    FE80::FE99:47FF:FE71:7A20
    2001:DB8:FEED:2::1
R3#
```

En IPv6 solo hay ACL con nombre. La configuración es similar a la de una ACL de IPv4 extendida con nombre.

En la figura 1, se muestra la sintaxis de los comandos para las ACL de IPv6. La sintaxis es similar a la que se utiliza en ACL de IPv4 extendidas. Una diferencia importante es el uso de la longitud de prefijo IPv6 en lugar de una máscara wildcard IPv4.

Hay tres pasos básicos para configurar una ACL de IPv6:

Paso 1. En el modo de configuración global, utilice el comando `ipv6 access-list nombre` para crear una ACL de IPv6. Al igual que las ACL de IPv4 con nombre, los nombres en IPv6 son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. A diferencia de IPv4, no hay necesidad de una opción estándar o extendida.

Paso 2. En el modo de configuración de ACL con nombre, utilice las instrucciones **permit** o **deny** para especificar una o más condiciones para determinar si un paquete se debe reenviar o descartar.

Paso 3. Regrese al modo EXEC privilegiado con el comando **end**.

En la figura 2, se muestran los pasos para crear una ACL de IPv6 con un ejemplo simple basado en la topología anterior. La primera instrucción da el nombre NO-R3-LAN-ACCESS a la lista de acceso de IPv6. Al igual sucede que con las ACL de IPv4 con nombre, no es necesario el uso de mayúsculas en los nombres de las ACL de IPv6, pero esto hace que se destaque cuando se observa el resultado de la configuración en ejecución.

La segunda instrucción deniega todos los paquetes 2001:DB8:CAFE:30::/64 destinados a cualquier red IPv6. La tercera instrucción permite el resto de los paquetes IPv6.

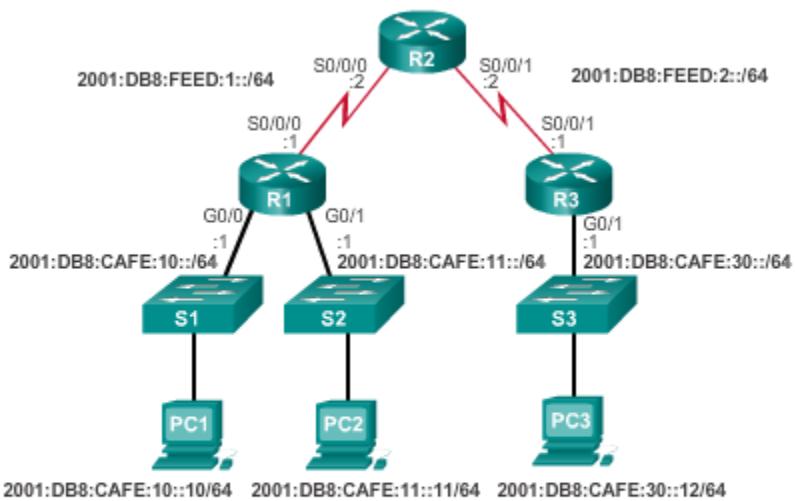
En la figura 3, se muestra la ACL en contexto con la topología.

R1(config)# ipv6 access-list access-list-name	
R1(config-ipv6-acl)# deny permit protocol {source-ipv6-prefix/prefix-length any host source-ipv6-address} [operator {port-number}] {destination-ipv6-prefix/prefix-length any host destination-ipv6-address} [operator {port-number}]	
Parámetro	Descripción
deny permit	Especifica si se deniega o se permite el paquete.
protocol	Introduzca el nombre o el número de un protocolo de Internet o un número entero que represente un número de protocolo IPv6.
prefixo-ipv6-origen/longitud-prefijo	La red IPv6 de origen o destino, o la clase de redes para las que se deben establecer condiciones de denegación o permiso.
dirección-ipv6-destino	
any	Introduzca any como abreviatura para el prefijo IPv6 ::/0. Este coincide con todas las direcciones.
Host	Para host dirección-ipv6-origen o dirección-ipv6-destino , introduzca la dirección host IPv6 de origen o destino para las que se deben establecer condiciones de denegación o permiso.
operator	(Optativo) Operando que compara los puertos de origen o destino del protocolo especificado. Los operandos son lt (menor que), gt (mayor que), eq (igual que), neq (distinto de) y range (rango).
número-puerto	(Optativo) Número decimal o nombre de un puerto TCP o UDP para filtrar TCP y UDP respectivamente.

ACL de IPv6 de ejemplo

```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#
```

Topología IPv6



```
R1(config)# ipv6 access-list NO-R3-LAN-ACCESS
R1(config-ipv6-acl)# deny ipv6 2001:db8:cafe:30::/64 any
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# end
R1#
```

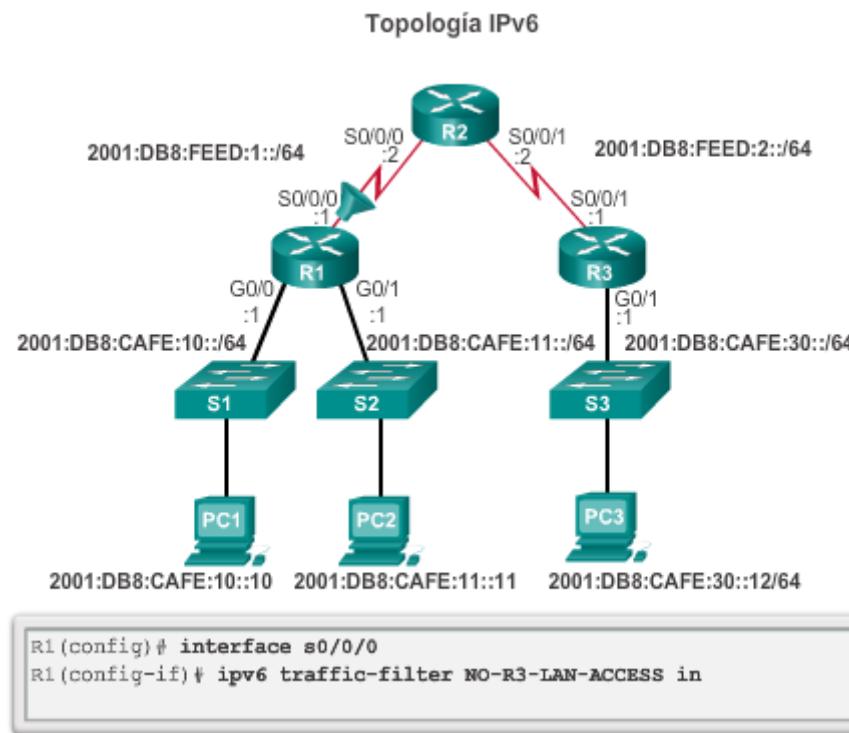
Después de que se configura una ACL de IPv6, se la vincula a una interfaz mediante el comando **ipv6 traffic-filter**:

```
Router(config-if)# ipv6 traffic-filter nombre-lista-acceso { pre | out }
```

En la ilustración, se muestra la ACL NO-R3-LAN-ACCESS configurada anteriormente y los comandos utilizados para aplicar la ACL de IPv6 de entrada a la interfaz S0/0/0. Si se aplica la ACL a la interfaz S0/0/0 de entrada, se denegarán los paquetes de 2001:DB8:CAFE:30::/64 en ambas LAN en el R1.

Para eliminar una ACL de una interfaz, primero introduzca el comando **no ipv6 traffic-filter** en la interfaz y, luego, introduzca el comando global **no ipv6 access-list** para eliminar la lista de acceso.

Nota: tanto en IPv4 como en IPv6 se utiliza el comando `ip access-class` para aplicar una lista de acceso a los puertos VTY.



Denegar FTP

La topología para los ejemplos se muestra en la figura 1.

En el primer ejemplo que se muestra en la figura 2, el router R1 está configurado con una lista de acceso de IPv6 para denegar el tráfico FTP a 2001:DB8:CAFE:11::/64. Se deben bloquear los puertos para los datos FTP (puerto 20) y el control FTP (puerto 21). Debido a que el filtro se aplica en sentido de entrada a la interfaz G0/0 en el R1, solo se denegará el tráfico de la red 2001:DB8:CAFE:10::/64.

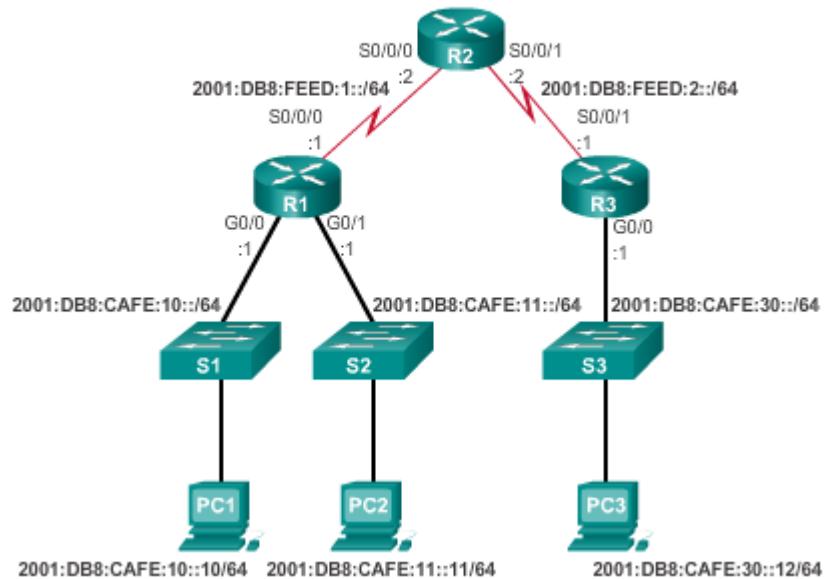
Acceso restringido

En el segundo ejemplo que se muestra en la figura 3, se configura una ACL de IPv6 para proporcionarle a la LAN en el R3 acceso limitado a las LAN en el R1. Se agregan comentarios en la configuración para documentar la ACL. Se marcaron las siguientes características en la ACL:

1. Las primeras dos instrucciones permit proporcionan acceso desde cualquier dispositivo al servidor web en 2001:DB8:CAFE:10::10.
2. El resto de los dispositivos tienen denegado el acceso a la red 2001:DB8:CAFE:10::/64.
3. A la PC3 en 2001:DB8:CAFE:30::12 se le permite el acceso por Telnet a la PC2, que tiene la dirección IPv6 2001:DB8:CAFE:11::11.
4. El resto de los dispositivos tiene denegado el acceso por Telnet a la PC2.

5. El resto del tráfico IPv6 se permite al resto de los destinos.
6. La lista de acceso de IPv6 se aplica a la interfaz G0/0 en sentido de entrada, por lo que solo la red 2001:DB8:CAFE:30::/64 se ve afectada.

Topología IPv6



Denegar FTP

```
R1(config)# ipv6 access-list NO-FTP-TO-11
R1(config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp
R1(config-ipv6-acl)# deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
R1(config-ipv6-acl)# permit ipv6 any any
R1(config-ipv6-acl)# exit
R1(config)# interface g0/0
R1(config-if)# ipv6 traffic-filter NO-FTP-TO-11 in
R1(config-if)#
```

Restricción del acceso

```
R3 (config) # ipv6 access-list RESTRICTED-ACCESS
R3 (config-ipv6-acl) # remark Permit access only HTTP and HTTPS to Network 10
R3 (config-ipv6-acl) # permit tcp any host 2001:db8:cafe:10::10 eq 80 ] 1
R3 (config-ipv6-acl) # permit tcp any host 2001:db8:cafe:10::10 eq 443
R3 (config-ipv6-acl) # remark Deny all other traffic to Network 10
R3 (config-ipv6-acl) # deny ipv6 any 2001:db8:cafe:10::/64 2
R3 (config-ipv6-acl) # remark Permit PC3 telnet access to PC2
R3 (config-ipv6-acl) # permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq 23 3
R3 (config-ipv6-acl) # remark Deny telnet access to PC2 for all other devices
R3 (config-ipv6-acl) # deny tcp any host 2001:db8:cafe:11::11 eq 23 4
R3 (config-ipv6-acl) # remark Permit access to everything else
R3 (config-ipv6-acl) # permit ipv6 any any 5
R3 (config-ipv6-acl) # exit
R3 (config) # interface g0/0
R3 (config-if) # ipv6 traffic-filter RESTRICTED-ACCESS in 6
R3 (config-if) #
```

Los comandos que se utilizan para verificar una lista de acceso de IPv6 son similares a los que se utilizan para las ACL de IPv4. Con estos comandos, se puede verificar la lista de acceso de IPv6 RESTRICTED-ACCESS que se configuró anteriormente. En la figura 1, se muestra el resultado del comando `show ipv6 interface`. El resultado confirma que la ACL RESTRICTED-ACCESS está configurada en sentido de entrada en la interfaz G0/0.

Como se muestra en la figura 2, el comando `show access-lists` muestra todas las listas de acceso en el router, incluidas las ACL de IPv4 y de IPv6. Observe que, en las ACL de IPv6, los números de secuencia se colocan al final de la instrucción y no al principio, como ocurre en las listas de acceso de IPv4. Aunque las instrucciones aparecen en el orden en que se introdujeron, no siempre se presentan en incrementos de 10. Esto se debe a que las instrucciones `remark` que se introdujeron utilizan un número de secuencia, pero no se muestran en el resultado del comando `show access-lists`.

Al igual que las ACL extendidas para IPv4, las listas de acceso de IPv6 se muestran y se procesan en el orden en que se introducen las instrucciones. Recuerde que las ACL de IPv4 estándar utilizan una lógica interna que cambia el orden y la secuencia de procesamiento.

Como se muestra en la figura 3, el resultado del comando `show running-config` incluye todas las ACE y las instrucciones `remark`. Las instrucciones `remark` pueden colocarse antes o después de las instrucciones `permit` o `deny`, pero se debe mantener una ubicación coherente.

```
R3# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Global unicast address(es):
    2001:DB8:CAFE:30::1, subnet mask 255:255:255:0
  Input features: Access List
    Inbound access list RESTRICTED-ACCESS
<resultado omitido>
```

```
R3# show access-lists
IPv6 access list RESTRICTED-ACCESS
  permit tcp any host 2001:DB8:CAFE:10::10 eq www sequence 20
  permit tcp any host 2001:DB8:CAFE:10::10 eq 443 sequence 30
  deny ipv6 any 2001:DB8:CAFE:10::/64 sequence 50
  permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11 eq
    telnet sequence 70
  deny tcp any host 2001:DB8:CAFE:11::11 eq telnet sequence 90
  permit ipv6 any any sequence 110
R3#
```

```
R3# show running-config
<resultado omitido>
ipv6 access-list RESTRICTED-ACCESS
  remark Permit access only HTTP and HTTPS to Network 10
  permit tcp any host 2001:DB8:CAFE:10::10 eq www
  permit tcp any host 2001:DB8:CAFE:10::10 eq 443
  remark Deny all other traffic to Network 10
  deny ipv6 any 2001:DB8:CAFE:10::/64
  remark Permit PC3 telnet access to PC2
  permit tcp host 2001:DB8:CAFE:30::12 host 2001:DB8:CAFE:11::11
    eq telnet
  remark Deny telnet access to PC2 for all other devices
  deny tcp any host 2001:DB8:CAFE:11::11 eq telnet
  remark Permit access to everything else
  permit ipv6 any any
```

9.6 Resumen

Los routers no filtran tráfico de manera predeterminada. El tráfico que ingresa al router se enruta solamente en función de la información de la tabla de routing.

El filtrado de paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes y la transferencia o el descarte de estos según criterios como la dirección IP de origen, la dirección IP de destino y el protocolo incluido en el paquete. Un router que filtra paquetes utiliza reglas para determinar si permite o deniega el tráfico. Un router también puede realizar el filtrado de paquetes en la capa 4, la capa de transporte.

Una ACL es una lista secuencial de instrucciones permit o deny. La última instrucción de una ACL siempre es una instrucción deny implícita que bloquea todo el tráfico. Para evitar que la instrucción deny any implícita al final de la ACL bloquee todo el tráfico, es posible agregar la instrucción **permit ip any any**.

Cuando el tráfico de la red atraviesa una interfaz configurada con una ACL, el router compara la información dentro del paquete con cada entrada, en orden secuencial, para determinar si el paquete coincide con una de las instrucciones. Si se encuentra una coincidencia, el paquete se procesa según corresponda.

Las ACL se configuran para aplicarse al tráfico entrante o al tráfico saliente.

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. La regla básica para la colocación de una ACL estándar es colocarla cerca del destino.

Las ACL extendidas filtran paquetes según varios atributos: el tipo de protocolo, la dirección IPv4 de origen o de destino y los puertos de origen o de destino. La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen.

El comando de configuración **global access-list** define una ACL estándar con un número en el intervalo de 1 a 99 o una ACL extendida con un número en el intervalo de 100 a 199 y de 2000 a 2699. Tanto las ACL estándar como las extendidas pueden tener un nombre. El comando **ip access-list standard** *nombre* se utiliza para crear una ACL estándar con nombre, mientras que el comando **ip access-list extended** *nombre* se utiliza para una lista de acceso extendida. Las ACE de IPv4 incluyen el uso de máscaras wildcard.

Después de que se configura una ACL, se vincula a una interfaz mediante el comando **ip access-group** del modo de configuración de interfaz. Recuerde la regla de las tres P: una ACL por protocolo, por sentido y por interfaz.

Para eliminar una ACL de una interfaz, primero introduzca el comando **no ip access-group** en la interfaz y, a continuación, introduzca el comando **global no access-list** para eliminar la ACL completa.

Los comandos **show running-config** y **show access-lists** se utilizan para verificar la configuración de la ACL. El comando **show ip interface** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó.

El comando **access-class** configurado en el modo de configuración de línea restringe las conexiones de entrada y salida entre una VTY determinada y las direcciones en una lista de acceso.

Al igual que las ACL de IPv4 con nombre, los nombres en IPv6 son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. A diferencia de IPv4, no hay necesidad de una opción estándar o extendida.

En el modo de configuración global, utilice el comando **ipv6 access-list** *nombre* para crear una ACL de IPv6. A diferencia de las ACL de IPv4, las ACL de IPv6 no utilizan máscaras wildcard.

En cambio, se utiliza la longitud de prefijo para indicar cuánto de una dirección IPv6 de origen o destino debe coincidir.

Después de que se configura una ACL de IPv6, se la vincula a una interfaz mediante el comando **ipv6 traffic-filter**.

Filtrado de tráfico en un router mediante ACL



Con dos interfaces y dos protocolos en ejecución, este router podría tener un total de ocho ACL distintas aplicadas.

Las tres P para utilizar ACL

Solo se puede tener una ACL por protocolo, por interfaz y por sentido:

- Una ACL por protocolo (p. ej., IPv4 o IPv6)
- Una ACL por sentido (es decir, de entrada o de salida)
- Una ACL por interfaz (p. ej., FastEthernet0/0)

10 DHCP

10.1 Introducción

Todo dispositivo que se conecta a una red necesita una dirección IP única. Los administradores de red asignan direcciones IP estáticas a los routers, a los servidores, a las impresoras y a otros dispositivos de red cuyas ubicaciones (físicas y lógicas) probablemente no cambien. Por lo general, se trata de dispositivos que proporcionan servicios a los usuarios y dispositivos en la red. Por lo tanto, las direcciones que se les asignan se deben mantener constantes. Además, las direcciones estáticas habilitan a los administradores para que administren estos dispositivos en forma remota. A los administradores de red les resulta más fácil acceder a un dispositivo cuando pueden determinar fácilmente su dirección IP.

Sin embargo, las computadoras y los usuarios en una organización, a menudo, cambian de ubicación, física y lógicamente. Para los administradores de red, asignar direcciones IP nuevas cada vez que un empleado cambia de ubicación puede ser difícil y llevar mucho tiempo. Además, para los empleados móviles que trabajan desde ubicaciones remotas, puede ser difícil establecer de forma manual los parámetros de red correctos. Incluso para los clientes de escritorio, la asignación manual de direcciones IP y otra información de direccionamiento plantea una carga administrativa, especialmente a medida que crece la red.

La introducción de un servidor de protocolo de configuración dinámica de host (DHCP) en la red local simplifica la asignación de direcciones IP tanto a los dispositivos de escritorio como a los móviles. El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la administración de direcciones IP sea más eficaz y asegura la coherencia en toda la organización, incluso en las sucursales.

DHCP está disponible tanto para IPv4 (DHCPv4) como para IPv6 (DHCPv6). En este capítulo, se explora la funcionalidad, la configuración y la resolución de problemas de DHCPv4 y de DHCPv6.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Describir el funcionamiento de DHCPv4 en una red de pequeña o mediana empresa.
- Configurar un router como servidor de DHCPv4.
- Configurar un router como cliente DHCPv4.
- Realizar la resolución de problemas de una configuración DHCP para IPv4 en una red commutada.
- Explicar el funcionamiento de DHCPv6.
- Configurar DHCPv6 sin estado para una pequeña o mediana empresa.
- Configurar DHCPv6 con estado para una pequeña o mediana empresa.
- Realizar la resolución de problemas de una configuración DHCP para IPv6 en una red commutada.



Los servidores de DHCP pueden simplificar las asignaciones de direcciones IP para las computadoras de escritorio y las terminales móviles.

10.2 Protocolo de configuración dinámica de host v4

10.2.1 Funcionamiento de DHCPv4

DHCPv4 asigna direcciones IPv4 y otra información de configuración de red en forma dinámica. Dado que los clientes de escritorio suelen componer gran parte de los nodos de red, DHCPv4 es una herramienta extremadamente útil para los administradores de red y que ahorra mucho tiempo.

Un servidor de DHCPv4 dedicado es escalable y relativamente fácil de administrar. Sin embargo, en una sucursal pequeña o ubicación SOHO, se puede configurar un router Cisco para proporcionar servicios DHCPv4 sin necesidad de un servidor dedicado. Un conjunto de características del IOS de Cisco (denominado "Easy IP") ofrece un servidor de DHCPv4 optativo con todas las características.

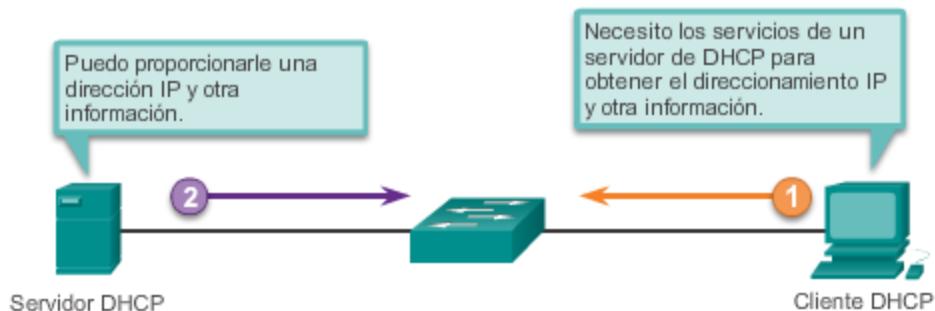
DHCPv4 incluye tres mecanismos diferentes de asignación de direcciones para proporcionar flexibilidad al asignar las direcciones IP:

- **Asignación manual:** el administrador asigna una dirección IPv4 preasignada al cliente, y DHCPv4 comunica solo la dirección IPv4 al dispositivo.
- **Asignación automática:** DHCPv4 asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo y la selecciona de un conjunto de direcciones disponibles. No hay arrendamiento, y la dirección se asigna de forma permanente al dispositivo.

- **Asignación dinámica:** DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado elegido por el servidor o hasta que el cliente ya no necesite la dirección.

La asignación dinámica es el mecanismo DHCPv4 que se utiliza más comúnmente y es el eje de esta sección. Al utilizar la asignación dinámica, los clientes arriendan la información del servidor durante un período definido administrativamente, como se muestra en la ilustración. Los administradores configuran los servidores de DHCPv4 para establecer los arrendamientos, a fin de que caduquen a distintos intervalos. El arrendamiento típicamente dura de 24 horas a una semana o más. Cuando caduca el arrendamiento, el cliente debe solicitar otra dirección, aunque generalmente se le vuelve a asignar la misma.

Protocolo de configuración dinámica de host (DHCP)



Como se muestra en la figura 1, DHCPv4 funciona en un modo cliente/servidor. Cuando un cliente se comunica con un servidor de DHCPv4, el servidor asigna o arrienda una dirección IPv4 a ese cliente. El cliente se conecta a la red con esa dirección IP arrendada hasta que caduque el arrendamiento. El cliente debe ponerse en contacto con el servidor de DHCP periódicamente para extender el arrendamiento. Este mecanismo de arrendamiento asegura que los clientes que se trasladan o se desconectan no mantengan las direcciones que ya no necesitan. Cuando caduca un arrendamiento, el servidor de DHCP devuelve la dirección al conjunto, donde se puede volver a asignar según sea necesario.

Origen del arrendamiento

Cuando el cliente arranca (o quiere unirse a una red), comienza un proceso de cuatro pasos para obtener un arrendamiento. Como se muestra en la figura 2, un cliente inicia el proceso con un mensaje de difusión DHCPDISCOVER con su propia dirección MAC para detectar los servidores de DHCPv4 disponibles.

Detección de DHCP (DHCPDISCOVER)

El mensaje DHCPDISCOVER encuentra los servidores de DHCPv4 en la red. Dado que el cliente no tiene información de IPv4 válida durante el arranque, utiliza direcciones de difusión de capa 2 y de capa 3 para comunicarse con el servidor.

Oferta de DHCP (DHCPoffer)

Cuando el servidor de DHCPv4 recibe un mensaje DHCPDISCOVER, reserva una dirección IPv4 disponible para arrendar al cliente. El servidor también crea una entrada ARP que consta de la dirección MAC del cliente que realiza la solicitud y la dirección IPv4 arrendada del cliente. Como se muestra en la figura 3, el servidor de DHCPv4 envía el mensaje DHCPoffer asignado al cliente que realiza la solicitud. El mensaje DHCPoffer se envía como una unidifusión, y se utiliza la dirección MAC de capa 2 del servidor como la dirección de origen y la dirección MAC de capa 2 del cliente como el destino.

Solicitud de DHCP (DHCPrequest)

Cuando el cliente recibe el mensaje DHCPoffer proveniente del servidor, envía un mensaje DHCPREQUEST, como se muestra en la figura 4. Este mensaje se utiliza tanto para el origen como para la renovación del arrendamiento. Cuando se utiliza para el origen del arrendamiento, el mensaje DHCPREQUEST sirve como notificación de aceptación vinculante al servidor seleccionado para los parámetros que ofreció y como un rechazo implícito a cualquier otro servidor que pudiera haber proporcionado una oferta vinculante al cliente.

Muchas redes empresariales utilizan varios servidores de DHCPv4. El mensaje DHCPREQUEST se envía en forma de difusión para informarle a este servidor de DHCPv4 y a cualquier otro servidor de DHCPv4 acerca de la oferta aceptada.

Acuse de recibo de DHCP (DHCPack)

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento con un ping ICMP a esa dirección para asegurarse de que no esté en uso, crea una nueva entrada ARP para el arrendamiento del cliente y responde con un mensaje DHCPACK de unidifusión, como se muestra en la figura 5. El mensaje DHCPACK es un duplicado del mensaje DHCPoffer, a excepción de un cambio en el campo de tipo de mensaje. Cuando el cliente recibe el mensaje DHCPACK, registra la información de configuración y realiza una búsqueda de ARP para la dirección asignada. Si no hay respuesta al ARP, el cliente sabe que la dirección IPv4 es válida y comienza a utilizarla como propia.

Renovación del arrendamiento

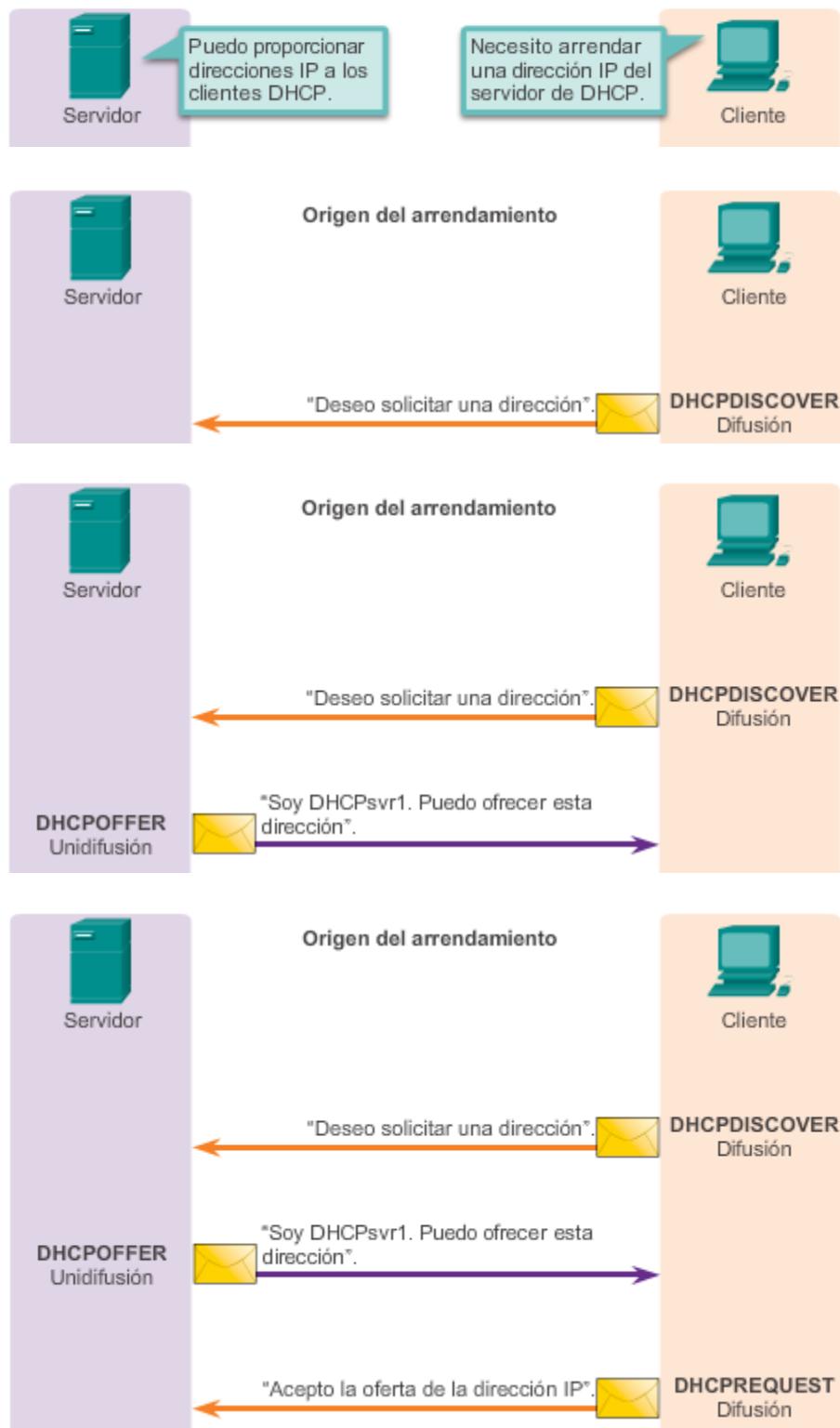
Solicitud de DHCP (DHCPrequest)

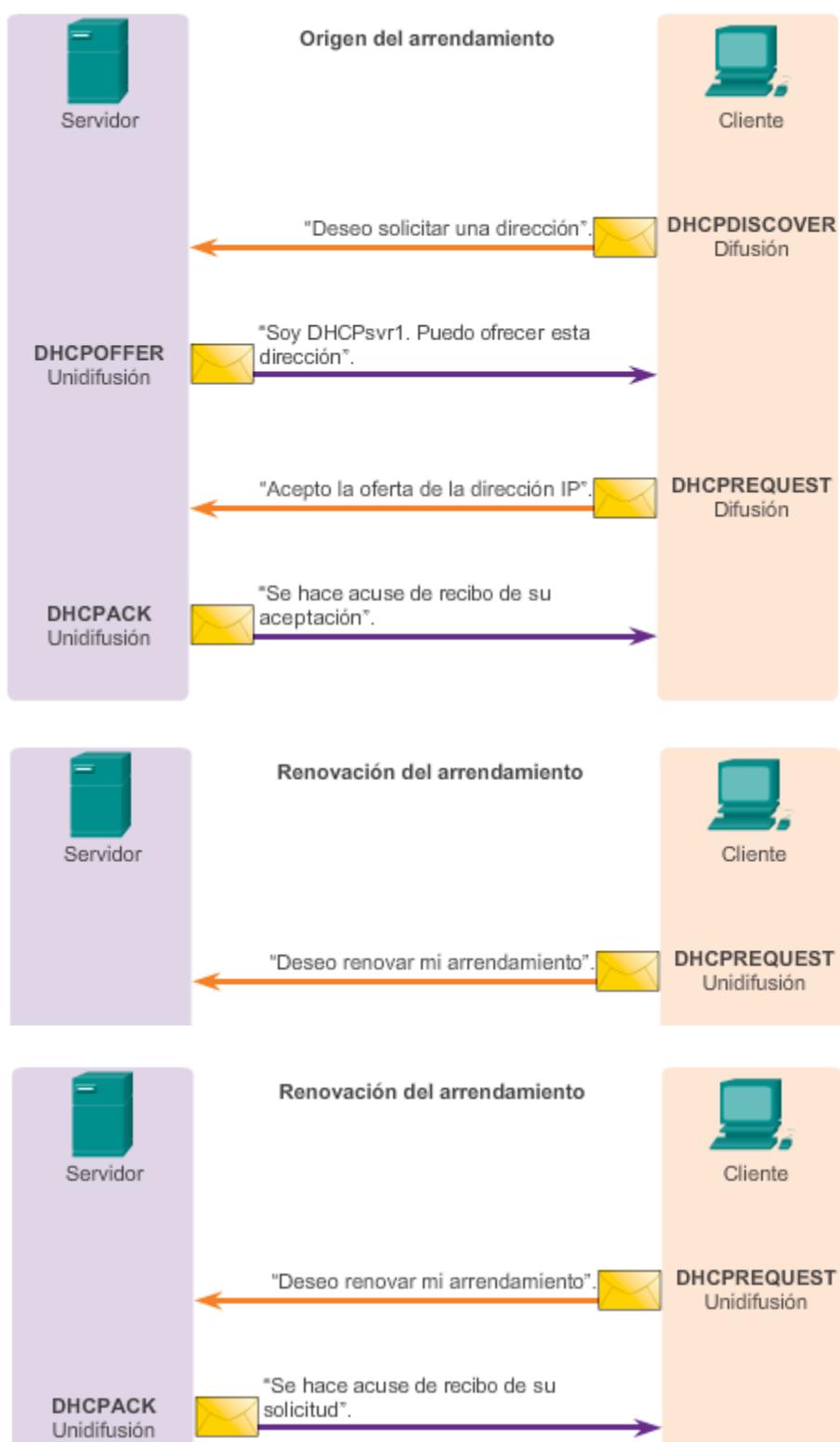
Como se muestra en la figura 6, cuando caduca el arrendamiento, el cliente envía un mensaje DHCPREQUEST directamente al servidor de DHCPv4 que ofreció la dirección IPv4 en primera instancia. Si no se recibe un mensaje DHCPACK dentro de una cantidad de tiempo especificada, el cliente transmite otro mensaje DHCPREQUEST de modo que uno de los otros servidores de DHCPv4 pueda extender el arrendamiento.

Acuse de recibo de DHCP (DHCPack)

Al recibir el mensaje DHCPREQUEST, el servidor verifica la información del arrendamiento al devolver un DHCPACK, como se muestra en la figura 7.

Funcionamiento de DHCPv4





El formato del mensaje DHCPv4 se utiliza para todas las transacciones DHCPv4. Los mensajes DHCPv4 se encapsulan dentro del protocolo de transporte UDP. Los mensajes DHCPv4 que se envían desde el cliente utilizan el puerto de origen UDP 68 y el puerto de destino 67. Los mensajes DHCPv4 que se envían del servidor al cliente utilizan el puerto de origen UDP 67 y el puerto de destino 68.

En la ilustración, se muestra el formato de un mensaje DHCPv4. Los campos son los siguientes:

- **Código de operación (OP):** especifica el tipo de mensaje general. El valor 1 indica un mensaje de solicitud y el valor 2 es un mensaje de respuesta.
- **Tipo de hardware:** identifica el tipo de hardware que se utiliza en la red. Por ejemplo, 1 es Ethernet, 15 es Frame Relay y 20 es una línea serial. Estos son los mismos códigos que se utilizan en mensajes ARP.
- **Longitud de dirección de hardware:** especifica la longitud de la dirección.
- **Saltos:** controla el reenvío de mensajes. Un cliente lo establece en 0 antes de transmitir una solicitud.
- **Identificador de transacción:** lo utiliza el cliente para hacer coincidir la solicitud con respuestas recibidas de los servidores de DHCPv4.
- **Segundos:** identifica la cantidad de segundos transcurridos desde que un cliente comenzó a intentar adquirir o renovar un arrendamiento. Lo utilizan los servidores de DHCPv4 para priorizar respuestas cuando hay varias solicitudes del cliente pendientes.
- **Indicadores:** los utiliza un cliente que no conoce su dirección IPv4 cuando envía una solicitud. Se utiliza solo uno de los 16 bits, que es el indicador de difusión. El valor 1 en este campo le indica al servidor de DHCPv4 o al agente de retransmisión que recibe la solicitud que la respuesta se debe enviar como una difusión.
- **Dirección IP del cliente:** la utiliza un cliente durante la renovación del arrendamiento cuando la dirección del cliente es válida y utilizable, no durante el proceso de adquisición de una dirección. El cliente coloca su propia dirección IPv4 en este campo solamente si tiene una dirección IPv4 válida mientras se encuentra en el estado vinculado. De lo contrario, establece el campo en 0.
- **Su dirección IP:** la utiliza el servidor para asignar una dirección IPv4 al cliente.
- **Dirección IP del servidor:** la utiliza el servidor para identificar la dirección del servidor que debe utilizar el cliente para el próximo paso en el proceso bootstrap, que puede ser, o no, el servidor que envía esta respuesta. El servidor emisor siempre incluye su propia dirección IPv4 en un campo especial llamado opción DHCPv4 Server Identifier (Identificador de servidores DHCPv4).
- **Dirección IP del gateway:** enruta los mensajes DHCPv4 cuando intervienen los agentes de retransmisión DHCPv4. La dirección del gateway facilita las comunicaciones de las solicitudes y respuestas de DHCPv4 entre el cliente y un servidor que se encuentran en distintas subredes o redes.
- **Dirección de hardware del cliente:** especifica la capa física del cliente.
- **Nombre del servidor:** lo utiliza el servidor que envía un mensaje DHCPOFFER o DHCPACK. El servidor puede, de manera optativa, colocar su nombre en este campo. Puede tratarse de un simple apodo de texto o un nombre de dominio DNS, como dhcpserver.netacad.net.

- **Nombre del archivo de arranque:** lo utiliza un cliente de manera optativa para solicitar un determinado tipo de archivo de arranque en un mensaje DHCPDISCOVER. Lo utiliza un servidor en un DHCPOFFER para especificar completamente un directorio de archivos y un nombre de archivo de arranque.
- **Opciones de DHCP:** contiene las opciones de DHCP, incluidos varios parámetros requeridos para el funcionamiento básico de DHCP. Este campo es de longitud variable. Tanto el cliente como el servidor pueden utilizarlo.

Formato del mensaje DHCPv4

8	16	24	32
Código OP (1)	Tipo de hardware (1)	Longitud de dirección de hardware (1)	Saltos (1)
Identificador de transacción			
Segundos: 2bytes		Indicadores: 2bytes	
Dirección IP del cliente (CIADDR): 4bytes			
Su dirección IP (YIADDR): 4bytes			
Dirección IP del servidor (SIADDR): 4bytes			
Dirección IP del gateway (GIADDR): 4bytes			
Dirección de hardware del cliente (CHADDR): 16bytes			
Nombre del servidor (SNAME): 64bytes			
Nombre del archivo de arranque: 128bytes			
Opciones de DHCP: variable			

Si un cliente está configurado para recibir su configuración IPv4 dinámicamente y desea unirse a la red, solicita valores de direccionamiento del servidor de DHCPv4. El cliente transmite un mensaje DHCPDISCOVER en su red local cuando arranca o detecta una conexión de red activa. Dado que el cliente no tiene forma de obtener información acerca de la subred a la que pertenece, el mensaje DHCPDISCOVER es una difusión IPv4 (dirección IPv4 de destino 255.255.255.255). El cliente aún no tiene una dirección IPv4 configurada, de modo que se utiliza la dirección IPv4 de origen 0.0.0.0.

Como se muestra en la figura 1, la dirección IPv4 del cliente (CIADDR), la dirección de gateway predeterminado (GIADDR) y la máscara de subred están marcados para indicar que se utiliza la dirección 0.0.0.0.

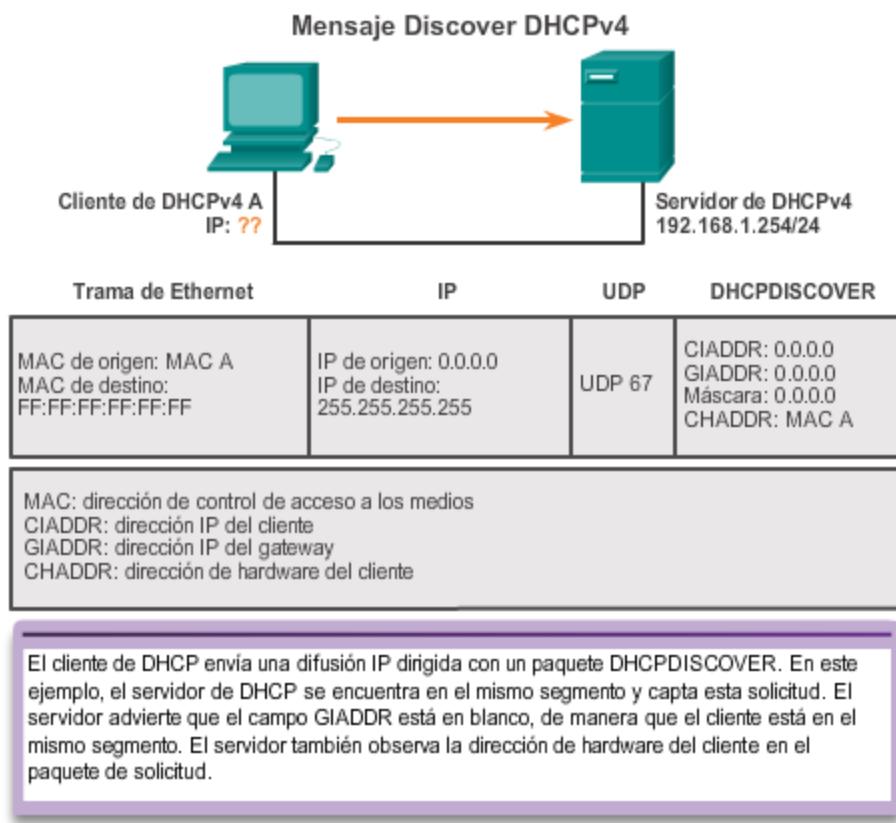
Nota: la información desconocida se envía como 0.0.0.0.

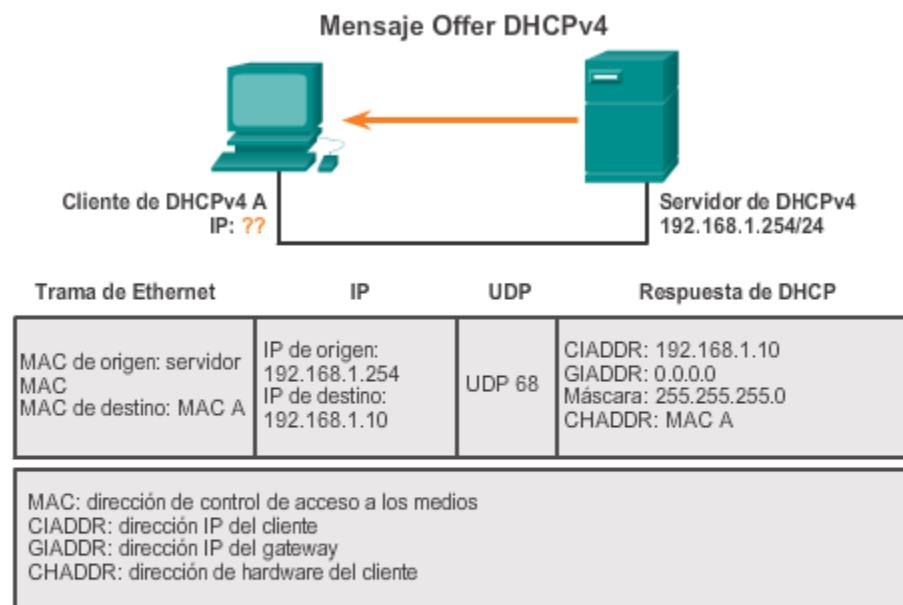
Cuando el servidor de DHCPv4 recibe el mensaje DHCPDISCOVER, responde con un mensaje DHCPOFFER. Este mensaje incluye información de configuración inicial para el cliente, como la dirección IPv4 que el servidor ofrece, la máscara de subred, la duración del arrendamiento y la dirección IPv4 del servidor de DHCPv4 que hace la oferta.

Es posible configurar el mensaje DHCPOFFER para que incluya otra información, como el tiempo de renovación del arrendamiento y la dirección DNS.

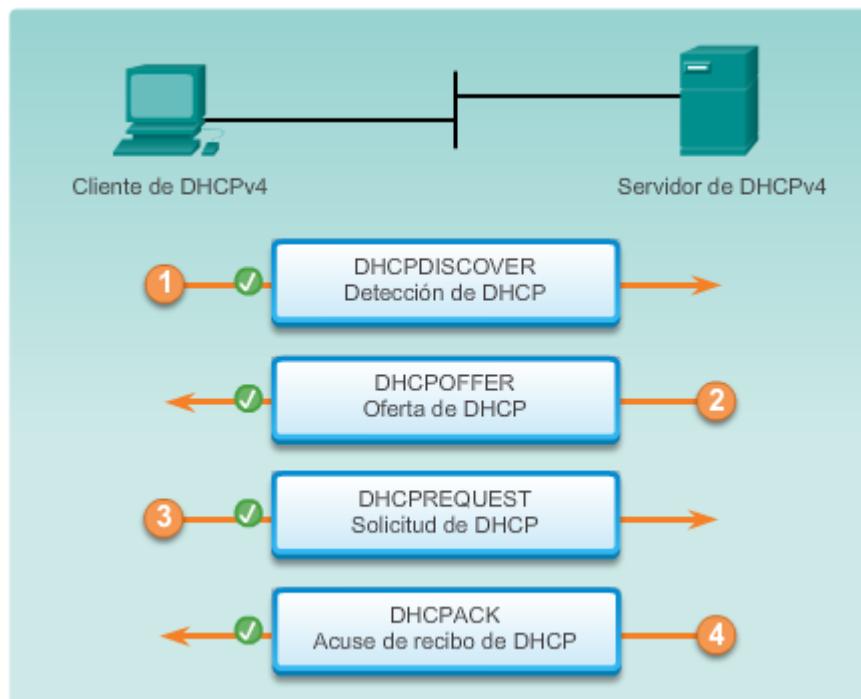
Como se muestra en la figura 2, el servidor de DHCP responde al mensaje DHCPDISCOVER asignando valores a la CIADDR y a la máscara de subred. La trama se crea mediante la dirección de hardware del cliente (CHADDR) y se envía al cliente que realiza la solicitud.

El cliente y el servidor envían mensajes de acuse de recibo, y finaliza el proceso.





El servidor de DHCP recoge una dirección IP del conjunto disponible para ese segmento, así como los parámetros globales y de los otros segmentos. El servidor de DHCP los coloca en los campos adecuados del paquete DHCP. A continuación, el servidor de DHCP usa la dirección de hardware A (en CHADDR) a fin de armar la trama adecuada para enviar al cliente.



10.2.2 Configuración de un servidor de DHCPv4 básico

Un router Cisco que ejecuta el software IOS de Cisco puede configurarse para que funcione como servidor de DHCPv4. El servidor de DHCPv4 que utiliza IOS de Cisco asigna y administra

direcciones IPv4 de conjuntos de direcciones especificados dentro del router para los clientes DHCPv4. La topología que se muestra en la figura 1 se utiliza para ilustrar esta funcionalidad.

Paso 1. Excluir direcciones IPv4

El router que funciona como servidor de DHCPv4 asigna todas las direcciones IPv4 en un conjunto de direcciones DHCPv4, a menos que esté configurado para excluir direcciones específicas. Generalmente, algunas direcciones IPv4 de un conjunto se asignan a dispositivos de red que requieren asignaciones de direcciones estáticas. Por lo tanto, estas direcciones IPv4 no deben asignarse a otros dispositivos. Para excluir direcciones específicas, utilice el comando `ip dhcp excluded-address`, como se muestra en la figura 2.

Se puede excluir una única dirección o un rango de direcciones especificando la dirección más baja y la dirección más alta del rango. Las direcciones excluidas deben incluir las direcciones asignadas a los routers, a los servidores, a las impresoras y a los demás dispositivos que se configuraron manualmente.

Paso 2. Configurar un pool de DHCPv4

La configuración de un servidor de DHCPv4 implica definir un conjunto de direcciones que se deben asignar. Como se muestra en la figura 3, el comando `ip dhcp pool nombre-pool` crea un pool con el nombre especificado e ingresa el router en el modo de configuración DHCPv4, que se identifica por la petición de entrada Router (dhcp-config) #.

Paso 3. Configurar tareas específicas

En la figura 4, se indican las tareas para finalizar la configuración del pool de DHCPv4. Algunas de ellas son optativas, mientras que otras deben configurarse.

El conjunto de direcciones y el router de gateway predeterminado deben estar configurados. Utilice la instrucción `network` para definir el rango de direcciones disponibles.

Utilice el comando `default-router` para definir el router de gateway predeterminado. Normalmente, el gateway es la interfaz LAN del router más cercano a los dispositivos clientes. Se requiere un gateway, pero se pueden indicar hasta ocho direcciones si hay varios gateways.

Otros comandos del pool de DHCPv4 son optativos. Por ejemplo, la dirección IPv4 del servidor DNS que está disponible para un cliente DHCPv4 se configura mediante el comando `dns-server`. El comando `domain-name dominio` se utiliza para definir el nombre de dominio. La duración del arrendamiento de DHCPv4 puede modificarse mediante el comando `lease`. El valor de arrendamiento predeterminado es un día. El comando `netbios-name-server` se utiliza para definir el servidor WINS con NetBIOS.

Ejemplo de DHCPv4

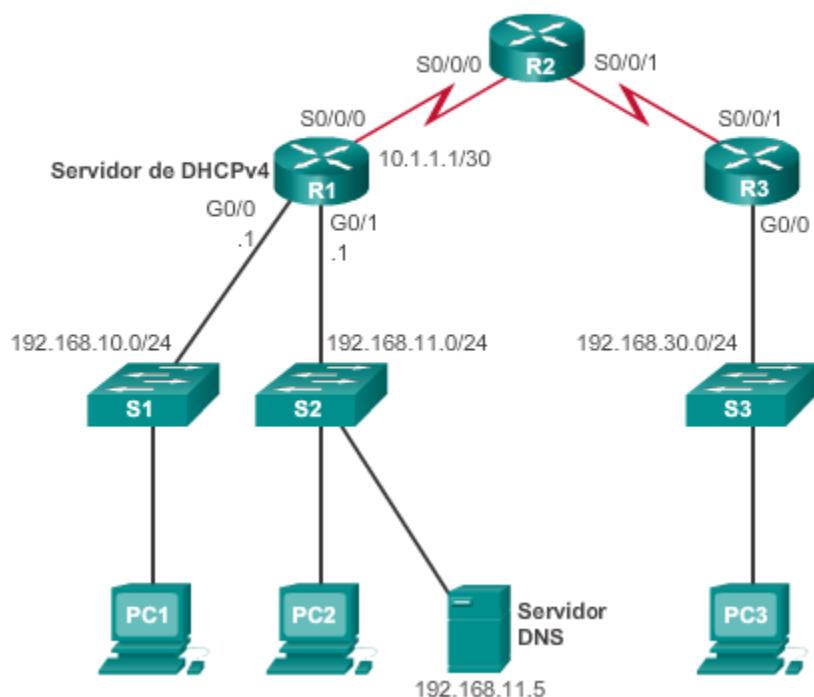
En la figura 5, se utiliza la topología de ejemplo de la figura 1 para mostrar una configuración de ejemplo con parámetros básicos de DHCPv4 configurados en el router R1, un servidor de DHCPv4 para la LAN 192.168.10.0/24.

Deshabilitación de DHCPv4

El servicio DHCPv4 está habilitado, de manera predeterminada, en versiones del software IOS de Cisco que lo admiten. Para deshabilitar el servicio, utilice el comando del modo de configuración global `no service dhcp`. Utilice el comando del modo de configuración global `service dhcp` para volver a habilitar el proceso del servidor de DHCPv4. Si los parámetros no se configuran, habilitar el servicio no tiene ningún efecto.

Utilice la actividad del verificador de sintaxis en la figura 6 para configurar parámetros de DHCPv4 similares en el R1 para la LAN 192.168.11.0/24.

Router R1 como servidor de DHCPv4



Paso 1 de la configuración de DHCPv4: exclusión de direcciones IPv4

```
R1(config)# ip dhcp excluded-address low-address [high-address]
```

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
```

Paso 2 de la configuración de DHCPv4: configuración de un pool de DHCPv4

```
R1(config)# ip dhcp pool pool-name
R1(dhcp-config)#End
```

```
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)#End
```

Paso 3 de la configuración de DHCPv4: configuración de tareas específicas

Tareas requeridas	Comando
Definir el conjunto de direcciones.	network <i>número-red</i> [máscara /longitud-prefijo]
Definir el router o gateway predeterminado.	default-router <i>dirección[dirección2...dirección8]</i>

Tareas opcionales	Comando
Definir un servidor DNS.	dns-server <i>dirección[dirección2...dirección8]</i>
Definir el nombre de dominio.	domain-name <i>dominio</i>
Definir la duración de la concesión DHCP.	lease { <i>días [horas]</i> [minutos] infinito}
Definir el servidor WINS con NetBIOS.	netbios-name-server <i>dirección[dirección2...dirección8]</i>

Ejemplo de DHCPv4

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

En el resultado de ejemplo, se utiliza la topología que se muestra en la figura 1. En este ejemplo, se configuró el R1 para que proporcione servicios DHCPv4. Dado que la PC1 no se encendió, no tiene una dirección IP.

Como se muestra en la figura 2, en el resultado del comando `show running-config | section dhcp`, se muestran los comandos de DHCPv4 configurados en el R1. El parámetro `| section` muestra solamente los comandos asociados a la configuración de DHCPv4.

Como se muestra en la figura 3, se puede verificar el funcionamiento de DHCPv4 mediante el comando `show ip dhcp binding`. Este comando muestra una lista de todas las vinculaciones de la dirección IPv4 con la dirección MAC que fueron proporcionadas por el servicio DHCPv4. El segundo comando en la figura 3, `show ip dhcp server statistics`, se utiliza para verificar si el router recibe o envía los mensajes. Este comando muestra información de conteo con respecto a la cantidad de mensajes DHCPv4 que se enviaron y recibieron.

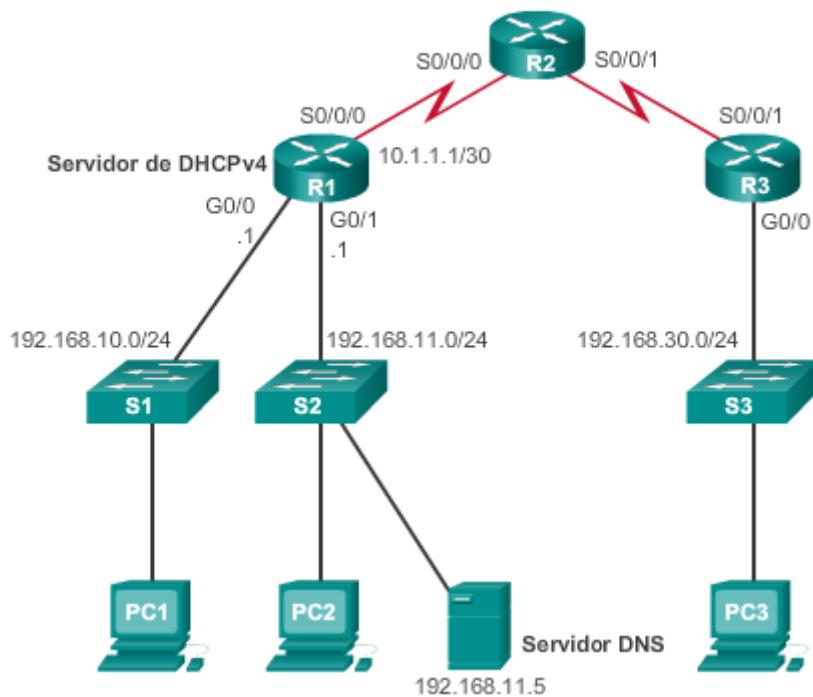
Como se observa en el resultado de estos comandos, actualmente no hay vinculaciones, y las estadísticas indican que no hay mensajes enviados o recibidos. En este momento, ningún dispositivo solicitó servicios DHCPv4 del router R1.

En la figura 4, los comandos se emiten después de que la PC1 y la PC2 se encendieron y finalizaron el proceso de arranque.

Observe que en la información acerca de las vinculaciones ahora se muestra que las direcciones IPv4 192.168.10.10 a 192.168.11.10 se unieron a las direcciones MAC. Las estadísticas también muestran actividad DHCPDISCOVER, DHCPREQUEST, DHCPOFFER y DHCPACK.

Como se muestra en la figura 5, el comando `ipconfig /all`, cuando se emite en la PC1, muestra los parámetros TCP/IP. Dado que la PC1 se conectó al segmento de red 192.168.10.0/24, recibió automáticamente un sufijo DNS, una dirección IPv4, una máscara de subred, un gateway predeterminado y una dirección del servidor DNS de ese pool. No se requiere configurar la interfaz del router. Si una computadora está conectada a un segmento de red que tiene un pool de DHCPv4 disponible, la computadora puede obtener una dirección IPv4 del pool adecuado de manera automática.

Router R1 como servidor de DHCPv4



Verificación de DHCPv4: comando show running-config

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp excluded-address 192.168.11.1 192.168.11.9
ip dhcp excluded-address 192.168.11.254
ip dhcp pool LAN-POOL-1
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 192.168.11.5
  domain-name example.com
ip dhcp pool LAN-POOL-2
  network 192.168.11.0 255.255.255.0
  default-router 192.168.11.1
  dns-server 192.168.11.5
  domain-name example.com
R1#
```

Antes de DHCPv4: comandos show ip dhcp

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration    Type
               Hardware address/
               User name

R1# show ip dhcp server statistics
Memory usage        23543
Address pools       1
Database agents     0
Automatic bindings  0
Manual bindings     0
Expired bindings    0
Malformed messages 0
Secure arp entries 0

Message            Received
BOOTREQUEST        0
DHCPDISCOVER       0
DHCPREQUEST        0
DHCPDECLINE        0
DHCPRELEASE        0
DHCPINFORM         0

Message            Sent
BOOTREPLY          0
DHCPoffer          0
```

Después de DHCPv4: comandos show ip dhcp

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/          Lease expiration      Type
                Hardware address/
                User name
192.168.10.10   0100.e018.5bdd.35  May 28 2013 01:06 PM Automatic
192.168.11.10   0100.b0d0.d817.e6  May 28 2013 01:10 PM Automatic

R1# show ip dhcp server statistics
Memory usage        25307
Address pools       2
Database agents     0
Automatic bindings  2
Manual bindings     0
Expired bindings    0
Malformed messages 0
Secure arp entries  0

Message            Received
BOOTREQUEST        0
DHCPDISCOVER       8
DHCPREQUEST        3
DHCPDECLINE        0
DHCPRELEASE        0
DHCPINFORM         0
```

Verificación de DHCPv4: cliente DHCPv4

```

C:\> C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\SpanPC>ipconfig /all

Windows IP Configuration

Host Name.....: ciscoLab
Primary Dns Suffix ..:
Node Type ....: Unknown
IP Routing Enabled...: No
WINS Proxy Enabled ...: No

Ethernet Adapter Local Area Connection

Connection-specific DNS Suffix.: example.com ←
Description .....: sis 900 PCI Fast Ethernet
Physical Address.....: 00-E0-18-5B-DD-35
Dhcp Enabled .....: Yes
Autoconfiguration Enabled....: Yes
IP Address .....: 192.168.10.10 ←
Subnet Mask.....: 255.255.255.0 ←
Default Gateway...: 192.168.10.1 ←
DHCP Server .....: 192.168.10.1
Lease Obtained.....: Monday, May 27, 2013 1:06:22PM
Lease Expires .....: Tuesday, May 28, 2013 1:06:22PM
DNS Servers .....: 192.168.11.5 ←

C:\Documents and settings\SpanPC>

```

¿Qué es la retransmisión de DHCP?

En una red jerárquica compleja, los servidores empresariales suelen estar ubicados en una granja de servidores. Estos servidores pueden proporcionar servicios DHCP, DNS, TFTP y FTP para la red. Generalmente, los clientes de red no se encuentran en la misma subred que esos servidores. Para ubicar los servidores y recibir servicios, los clientes con frecuencia utilizan mensajes de difusión.

En la figura 1, la PC1 intenta adquirir una dirección IPv4 de un servidor de DHCP mediante un mensaje de difusión. En esta situación, el router R1 no está configurado como servidor de DHCPv4 y no reenvía el mensaje de difusión. Dado que el servidor de DHCPv4 está ubicado en una red diferente, la PC1 no puede recibir una dirección IP mediante DHCP.

En la figura 2, la PC1 intenta renovar su dirección IPv4. Para hacerlo, se emite el comando `ipconfig /release`. Observe que se libera la dirección IPv4, y se muestra que la dirección es 0.0.0.0. A continuación, se emite el comando `ipconfig /renew`. Este comando hace que la PC1 transmita por difusión un mensaje DHCPDISCOVER. En el resultado se muestra que la PC1 no puede ubicar el servidor de DHCPv4. Dado que los routers no reenvían mensajes de difusión, la solicitud no es correcta.

Como solución a este problema, un administrador puede agregar servidores de DHCPv4 en todas las subredes. Sin embargo, ejecutar estos servicios en varias computadoras genera un costo adicional y sobrecarga administrativa.

Una mejor solución consiste en configurar una dirección de ayuda de IOS de Cisco. Esta solución permite que el router reenvíe difusiones de DHCPv4 al servidor de DHCPv4. Cuando un router reenvía solicitudes de asignación/parámetros de direcciones, actúa como agente de retransmisión DHCPv4. En la topología de ejemplo, la PC1 transmitiría por difusión una solicitud para ubicar un servidor de DHCPv4. Si el R1 estuviera configurado como agente de retransmisión DHCPv4, reenviaría la solicitud al servidor de DHCPv4 ubicado en la subred 192.168.11.0.

Como se muestra en la figura 3, la interfaz en el R1 que recibe la difusión se configura con el comando del modo de configuración de interfaz **ip helper-address**. La dirección del servidor de DHCPv4 se configura como el único parámetro.

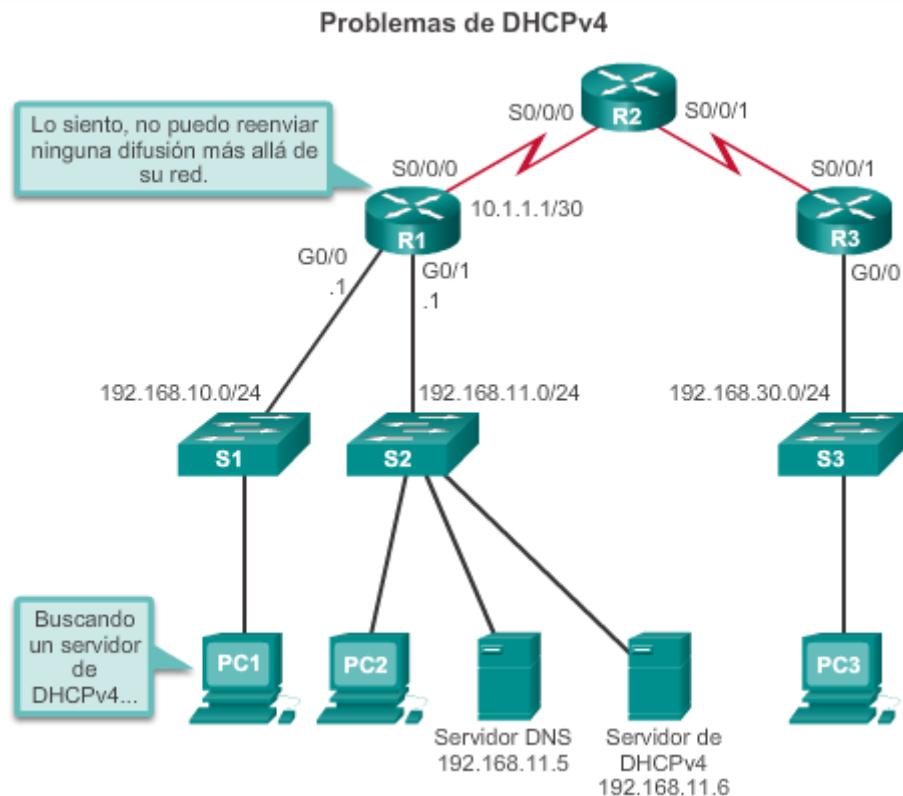
Cuando se configura el R1 como agente de retransmisión DHCPv4, acepta solicitudes de difusión para el servicio DHCPv4 y, a continuación, reenvía dichas solicitudes en forma de unidifusión a la dirección IPv4 192.168.11.6. El comando **show ip interface** se utiliza para verificar la configuración.

Como se muestra en la figura 4, la PC1 ahora puede adquirir una dirección IPv4 del servidor de DHCPv4.

DHCPv4 no es el único servicio que puede configurarse para que retransmita el router. De manera predeterminada, el comando **ip helper-address** reenvía los siguientes ocho siguientes servicios UDP:

- Puerto 37: Tiempo
- Puerto 49: TACACS
- Puerto 53: DNS
- Puerto 67: cliente DHCP/BOOTP
- Puerto 68: servidor de DHCP/BOOTP
- Puerto 69: TFTP
- Puerto 137: servicio de nombres NetBIOS
- Puerto 138: servicio de datagrama NetBIOS

Mediante el verificador de sintaxis de la figura 5, configure los comandos de retransmisión de DHCPv4 en el router correcto de modo que la PC3 pueda recibir información de direccionamiento IPv4 del servidor de DHCPv4. Consulte nuevamente la figura 1 para ver la topología de la red.



PC1: sin dirección IPv4

```
C:\ C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix.:
IP Address .....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway....:

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP Configuration

An error occurred while renewing interface Local Area Connection:
unable to contact your DHCP server. Request has timed out.
```

Comandos de retransmisión de DHCPv4

```
R1(config)# interface g0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1# show ip interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
<resultado omitido>
```

PC1: renovación de la dirección IPv4

```
C:\Documents and Settings\Administrator>ipconfig /release

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix.:
  IP Address .....: 0.0.0.0
  Subnet Mask.....: 0.0.0.0
  Default Gateway....:

C:\Documents and Settings\Administrator>ipconfig /renew

Windows IP Configuration

Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix.:
  IP Address .....: 192.168.10.11
  Subnet Mask.....: 255.255.255.0
  Default Gateway....: 192.168.10.1

C:\Documents and Settings\Administrator>
```

10.2.3 Configuración de cliente DHCPv4

En ocasiones, los routers Cisco en oficinas pequeñas y oficinas domésticas (SOHO) y en los sitios de sucursales deben configurarse como clientes DHCPv4 de manera similar a los equipos cliente. El método específico utilizado depende del ISP. Sin embargo, en su configuración más simple, se utiliza la interfaz Ethernet para conectarse a un cable módem o a un módem DSL. Para configurar una interfaz Ethernet como cliente DHCP, utilice el comando del modo de configuración de interfaz **ip address dhcp**.

En la figura 1, suponga que un ISP se configuró para proporcionar direcciones IP del rango de red 209.165.201.0/27 a clientes selectos. Después de que se configura la interfaz G0/1 con el

comando `ip address dhcp`, el comando `show ip interface g0/1` confirma que la interfaz está activada y que la dirección fue asignada por un servidor de DHCPv4.

Utilice el verificador de sintaxis de la figura 2 para configurar la interfaz que está conectada al ISP, a fin de adquirir una dirección del servidor de DHCP.

Configuración de un router como cliente de DHCP



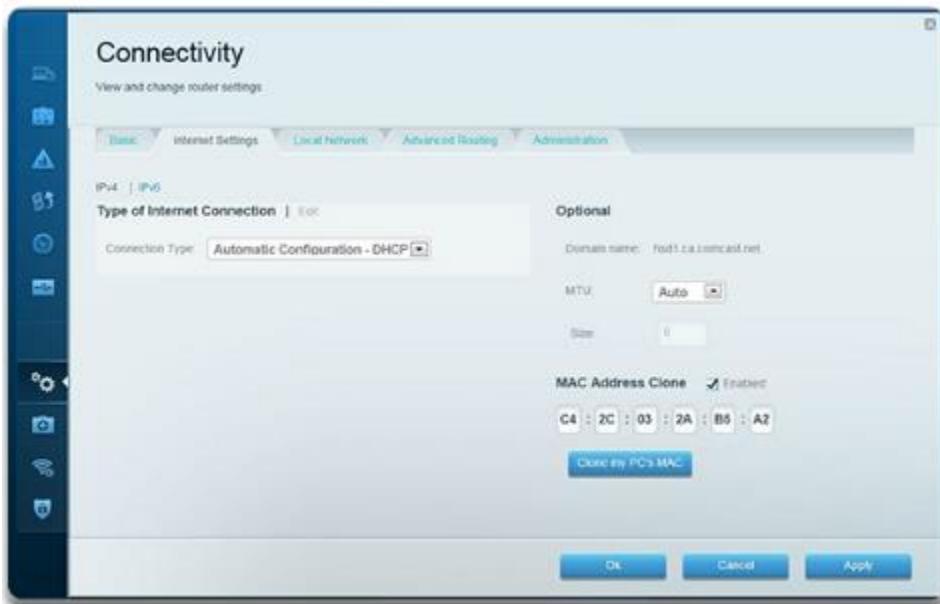
```

SOHO(config)# interface g0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
SOHO(config-if)#
*Jan 31 17:31:11.507: %DHCP-6-ADDRESS_ASSIGN: Interface
GigabitEthernet0/1 assigned DHCP address 209.165.201.12, mask
255.255.255.224, hostname SOHO
SOHO(config-if)# end
SOHO# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
<resultado omitido>
  
```

Normalmente, los routers con poca banda ancha para uso doméstico, como los routers Linksys, se pueden configurar para conectarse a un ISP mediante un cable módem o un módem DSL. En la mayoría de los casos, los routers SOHO están establecidos para adquirir una dirección IPv4 automáticamente del ISP.

Por ejemplo, en la ilustración se muestra la página de configuración de WAN predeterminada para un router Linksys EA6500. Observe que el tipo de conexión a Internet está establecido en Automatic Configuration - DHCP (Configuración automática, DHCP). Esto significa que cuando el router se conecta a un cable módem, por ejemplo, es un cliente DHCPv4 y solicita una dirección IPv4 del ISP.

Nota: la característica de clonación de la dirección MAC utiliza una dirección especificada como la dirección MAC de origen en el ISP que interactúa con la interfaz del router. Muchos ISP asignan direcciones IPv4 sobre la base de la dirección MAC del dispositivo durante la instalación inicial. Cuando otro dispositivo, como un router SOHO, está conectado al ISP, el ISP puede requerir que se configure la dirección MAC del dispositivo original en la interfaz WAN.



10.2.4 Resolución de problemas de DHCPv4

Los problemas de DHCPv4 pueden surgir debido a diversos motivos, como defectos de software en los sistemas operativos, controladores de NIC o agentes de retransmisión DHCP. Sin embargo, la causa más frecuente son los problemas de configuración. Debido a la cantidad de áreas posiblemente problemáticas, se requiere adoptar un enfoque sistemático a la resolución de problemas, como se muestra en la ilustración.

Tarea 1 de la resolución de problemas: resolver conflictos de direcciones IPv4

El arrendamiento de una dirección IPv4 puede caducar en un cliente que aún está conectado a una red. Si el cliente no renueva el arrendamiento, el servidor de DHCPv4 puede volver a asignar esa dirección IPv4 a otro cliente. Cuando el cliente se reinicia, solicita una dirección IPv4. Si el servidor de DHCPv4 no responde rápidamente, el cliente utiliza la última dirección IPv4. El problema surge cuando dos clientes utilizan la misma dirección IPv4, lo cual crea un conflicto.

El comando **show ip dhcp conflicto** muestra todos los conflictos de direcciones que registra el servidor de DHCPv4. El servidor utiliza el comando **ping** para detectar clientes. El cliente utiliza el protocolo de resolución de direcciones (ARP) para detectar conflictos. Si se detecta un conflicto de dirección, esta última se elimina del pool y no se asigna hasta que un administrador resuelva el conflicto.

Este resultado muestra las direcciones IP que tienen conflictos con el servidor de DHCP. Muestra el método de detección y el tiempo de detección para las direcciones IP en conflicto que ofreció el servidor de DHCP.

```
R1# show ip dhcp conflict
```

IP address	Detection Method	Detection time
192.168.10.32	Ping	Feb 16 2013 12:28 PM

192.168.10.64 Gratuitous ARP Feb 23 2013 08:12 AM

Tarea 2 de la resolución de problemas: verificar la conectividad física

Primero, utilice el comando **show interface interfaz** para confirmar que la interfaz del router que funciona como el gateway predeterminado para el cliente esté en funcionamiento. Si la interfaz tiene otro estado que no sea activado, el puerto no pasa tráfico, incluso solicitudes de cliente DHCP.

Tarea 3 de la resolución de problemas: probar la conectividad mediante una dirección IP estática

Al llevar a cabo la resolución de cualquier problema de DHCPv4, verifique la conectividad de red configurando información de la dirección IPv4 estática en una estación de trabajo cliente. Si la estación de trabajo no puede llegar a los recursos de red con una dirección IPv4 configurada estáticamente, la causa raíz del problema no es DHCPv4. En este punto, es necesario resolver los problemas de conectividad de la red.

Tarea 4 de la resolución de problemas: verificar la configuración de puertos del switch

Si el cliente DHCPv4 no puede obtener una dirección IPv4 del servidor de DHCPv4 durante el inicio, intente obtener una dirección IPv4 del servidor de DHCPv4 forzando manualmente al cliente para que envíe una solicitud de DHCPv4.

Nota: si hay un switch entre el cliente y el servidor de DHCPv4 y el cliente no puede obtener la configuración de DHCP, la causa pueden ser problemas con la configuración de puertos del switch. Estas causas pueden incluir problemas de enlaces troncales y canalización, STP y RSTP. Mediante la configuración de PortFast y las configuraciones de los puertos perimetrales se resuelven los problemas de cliente DHCPv4 más comunes que se presentan con la instalación inicial de un switch Cisco.

Tarea 5 de la resolución de problemas: probar el funcionamiento de DHCPv4 en la misma subred o VLAN

Es importante distinguir si DHCPv4 funciona correctamente cuando el cliente se encuentra en la misma subred o VLAN que el servidor de DHCPv4. Si DHCPv4 funciona correctamente cuando el cliente se encuentra en la misma subred o VLAN, el problema puede ser el agente de retransmisión DHCP. Si el problema persiste incluso con la prueba de DHCPv4 en la misma subred o VLAN que el servidor de DHCPv4, en realidad puede haber un problema con el servidor de DHCPv4.

Resolución de problemas de DHCPv4

Tarea 1 de la resolución de problemas:	Resolver conflictos de dirección.
Tarea 2 de la resolución de problemas:	Verificar la conectividad física.
Tarea 3 de la resolución de problemas:	Probar con una dirección IPv4 estática.
Tarea 4 de la resolución de problemas:	Verificar la configuración de puertos del switch.
Tarea 5 de la resolución de problemas:	Probar desde la misma subred o VLAN.

Cuando el servidor de DHCPv4 está ubicado en una LAN distinta de la del cliente, la interfaz del router que interactúa con el cliente se debe configurar para retransmitir las solicitudes de DHCPv4 mediante la configuración de la dirección IPv4 de ayuda. Si la dirección IPv4 de ayuda no se configura correctamente, las solicitudes de cliente DHCPv4 no se reenvían al servidor de DHCPv4.

Siga estos pasos para verificar la configuración del router:

Paso 1. Verificar que el comando **ip helper-address** esté configurado en la interfaz correcta. Este comando debe estar presente en la interfaz de entrada de la LAN que contiene las estaciones de trabajo cliente DHCPv4 y debe estar dirigido al servidor de DHCPv4 correcto. En la ilustración, el resultado del comando **show running-config** verifica que la dirección IPv4 de retransmisión DHCP hace referencia a la dirección del servidor de DHCPv4 en 192.168.11.6.

El comando **show ip interface** también se puede utilizar para verificar la retransmisión DHCPv4 en una interfaz.

Paso 2. Verificar que no se haya configurado el comando de configuración global **no service dhcp**. Este comando deshabilita toda la funcionalidad del servidor de DHCP y de retransmisión del router. El comando **service dhcp** no aparece en la configuración en ejecución, debido a que es la configuración predeterminada

En la ilustración, el comando **show running-config | include no service dhcp** verifica que el servicio DHCPv4 esté habilitado, debido a que no hay coincidencia para el comando **show running-config | include no service dhcp**. Si se hubiera deshabilitado el servicio, en el resultado se mostraría el comando **no service dhcp**.

Verificación de la retransmisión de DHCPv4 y de los servicios DHCPv4

```
R1# show running-config | section interface GigabitEthernet0/0
interface GigabitEthernet0/0
  ip address 192.168.10.1 255.255.255.0
  ip helper-address 192.168.11.6
  duplex auto
  speed auto
R1#
R1# show running-config | include no service dhcp
R1#
```

En los routers configurados como servidores de DHCPv4, el proceso DHCPv4 falla si el router no recibe solicitudes del cliente. A modo de tarea de resolución de problemas, verifique que el router reciba la solicitud de DHCPv4 del cliente. Este paso de la resolución de problemas comprende la configuración de una ACL para el resultado de la depuración.

En la ilustración, se muestra una ACL extendida que permite solamente paquetes con puertos de destino UDP de 67 o 68. Estos son los puertos típicos que utilizan los clientes y los servidores de DHCPv4 al enviar mensajes DHCPv4. La ACL extendida se utiliza con el comando **debug ip packet** para mostrar solamente los mensajes DHCPv4.

En el resultado que aparece en la ilustración, se muestra que el router recibe solicitudes de DHCP del cliente. La dirección IP de origen es 0.0.0.0, debido a que el cliente aún no tiene una dirección IP. El destino es 255.255.255.255, debido a que el mensaje de detección de DHCP del cliente se envía como difusión. En este resultado, solo se muestra un resumen del paquete, y no el mensaje DHCPv4 en sí. Sin embargo, el router recibió un paquete de difusión con los puertos UDP e IP de origen y destino adecuados para DHCPv4. En el resultado de depuración completo, se muestran todos los paquetes en las comunicaciones DHCPv4 entre el cliente y el servidor de DHCPv4.

Otro comando útil para llevar a cabo la resolución de problemas del funcionamiento de DHCPv4 es el comando **debug ip dhcp server events**. Este comando informa eventos del servidor, como asignaciones de direcciones y actualizaciones de bases de datos. También se utiliza para decodificar recepciones y transmisiones DHCPv4.

Verificación de DHCPv4 mediante los comandos de router debug

```
R1(config)# access-list 100 permit udp any any eq 67
R1(config)# access-list 100 permit udp any any eq 68
R1(config)# end
R1# debug ip packet 100
IP packet debugging is on for access list 100
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255, len 333,
rcvd 2
*IP: s=0.0.0.0 (GigabitEthernet0/1), d=255.255.255.255, len 333,
stop process pak for forus packet
*IP: s=192.168.11.1 (local), d=255.255.255.255
(GigabitEthernet0/1), len 328, sending broad/multicast

<resultado omitido>

R1# debug ip dhcp server events
DHCPD: returned 192.168.10.11 to address pool LAN-POOL-1
DHCPD: assigned IP address 192.168.10.12 to client
0100.0103.85e9.87.
DHCPD: checking for expired leases.
DHCPD: the lease for address 192.168.10.10 has expired.
DHCPD: returned 192.168.10.10 to address pool LAN-POOL-1
```

10.3 Protocolo de configuración dinámica de host v6

10.3.1 SLAAC y DHCPv6

De manera similar a lo que ocurre con IPv4, las direcciones IPv6 de unidifusión global pueden configurarse manualmente o de forma dinámica. Sin embargo, existen dos métodos en los que las direcciones IPv6 de unidifusión global pueden asignarse dinámicamente:

- Configuración automática de dirección sin estado (SLAAC), como se muestra en la ilustración
- Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

Introducción a SLAAC

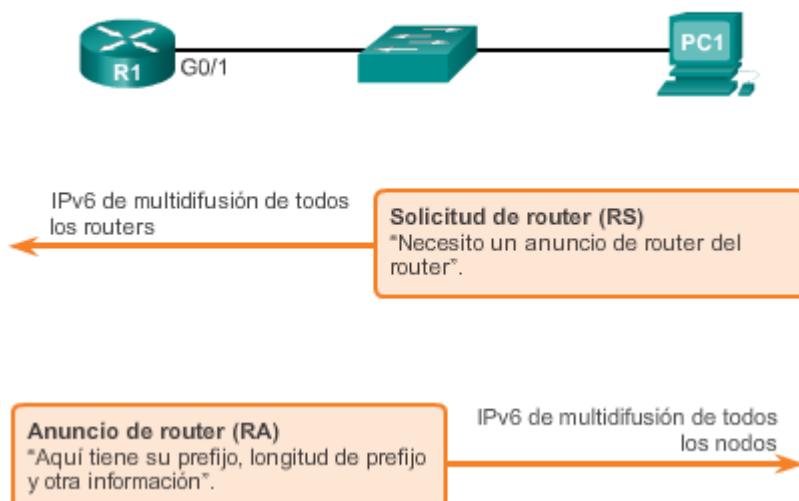
SLAAC es un método en el cual un dispositivo puede obtener una dirección IPv6 de unidifusión global sin los servicios de un servidor de DHCPv6. ICMPv6 se encuentra en el centro de SLAAC. ICMPv6 es similar a ICMPv4, pero incluye funcionalidad adicional y es un protocolo mucho más sólido. SLAAC utiliza mensajes de solicitud y de anuncio de router ICMPv6 para proporcionar direccionamiento y otra información de configuración que normalmente proporcionaría un servidor de DHCP:

- **Mensaje de solicitud de router (RS):**cuando un cliente está configurado para obtener la información de direccionamiento de forma automática mediante SLAAC, el cliente envía un mensaje RS al router. El mensaje RS se envía a la dirección IPv6 de multidifusión de todos los routers, FF02::2.
- **Mensaje de anuncio de router (RA):**los routers envían mensajes RA para proporcionar información de direccionamiento a los clientes configurados para obtener sus direcciones

IPv6 de forma automática. El mensaje RA incluye el prefijo y la longitud de prefijo del segmento local. Un cliente utiliza esta información para crear su propia dirección IPv6 de unidifusión global. Los routers envían mensajes RA de forma periódica o en respuesta a un mensaje RS. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos. Los mensajes RA siempre se envían a la dirección IPv6 de multidifusión de todos los nodos, FF02::1.

Como lo indica el nombre, SLAAC quiere decir “sin estado”. Un servicio sin estado significa que no hay ningún servidor que mantenga la información de la dirección de red. A diferencia de DHCP, no hay servidor de SLAAC que tenga información acerca de cuáles son las direcciones IPv6 que están en uso y cuáles son las que se encuentran disponibles.

Configuración automática de dirección sin estado ICMPv6



Para poder enviar mensajes RA, un router se debe habilitar como router IPv6. Para habilitar el routing IPv6, un router se configura con el siguiente comando:

```
Router(config)# ipv6 unicast-routing
```

1. En la topología de ejemplo que se muestra en la figura 1, la PC1 está configurada para obtener el direccionamiento IPv6 de manera automática. Desde el arranque, la PC1 no recibió un mensaje RA, de modo que envía un mensaje RS a la dirección de multidifusión de todos los routers para informarle al router IPv6 local que necesita un RA.
2. Como se muestra en la figura 2, el R1 recibe el mensaje RS y responde con un mensaje RA. En el mensaje RA, se incluyen el prefijo y la longitud de prefijo de la red. El mensaje RA se envía a la dirección IPv6 de multidifusión de todos los nodos, FF02::1, con la dirección link-local del router como la dirección IPv6 de origen.
3. La PC1 recibe el mensaje RA que contiene el prefijo y la longitud de prefijo para la red local. La PC1 utiliza esta información para crear su propia dirección IPv6 de unidifusión global. La PC1 ahora tiene un prefijo de red de 64 bits, pero necesita una ID de interfaz (IID) de 64 bits para crear una dirección de unidifusión global.

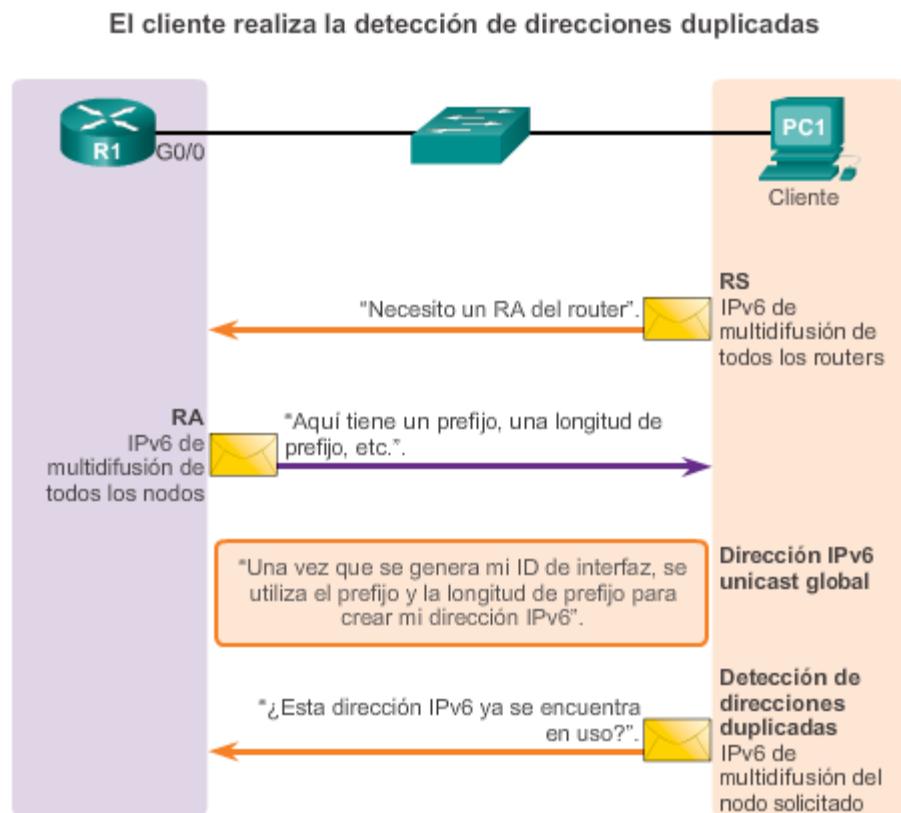
Hay dos maneras en las que la PC1 puede crear su propia IID única:

- **EUI-64:** mediante el proceso EUI-64, la PC1 crea una IID utilizando su dirección MAC de 48 bits.
- **De generación aleatoria:** la IID de 64 bits puede ser un número aleatorio generado por el sistema operativo cliente.

Como se muestra en la figura 3, la PC1 puede crear una dirección IPv6 de unidifusión global de 128 bits combinando el prefijo de 64 bits con la IID de 64 bits. La PC1 utiliza la dirección link-local del router como su dirección IPv6 de gateway predeterminado.

4. Dado que SLAAC es un proceso sin estado, para que la PC1 pueda utilizar esta dirección IPv6 creada recientemente, debe verificar que sea única. Como se muestra en la figura 4, la PC1 envía un mensaje de solicitud de vecino ICMPv6 con su propia dirección como la dirección IPv6 de destino. Si ningún otro dispositivo responde con un mensaje de anuncio de vecino, la dirección es única y puede ser utilizada por la PC1. Si la PC1 recibe un anuncio de vecino, la dirección no es única, y el sistema operativo debe determinar una nueva ID de interfaz para utilizar.

Este proceso forma parte de la detección de vecinos ICMPv6 y se conoce como “detección de direcciones duplicadas (DAD)”.



La decisión de si un cliente se configura para obtener su información de direccionamiento IPv6 de forma automática mediante SLAAC, mediante DHCPv6 o mediante una combinación de ambos depende de la configuración dentro del mensaje RA. Los mensajes RA ICMPv6 contienen dos indicadores para señalar cuál es la opción que debe utilizar el cliente.

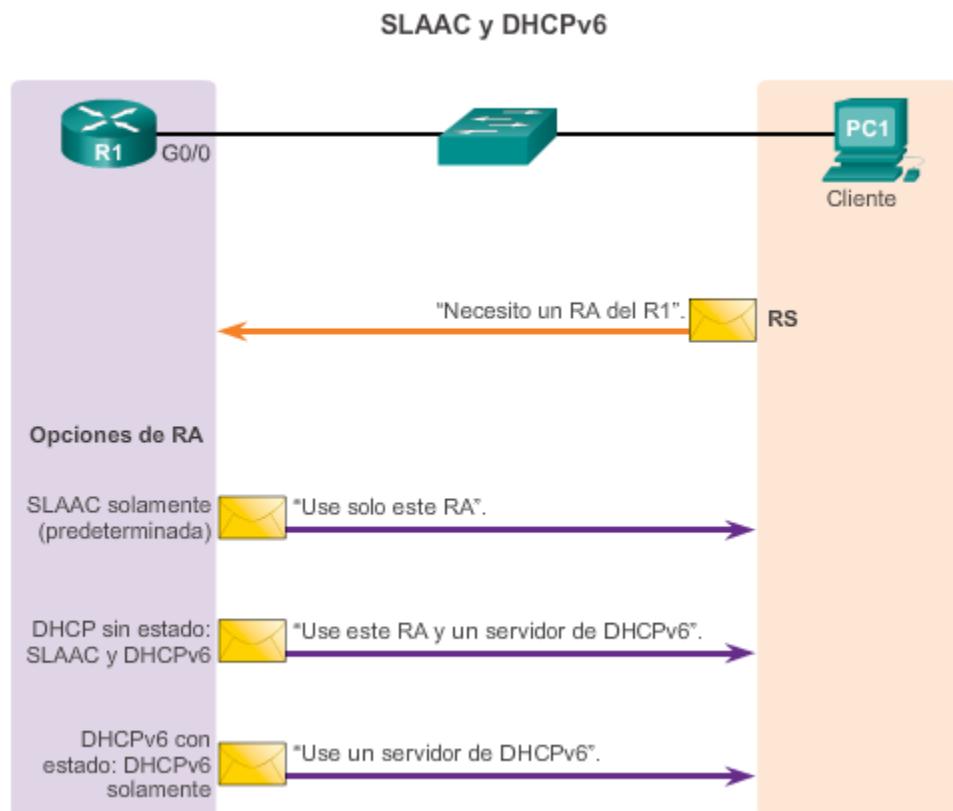
Los dos indicadores son el indicador de configuración de dirección administrada (indicador M) y el indicador de otra configuración (indicador O).

Mediante distintas combinaciones de los indicadores M y O, los mensajes RA tienen una de tres opciones de direccionamiento para el dispositivo IPv6, como se muestra en la ilustración:

- SLAAC (anuncio de router solamente)
- DHCPv6 sin estado (anuncio de router y DHCPv6)
- DHCPv6 con estado (DHCPv6 solamente)

Independientemente de la opción que se utilice, en RFC 4861 se recomienda que todos los dispositivos IPv6 realicen la detección de direcciones duplicadas (DAD) en cualquier dirección de unidifusión, entre las que se incluyen las direcciones configuradas mediante SLAAC o DHCPv6.

Nota: aunque el mensaje RA especifique el proceso que debe utilizar el cliente para obtener una dirección IPv6 de forma dinámica, el sistema operativo cliente puede elegir omitir el mensaje RA y utilizar los servicios de un servidor de DHCPv6 exclusivamente.



Opción de SLAAC (anuncio de router solamente)

SLAAC es la opción predeterminada en los routers Cisco. Tanto el indicador M como el indicador O están establecidos en 0 en el RA, como se muestra en la ilustración.

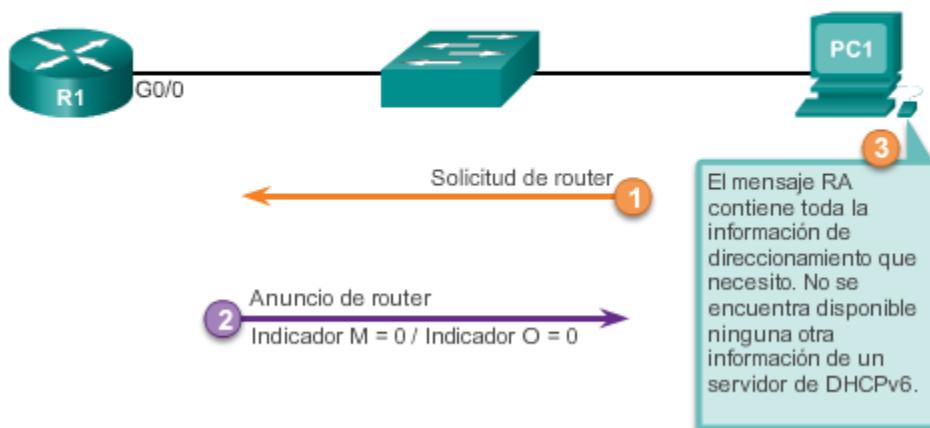
Esta opción le indica al cliente que utilice la información que se incluye en el mensaje RA de manera exclusiva. Esto incluye información del prefijo, de la longitud de prefijo, del servidor DNS, de la MTU y del gateway predeterminado. No se encuentra disponible ninguna otra información de un servidor de DHCPv6. La dirección IPv6 de unidifusión global se crea combinando el prefijo del mensaje RA y la ID de interfaz mediante EUI-64 o mediante un valor generado aleatoriamente.

Los mensajes RA se configuran en una interfaz individual de un router. Para volver a habilitar una interfaz para SLAAC que pudo haberse establecido en otra opción, se deben restablecer los indicadores M y O a sus valores iniciales de 0. Esto se realiza mediante los siguientes comandos del modo de configuración de interfaz:

```
Router(config-if)# no ipv6 nd managed-config-flag
```

```
Router(config-if)# no ipv6 nd other-config-flag
```

Opción de SLAAC



Si bien DHCPv6 es similar a DHCPv4 en cuanto a lo que proporciona, los dos protocolos son independientes respecto sí. DHCPv6 se define en RFC 3315. Se trabajó mucho en esta especificación a través de los años, como lo indica el hecho de que RFC DHCPv6 tiene el número de revisión más alto que cualquier borrador de Internet.

Opción de DHCPv6 sin estado (anuncio de router y DHCPv6)

La opción de DHCPv6 sin estado informa al cliente que utilice la información del mensaje RA para el direccionamiento, pero que hay más parámetros de configuración disponibles de un servidor de DHCPv6.

Mediante el prefijo y la longitud de prefijo en el mensaje RA, junto con EUI-64 o una IID generada aleatoriamente, el cliente crea la dirección IPv6 de unidifusión global.

A continuación, el cliente se comunica con un servidor de DHCPv6 sin estado para obtener información adicional que no se proporciona en el mensaje RA. Puede tratarse de una lista de direcciones IPv6 del servidor DNS, por ejemplo. Este proceso se conoce como DHCPv6 sin estado,

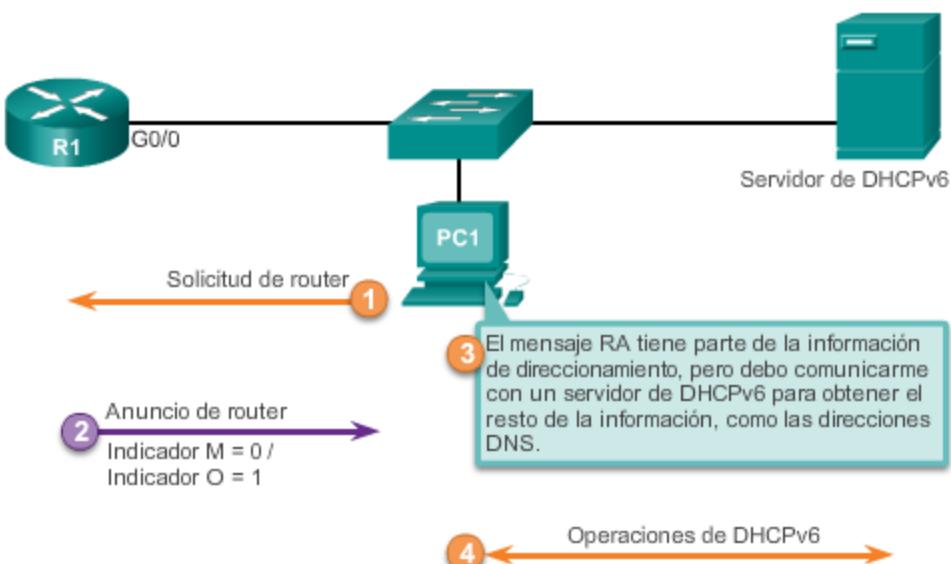
debido a que el servidor no mantiene información de estado del cliente (es decir, una lista de direcciones IPv6 asignadas y disponibles). El servidor de DHCPv6 sin estado solo proporciona parámetros de configuración para los clientes, no direcciones IPv6.

Para DHCPv6 sin estado, el indicador O se configura en 1 y el indicador M se deja en la configuración predeterminada de 0. El valor 1 del indicador O se utiliza para informarle al cliente que hay información de configuración adicional disponible de un servidor de DHCPv6 sin estado.

Para modificar el mensaje RA enviado en la interfaz de un router e indicar DHCPv6 sin estado, utilice el siguiente comando:

```
Router(config-if)# ipv6 nd other-config-flag
```

Opción de DHCPv6 sin estado

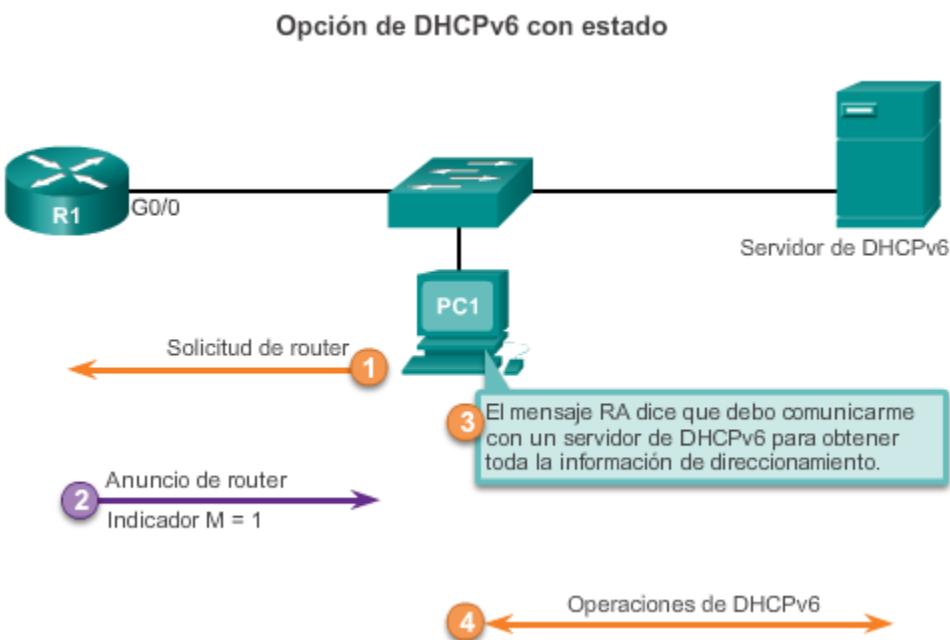


DHCPv6 con estado (DHCPv6 solamente)

Esta opción es la más similar a DHCPv4. En este caso, el mensaje RA le informa al cliente que no utilice la información contenida en el mensaje RA. Toda la información de direccionamiento y de configuración debe obtenerse de un servidor de DHCPv6 con estado. Esto se conoce como DHCPv6 con estado, debido a que el servidor de DHCPv6 mantiene información de estado de IPv6. Esto es similar a la asignación de direcciones para IPv4 por parte de un servidor de DHCPv4.

El indicador M señala si se debe utilizar DHCPv6 con estado o no. El indicador O no interviene. El siguiente comando se utiliza para cambiar el indicador M de 0 a 1 para indicar DHCPv6 con estado:

```
Router(config-if)# ipv6 nd managed-config-flag
```



Como se muestra en la figura 1, DHCPv6 sin estado o con estado, o ambos, comienzan con un mensaje RA ICMPv6 del router. El mensaje RA puede ser un mensaje periódico o un mensaje solicitado por el dispositivo mediante un mensaje RS.

Si en el mensaje RA se indica DHCPv6 con estado o sin estado, el dispositivo inicia las comunicaciones cliente/servidor DHCPv6.

Comunicaciones DHCPv6

Cuando el mensaje RA indica DHCPv6 sin estado o DHCPv6 con estado, se invoca el funcionamiento de DHCPv6. Los mensajes DHCPv6 se envían a través de UDP. Los mensajes DHCPv6 del servidor al cliente utilizan el puerto de destino UDP 546. El cliente envía mensajes DHCPv6 al servidor mediante el puerto de destino UDP 547.

El cliente, ahora un cliente DHCPv6, necesita ubicar el servidor de DHCPv6. En la figura 2, el cliente envía un mensaje DHCPv6 SOLICIT a la dirección IPv6 de multidifusión de todos los servidores de DHCPv6 reservada, FF02::1:2. Esta dirección de multidifusión tiene alcance link-local, lo cual significa que los routers no reenvían los mensajes a otras redes.

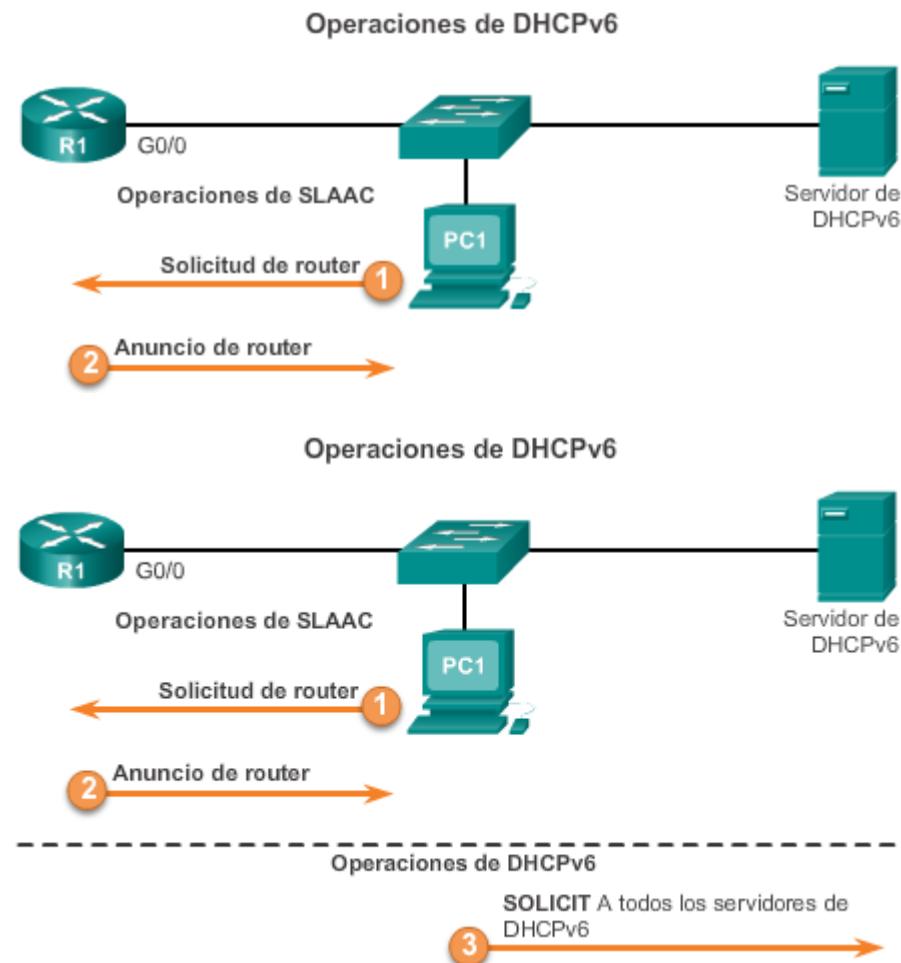
Uno o más servidores de DHCPv6 responden con un mensaje DHCPv6 ADVERTISE, como se muestra en la figura 3. El mensaje ADVERTISE le informa al cliente DHCPv6 que el servidor se encuentra disponible para el servicio DHCPv6.

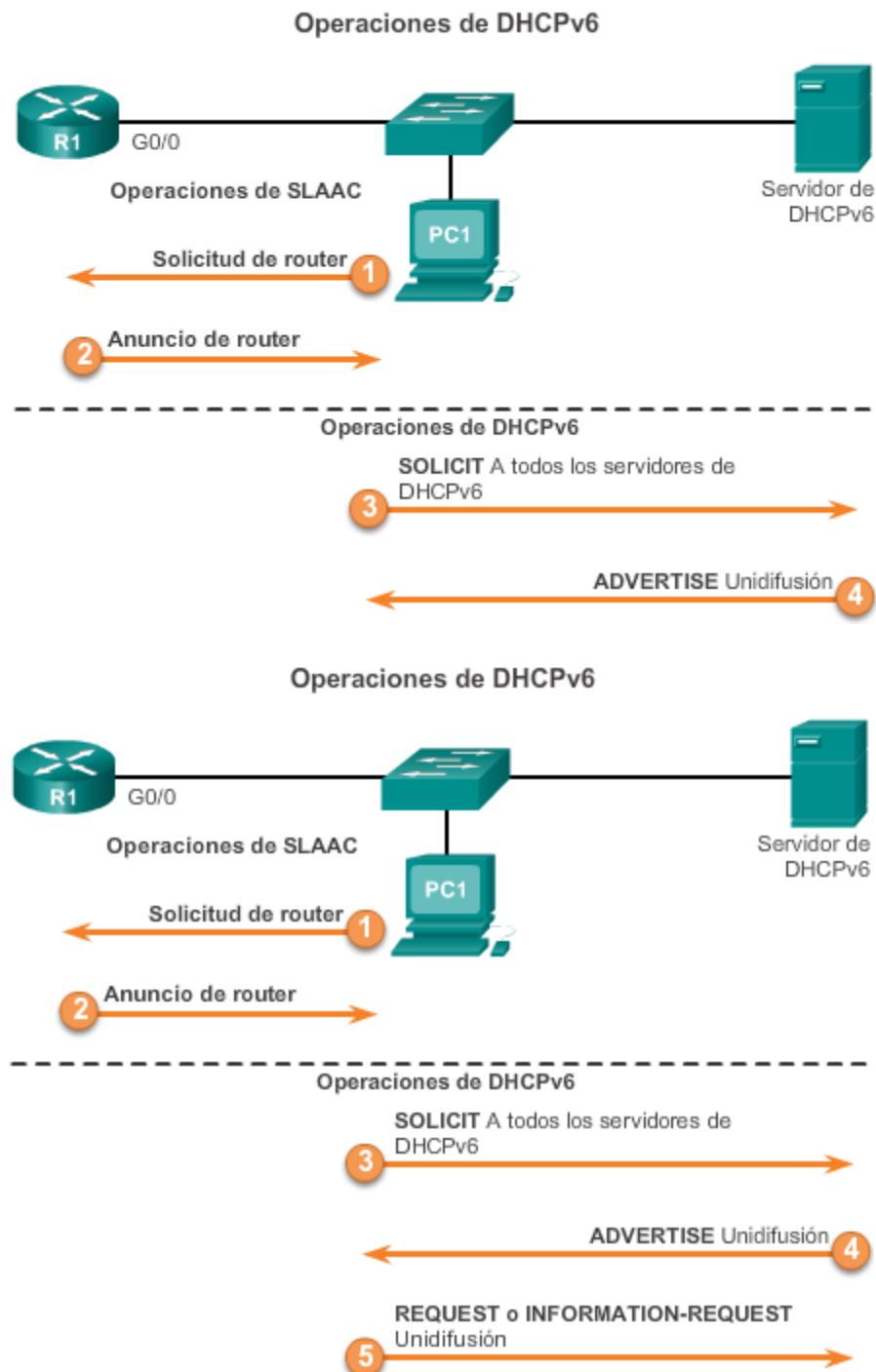
En la figura 4, el cliente responde con un mensaje INFORMATION-REQUEST o DHCPv6 REQUEST al servidor, según si utiliza DHCPv6 con estado o DHCPv6 sin estado.

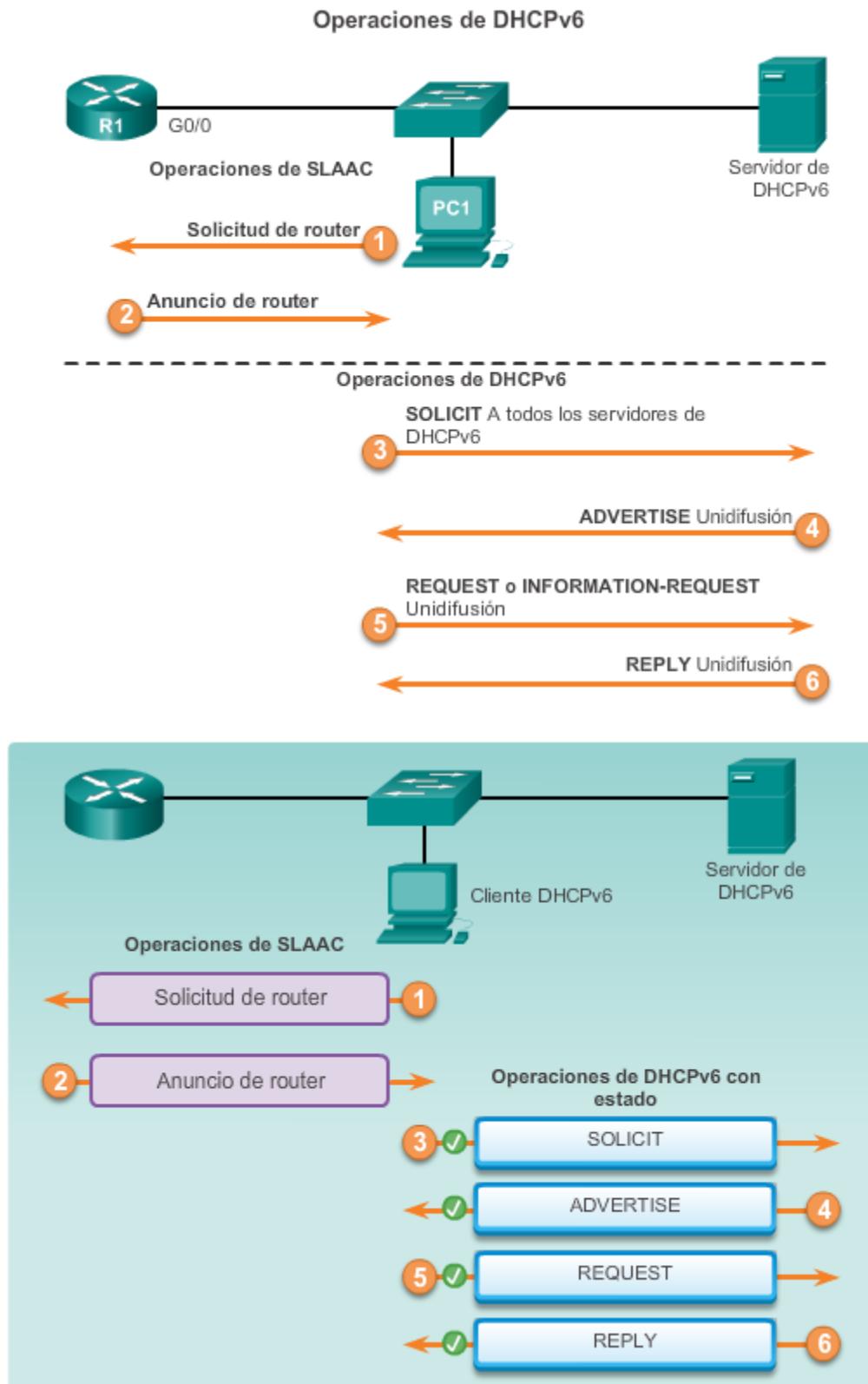
- **Cliente DHCPv6 sin estado:** el cliente envía un mensaje DHCPv6 INFORMATION-REQUEST al servidor de DHCPv6 en el que solicita solamente parámetros de configuración, como la dirección del servidor DNS. El cliente creó su propia dirección IPv6 mediante el uso del prefijo del mensaje RA y una ID de interfaz autogenerada aleatoriamente.

- **Cliente DHCPv6 con estado:** el cliente envía un mensaje DHCPv6 REQUEST al servidor para obtener una dirección IPv6 y todos los demás parámetros de configuración del servidor.

El servidor envía un mensaje DHCPv6 REPLY al cliente que contiene la información solicitada en el mensaje REQUEST o INFORMATION-REQUEST, como se muestra en la figura 5.







10.3.2 DHCPv6 sin estado

Como se muestra en la figura 1, hay cuatro pasos para configurar un router como servidor de DHCPv6:

Paso 1. Habilitar el routing IPv6

Se requiere el uso del comando `ipv6 unicast-routing` para habilitar el routing IPv6. Este comando no es necesario para que el router sea un servidor de DHCPv6 sin estado, pero se requiere para enviar mensajes RA ICMPv6.

Paso 2. Configurar un pool de DHCPv6

El comando `ipv6 dhcp pool nombre-pool` crea un pool e ingresa el router en el modo de configuración DHCPv6, que se identifica por la petición de entradaRouter (config-dhcpv6) #.

Paso 3. Configurar los parámetros del pool

Durante el proceso SLAAC, el cliente recibió la información que necesitaba para crear una dirección IPv6 de unidifusión global. El cliente también recibió la información de gateway predeterminado mediante la dirección IPv6 de origen del mensaje RA, que es la dirección link-local del router. Sin embargo, el servidor de DHCPv6 sin estado puede configurarse para proporcionar otra información que pudo no haberse incluido en el mensaje RA, como la dirección del servidor DNS y el nombre de dominio.

Paso 4. Configurar la interfaz DHCPv6

El comando del modo de configuración de interfaz `ipv6 dhcp server nombre-pool` vincula el pool de DHCPv6 con la interfaz. El router responde a las solicitudes de DHCPv6 sin estado en esta interfaz con la información incluida en el pool. El indicador O debe cambiarse de 0 a 1 mediante el comando de interfaz `ipv6 nd other-config-flag`. Los mensajes RA enviados en esta interfaz indican que hay información adicional disponible de un servidor de DHCPv6 sin estado.

Ejemplo de servidor de DHCPv6 sin estado

En la figura 2, se muestra una configuración de ejemplo para que un router se configure como servidor de DHCPv6 sin estado. Observe que el router R3 se muestra como cliente DHCPv6. El R3 está configurado como cliente para ayudar a verificar las operaciones de DHCPv6 sin estado.

Configuración de DHCPv6 sin estado en un router

Paso 1: habilitar el routing IPv6

```
Router(config)# ipv6 unicast-routing
```

Paso 2: configurar un pool de DHCPv6

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6)#End
```

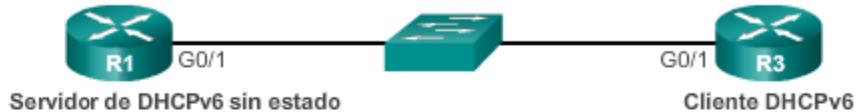
Paso 3: configurar los parámetros del pool

```
Router(config-dhcpv6)#End dns-server dns-server-address
Router(config-dhcpv6)#End domain-name domain-name
```

Paso 4: configurar la interfaz DHCPv6

```
Router(config)# interface type number
Router(config-if)# ipv6 dhcp server pool-name
Router(config-if)# ipv6 nd other-config-flag
```

Configuración del router R1 como servidor de DHCPv6 sin estado



```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)#End dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)#End domain-name example.com
R1(config-dhcpv6)#End exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

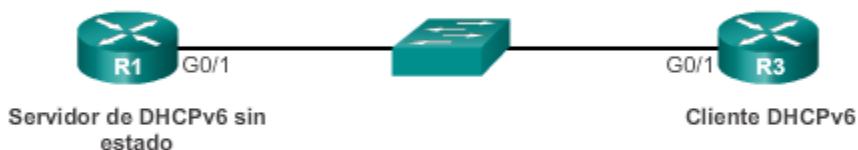
En el ejemplo de esta ilustración, se utiliza un router Cisco como cliente DHCPv6 sin estado. Esta no es una situación típica y se utiliza solo con fines de demostración. Generalmente, un cliente DHCPv6 sin estado es un dispositivo, como una computadora, una tablet PC, un dispositivo móvil o una cámara web.

El router cliente necesita una dirección IPv6 link-local en la interfaz para enviar y recibir mensajes IPv6, como mensajes RS y mensajes DHCPv6. La dirección link-local de un router se crea automáticamente cuando se habilita IPv6 en la interfaz. Esto puede suceder cuando se configura una dirección de unidifusión global en la interfaz o cuando se utiliza el comando `ipv6 enable`. Una vez que el router recibe una dirección link-local, puede enviar mensajes RS y participar en DHCPv6.

En este ejemplo, se utiliza el comando `ipv6 enable`, porque el router aún no tiene una dirección de unidifusión global.

El comando `ipv6 address autoconfig` habilita la configuración automática del direccionamiento IPv6 mediante SLAAC. A continuación, se utiliza un mensaje RA para informarle al router cliente que utilice DHCPv6 sin estado.

Configuración de un router como cliente DHCPv6 sin estado



```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address autoconfig
R3(config-if)#{
```

Verificación del servidor de DHCPv6 sin estado

En la figura 1, el comando `show ipv6 dhcp pool` verifica el nombre del pool de DHCPv6 y sus parámetros. La cantidad de clientes activos es 0, porque el servidor no mantiene ningún estado.

El comando `show running-config` también se puede utilizar para verificar todos los comandos que se configuraron anteriormente.

Verificación del cliente DHCPv6 sin estado

En este ejemplo, se utiliza un router como cliente DHCPv6 sin estado. En la figura 2, el resultado del comando `show ipv6 interface` muestra que el router tiene "Stateless address autoconfig enabled" (Configuración automática de dirección sin estado habilitada) y una dirección IPv6 de unidifusión global. La dirección IPv6 de unidifusión global se creó mediante

SLAAC, que incluye el prefijo contenido en el mensaje RA. La IID se generó mediante EUI-64. No se utilizó DHCPv6 para asignar la dirección IPv6.

La información de router predeterminado también proviene del mensaje RA. Esta era la dirección IPv6 de origen del paquete que contenía el mensaje RA y la dirección link-local del router.

En el resultado del comando `debug ipv6 dhcp detail` de la figura 3, se muestran los mensajes DHCPv6 intercambiados entre el cliente y el servidor. En este ejemplo, se introdujo el comando en el cliente. Se muestra el mensaje INFORMATION-REQUEST, debido a que se envía desde un cliente DHCPv6 sin estado. Observe que el cliente, el router R3, envía los mensajes DHCPv6 desde su dirección link-local hacia la dirección de todos los agentes de retransmisión y servidores de DHCPv6, FF02::1:2.

El resultado de depuración muestra todos los mensajes DHCPv6 enviados entre el cliente y el servidor, entre los que se incluyen las opciones de servidor DNS y de nombre de dominio que se configuraron en el servidor.

Utilice el verificador de sintaxis de la figura 4 para configurar y verificar DHCPv6 sin estado en el router.

Verificación del servidor de DHCPv6 sin estado



```

R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATELESS
  DNS server: 2001:DB8:CAFE:AAAA::5
  Domain name: example.com
  Active clients: 0
R1#
    
```

Verificación del cliente DHCPv6 sin estado: comando `show ipv6 interface`

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
    FE80::32F7:DFF:FE25:2DE1
    No Virtual link-local address(es):
    Stateless address autoconfig enabled
    Global unicast address(es):
      2001:DB8:CAFE:1:32F7:DFF:FE25:2DE1, subnet is
        2001:DB8:CAFE:1::/64 [EUI/CAL/PRE]
          valid lifetime 2591935 preferred lifetime 604735
    Joined group address(es):
      FF02::1
      FF02::1:FF25:2DE1
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ICMP unreachable messages are sent
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds (using 30000)
    ND NS retransmit interval is 1000 milliseconds
    Default router is FE80::D68C:B5FF:FECE:A0C1 on
      GigabitEthernet0/1
R3#
```

Verificación del cliente DHCPv6 sin estado: comando `debug ipv6 dhcp detail`

```
R3# debug ipv6 dhcp detail
  IPv6 DHCP debugging is on (detailed)
R3#
*Feb  3 02:39:10.454: IPv6 DHCP: Sending INFORMATION-REQUEST
  to FF02::1:2 on GigabitEthernet0/1
*Feb  3 02:39:10.454: IPv6 DHCP: detailed packet contents
*Feb  3 02:39:10.454:   src FE80::32F7:DFF:FE25:2DE1
*Feb  3 02:39:10.454:   dst FF02::1:2 (GigabitEthernet0/1)
*Feb  3 02:39:10.454:   type INFORMATION-REQUEST(11), xid
  12541745
<resultado omitido>
*Feb  3 02:39:10.454:   IPv6 DHCP: Adding server
    FE80::D68C:B5FF:FECE:A0C1
*Feb  3 02:39:10.454:   IPv6 DHCP: Processing options
*Feb  3 02:39:10.454:   IPv6 DHCP: Configuring DNS server
    2001:DB8:CAFE:AAAA::5
*Feb  3 02:39:10.454:   IPv6 DHCP: Configuring domain name
    example.com
*Feb  3 02:39:10.454: IPv6 DHCP: DHCPv6 changes state from
  INFORMATION-REQUEST to IDLE (REPLY_RECEIVED) on
  GigabitEthernet0/1
R3#
```

10.3.3 Servidor de DHCPv6 con estado

Configurar un servidor de DHCPv6 con estado es similar a configurar un servidor sin estado. La diferencia más importante es que un servidor con estado también incluye información de direccionamiento IPv6 de manera similar a un servidor DHCPv4.

Paso 1. Habilitar el routing IPv6

Como se muestra en la ilustración, se requiere el uso del comando `ipv6 unicast-routing` para habilitar el routing IPv6. Este comando no es necesario para que el router sea un servidor de DHCPv6 con estado, pero se requiere para enviar mensajes RA ICMPv6.

Paso 2. Configurar un pool de DHCPv6

El comando `ipv6 dhcp pool nombre-pool` crea un pool e ingresa el router en el modo de configuración DHCPv6, que se identifica por la petición de entrada Router (config-dhcpv6) #.

Paso 3. Configurar los parámetros del pool

Con DHCPv6 con estado, todos los parámetros de direccionamiento y otros parámetros de configuración deben ser asignados por el servidor de DHCPv6. El comando `address longitud/prefijo` se utiliza para indicar el conjunto de direcciones que debe asignar el servidor. La opción `lifetime` indica el tiempo de arrendamiento válido y preferido en segundos. Al igual que con DHCPv6 sin estado, el cliente utiliza la dirección IPv6 de origen del paquete que contenía el mensaje RA.

Otra información proporcionada por el servidor de DHCPv6 con estado suele incluir la dirección del servidor DNS y el nombre de dominio.

Paso 4. Comandos de interfaz

El comando de interfaz `ipv6 dhcp server nombre-pool` vincula el pool de DHCPv6 con la interfaz. El router responde a las solicitudes de DHCPv6 sin estado en esta interfaz con la información incluida en el pool. El indicador M debe cambiarse de 0 a 1 mediante el comando de interfaz `ipv6 nd managed-config-flag`. Esto le informa al dispositivo que no utilice SLAAC, sino que obtenga el direccionamiento IPv6 y todos los parámetros de configuración de un servidor de DHCPv6 con estado.

Ejemplo de servidor de DHCPv6 con estado

En la figura 2, se muestra un ejemplo de comandos de servidor de DHCPv6 con estado para un router configurado en el R1. Observe que no se especifica el gateway predeterminado, debido a que el router enviará automáticamente su propia dirección link-local como el gateway predeterminado. El router R3 está configurado como cliente para ayudar a verificar las operaciones de DHCPv6 con estado.

Configuración de un router DHCPv6 con estado

Paso 1: habilitar el routing IPv6

```
Router(config)# ipv6 unicast-routing
```

Paso 2: configurar un pool de DHCPv6

```
Router(config)# ipv6 dhcp pool pool-name
Router(config-dhcpv6) #
```

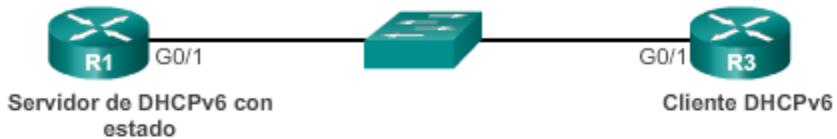
Paso 3: configurar los parámetros del pool

```
Router(config-dhcpv6) # address prefix/length [lifetime
                      valid-lifetime preferred-lifetime
                      | infinite]
Router(config-dhcpv6) # dns-server dns-server-address
Router(config-dhcpv6) # domain-name domain-name
```

Paso 4: configurar la interfaz DHCPv6

```
Router(config)# interface type number
Router(config-if) # ipv6 dhcp server pool-name
Router(config-if) # ipv6 nd managed-config-flag
```

Configuración del router R1 como servidor de DHCPv6 con estado

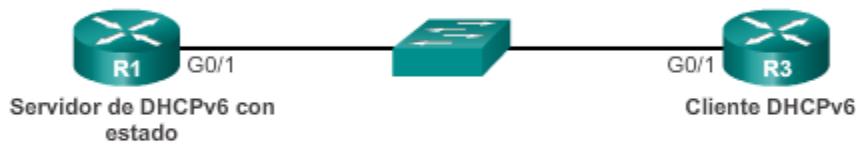


```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6) # address prefix 2001:DB8:CAFE:1::/64
                  lifetime infinite
R1(config-dhcpv6) # dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6) # domain-name example.com
R1(config-dhcpv6) # exit
R1(config)# interface g0/1
R1(config-if) # ipv6 address 2001:db8:cafe:1::1/64
R1(config-if) # ipv6 dhcp server IPV6-STATEFUL
R1(config-if) # ipv6 nd managed-config-flag
```

Como se muestra en la ilustración, utilice el comando del modo de configuración de interfaz `ipv6 enable` para permitir que el router reciba una dirección link-local para enviar mensajes RS y participe en DHCPv6.

El comando del modo de configuración de interfaz **ipv6 address dhcp** habilita al router para que funcione como cliente DHCPv6 en esta interfaz.

Configuración de un router como cliente DHCPv6 con estado



```
R3(config)# interface g0/1
R3(config-if)# ipv6 enable
R3(config-if)# ipv6 address dhcp
R3(config-if)#{
```

Verificación del servidor de DHCPv6 con estado

En la figura 1, el comando **show ipv6 dhcp pool** verifica el nombre del pool de DHCPv6 y sus parámetros. La cantidad de clientes activos es 1, lo que refleja que el R3 cliente recibe su dirección IPv6 de unidifusión global de este servidor.

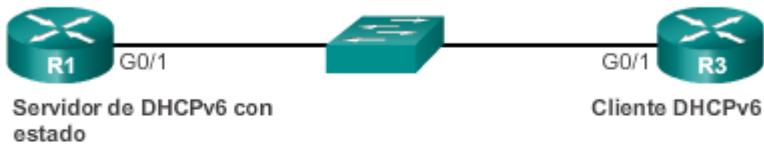
El comando **show ipv6 dhcp binding**, como se muestra en la figura 2, muestra la vinculación automática entre la dirección link-local del cliente y la dirección asignada por el servidor. FE80::32F7:DFF:FE25:2DE1 es la dirección link-local del cliente. En este ejemplo, esta es la interfaz G0/1 del R3. Esta dirección está vinculada a la dirección IPv6 de unidifusión global, 2001:DB8:CAFE:1:5844:47B2:2603:C171, la cual fue asignada por el R1, el servidor de DHCPv6. Esta información la mantiene un servidor de DHCPv6 con estado, y no un servidor de DHCPv6 sin estado.

Verificación del cliente DHCPv6 con estado

El resultado del comando **show ipv6 interface** que se muestra en la figura 3 verifica la dirección IPv6 de unidifusión global en el R3 cliente DHCPv6 que asignó el servidor de DHCPv6. La información de router predeterminado no proviene del servidor de DHCPv6, sino que se determinó mediante el uso de la dirección IPv6 de origen del mensaje RA. Si bien el cliente no utiliza la información contenida en el mensaje RA, puede utilizar la dirección IPv6 de origen para obtener la información del gateway predeterminado.

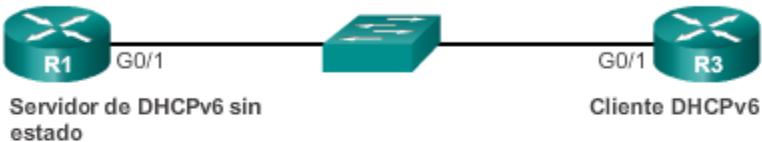
Utilice el verificador de sintaxis de la figura 4 para configurar y verificar DHCPv6 sin estado.

Verificación del servidor de DHCPv6 con estado: comando `show ipv6 dhcp pool`



```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
Address allocation prefix: 2001:DB8:CAFE:1::/64 valid
4294967295 preferred 4294967295 (1 in use, 0 conflicts)
DNS server: 2001:DB8:CAFE:AAAA::5
Domain name: example.com
Active clients: 1
R1#
```

Verificación del servidor de DHCPv6 con estado



```
R1# show ipv6 dhcp binding
Client: FE80::32F7:DFF:FE25:2DE1
DUID: 0003000130F70D252DE0
Username : unassigned
IA NA: IA ID 0x00040001, T1 43200, T2 69120
Address: 2001:DB8:CAFE:1:5844:47B2:2603:C171
preferred lifetime INFINITY, , valid lifetime
INFINITY,
R1#
```

**Verificación del cliente DHCPv6 con estado: comando
show ipv6 interface**

```
R3# show ipv6 interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is
    FE80::32F7:DFF:FE25:2DE1
    No Virtual link-local address(es):
    Global unicast address(es):
      2001:DB8:CAFE:1:5844:47B2:2603:C171, subnet is
      2001:DB8:CAFE:1:5844:47B2:2603:C171/128
    Joined group address(es):
      FF02::1
      FF02::1:FF03:C171
      FF02::1:FF25:2DE1
    MTU is 1500 bytes
    ICMP error messages limited to one every 100 milliseconds
    ICMP redirects are enabled
    ICMP unreachables are sent
    ND DAD is enabled, number of DAD attempts: 1
    ND reachable time is 30000 milliseconds (using 30000)
    ND NS retransmit interval is 1000 milliseconds
    Default router is FE80::D68C:B5FF:FECE:A0C1 on
      GigabitEthernet0/1
R3#
```

Si el servidor de DHCPv6 está ubicado en una red distinta de la del cliente, el router IPv6 puede configurarse como agente de retransmisión DHCPv6. La configuración de un agente de retransmisión DHCPv6 es similar a la configuración de un router IPv4 como retransmisor DHCPv4.

Nota: si bien la configuración de un agente de retransmisión DHCPv6 es similar a DHCPv4, los routers o los agentes de retransmisión IPv6 reenvían mensajes DHCPv6 de manera ligeramente distinta que los retransmisores DHCPv4. Los mensajes y el proceso exceden el ámbito de este currículo.

En la figura 1, se muestra una topología de ejemplo en la que un servidor de DHCPv6 se encuentra en la red 2001:DB8:CAFE:1::/64. El administrador de red desea utilizar este servidor de DHCPv6 como un servidor de DHCPv6 central con estado para asignar direcciones IPv6 a todos los clientes. Por lo tanto, los clientes en otras redes, como la PC1 en la red 2001:DB8:CAFE:A::/64, deben comunicarse con el servidor de DHCPv6.

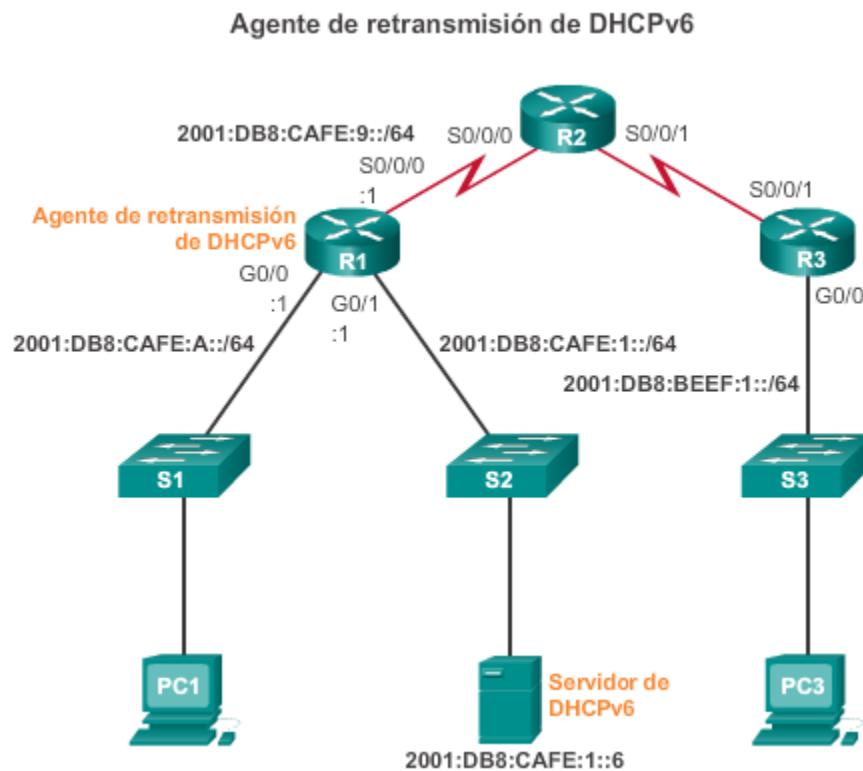
Los mensajes DHCPv6 de los clientes se envían a la dirección IPv6 de multidifusión FF02::1:2. Dirección de todos los agentes de retransmisión y servidores de DHCPv6: esta dirección tiene alcance link-local, lo que significa que los routers no reenvían estos mensajes. El router se debe configurar como agente de retransmisión DHCPv6 para habilitar al cliente y al servidor de DHCPv6 para que se comuniquen.

Configuración del agente de retransmisión DHCPv6

Como se muestra en la figura 2, un agente de retransmisión DHCPv6 se configura mediante el comando **ipv6 dhcp relay destination**. Este comando se configura en la interfaz que interactúa con el cliente DHCPv6, y se utiliza la dirección del servidor de DHCPv6 como destino.

El comando `show ipv6 dhcp interface` verifica que la interfaz G0/0 esté en modo de retransmisión con 2001:DB8:CAFE:1::6 configurado como el servidor de DHCPv6.

Mediante el verificador de sintaxis de la figura 3, configure los comandos de retransmisión de DHCPv6 en el router correcto de modo que la PC3 pueda recibir información de direccionamiento IPv6 del servidor de DHCPv6. Consulte la figura 1 para ver la topología de la red.



Comandos de agente de retransmisión de DHCPv6

```
R1(config)# interface g0/0
R1(config-if)# ipv6 dhcp relay destination 2001:db8:cafe:1::6
R1(config-if)# end
R1# show ipv6 dhcp interface g0/0
GigabitEthernet0/0 is in relay mode
  Relay destinations:
    2001:DB8:CAFE:1::6
R1#
```

10.3.4 Resolución de problemas de DHCPv6

El proceso de resolución de problemas de DHCPv6 es similar al de DHCPv4.

Tarea 1 de la resolución de problemas: resolver conflictos

De manera similar a lo que sucede con las direcciones IPv4, el arrendamiento de una dirección IPv6 puede caducar en un cliente que aún necesita conectarse a la red. El comando `show ipv6 dhcp conflicto` muestra todos los conflictos de direcciones que registra el servidor de DHCPv6 con estado. Si se detecta un conflicto de dirección IPv6, el cliente, por lo general, elimina la dirección y genera una nueva mediante SLAAC o mediante DHCPv6 con estado.

Tarea 2 de la resolución de problemas: verificar el método de asignación

El comando `show ipv6 interface interfaz` puede utilizarse para verificar el método de asignación de direcciones que aparece en el mensaje RA, según lo indica la configuración de los indicadores M y O. Esta información se muestra en las últimas líneas del resultado. Si un cliente no recibe la información de la dirección IPv6 de un servidor de DHCPv6 con estado, esto podría deberse a indicadores M y O incorrectos en el mensaje RA.

Tarea 3 de la resolución de problemas: probar con una dirección IPv6 estática

Al llevar a cabo la resolución de cualquier problema de DHCP, ya sea DHCPv4 o DHCPv6, se puede verificar la conectividad de red mediante la configuración de una dirección IP estática en una estación de trabajo cliente. En el caso de IPv6, si la estación de trabajo no puede llegar a los recursos de red con una dirección IPv6 configurada estáticamente, la causa raíz del problema no es SLAAC o DHCPv6. En este punto, es necesario resolver los problemas de conectividad de la red.

Tarea 4 de la resolución de problemas: verificar la configuración de puertos del switch

Si el cliente DHCPv6 no puede obtener información de un servidor de DHCPv6, verifique que el puerto de switch esté habilitado y funcione correctamente.

Nota: si hay un switch entre el cliente y el servidor de DHCPv6, y el cliente no puede obtener la configuración de DHCP, las causas pueden ser problemas con la configuración de puertos del switch. Estas causas pueden incluir problemas de enlaces troncales y canalización, STP y RSTP. Mediante la configuración de PortFast y las configuraciones de los puertos perimetrales se resuelven los problemas de cliente DHCPv6 más comunes que se presentan con la instalación inicial de un switch Cisco.

Tarea 5 de la resolución de problemas: probar el funcionamiento de DHCPv6 en la misma subred o VLAN

Si el servidor de DHCPv6 con estado o sin estado funciona correctamente pero se encuentra en una VLAN o red IPv6 distinta de la del cliente, es posible que el problema sea el agente de retransmisión DHCPv6. El cliente que interactúa con la interfaz en el router debe configurarse con el comando `ipv6 dhcp relay destination`.

Resolución de problemas de DHCPv6

Tarea 1 de la resolución de problemas:	Resolver conflictos de dirección.
Tarea 2 de la resolución de problemas:	Verificar el método de asignación.
Tarea 3 de la resolución de problemas:	Probar con una dirección IPv6 estática.
Tarea 4 de la resolución de problemas:	Verificar la configuración de puertos del switch.
Tarea 5 de la resolución de problemas:	Probar desde la misma subred o VLAN.

Las configuraciones del router para los servicios DHCPv6 con estado y sin estado tienen muchas similitudes, pero también incluyen diferencias significativas. En la figura 1, se muestran los comandos de configuración para los dos tipos de servicios DHCPv6.

DHCPv6 con estado

Los routers configurados para servicios DHCPv6 con estado tienen el comando **address prefix** para proporcionar información de direccionamiento.

Para servicios DHCPv6 con estado, se utiliza el comando del modo de configuración de interfaz **ipv6 nd managed-config-flag**. En este caso, el cliente omite la información de direccionamiento en el mensaje RA y se comunica con un servidor de DHCPv6 para obtener información de direccionamiento y otra información.

DHCPv6 sin estado

Para servicios DHCPv6 sin estado, se utiliza el comando del modo de configuración de interfaz **ipv6 nd other-config-flag**. Esto le informa al dispositivo que utilice SLAAC para la información de direccionamiento y un servidor de DHCPv6 sin estado para otros parámetros de configuración.

El comando **show ipv6 interface** puede utilizarse para ver la configuración actual para el método de asignación. Como se muestra en la figura 2, la última línea del resultado indica la forma en que los clientes obtienen direcciones y otros parámetros.

Servicios DHCPv6 con estado

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime
infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Servicios DHCPv6 sin estado

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Servicios DHCPv6 con estado

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:CAFE:1::/64 lifetime
infinite
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# ipv6 nd managed-config-flag
```

Servicios DHCPv6 sin estado

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:db8:cafe:aaaa::5
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:cafe:1::1/64
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# ipv6 nd other-config-flag
```

Cuando el router está configurado como servidor de DHCPv6 con estado o sin estado, el comando `debug ipv6 dhcp detail` es útil para verificar la recepción y la transmisión de

mensajes DHCPv6. Como se muestra en la ilustración, un router DHCPv6 con estado recibió un mensaje SOLICIT de un cliente. El router utiliza la información de direccionamiento en su pool IPV6-STATEFUL para la información de asignación.

Depuración de DHCPv6

```
R1# debug ipv6 dhcp detail
  IPv6 DHCP debugging is on (detailed)
R1#
*Feb  3 21:27:41.123: IPv6 DHCP: Received SOLICIT from
FE80::32F7:DFF:FE25:2DE1 on GigabitEthernet0/1
*Feb  3 21:27:41.123: IPv6 DHCP: detailed packet contents
*Feb  3 21:27:41.123:     src FE80::32F7:DFF:FE25:2DE1
(GigabitEthernet0/1)
*Feb  3 21:27:41.127:     dst FF02::1:2
*Feb  3 21:27:41.127:     type SOLICIT(1), xid 13190645
*Feb  3 21:27:41.127:     option ELAPSED-TIME(8), len 2
*Feb  3 21:27:41.127:         elapsed-time 0
*Feb  3 21:27:41.127:     option CLIENTID(1), len 10
*Feb  3 21:27:41.127:         000
*Feb  3 21:27:41.127: IPv6 DHCP: Using interface pool IPV6-
STATEFUL
*Feb  3 21:27:41.127: IPv6 DHCP: Creating binding for
FE80::32F7:DFF:FE25:2DE1 in pool IPV6-STATEFUL
<resultado omitido>
```

10.4 Resumen

Todos los nodos en una red requieren una dirección IP única que se comunique con otros dispositivos. La asignación estática de información de direccionamiento IP en una red grande produce una carga administrativa que puede eliminarse mediante el uso de DHCPv4 o DHCPv6 para asignar de forma dinámica información de direccionamiento IPv4 e IPv6, respectivamente.

DHCPv4 incluye tres mecanismos diferentes de asignación de direcciones para proporcionar flexibilidad al asignar las direcciones IP:

- **Asignación manual:** el administrador asigna una dirección IPv4 preasignada al cliente, y DHCPv4 comunica solo la dirección IPv4 al dispositivo.
- **Asignación automática:** DHCPv4 asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo y la selecciona de un conjunto de direcciones disponibles. No hay arrendamiento, y la dirección se asigna de forma permanente al dispositivo.
- **Asignación dinámica:** DHCPv4 asigna dinámicamente, o arrienda, una dirección IPv4 de un conjunto de direcciones durante un período limitado según lo configurado en el servidor o hasta que el cliente ya no necesite la dirección.

La asignación dinámica es el mecanismo DHCPv4 utilizado más comúnmente y comprende el intercambio de diversos paquetes entre el servidor de DHCPv4 y el cliente DHCPv4, lo que deriva en el arrendamiento de información de direccionamiento válida durante un período predefinido.

Los mensajes cuyo origen es el cliente (DHCPDISCOVER, DHCPREQUEST) son mensajes de difusión para permitir que todos los servidores de DHCPv4 en la red escuchen la solicitud de información de direccionamiento y la recepción de dicha información por parte del cliente. Los mensajes cuyo origen es el servidor de DHCPv4 (DHCPOFFER, DHCPACK) se envían como mensajes de unidifusión directamente al cliente que solicita la información.

Existen dos métodos disponibles para la configuración dinámica de las direcciones IPv6 de unidifusión global.

- Configuración automática de dirección sin estado (SLAAC)
- Protocolo de configuración dinámica de host para IPv6 (DHCPv6 con estado)

Con la configuración automática sin estado, el cliente utiliza información proporcionada por el mensaje RA IPv6 para seleccionar y configurar automáticamente una dirección IPv6 única. La opción de DHCPv6 sin estado informa al cliente que utilice la información del mensaje RA para el direccionamiento, pero que hay más parámetros de configuración disponibles de un servidor de DHCPv6.

DHCPv6 con estado es similar a DHCPv4. En este caso, el mensaje RA le informa al cliente que no utilice la información contenida en el mensaje RA. Toda la información de direccionamiento y de configuración se obtiene de un servidor de DHCPv6 con estado. El servidor de DHCPv6 mantiene la información de estado IPv6 de manera similar a la que un servidor de DHCPv4 asigna direcciones para IPv4.

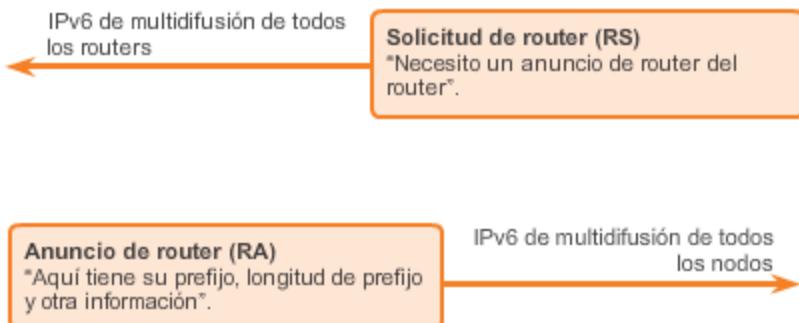
Si el servidor de DHCP está ubicado en un segmento de red distinto del segmento del cliente DHCP, se debe configurar un agente de retransmisión. El agente de retransmisión reenvía mensajes de difusión específicos que se originan en un segmento LAN a un servidor especificado ubicado en un segmento LAN distinto (en este caso, un mensaje de difusión DHCP se reenviaría a un servidor de DHCP).

La resolución de problemas con DHCPv4 y DHCPv6 incluye las mismas tareas:

- Resolver conflictos de dirección
- Verificar la conectividad física
- Probar la conectividad con una dirección IP estática
- Verificar la configuración de puertos del switch
- Probar el funcionamiento en la misma subred o VLAN



Configuración automática de dirección sin estado ICMPv6



11 Traducción de direcciones de red para IPv4 NAT.

11.1 Introducción

Todas las direcciones IPv4 públicas que se usan en Internet deben registrarse en un registro regional de Internet (RIR). Las organizaciones pueden arrendar direcciones públicas de un SP, pero solo el titular registrado de una dirección pública de Internet puede asignar esa dirección a un dispositivo de red. Sin embargo, con un máximo teórico de 4300 millones de direcciones, el espacio de direcciones IPv4 es muy limitado. Cuando Bob Kahn y Vint Cerf desarrollaron por primera vez la suite de protocolos TCP/IP que incluía IPv4 en 1981, nunca imaginaron en qué podría llegar a convertirse Internet. En aquel entonces, la computadora personal era, en la mayoría de los casos, una curiosidad para los aficionados, y todavía faltaba más de una década para la aparición de la World Wide Web.

Con la proliferación de los dispositivos informáticos personales y la llegada de la World Wide Web, pronto resultó evidente que las 4300 millones de direcciones IPv4 no serían suficientes. La solución a largo plazo era el protocolo IPv6, pero se necesitaban soluciones más inmediatas para abordar el agotamiento. A corto plazo, el IETF implementó varias soluciones, entre las que se incluía la traducción de direcciones de red (NAT) y las direcciones IPv4 privadas definidas en RFC 1918. En este capítulo, se analiza cómo se utiliza NAT combinada con el espacio de direcciones privadas para conservar y usar de forma más eficaz las direcciones IPv4, a fin de proporcionar acceso a Internet para las redes de todos los tamaños. En este capítulo, se abordan los siguientes temas:

- Las características, la terminología y las operaciones generales de NAT
- Los diferentes tipos de NAT, incluidas la NAT estática, la NAT dinámica y la NAT con sobrecarga
- Las ventajas y las desventajas de NAT
- La configuración, la verificación y el análisis de la NAT estática, la NAT dinámica y la NAT con sobrecarga
- La forma en que se puede usar el reenvío de puertos para acceder a los dispositivos internos desde Internet
- La resolución de problemas de NAT mediante los comandos `show` y `debug`
- La forma en que se utiliza NAT para IPv6 para traducir entre direcciones IPv6 y direcciones IPv4

Al finalizar este capítulo, podrá hacer lo siguiente:

- Describir las características de NAT.
- Describir las ventajas y las desventajas de NAT.
- Configurar la NAT estática mediante la CLI.
- Configurar la NAT dinámica mediante la CLI.
- Configurar PAT mediante la CLI.
- Configurar el reenvío de puertos mediante la CLI.
- Configurar NAT-PT (de v6 a v4).
- Usar los comandos show para verificar el funcionamiento de NAT.



NAT es un proceso que usan muchas pequeñas y medianas empresas para conservar las direcciones IPv4 y proporcionar privacidad y seguridad a los usuarios finales.

11.2 Funcionamiento de NAT

11.2.1 Características de NAT

No existen suficientes direcciones IPv4 públicas para asignar una dirección única a cada dispositivo conectado a Internet. Las redes suelen implementarse mediante el uso de direcciones IPv4 privadas, según se definen en RFC 1918. En la figura 1, se muestra el rango de direcciones incluidas en RFC 1918. Es muy probable que la computadora que utiliza para ver este curso tenga asignada una dirección privada.

Estas direcciones privadas se utilizan dentro de una organización o un sitio para permitir que los dispositivos se comuniquen localmente. Sin embargo, como estas direcciones no identifican empresas u organizaciones individuales, las direcciones privadas IPv4 no se pueden enrutar a través de Internet. Para permitir que un dispositivo con una dirección IPv4 privada acceda a recursos y dispositivos fuera de la red local, primero se debe traducir la dirección privada a una dirección pública.

Como se muestra en la figura 2, NAT proporciona la traducción de direcciones privadas a direcciones públicas. Esto permite que un dispositivo con una dirección IPv4 privada acceda a recursos fuera de su red privada, como los que se encuentran en Internet. La combinación de NAT con las direcciones IPv4 privadas resultó ser un método útil para preservar las direcciones IPv4 públicas. Se puede compartir una única dirección IPv4 pública entre cientos o incluso miles de dispositivos, cada uno configurado con una dirección IPv4 privada exclusiva.

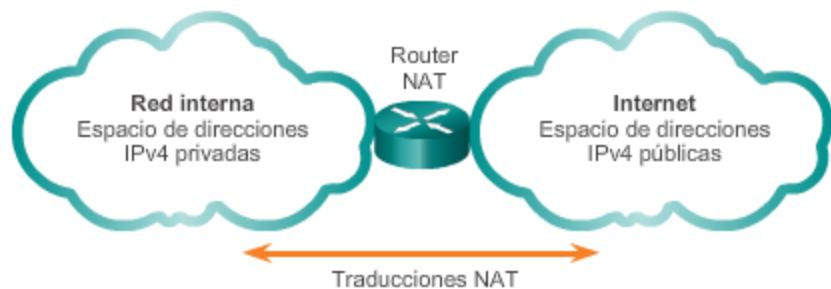
Sin NAT, el agotamiento del espacio de direcciones IPv4 habría ocurrido mucho antes del año 2000. Sin embargo, NAT presenta algunas limitaciones, las cuales se analizan más adelante en este capítulo. La solución al agotamiento del espacio de direcciones IPv4 y a las limitaciones de NAT es la transición final a IPv6.

Direcciones IPv4 privadas

Las direcciones privadas de Internet están definidas en RFC 1918:

Clase	Rango de direcciones internas RFC 1918	Prefijo CIDR
A	10.0.0.0 a 10.255.255.255	10.0.0.0/8
B	172.16.0.0 a 172.31.255.255	172.16.0.0/12
C	192.168.0.0 a 192.168.255.255	192.168.0.0/16

Traducción entre direcciones privadas y públicas



NAT tiene muchos usos, pero el principal es conservar las direcciones IPv4 públicas. Esto se logra al permitir que las redes utilicen direcciones IPv4 privadas internamente y al proporcionar la traducción a una dirección pública solo cuando sea necesario. NAT tiene el beneficio adicional de proporcionar cierto grado de privacidad y seguridad adicional a una red, ya que oculta las direcciones IPv4 internas de las redes externas.

Los routers con NAT habilitada se pueden configurar con una o más direcciones IPv4 públicas válidas. Estas direcciones públicas se conocen como "conjunto de NAT". Cuando un dispositivo interno envía tráfico fuera de la red, el router con NAT habilitada traduce la dirección IPv4 interna

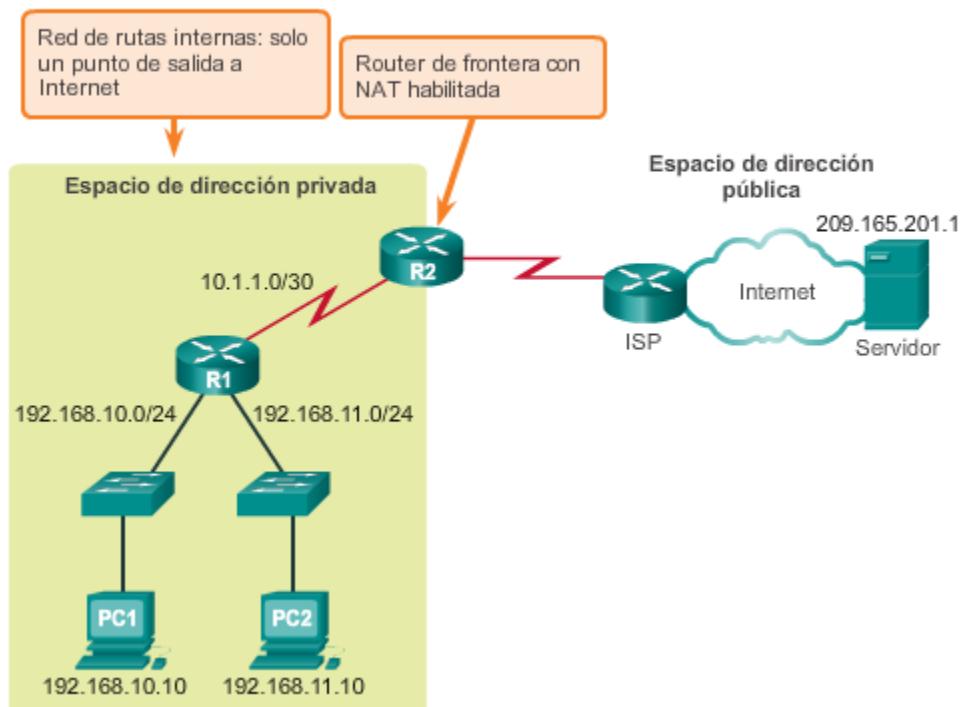
del dispositivo a una dirección pública del conjunto de NAT. Para los dispositivos externos, todo el tráfico entrante y saliente de la red parece tener una dirección IPv4 pública del conjunto de direcciones proporcionado.

En general, los routers NAT funcionan en la frontera de una red de rutas internas. Una red de rutas internas es aquella que tiene una única conexión a su red vecina, una entrada hacia la red y una salida desde ella. En el ejemplo de la ilustración, el R2 es un router de frontera. Visto desde el ISP, el R2 forma una red de rutas internas.

Cuando un dispositivo dentro de la red de rutas internas desea comunicarse con un dispositivo fuera de su red, el paquete se reenvía al router de frontera. El router de frontera realiza el proceso de NAT, es decir, traduce la dirección privada interna del dispositivo a una dirección pública, externa y enrutable.

Nota: la conexión al ISP también puede utilizar una dirección privada o pública compartida entre clientes. A los fines de este capítulo, se muestra una dirección pública.

Frontera de NAT



Según la terminología de NAT, la red interna es el conjunto de redes sujetas a traducción. La red externa se refiere a todas las otras redes.

Al utilizar NAT, las direcciones IPv4 se designan de distinto modo, según si están en la red privada o en la red pública (Internet), y si el tráfico es entrante o saliente.

NAT incluye cuatro tipos de direcciones:

- Dirección local interna

- Dirección global interna
- Dirección local externa
- Dirección global externa

Al determinar qué tipo de dirección se utiliza, es importante recordar que la terminología de NAT siempre se aplica desde la perspectiva del dispositivo con la dirección traducida:

- **Dirección interna:** la dirección del dispositivo que se traduce por medio de NAT.
- **Dirección externa:** la dirección del dispositivo de destino.

NAT también usa los conceptos de local o global con relación a las direcciones:

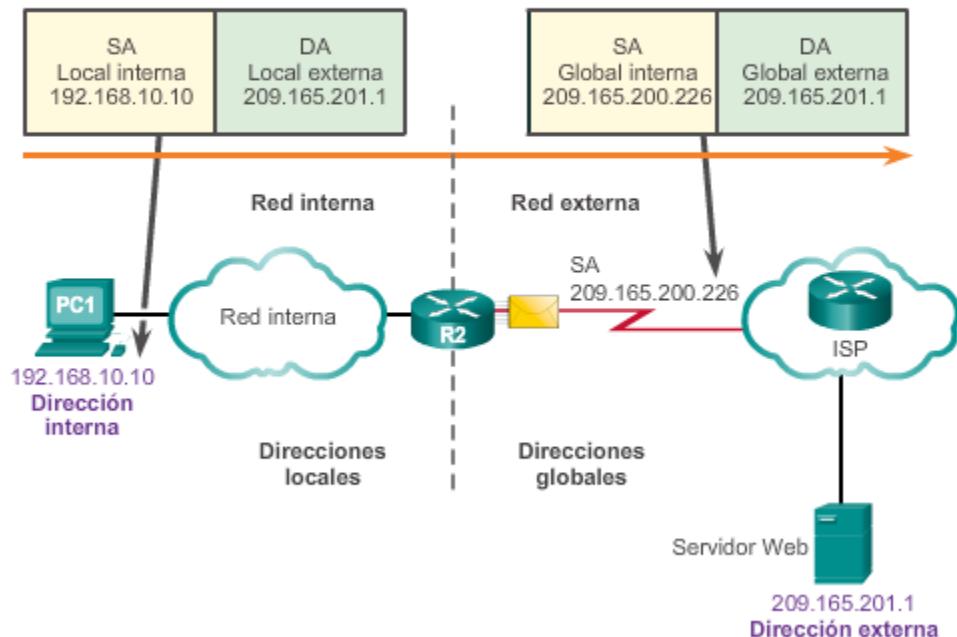
- **Dirección local:** cualquier dirección que aparece en la porción interna de la red.
- **Dirección global:** cualquier dirección que aparece en la porción externa de la red.

En la ilustración, la PC1 tiene la dirección local interna 192.168.10.10. Desde la perspectiva de la PC1, el servidor web tiene la dirección externa 209.165.201.1. Cuando se envían los paquetes de la PC1 a la dirección global del servidor web, la dirección local interna de la PC1 se traduce a 209.165.200.226 (dirección global interna). En general, la dirección del dispositivo externo no se traduce, ya que suele ser una dirección IPv4 pública.

Observe que la PC1 tiene distintas direcciones locales y globales, mientras que el servidor web tiene la misma dirección IPv4 pública en ambos casos. Desde la perspectiva del servidor web, el tráfico que se origina en la PC1 parece provenir de 209.165.200.226, la dirección global interna.

El router NAT, el R2 en la ilustración, es el punto de demarcación entre las redes internas y externas, así como entre las direcciones locales y globales.

Tipos de direcciones NAT



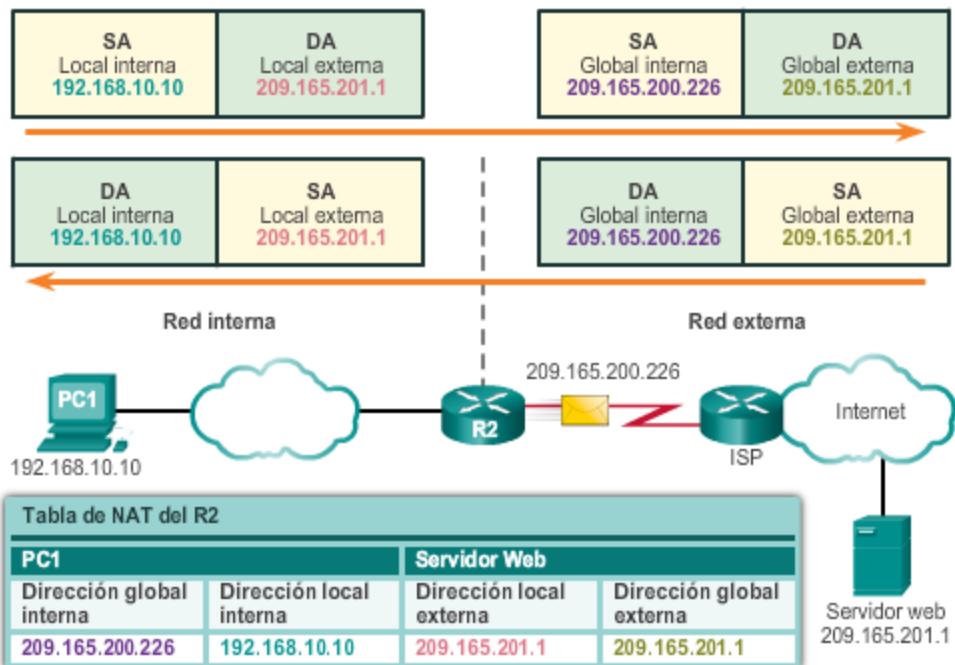
Los términos “interna” y “externa” se combinan con los términos “global” y “local” para hacer referencia a direcciones específicas. En la ilustración, el router R2 se configuró para proporcionar NAT. Este tiene un conjunto de direcciones públicas para asignar a los hosts internos.

- **Dirección local interna:** la dirección de origen vista desde el interior de la red. En la ilustración, la dirección IPv4 192.168.10.10 se asignó a la PC1. Esta es la dirección local interna de la PC1.
- **Dirección global interna:** la dirección de origen vista desde la red externa. En la ilustración, cuando se envía el tráfico de la PC1 al servidor web en 209.165.201.1, el R2 traduce la dirección local interna a una dirección global interna. En este caso, el R2 cambia la dirección IPv4 de origen de 192.168.10.10 a 209.165.200.226. De acuerdo con la terminología de NAT, la dirección local interna 192.168.10.10 se traduce a la dirección global interna 209.165.200.226.
- **Dirección global externa:** la dirección del destino vista desde la red externa. Es una dirección IPv4 enrutable globalmente y asignada a un host en Internet. Por ejemplo, se puede llegar al servidor web en la dirección IPv4 209.165.201.1. Por lo general, las direcciones externas globales y locales son iguales.
- **Dirección local externa:** la dirección del destino vista desde la red interna. En este ejemplo, la PC1 envía tráfico al servidor web en la dirección IPv4 209.165.201.1. Si bien es poco frecuente, esta dirección podría ser diferente de la dirección globalmente enrutable del destino.

En la ilustración, se muestra cómo se dirige el tráfico que se envía desde una computadora interna hacia un servidor web externo a través del router con NAT habilitada. También se muestra cómo se dirige y se traduce inicialmente el tráfico de retorno.

Nota: el uso de la dirección local externa excede el ámbito de este curso.

Ejemplos de direcciones NAT



En este ejemplo, la PC1 con la dirección privada 192.168.10.10 desea comunicarse con un servidor web externo con la dirección pública 209.165.201.1.

Haga clic en el botón Reproducir de la figura para iniciar la animación.

La PC1 envía un paquete dirigido al servidor web. El R1 reenvía el paquete al R2.

Cuando el paquete llega al R2, el router con NAT habilitada para la red, el R2 lee la dirección IPv4 de destino del paquete para determinar si este cumple con los criterios especificados para la traducción.

En este caso, la dirección IPv4 de origen cumple con los criterios y se traduce de 192.168.10.10 (dirección local interna) a 209.165.200.226 (dirección global interna). El R2 agrega esta asignación de dirección local a global a la tabla de NAT.

El R2 envía el paquete con la dirección de origen traducida hacia el destino.

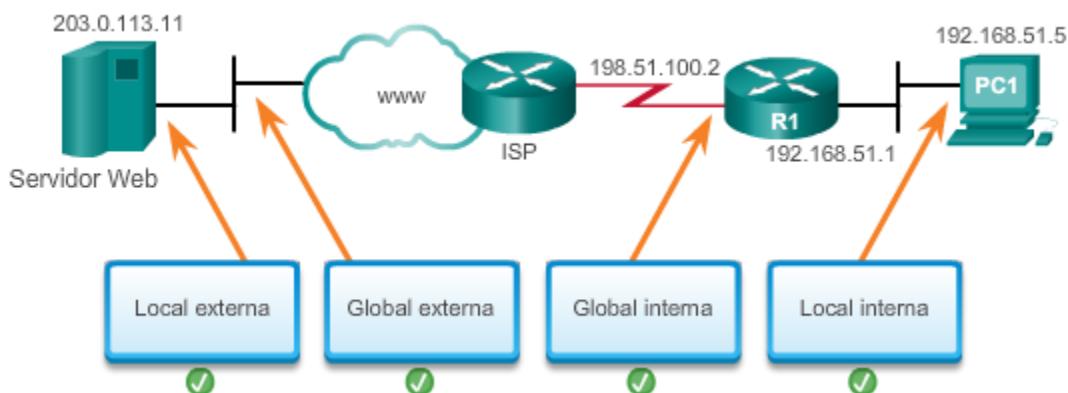
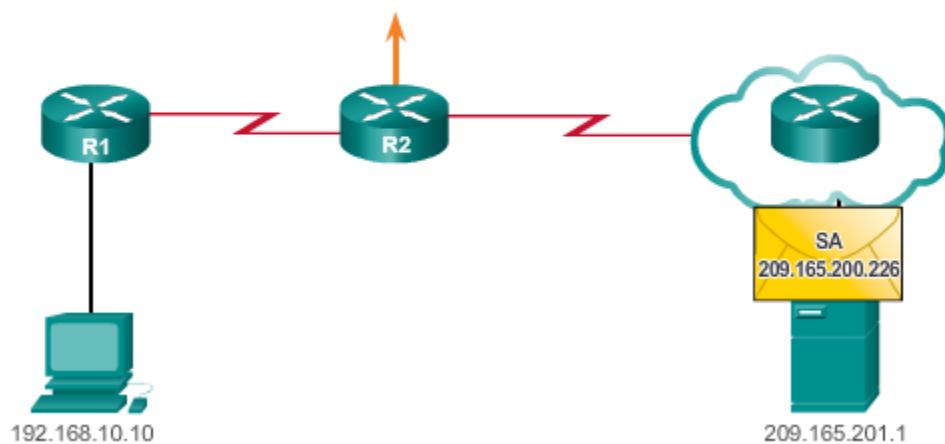
El servidor web responde con un paquete dirigido a la dirección global interna de la PC1 (209.165.200.226).

El R2 recibe el paquete con la dirección de destino 209.165.200.226. El R2 revisa la tabla de NAT y encuentra una entrada para esta asignación. El R2 usa esta información y traduce la dirección

global interna (209.165.200.226) a la dirección local interna (192.168.10.10), y el paquete se reenvía a la PC1.

NAT en acción

Tabla NAT			
Global interna	Local interna	Local externa	Global externa
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



11.2.2 Tipos de NAT

Existen tres tipos de traducción NAT:

- **Traducción estática de direcciones (NAT estática):** asignación de direcciones uno a uno entre una dirección local y una global.
- **Traducción dinámica de direcciones (NAT dinámica):** asignación de varias direcciones a varias direcciones entre direcciones locales y globales.
- **Traducción de la dirección del puerto (PAT):** asignación de varias direcciones a una dirección entre direcciones locales y globales. Este método también se conoce como "sobrecarga" (NAT con sobrecarga).

NAT estática

La NAT estática consiste en una asignación uno a uno entre direcciones locales y globales. Estas asignaciones son configuradas por el administrador de red y se mantienen constantes.

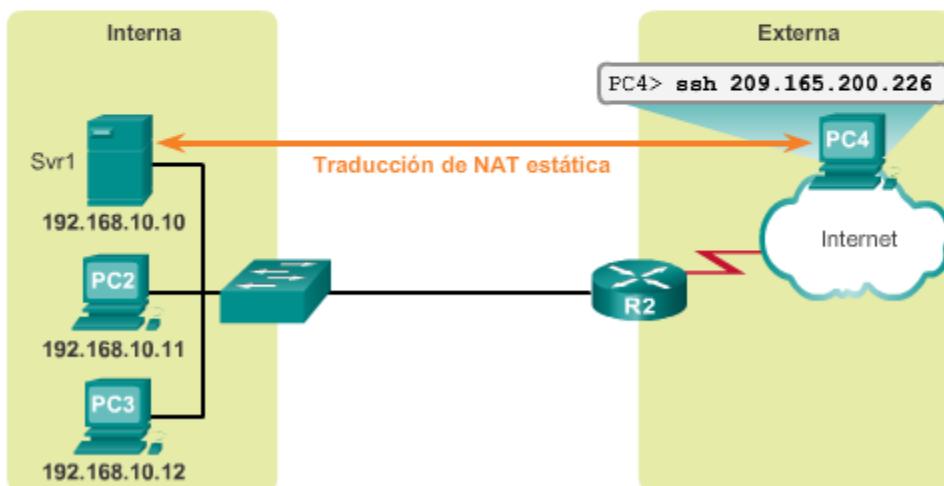
En la ilustración, el R2 se configuró con las asignaciones estáticas para las direcciones locales internas del Srv1, la PC2 y la PC3. Cuando estos dispositivos envían tráfico a Internet, sus direcciones locales internas se traducen a las direcciones globales internas configuradas. Para las redes externas, estos dispositivos tienen direcciones IPv4 públicas.

La NAT estática resulta útil, en especial para los servidores web o los dispositivos que deben tener una dirección constante que sea accesible tanto desde Internet, como desde el servidor web de una empresa. También es útil para los dispositivos a los que debe poder acceder el personal autorizado cuando no está en su lugar de trabajo, pero no el público en general en Internet. Por ejemplo, un administrador de red puede acceder a la dirección global interna del Srv1 (209.165.200.226) desde la PC4 mediante SSH. El R2 traduce esta dirección global interna a la dirección local interna y conecta la sesión del administrador al Srv1.

La NAT estática requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.

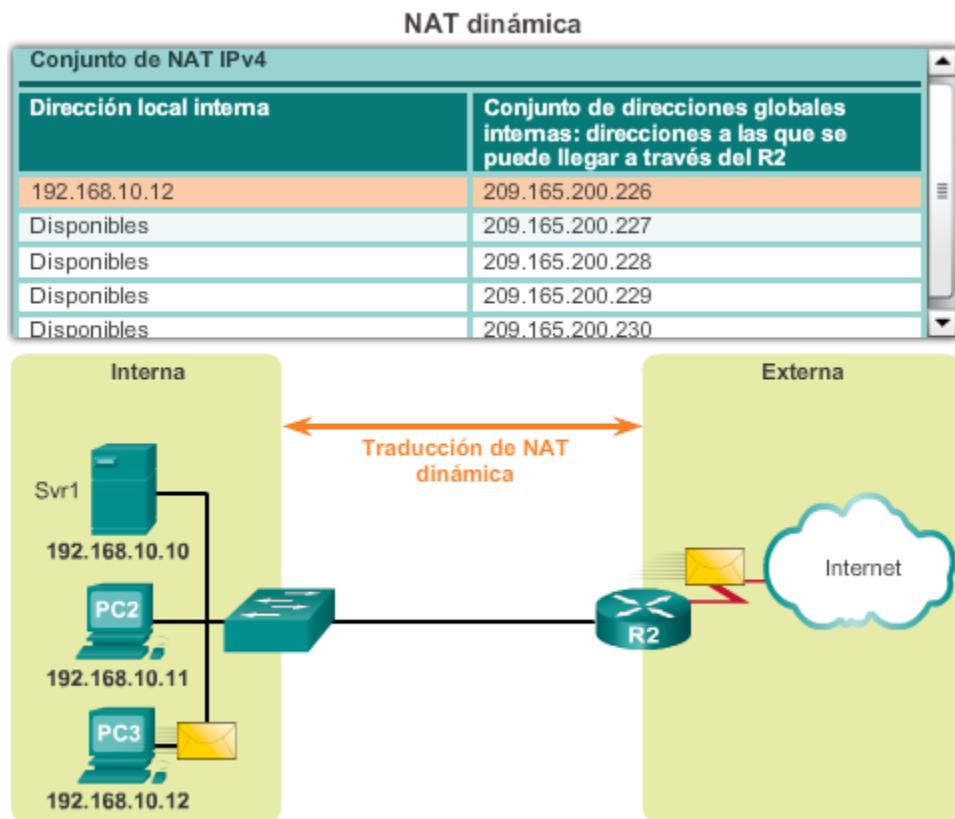
NAT estática

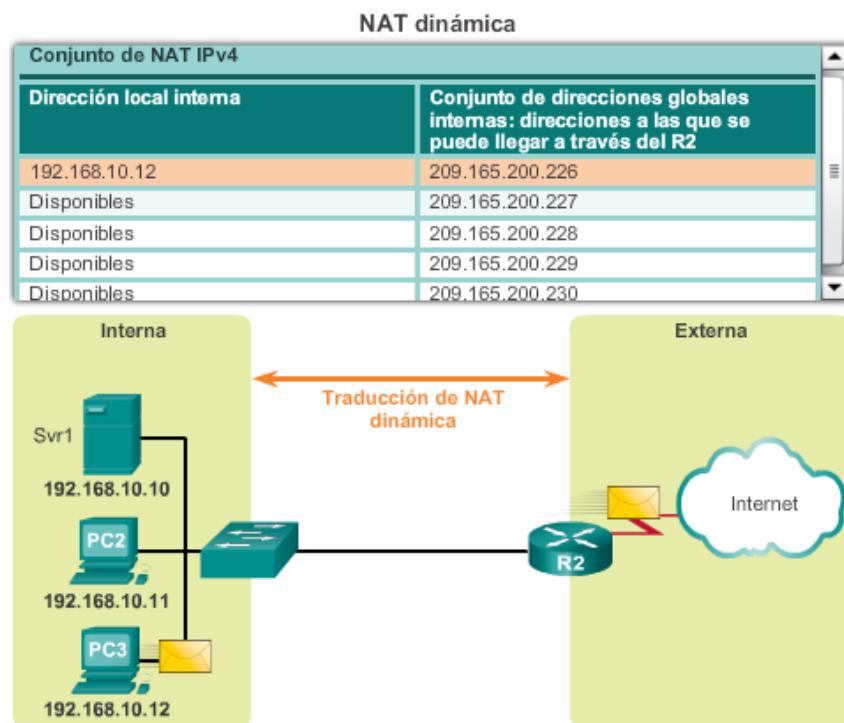
Tabla de NAT estática	
Dirección local interna	Dirección global interna: direcciones a las que se puede llegar a través del R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



La NAT dinámica utiliza un conjunto de direcciones públicas y las asigna según el orden de llegada. Cuando un dispositivo interno solicita acceso a una red externa, la NAT dinámica asigna una dirección IPv4 pública disponible del conjunto.

En la ilustración, la PC3 accede a Internet mediante la primera dirección disponible del conjunto de NAT dinámica. Las demás direcciones siguen disponibles para utilizarlas. Al igual que la NAT estática, la NAT dinámica requiere que haya suficientes direcciones públicas disponibles para satisfacer la cantidad total de sesiones de usuario simultáneas.





La traducción de la dirección del puerto (PAT), también conocida como “NAT con sobrecarga”, asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública o a algunas direcciones. Esto es lo que hace la mayoría de los routers domésticos. El ISP asigna una dirección al router, no obstante, varios miembros del hogar pueden acceder a Internet de manera simultánea. Esta es la forma más común de NAT.

Con PAT, se pueden asignar varias direcciones a una o más direcciones, debido a que cada dirección privada también se rastrea con un número de puerto. Cuando un dispositivo inicia una sesión TCP/IP, genera un valor de puerto de origen TCP o UDP para identificar la sesión de forma exclusiva. Cuando el router NAT recibe un paquete del cliente, utiliza su número de puerto de origen para identificar de forma exclusiva la traducción NAT específica.

PAT garantiza que los dispositivos usen un número de puerto TCP distinto para cada sesión con un servidor en Internet. Cuando llega una respuesta del servidor, el número de puerto de origen, que se convierte en el número de puerto de destino en la devolución, determina a qué dispositivo el router reenvía los paquetes. El proceso de PAT también valida que los paquetes entrantes se hayan solicitado, lo que añade un grado de seguridad a la sesión.

Haga clic en los botones Reproducir y Pausa de la ilustración para controlar la animación.

En la animación, se muestra el proceso de PAT. PAT agrega números de puerto de origen únicos a la dirección global interna para distinguir las traducciones.

A medida que el R2 procesa cada paquete, utiliza un número de puerto (1331 y 1555, en este ejemplo) para identificar el dispositivo en el que se originó el paquete. La dirección de origen (SA) es la dirección local interna a la que se agregó el número de puerto TCP/IP asignado. La dirección de destino (DA) es la dirección local externa a la que se agregó el número de puerto de servicio. En este ejemplo, el puerto de servicio es 80: HTTP.

Para la dirección de origen, el R2 traduce la dirección local interna a una dirección global interna con el número de puerto agregado. La dirección de destino no se modifica, pero ahora se la denomina "dirección IP global externa". Cuando el servidor web responde, se invierte la ruta.

Proceso PAT

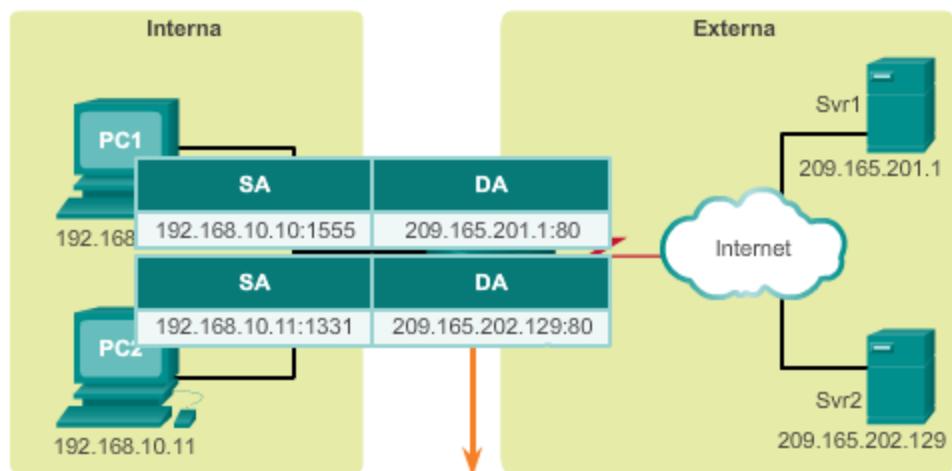


Tabla NAT con sobrecarga

Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Proceso PAT

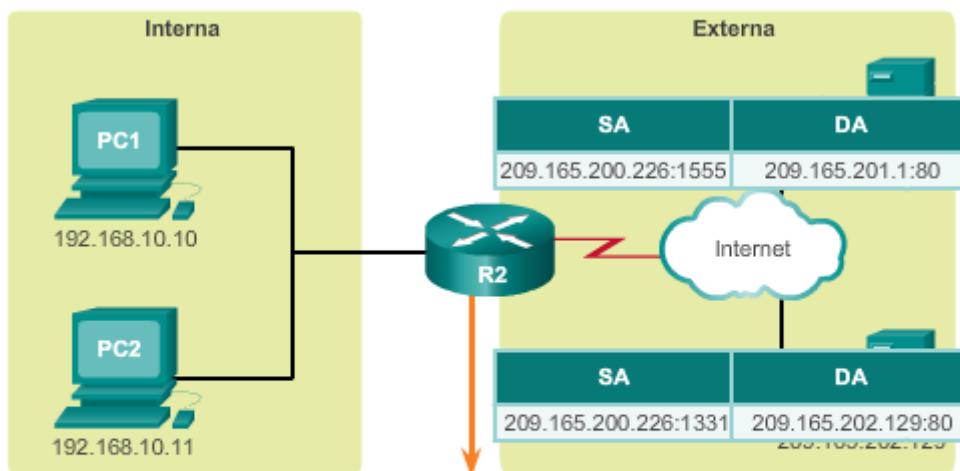


Tabla NAT con sobrecarga

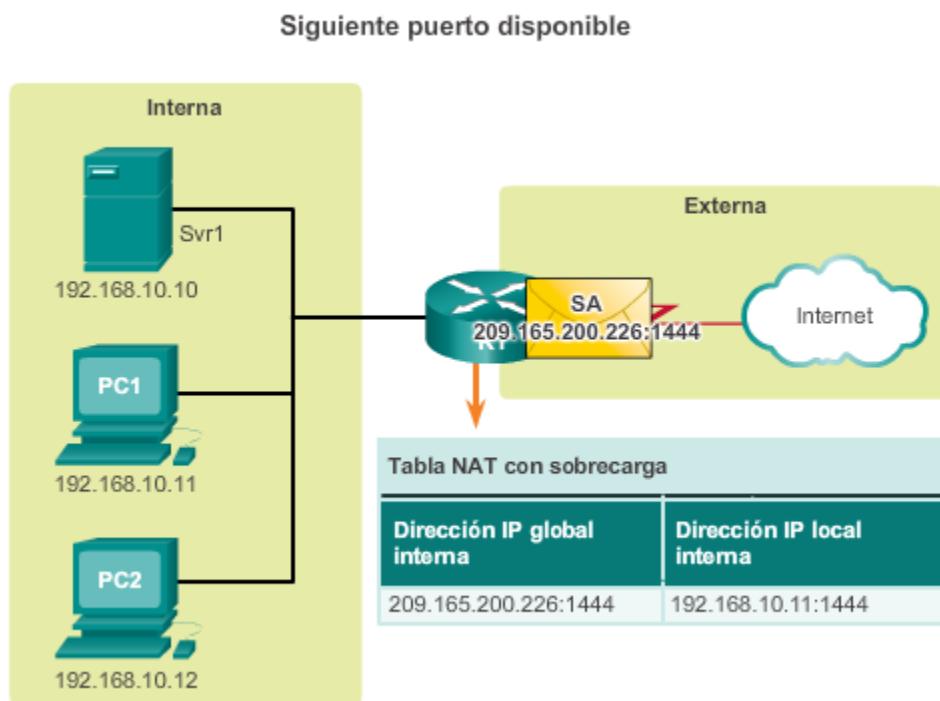
Dirección IP global interna	Dirección IP local interna	Dirección IP local externa	Dirección IP global externa
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

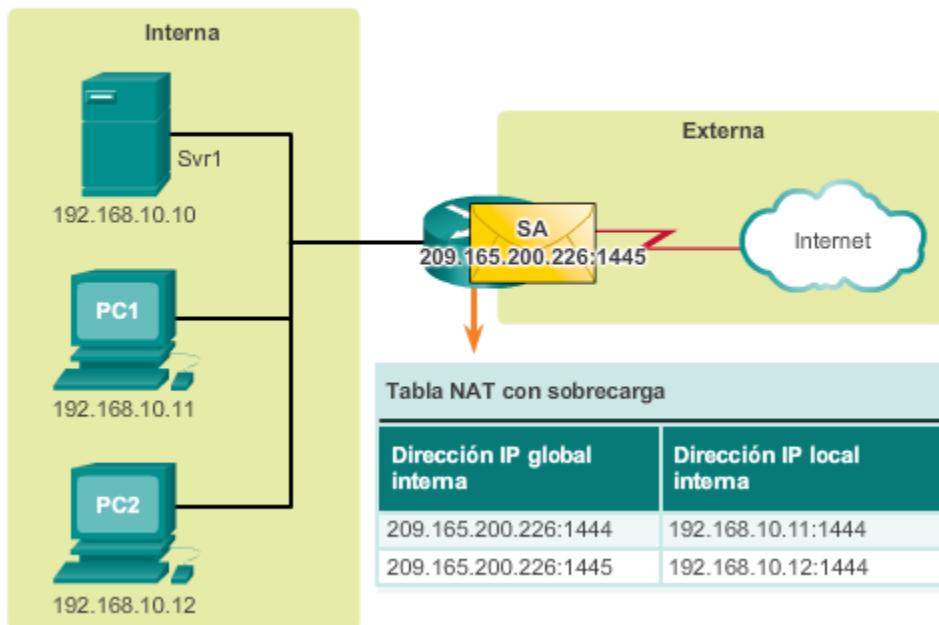
En el ejemplo anterior, los números de puerto del cliente, 1331 y 1555, no se modificaron en el router con NAT habilitada. Esta no es una situación muy probable, porque existe una gran posibilidad de que estos números de puerto ya se hayan conectado a otras sesiones activas.

PAT intenta conservar el puerto de origen inicial. Sin embargo, si el puerto de origen inicial ya está en uso, PAT asigna el primer número de puerto disponible desde el comienzo del grupo de puertos correspondiente de 0 a 511, 512 a 1023 o 1024 a 65 535. Cuando no hay más puertos disponibles y hay más de una dirección externa en el conjunto de direcciones, PAT avanza a la siguiente dirección para intentar asignar el puerto de origen inicial. Este proceso continúa hasta que no haya más direcciones IP externas o puertos disponibles.

Haga clic en el botón Reproducir de la ilustración para ver el funcionamiento de PAT.

En la animación, los hosts eligieron el mismo número de puerto 1444. Esto resulta aceptable para la dirección interna, porque los hosts tienen direcciones IP privadas únicas. Sin embargo, en el router NAT, se deben cambiar los números de puerto; de lo contrario, los paquetes de dos hosts distintos saldrían del R2 con la misma dirección de origen. En este ejemplo, PAT asignó el siguiente puerto disponible (1445) a la segunda dirección host.



Siguiente puerto disponible

Hacer un resumen de las diferencias entre NAT y PAT contribuye a la comprensión de ambas.

Como se muestran en la ilustración, NAT traduce direcciones IPv4 en una relación de 1:1 entre direcciones IPv4 privadas y direcciones IPv4 públicas. Sin embargo, PAT modifica la dirección y el número de puerto.

NAT reenvía los paquetes entrantes a su destino interno mediante la dirección IPv4 de origen de entrada proporcionada por el host en la red pública. En general, con PAT hay solo una o muy pocas direcciones IPv4 públicamente expuestas. Los paquetes entrantes de la red pública se enrutan a sus destinos en la red privada consultando una tabla en el router NAT. Esta tabla hace un seguimiento de los pares de puertos públicos y privados. Esto se denomina “seguimiento de conexiones”.

Paquetes sin segmento de capa 4

¿Qué sucede con los paquetes IPv4 que transportan datos que no son segmentos TCP o UDP? Estos paquetes no contienen un número de puerto de capa 4. PAT traduce la mayoría de los protocolos comunes transmitidos mediante IPv4 que no utilizan TCP o UDP como protocolo de la capa de transporte. El más común de ellos es ICMPv4. PAT maneja cada uno de estos tipos de protocolos de manera diferente. Por ejemplo, los mensajes de consulta, las solicitudes de eco y las respuestas de eco de ICMPv4 incluyen una ID de consulta. ICMPv4 utiliza la ID de consulta para identificar una solicitud de eco con su respectiva respuesta. La ID de consulta aumenta con cada solicitud de eco enviada. PAT utiliza la ID de consulta en lugar de un número de puerto de capa 4.

Nota: otros mensajes ICMPv4 no utilizan la ID de consulta. Estos mensajes y otros protocolos que no utilizan los números de puerto TCP o UDP varían y exceden el ámbito de este currículo.

Comparación entre NAT y PAT

NAT	
Conjunto de direcciones globales internas	Dirección local interna
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT	
Dirección global interna	Dirección local interna
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

11.2.3 Beneficios de NAT

NAT ofrece varios beneficios, incluidos los siguientes:

- NAT conserva el esquema de direccionamiento legalmente registrado al permitir la privatización de las intranets. NAT conserva las direcciones mediante la multiplexación de aplicaciones en el nivel de puerto. Con la NAT con sobrecarga, los hosts internos pueden compartir una única dirección IPv4 pública para todas las comunicaciones externas. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir varios hosts internos.
- NAT aumenta la flexibilidad de las conexiones a la red pública. Se pueden implementar varios conjuntos y conjuntos de respaldo y de equilibrio de carga para asegurar conexiones de red pública confiables.
- NAT proporciona coherencia a los esquemas de direccionamiento de red interna. Para cambiar el esquema de direcciones IPv4 públicas en una red que no utiliza direcciones IPv4 privadas ni NAT, se requiere redireccionar todos los hosts en la red existente. Los costos de redireccionamiento de hosts pueden ser considerables. NAT permite mantener el esquema de direcciones IPv4 privadas existente a la vez que facilita el cambio a un nuevo esquema de direccionamiento público. Esto significa que una organización podría cambiar los ISP sin necesidad de modificar ninguno de sus clientes internos.
- NAT proporciona seguridad de red. Debido a que las redes privadas no anuncian sus direcciones ni su topología interna, son razonablemente seguras cuando se utilizan en conjunto con NAT para obtener acceso externo controlado. Sin embargo, NAT no reemplaza a los firewalls.

Ventajas de la NAT

- Conserva el esquema de direccionamiento legalmente registrado.
- Aumenta la flexibilidad de las conexiones a la red pública.
- Proporciona coherencia a los esquemas de direccionamiento de red interna.
- Proporciona seguridad de red.

NAT presenta algunas desventajas. El hecho de que los hosts en Internet parezcan comunicarse de forma directa con el dispositivo con NAT habilitada, en lugar de hacerlo con el host real dentro de la red privada, genera una serie de inconvenientes.

Una desventaja del uso de NAT se relaciona con el rendimiento de la red, en especial, en el caso de los protocolos en tiempo real como VoIP. NAT aumenta los retrasos de switching porque la traducción de cada dirección IPv4 dentro de los encabezados del paquete lleva tiempo. Al primer paquete se aplica el switching de procesos; esto siempre se realiza por la ruta más lenta. El router debe revisar todos los paquetes para decidir si necesitan traducción. El router debe modificar el encabezado de IPv4 y, posiblemente, el encabezado TCP o UDP. El checksum del encabezado de IPv4, junto con el checksum de TCP o UDP, se debe volver a calcular cada vez que se realiza una traducción. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido; de lo contrario, también se demoran.

Otra desventaja del uso de NAT es que se pierde el direccionamiento de extremo a extremo. Muchos protocolos y aplicaciones de Internet dependen del direccionamiento de extremo a extremo desde el origen hasta el destino. Algunas aplicaciones no funcionan con NAT. Por ejemplo, algunas aplicaciones de seguridad, como las firmas digitales, fallan porque la dirección IPv4 de origen cambia antes de llegar a destino. Las aplicaciones que utilizan direcciones físicas, en lugar de un nombre de dominio calificado, no llegan a los destinos que se traducen a través del router NAT. En ocasiones, este problema se puede evitar al implementar las asignaciones de NAT estática.

También se reduce el seguimiento IPv4 de extremo a extremo. El seguimiento de los paquetes que pasan por varios cambios de dirección a través de varios saltos de NAT se torna mucho más difícil y, en consecuencia, dificulta la resolución de problemas.

El uso de NAT también genera complicaciones para los protocolos de tunneling como IPsec, ya que NAT modifica los valores en los encabezados que interfieren en las verificaciones de integridad que realizan IPsec y otros protocolos de tunneling.

Los servicios que requieren que se inicie una conexión TCP desde la red externa, o “protocolos sin estado”, como los servicios que utilizan UDP, pueden interrumpirse. A menos que el router NAT esté configurado para admitir dichos protocolos, los paquetes entrantes no pueden llegar a su destino. Algunos protocolos pueden admitir una instancia de NAT entre los hosts participantes (por ejemplo, FTP de modo pasivo), pero fallan cuando NAT separa a ambos sistemas de Internet.

Desventajas de la NAT

- Se deteriora el rendimiento.
- Se deteriora la funcionalidad de extremo a extremo.
- Se reduce el seguimiento IP de extremo a extremo.
- El tunneling se torna más complicado.
- El inicio de las conexiones TCP puede interrumpirse.

11.3 Configuración de NAT estática

La NAT estática es una asignación uno a uno entre una dirección interna y una dirección externa. La NAT estática permite que los dispositivos externos inicien conexiones a los dispositivos internos mediante la dirección pública asignada de forma estática. Por ejemplo, se puede asignar una dirección global interna específica a un servidor web interno de modo que se pueda acceder a este desde redes externas.

En la figura 1, se muestra una red interna que contiene un servidor web con una dirección IPv4 privada. El router R2 se configuró con NAT estática para permitir que los dispositivos en la red externa (Internet) accedan al servidor web. El cliente en la red externa accede al servidor web mediante una dirección IPv4 pública. La NAT estática traduce la dirección IPv4 pública a la dirección IPv4 privada.

Existen dos pasos básicos para configurar las traducciones NAT estáticas.

Paso 1. El primer paso consiste en crear una asignación entre la dirección local interna y las direcciones globales internas. Por ejemplo, en la figura 1, la dirección local interna 192.168.10.254 y la dirección global interna 209.165.201.5 se configuraron como traducción NAT estática.

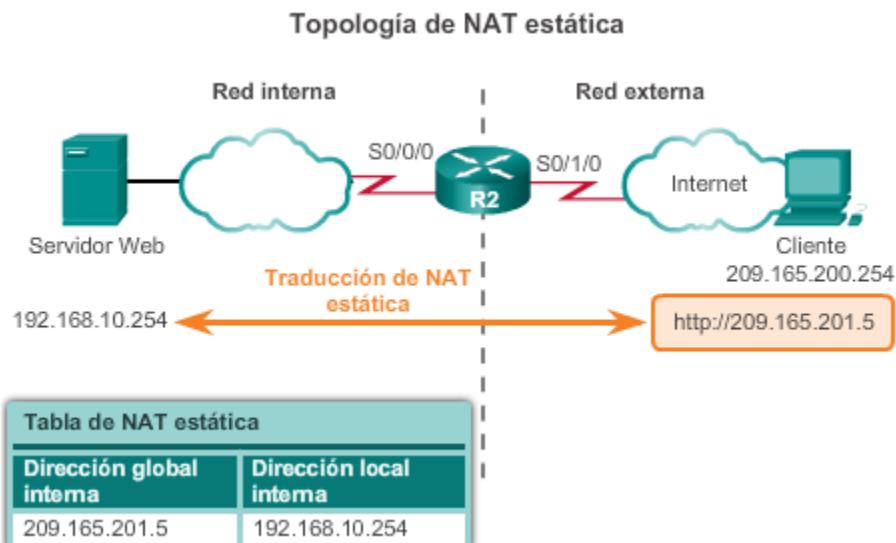
Paso 2. Una vez configurada la asignación, las interfaces que participan en la traducción se configuran como interna o externa con respecto a NAT. En el ejemplo, la interfaz Serial 0/0/0 del R2 es una interfaz interna, y la interfaz Serial 0/1/0 es una interfaz externa.

Los paquetes que llegan hasta la interfaz interna del R2 (Serial 0/0/0) desde la dirección IPv4 local interna configurada (192.168.10.254) se traducen y, luego, se reenvían hacia la red externa. Los paquetes que llegan a la interfaz externa del R2 (Serial 0/1/0), que están dirigidos a la dirección IPv4 global interna configurada (209.165.201.5), se traducen a la dirección local interna (192.168.10.254) y, luego, se reenvían a la red interna.

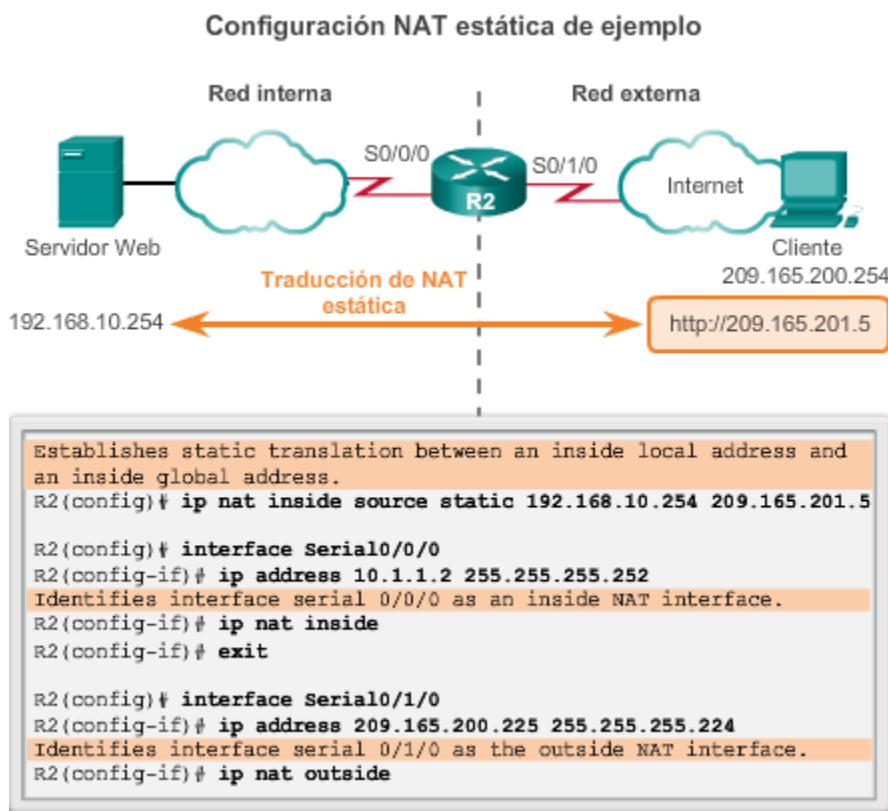
En la figura 2, se describen los comandos necesarios para configurar la NAT estática.

En la figura 3, se muestran los comandos necesarios en el R2 para crear una asignación de NAT estática al servidor web en la topología de ejemplo. Con la configuración que se muestra, el R2 traduce los paquetes del servidor web con la dirección 192.168.10.254 a la dirección IPv4 pública 209.165.201.5. El cliente de Internet dirige solicitudes web a la dirección IPv4 pública 209.165.201.5. El R2 reenvía ese tráfico al servidor web en 192.168.10.254.

Utilice el verificador de sintaxis de la figura 4 para configurar una entrada de NAT estática adicional en el R2.

**Configuración de NAT estática**

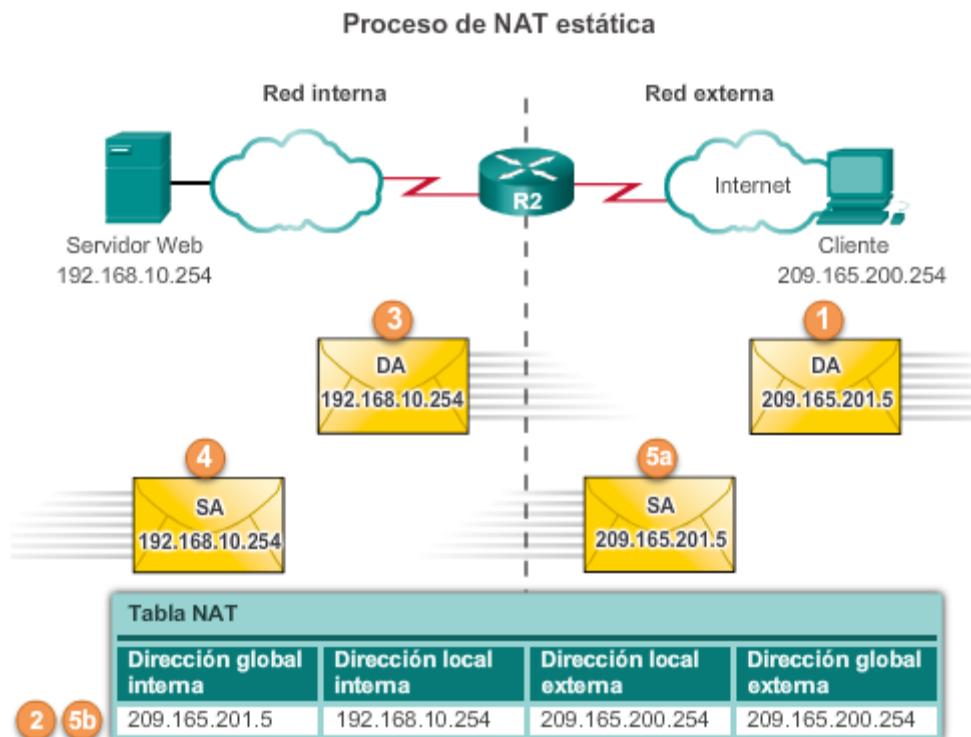
Revi se	Acción	Notas
1	Se establece la traducción estática entre una dirección local interna y una dirección global interna. Router (config)# ip nat inside source static ip-local ip-global	Introduzca el comando no ip nat inside source static del modo de configuración global para eliminar la traducción dinámica de origen.
2	Especificar la interfaz interna. Router (config)# interface tipo número	Introduzca el comando interface . La petición de entrada de la CLI cambia de (config)# a (config-if)#.
3	Marque la interfaz como conectada al interior. Router (config-if)# ip nat inside	
4	Salga del modo de configuración de interfaz. Router (config-if)# exit	
5	Especificar la interfaz externa. Router (config)# interface tipo número	
6	Marque la interfaz como conectada al exterior. Router (config-if)# ip nat outside	



Con la configuración anterior, en la ilustración se muestra el proceso de traducción de NAT estática entre el cliente y el servidor web. En general, las traducciones estáticas se utilizan cuando los clientes en la red externa (Internet) necesitan llegar a los servidores en la red interna.

- El cliente desea establecer una conexión al servidor web. El cliente envía un paquete al servidor web con la dirección IPv4 pública de destino 209.165.201.5. Esta es la dirección global interna del servidor web.
- El primer paquete que recibe del cliente en su interfaz NAT externa ocasiona que el R2 revise su tabla de NAT. Una vez que se encuentra la dirección IPv4 de destino en la tabla de NAT, se traduce.
- El R2 reemplaza la dirección global interna 209.165.201.5 por la dirección local interna 192.168.10.254. Luego, el R2 reenvía el paquete hacia el servidor web.
- El servidor web recibe el paquete y responde al cliente con la dirección local interna, 192.168.10.254.
- a. El R2 recibe el paquete del servidor web en su interfaz NAT interna con la dirección de origen de la dirección local interna del servidor web, 192.168.10.254.
- b. El R2 busca una traducción para la dirección local interna en la tabla de NAT. La dirección se encuentra en esa tabla. El R2 traduce la dirección de origen a la dirección global interna 209.165.201.5 y reenvía el paquete por su interfaz serial 0/1/0 hacia el cliente.

6. El cliente recibe el paquete y continúa la conversación. El router NAT lleva a cabo los pasos 2 a 5b para cada paquete. (El paso 6 no aparece en la ilustración).



El comando `show ip nat translations` es útil para verificar el funcionamiento de NAT. Este comando muestra las traducciones NAT activas. A diferencia de las traducciones dinámicas, las traducciones estáticas siempre figuran en la tabla de NAT. En la figura 1, se muestra el resultado de este comando con el ejemplo de configuración anterior. Debido a que el ejemplo es una configuración NAT estática, siempre figura una traducción en la tabla de NAT, independientemente de que haya comunicaciones activas. Si se emite el comando durante una sesión activa, el resultado también indica la dirección del dispositivo externo, como se muestra en la figura 1.

Otro comando útil es `show ip nat statistics`. Como se muestra en la figura 2, el comando `show ip nat statistics` muestra información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

Para verificar que la traducción NAT funcione, es conveniente borrar las estadísticas de todas las traducciones anteriores con el comando `clear ip nat statistics` antes de realizar la prueba.

Antes de cualquier comunicación con el servidor web, el comando `show ip nat statistics` no muestra ningún acierto actual. Una vez que el cliente establece una sesión con el servidor web, el comando `show ip nat statistics` muestra cinco aciertos. De este modo, se verifica que se lleva a cabo la traducción de NAT estática en el R2.

Verificación de las traducciones de NAT estática

La traducción estática siempre está presente en la tabla de NAT.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local   outside global
--- 209.165.201.5  192.168.10.254  ---           ---
```

La traducción estática durante una sesión activa.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local   Outside global
--- 209.165.201.5  192.168.10.254  209.165.200.254  209.165.200.254
R2#
```

Verificación de las estadísticas de NAT estática

```
R2# clear ip nat statistics
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0 Misses: 0
<resultado omitido>
Client PC establishes a session with the web server
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5 Misses: 0
<resultado omitido>
```

11.3.1 Configuración de NAT dinámica

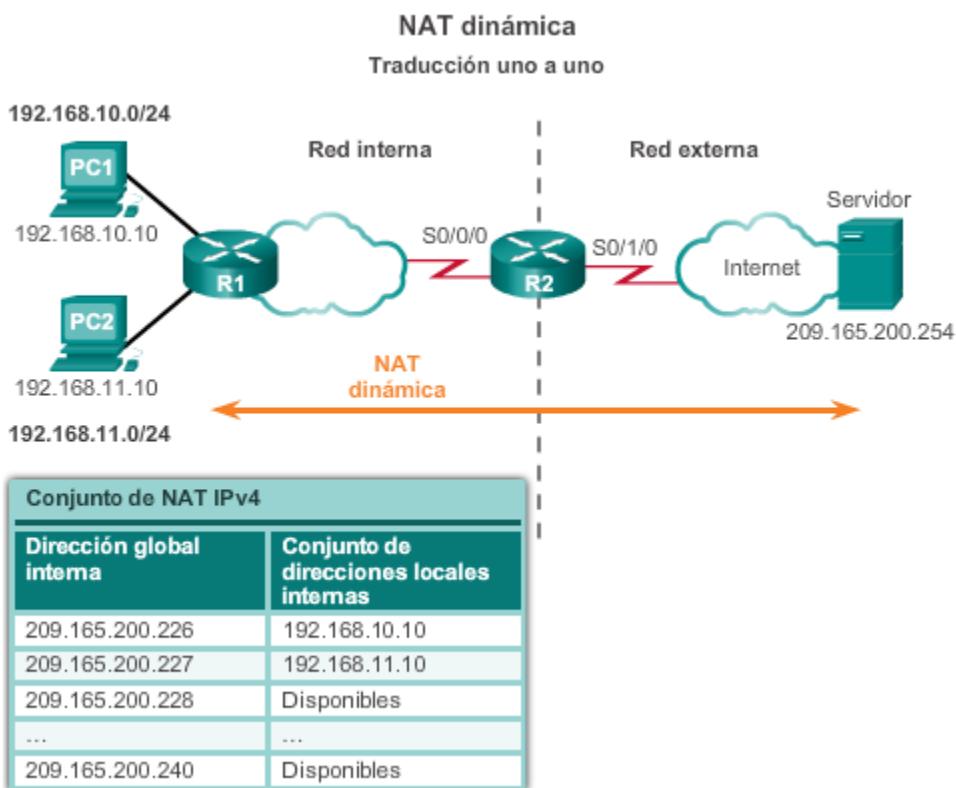
Mientras que la NAT estática proporciona una asignación permanente entre una dirección local interna y una dirección global interna, la NAT dinámica permite la asignación automática de direcciones locales internas a direcciones globales internas. Por lo general, estas direcciones globales internas son direcciones IPv4 públicas. La NAT dinámica utiliza un grupo o un conjunto de direcciones IPv4 públicas para la traducción.

Al igual que la NAT estática, la NAT dinámica requiere que se configuren las interfaces interna y externa que participan en la NAT. Sin embargo, mientras que la NAT estática crea una asignación permanente a una única dirección, la NAT dinámica utiliza un conjunto de direcciones.

Nota: la traducción entre direcciones IPv4 públicas y privadas es el uso más frecuente de NAT. No obstante, las traducciones de NAT se pueden realizar entre cualquier par de direcciones.

La topología de ejemplo que se muestra en la ilustración tiene una red interna que usa direcciones del espacio de direcciones privadas definido en RFC 1918. Hay dos LAN conectadas al router R1: 192.168.10.0/24 y 192.168.11.0/24. El router R2, es decir, el router de frontera, se configuró para NAT dinámica con un conjunto de direcciones IPv4 públicas de 209.165.200.226 a 209.165.200.240.

El conjunto de direcciones IPv4 públicas (conjunto de direcciones globales internas) se encuentra disponible para cualquier dispositivo en la red interna según el orden de llegada. Con la NAT dinámica, una única dirección interna se traduce a una única dirección externa. Con este tipo de traducción, debe haber suficientes direcciones en el conjunto para admitir a todos los dispositivos internos que necesiten acceso a la red externa al mismo tiempo. Si se utilizaron todas las direcciones del conjunto, los dispositivos deben esperar que haya una dirección disponible para poder acceder a la red externa.



En la figura 1, se muestran los pasos y los comandos utilizados para configurar la NAT dinámica.

Paso 1. Defina el conjunto de direcciones que se utilizará para la traducción con el comando `ip nat pool`. Por lo general, este conjunto es un grupo de direcciones públicas. Las direcciones se definen indicando la primera y la última dirección IP del conjunto. Las palabras `clavenetmask` o `prefix-length` indican qué bits de la dirección pertenecen a la red y cuáles al host en el rango de direcciones.

Paso 2. Configure una ACL estándar para identificar (permitir) solo aquellas direcciones que se deben traducir. Una ACL demasiado permisiva puede generar resultados impredecibles. Recuerde que al final de cada ACL hay una instrucción implícita para **denegar todo**.

Paso 3. Conecte la ACL al conjunto. Para conectar la ACL al conjunto, se utiliza el comando `ip nat inside source list número-lista-acceso number pool nombre-conjunto`. El router utiliza esta configuración para determinar qué dirección (`pool`) recibe cada dispositivo (`list`).

Paso 4. Identifique qué interfaces son internas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red interna.

Paso 5. Identifique qué interfaces son externas con respecto a NAT; es decir, cualquier interfaz que se conecte a la red externa.

En la figura 2, se muestra una topología y una configuración de ejemplo. Esta configuración permite la traducción para todos los hosts en la red 192.168.0.0/16, que incluye las LAN 192.168.10.0 y 192.168.11.0, cuando generan tráfico que ingresa por S0/0/0 y sale por S0/1/0.

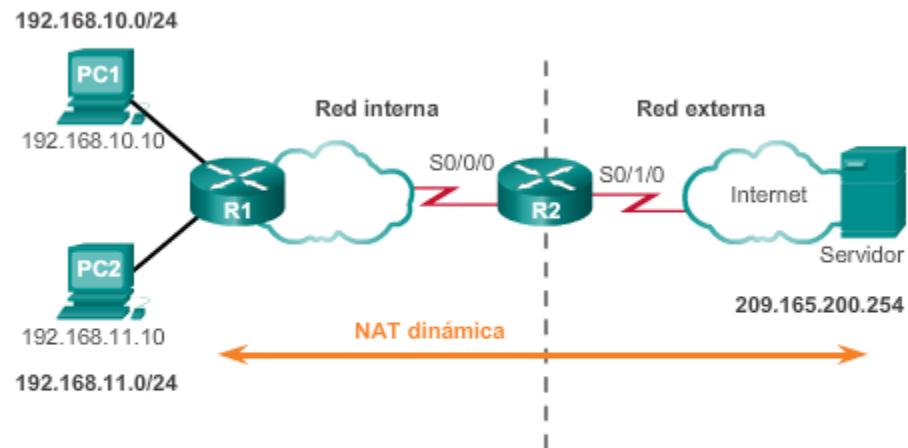
Estos hosts se traducen a una dirección disponible del conjunto en el rango de 209.165.200.226 a 209.165.200.240.

En la figura 3, se muestra la topología utilizada para la configuración del verificador de sintaxis. Utilice el verificador de sintaxis de la figura 4 para configurar la NAT dinámica en el R2.

Pasos de configuración de NAT dinámica

Pasos de configuración de NAT dinámica	
Paso 1	Definir el conjunto de direcciones globales que se debe usar para la traducción. ip nat pool <i>nombre primera-ip última-ip {netmask máscara-red prefix-length longitud-prefijo}</i>
Paso 2	Configurar una lista de acceso estándar que permita las direcciones que se deben traducir. access-list <i>número-lista-acceso permit origen[wildcard-origen]</i>
Paso 3	Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción dinámica de origen. ip nat inside source list <i>número-lista-acceso pool nombre</i>
Paso 4	Identificar la interfaz interna. interface <i>tipo número</i> ip nat inside
Paso 5	Identificar la interfaz externa. interface <i>tipo número</i> ip nat outside

Configuración de NAT dinámica de ejemplo



Defines a pool of public IPv4 addresses under the pool name NAT-POOL1.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Defines which addresses are eligible to be translated.

```
R2 (config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Binds NAT-POOL1 with ACL 1.

```
R2 (config)# ip nat inside source list 1 pool NAT-POOL1
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2 (config)# interface Serial0/0/0
```

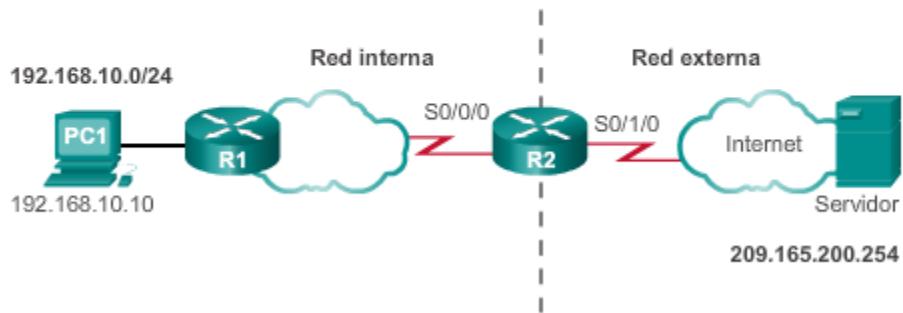
```
R2 (config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as an outside NAT interface.

```
R2 (config)# interface Serial0/1/0
```

```
R2 (config-if)# ip nat outside
```

Configuración de NAT dinámica



Con la configuración anterior, en las ilustraciones se muestra el proceso de traducción de NAT dinámica entre dos clientes y el servidor web:

En la figura 1, se muestra el flujo de tráfico desde adentro hacia fuera:

1. Los hosts con las direcciones IPv4 de origen (192.168.10.10 [PC1] y 192.168.11.10 [PC2]) envían paquetes para solicitar la conexión al servidor en la dirección IPv4 pública (209.165.200.254).
2. El R2 recibe el primer paquete del host 192.168.10.10. Debido a que este paquete se recibió en una interfaz configurada como interfaz NAT interna, el R2 verifica la configuración NAT para determinar si este paquete debe traducirse. Como la ACL permite este paquete, el R2 lo traduce. El R2 consulta su tabla de NAT. Debido a que no hay entrada de traducción para esta dirección IP, el R2 determina que la dirección de origen 192.168.10.10 se debe traducir de manera dinámica. El R2 selecciona una dirección global disponible del conjunto de direcciones dinámicas y crea una entrada de traducción, 209.165.200.226. La dirección IPv4 de origen inicial (192.168.10.10) es la dirección local interna, y la dirección traducida es la dirección global interna (209.165.200.226) en la tabla de NAT.

Para el segundo host, 192.168.11.10, el R2 repite el procedimiento, selecciona la siguiente dirección global disponible del conjunto de direcciones dinámicas y crea una segunda entrada de traducción, 209.165.200.227.

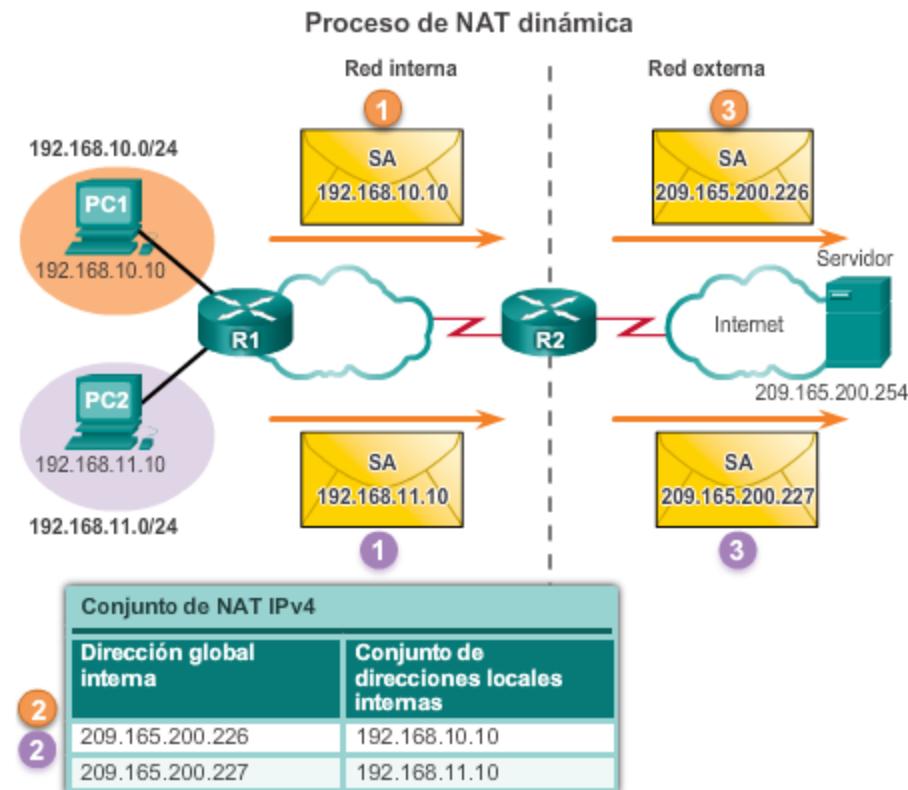
3. El R2 reemplaza la dirección de origen local interna de la PC1, 192.168.10.10, por la dirección global interna traducida 209.165.200.226 y reenvía el paquete. El mismo proceso se lleva a cabo para el paquete de la PC2 con la dirección traducida para esta computadora (209.165.200.227).

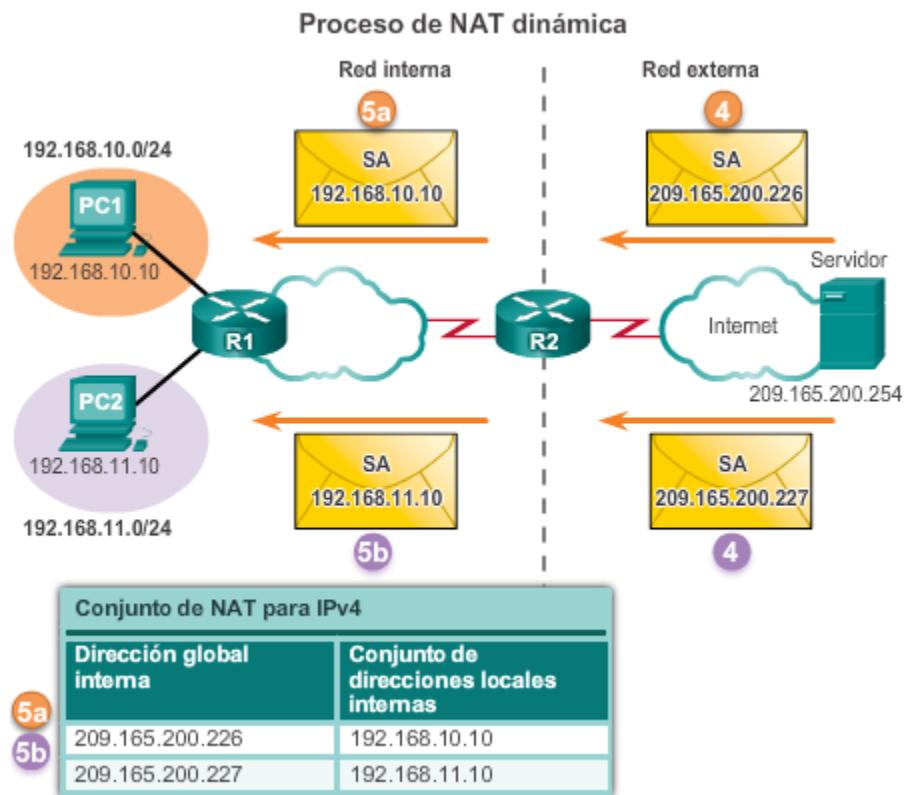
En la figura 2, se muestra el flujo de tráfico desde adentro hacia fuera:

4. El servidor recibe el paquete de la PC1 y responde con la dirección IPv4 de destino 209.165.200.226. Cuando el servidor recibe el segundo paquete, responde a la PC2 con la dirección IPv4 de destino 209.165.200.227.
- 5a. Cuando el R2 recibe el paquete con la dirección IPv4 de destino 209.165.200.226, realiza una búsqueda en la tabla de NAT. Con la asignación de la tabla, el R2 vuelve a traducir la dirección a la dirección local interna (192.168.10.10) y reenvía el paquete hacia la PC1.

5b. Cuando el R2 recibe el paquete con la dirección IPv4 de destino 209.165.200.227, realiza una búsqueda en la tabla de NAT. Con la asignación de la tabla, el R2 vuelve a traducir la dirección a la dirección local interna (192.168.11.10) y reenvía el paquete hacia la PC2.

6. La PC1 en 192.168.10.10 y la PC2 en 192.168.11.10 reciben los paquetes y continúan la conversación. El router lleva a cabo los pasos 2 a 5 para cada paquete. (El paso 6 no aparece en las ilustraciones).





El resultado del comando `show ip nat translations` que aparece en la figura 1 muestra los detalles de las dos asignaciones de NAT anteriores. El comando muestra todas las traducciones estáticas que se configuraron y todas las traducciones dinámicas que se crearon a causa del tráfico.

Si se agrega la palabra clave `verbose`, se muestra información adicional acerca de cada traducción, incluido el tiempo transcurrido desde que se creó y se utilizó la entrada.

De manera predeterminada, a las entradas de traducción se les agota el tiempo de espera después de 24 horas, a menos que se vuelvan a configurar los temporizadores con el comando `ip nat translation timeout segundos-tiempo-espera` en el modo de configuración global.

Para borrar las entradas dinámicas antes de que se agote el tiempo de espera, utilice el comando `clear ip nat translation` en el modo de configuración global (figura 2). Es útil borrar las entradas dinámicas al probar la configuración NAT. Como se muestra en la tabla, este comando se puede utilizar con palabras clave y variables para controlar qué entradas se deben borrar. Se pueden borrar entradas específicas para evitar interrumpir las sesiones activas. Utilice el comando de configuración global `clear ip nat translation *` para borrar todas las traducciones de la tabla.

Nota: solo se borran de la tabla las traducciones dinámicas. Las traducciones estáticas no pueden borrarse de la tabla de traducción.

En la figura 3, el comando `show ip nat statistics` muestra la información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad de direcciones que se asignaron.

También puede utilizar el comando **show running-config** y buscar los comandos de NAT, ACL, interfaz o conjunto con los valores requeridos. Examínelos detenidamente y corrija cualquier error que detecte.

Verificación de NAT dinámica con **show ip nat translations**

```
R2# show ip nat translations
Pro Inside global      Inside local    Outside local   Outside global
--- 209.165.200.226   192.168.10.10 ---      ---
--- 209.165.200.227   192.168.11.10 ---      ---
R2#
R2# show ip nat translations verbose
Pro Inside global      Inside local    Outside local   Outside global
--- 209.165.200.226   192.168.10.10 ---      ---
      create 00:17:25, use 00:01:54 timeout:86400000, left
23:58:05, Map-Id(In): 1,
      flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227   192.168.11.10 ---      ---
      create 00:17:22, use 00:01:51 timeout:86400000, left
23:58:08, Map-Id(In): 1,
      flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

Despejar traducciones NAT

```
R2# clear ip nat translation *
R2# show ip nat translations
R2#
```

Comando	Descripción
clear ip nat translation *	Elimina todas las entradas de traducción dinámica de direcciones de la tabla de traducción NAT.
clear ip nat translation inside ip-global ip-local [outside ip-local ip-global]	Elimina una entrada de traducción dinámica simple que contiene una traducción interna o una traducción interna y una externa.
clear ip nat translation protocolo inside ip-global puerto-global ip-local puerto-local [outside ip-local puerto local ip-global puerto-global]	Elimina una entrada de traducción dinámica extendida.

Verificación de NAT dinámica con show ip nat statistics

```
R2# clear ip nat statistics
PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
  Hits: 24 Misses: 0
  CEF Translated packets: 24, CEF Punted packets: 0
  Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
  pool NAT-POOL1: netmask 255.255.255.224
  start 209.165.200.226 end 209.165.200.240
  type generic, total addresses 15, allocated 2 (13%), misses 0

  Total doors: 0
  Appl doors: 0
  Normal doors: 0
  Queued Packets: 0
R2#
```

11.3.2 Configuración de la traducción de la dirección del puerto (PAT)

PAT (también denominada “NAT con sobrecarga”) conserva las direcciones del conjunto de direcciones globales internas al permitir que el router use una dirección global interna para muchas direcciones locales internas. En otras palabras, se puede utilizar una única dirección IPv4 pública para cientos, incluso miles de direcciones IPv4 privadas internas. Cuando se configura este tipo de traducción, el router mantiene suficiente información acerca de los protocolos de nivel superior, de los números de puerto TCP o UDP, por ejemplo, para volver a traducir la dirección global interna a la dirección local interna correcta. Cuando se asignan varias direcciones locales internas a una dirección global interna, los números de puerto TCP o UDP de cada host interno distinguen entre las direcciones locales.

Nota: la cantidad total de direcciones internas que se pueden traducir a una dirección externa teóricamente podría ser de hasta 65 536 por dirección IP. Sin embargo, la cantidad de direcciones internas a las que se puede asignar una única dirección IP es aproximadamente 4000.

Existen dos formas de configurar PAT, según cómo el ISP asigne las direcciones IPv4 públicas. En primer lugar, el ISP asigna más de una dirección IPv4 pública a la organización y, en segundo lugar, asigna una única dirección IPv4 pública que se requiere para que la organización se conecte al ISP.

Configuración de PAT para un conjunto de direcciones IP públicas

Si se emitió más de una dirección IPv4 pública para un sitio, estas direcciones pueden ser parte de un conjunto utilizado por PAT. Esto es similar a la NAT dinámica, con la excepción de que no existen suficientes direcciones públicas para realizar una asignación uno a uno entre direcciones

internas y externas. Una gran cantidad de dispositivos comparte el pequeño conjunto de direcciones.

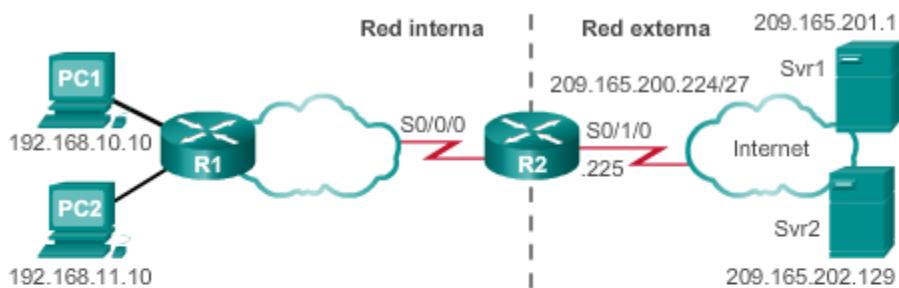
En la figura 1, se muestran los pasos para configurar PAT a fin de que utilice un conjunto de direcciones. La diferencia principal entre esta configuración y la configuración para NAT dinámica uno a uno es que se utiliza la palabra clave **overload**. La palabra clave **overload** habilita PAT.

La configuración de ejemplo que se muestra en la figura 2 establece la traducción de sobrecarga para el conjunto de NAT denominado NAT-POOL2. NAT-POOL2 contiene las direcciones de 209.165.200.226 a 209.165.200.240. Los hosts en la red 192.168.0.0/16 están sujetos a traducción. La interfaz S0/0/0 se identifica como interfaz interna, y la interfaz S0/1/0 se identifica como interfaz externa.

Utilice el verificador de sintaxis de la figura 3 para configurar PAT con un conjunto de direcciones en el R2.

Paso 1	Definir el conjunto de direcciones globales que se debe usar para la traducción de sobrecarga. <code>ip nat pool nombre primera-ip última-ip {netmask máscara-red prefix-length longitud-prefijo}</code>
Paso 2	Definir una lista de acceso estándar que permita las direcciones que se deben traducir. <code>access-list número-lista-acceso permit origen [wildcard-origen]</code>
Paso 3	Especificar la lista de acceso y el conjunto que se definieron en los pasos anteriores para establecer la traducción de sobrecarga. <code>ip nat inside source list número-lista-acceso pool nombre overload</code>
Paso 4	Identificar la interfaz interna. <code>interface tipo número ip nat inside</code>
Paso 5	Identificar la interfaz externa. <code>interface tipo número ip nat outside</code>

Ejemplo de PAT con conjunto de direcciones



Defina un conjunto de direcciones IPv4 públicas con el nombre de conjunto NAT-POOL2.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Defina las direcciones que se pueden traducir.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Vincule NAT-POOL2 a la ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL2
overload
```

Identifique la interfaz serial 0/0/0 como interfaz NAT interna.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifique la interfaz serial 0/1/0 como interfaz NAT externa.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Configuración de PAT para una única dirección IPv4 pública

En la figura 1, se muestra la topología de una implementación de PAT para la traducción de una única dirección IPv4 pública. En el ejemplo, todos los hosts de la red 192.168.0.0/16 (que coincide con la ACL 1) que envían tráfico a Internet a través del router R2 se traducen a la dirección IPv4 209.165.200.225 (dirección IPv4 de la interfaz S0/1/0). Los flujos de tráfico se identifican por los números de puerto en la tabla de NAT, ya que se utilizó la palabra clave **overload**.

En la figura 2, se muestran los pasos que se deben seguir para configurar PAT con una única dirección IPv4. Si solo hay una única dirección IPv4 pública disponible, la configuración de sobrecarga generalmente asigna la dirección pública a la interfaz externa que se conecta al ISP. Todas las direcciones internas se traducen a la única dirección IPv4 cuando salen de la interfaz externa.

Paso 1. Defina una ACL para permitir que se traduzca el tráfico.

Paso 2. Configure la traducción de origen con las palabras clave **interface** y **overload**. La palabra clave **interface** identifica la dirección IP de la interfaz que se debe utilizar en la traducción de las direcciones internas. La palabra clave **overload** le indica al router que realice un seguimiento de los números de puerto con cada entrada de NAT.

Paso 3. Identifique cuáles son las interfaces internas con respecto a NAT. Es decir, toda interfaz que se conecte a la red interna.

Paso 4. Identifique cuál es la interfaz externa con respecto a NAT. Esta debe ser la misma interfaz identificada en la instrucción de la traducción de origen del paso 2.

La configuración es similar a la de NAT dinámica, excepto que, en lugar de un conjunto de direcciones, se utiliza la palabra clave **interface** para identificar la dirección IPv4 externa. Por lo tanto, no se define ningún pool de NAT.

Utilice el verificador de sintaxis de la figura 3 para configurar PAT con una única dirección en el R2.

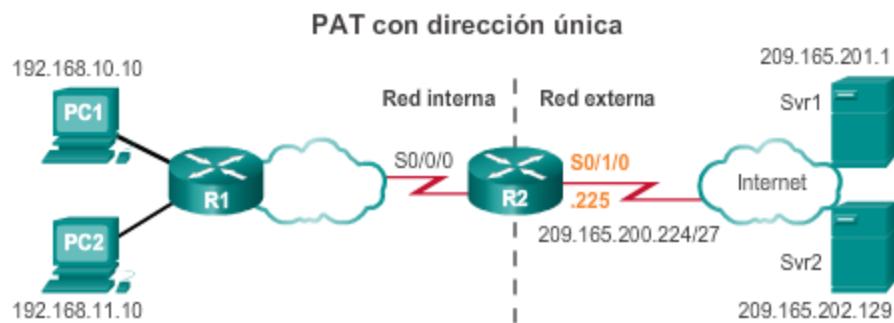


Tabla NAT

Dirección global interna	Dirección local interna	Dirección local externa	Dirección global externa
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.10.11:1444	209.165.202.129:80	209.165.202.129:80

Pasos de configuración de PAT

Paso 1	Definir una lista de acceso estándar que permita las direcciones que se deben traducir. <code>access-list número-lista-acceso permit origen [wildcard-origen]</code>
Paso 2	Especificar las opciones de ACL, interfaz de salida y sobrecarga para establecer la traducción dinámica de origen. <code>ip nat inside source list número-lista-acceso interface tipo número overload</code>
Paso 3	Identificar la interfaz interna. <code>interface tipo número ip nat inside</code>
Paso 4	Identificar la interfaz externa. <code>interface tipo número ip nat outside</code>

El proceso de NAT con sobrecarga es el mismo, ya sea que se utilice un conjunto de direcciones o una única dirección. En el ejemplo anterior de PAT, la PC1 desea comunicarse con el servidor web

Srv1 por medio de una única dirección IPv4 pública. Al mismo tiempo, otro cliente, la PC2, desea establecer una sesión similar con el servidor web Srv2. Tanto la PC1 como la PC2 se configuraron con direcciones IPv4 privadas, con el R2 habilitado para PAT.

Proceso de la computadora al servidor

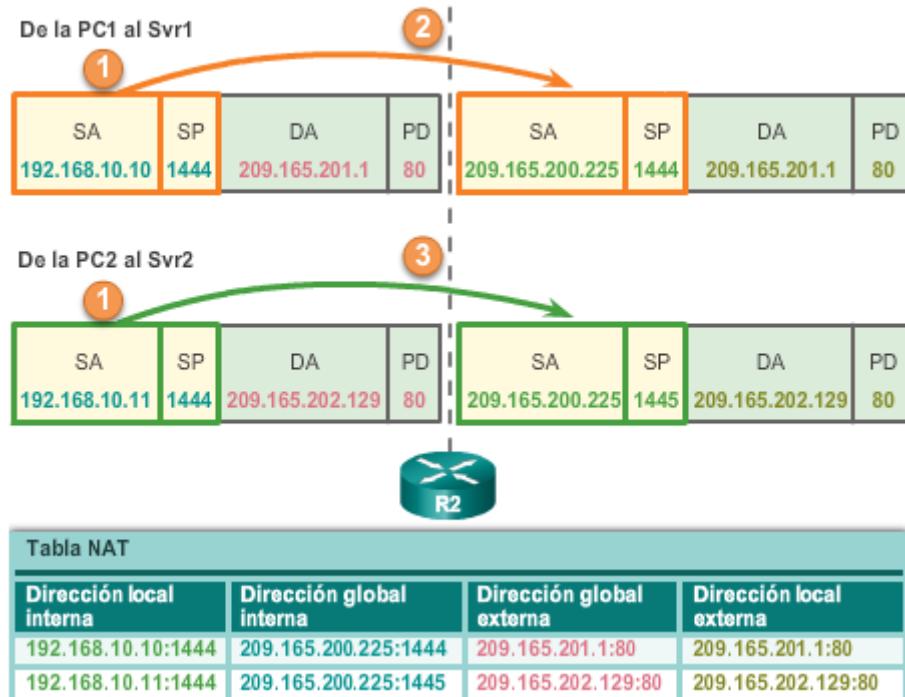
1. En la figura 1, se muestra que la PC1 y la PC2 envían paquetes a los servidores Srv1 y Srv2, respectivamente. La PC1 tiene la dirección IPv4 de origen 192.168.10.10 y utiliza el puerto de origen TCP 1444. La PC2 tiene la dirección IPv4 de origen 192.168.10.11 y, por casualidad, se le asigna el mismo puerto de origen 1444.
2. El paquete de la PC1 llega primero al R2. Mediante el uso de PAT, el R2 modifica la dirección IPv4 de origen a 209.165.200.225 (dirección global interna). En la tabla de NAT, no hay ningún otro dispositivo que use el puerto 1444, de modo que PAT mantiene el mismo número de puerto. El paquete luego se reenvía hacia el Srv1 en 209.165.201.1.
3. A continuación, llega el paquete de la PC2 al R2. PAT está configurada para utilizar una única dirección IPv4 global interna para todas las traducciones, 209.165.200.225. Al igual que con el proceso de traducción para la PC1, PAT cambia la dirección IPv4 de origen de la PC2 a la dirección global interna 209.165.200.225. Sin embargo, la PC2 tiene el mismo número de puerto de origen que una entrada actual de PAT, la traducción para la PC1. PAT aumenta el número de puerto de origen hasta que sea un valor único en su tabla. En este caso, la entrada del puerto de origen en la tabla de NAT y el paquete de la PC2 reciben el número 1445.

Si bien la PC1 y la PC2 usan la misma dirección traducida, la dirección global interna 209.165.200.225, y el mismo número de puerto de origen 1444, el número de puerto modificado para la PC2 (1445) hace que cada entrada en la tabla de NAT sea única. Esto se torna evidente cuando los paquetes se devuelven desde los servidores hacia los clientes.

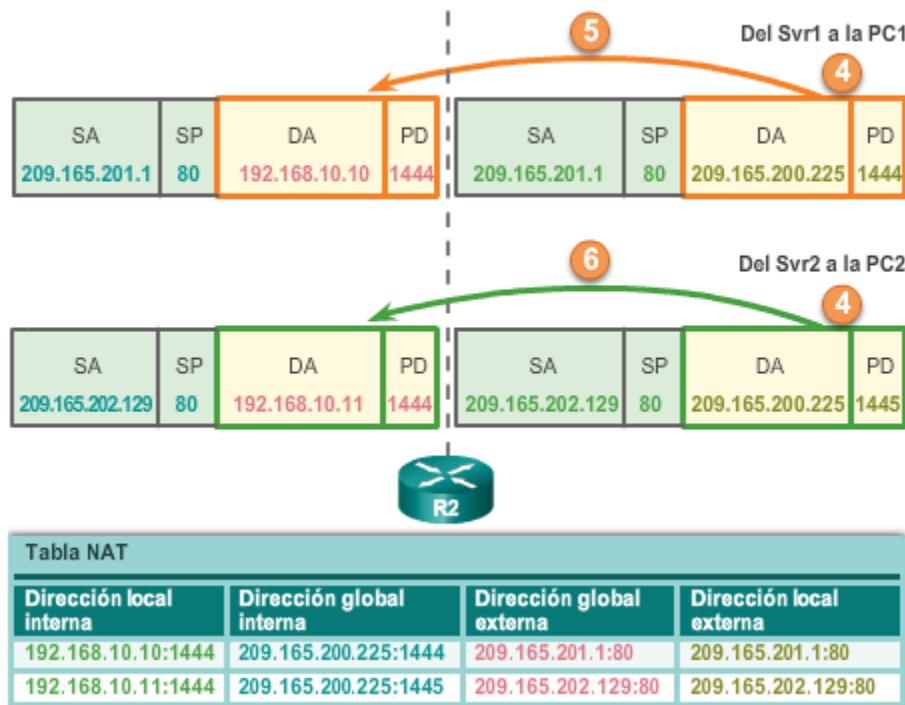
Proceso del servidor a la computadora

4. Como se muestra en la figura 2, en un intercambio típico entre cliente y servidor, los servidores Srv1 y Srv2 responden a las solicitudes recibidas de la PC1 y la PC2, respectivamente. Los servidores usan el puerto de origen del paquete recibido como puerto de destino y la dirección de origen como dirección de destino para el tráfico de retorno. Al parecer, los servidores se comunican con el mismo host en 209.165.200.225, pero no es así.
5. A medida que llegan los paquetes, el R2 ubica una única entrada en su tabla de NAT mediante la dirección de destino y el puerto de destino de cada paquete. En el caso del paquete del Srv1, la dirección IPv4 de destino 209.165.200.225 tiene varias entradas, pero solo una con el puerto de destino 1444. Mediante la entrada de su tabla, el R2 cambia la dirección IPv4 de destino del paquete a 192.168.10.10, sin necesidad de modificar el puerto de destino. Luego, el paquete se reenvía hacia la PC1.
6. Cuando llega el paquete del Srv2, el R2 realiza una traducción similar. La dirección IPv4 de destino 209.165.200.225 vuelve a aparecer en varias entradas. Sin embargo, con el puerto de destino 1445, el R2 puede identificar una única entrada de traducción. La dirección IPv4 de destino se modifica a 192.168.10.11. En este caso, el puerto de destino también se debe volver a modificar a su valor original de 1444, que está almacenado en la tabla de NAT. Luego, el paquete se reenvía hacia la PC2.

Análisis de PAT de las computadoras a los servidores



Análisis de PAT de los servidores a las computadoras



El router R2 se configuró para proporcionar PAT a los clientes de 192.168.0.0/16. Cuando los hosts internos salen del router R2 a Internet, se traducen a una dirección IPv4 del conjunto de PAT con un único número de puerto de origen.

Para verificar PAT, se usan los mismos comandos que se usan para verificar la NAT estática y dinámica, como se muestra en la figura 1. El comando **show ip nat translations** muestra las traducciones de dos hosts distintos a servidores web distintos. Observe que se asigna la misma dirección IPv4 209.165.200.226 (dirección global interna) a dos hosts internos distintos. Los números de puerto de origen en la tabla de NAT distinguen las dos transacciones.

Como se muestra en la figura 2, el comando **show ip nat statistics** verifica que NAT-POOL2 haya asignado una única dirección para ambas traducciones. El resultado incluye información sobre la cantidad y el tipo de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad que se asignó.

Verificación de las traducciones PAT

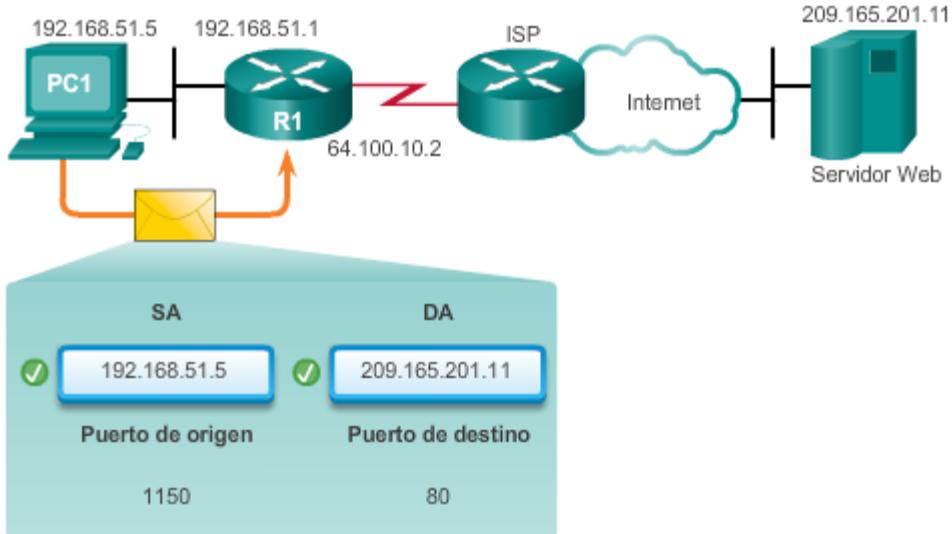
```
R2# show ip nat translations
Pro Inside global           Inside local           Outside local
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:51839
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.125:42558
R2#
```

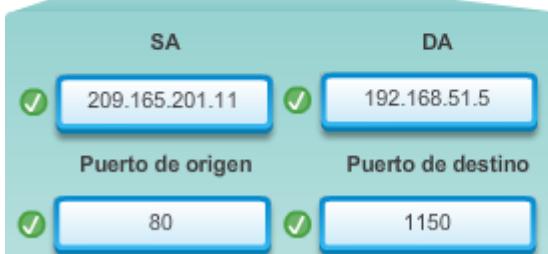
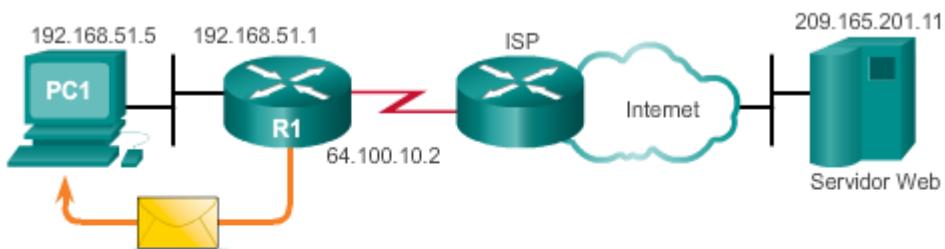
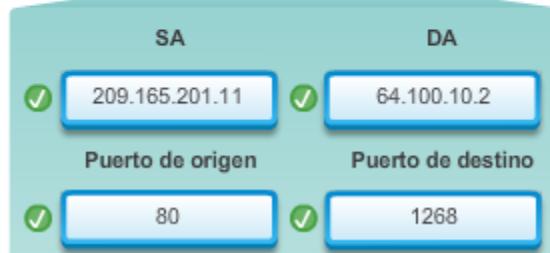
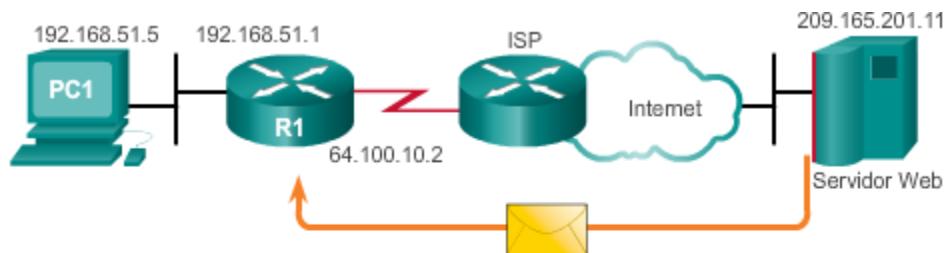
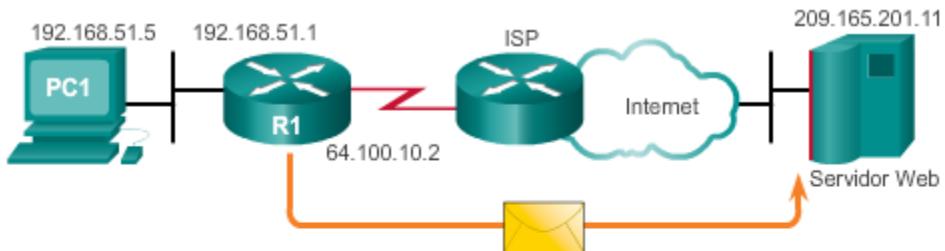
Verificación de las estadísticas de PAT

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
pool NAT-POOL2: netmask 255.255.255.224
  start 209.165.200.226 end 209.165.200.240
    type generic, total addresses 15, allocated 1 (6%),
misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```





11.3.3 Reenvío de puertos

El reenvío de puertos (a veces, denominado “tunneling”) consiste en reenviar un puerto de red desde un nodo de red hacia otro. Esta técnica permite que un usuario externo alcance un puerto en una dirección IPv4 privada (dentro de una LAN) desde el exterior a través de un router con NAT habilitada.

En general, las operaciones y los programas peer-to-peer para compartir archivos, como las aplicaciones de servidores web y los FTP salientes, requieren que los puertos del router se reenvíen o se abran para permitir que estas aplicaciones funcionen, como se muestra en la figura 1. Debido a que NAT oculta las direcciones internas, la comunicación peer-to-peer solo funciona desde adentro hacia fuera donde NAT puede asignar las solicitudes salientes a las respuestas entrantes.

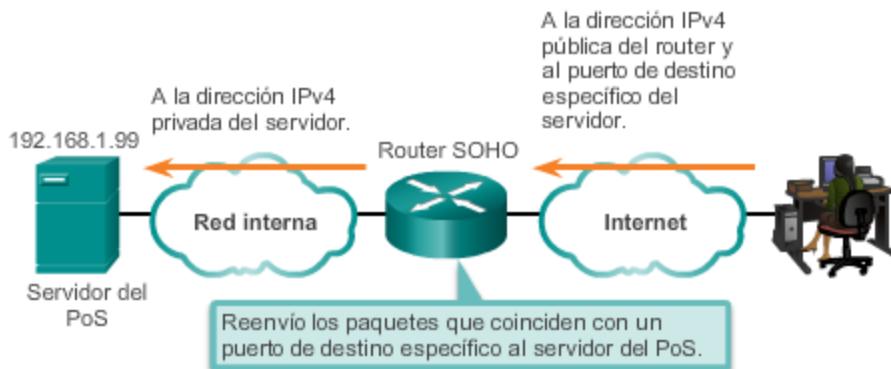
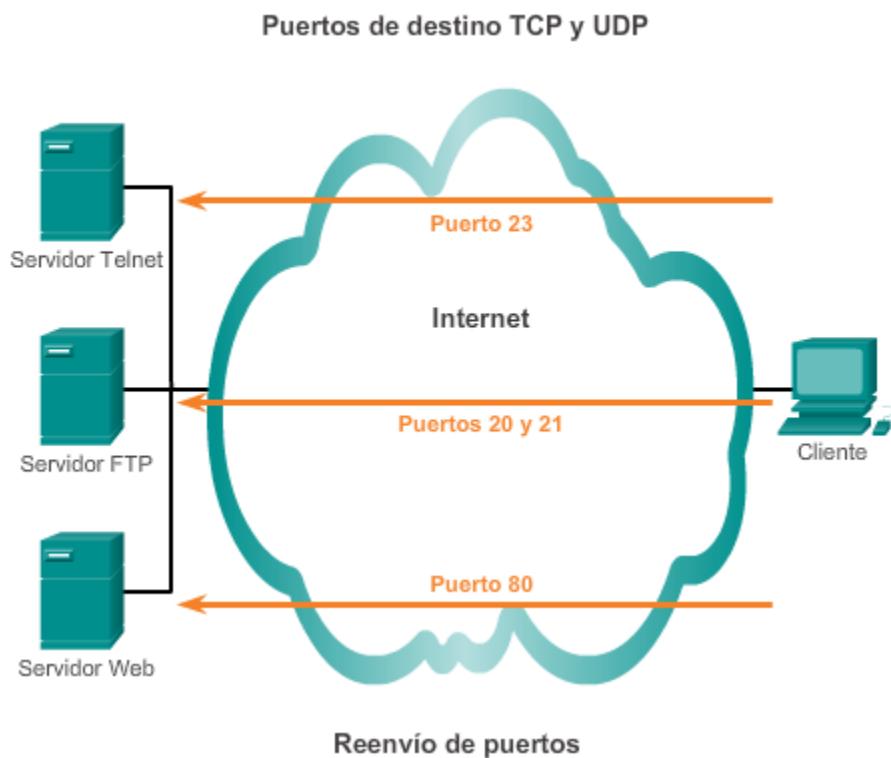
El problema es que NAT no permite las solicitudes iniciadas desde el exterior. Esta situación se puede resolver de forma manual. El reenvío de puertos se puede configurar para identificar los puertos específicos que se pueden reenviar a los hosts internos.

Recuerde que las aplicaciones de software de Internet interactúan con los puertos de usuario que necesitan estar abiertos o disponibles para dichas aplicaciones. Las distintas aplicaciones usan puertos diferentes. Esto hace que las aplicaciones y los routers identifiquen los servicios de red de manera predecible. Por ejemplo, HTTP funciona a través del puerto bien conocido 80. Cuando alguien introduce la dirección <http://cisco.com>, el explorador muestra el sitio web de Cisco Systems, Inc. Tenga en cuenta que no es necesario especificar el número de puerto HTTP para la solicitud de página, ya que la aplicación asume que se trata del puerto 80.

Si se requiere un número de puerto diferente, se puede agregar al URL separado por dos puntos (:). Por ejemplo, si el servidor web escuchara en el puerto 8080, el usuario escribiría <http://www.ejemplo.com:8080>.

El reenvío de puertos permite que los usuarios en Internet accedan a los servidores internos mediante el uso de la dirección de puerto de WAN del router y del número de puerto externo que coincida. En general, los servidores internos se configuran con direcciones IPv4 privadas definidas en RFC 1918. Cuando se envía una solicitud a la dirección IPv4 del puerto de WAN a través de Internet, el router reenvía la solicitud al servidor correspondiente en la LAN. Por motivos de seguridad, los routers de banda ancha no permiten que se reenvíe ninguna solicitud de redes externas a un host interno de manera predeterminada.

En la figura 2, se muestra al propietario de una pequeña empresa que utiliza un servidor del punto de venta (PoS) para hacer un seguimiento de las ventas y los inventarios en la tienda. Se puede acceder al servidor desde la tienda pero, debido a que tiene una dirección IPv4 privada, no es posible acceder a este de manera pública desde Internet. Habilitar el router local para el reenvío de puertos permitiría que el propietario acceda al servidor del punto de venta en cualquier lugar desde Internet. El reenvío de puertos en el router se configura con el número de puerto de destino y la dirección IPv4 privada del servidor del punto de venta. Para acceder al servidor, el software de cliente utilizaría la dirección IPv4 pública del router y el puerto de destino del servidor.



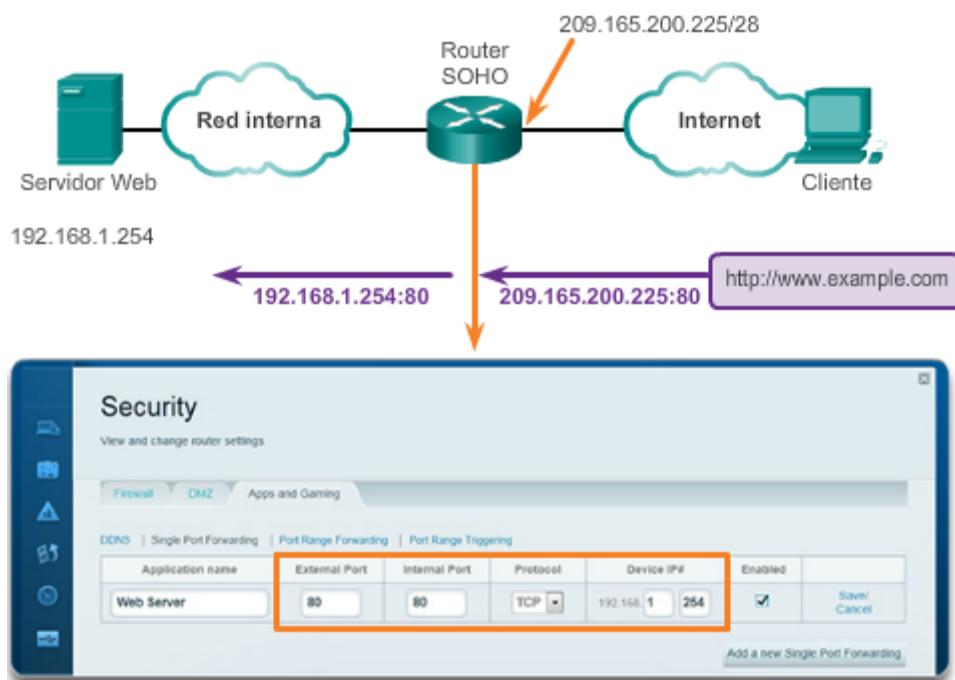
En la ilustración, se muestra la ventana de configuración Single Port Forwarding (Reenvío de puerto único) de un router SOHO Linksys EA6500. De manera predeterminada, el reenvío de puertos no está habilitado en el router.

Si se especifica la dirección local interna a la cual se deben reenviar las solicitudes, es posible habilitar el reenvío de puertos para las aplicaciones. En la ilustración, las solicitudes de servicio HTTP que llegan a este router Linksys se reenvían al servidor web con la dirección local interna 192.168.1.254. Si la dirección IPv4 WAN externa del router SOHO es 209.165.200.225, el usuario externo puede introducir <http://www.ejemplo.com>, y el router Linksys redirige la solicitud HTTP al servidor web interno en la dirección IPv4 192.168.1.254, con el número de puerto predeterminado 80.

Se puede especificar un puerto distinto al puerto predeterminado 80. Sin embargo, el usuario externo tendría que saber el número de puerto específico que debe utilizar. Para especificar un puerto diferente, se modifica el valor del campo External Port (Puerto externo) en la ventana Single Port Forwarding (Reenvío de puerto único).

El enfoque adoptado para configurar el reenvío de puertos depende de la marca y el modelo del router de banda ancha en la red. No obstante, hay algunos pasos genéricos que se deben seguir. Si las instrucciones que suministra el ISP o las que vienen con el router no proporcionan una orientación adecuada, en el sitio web <http://www.portforward.com> se ofrecen guías para varios routers de banda ancha. Puede seguir las instrucciones para agregar o eliminar puertos según sea necesario para satisfacer las necesidades de todas las aplicaciones que deseé permitir o denegar.

Reenvío de puertos en un router SOHO



Los comandos de IOS que se usan para implementar el reenvío de puertos son similares a los que se usan para configurar la NAT estática. Básicamente, el reenvío de puertos es una traducción de NAT estática con un número de puerto TCP o UDP específico.

En la figura 1, se muestra el comando de NAT estática que se usa para configurar el reenvío de puertos con IOS.

En la figura 2, se muestra un ejemplo de configuración del reenvío de puertos con comandos de IOS en el router R2. La dirección 192.168.10.254 es la dirección IPv4 local interna del servidor web que escucha en el puerto 80. Los usuarios acceden a este servidor web interno con la dirección IP global 209.165.200.225, una dirección IPv4 pública globalmente única. En este caso, es la dirección de la interfaz Serial 0/1/0 del R2. El puerto global se configura como 8080. Este es el puerto de destino que se utiliza junto con la dirección IPv4 global 209.165.200.225 para acceder al servidor web interno. Observe los siguientes parámetros de comando dentro de la configuración NAT:

- *ip-local* = 192.168.10.254
- *puerto-local* = 80
- *ip-global* = 209.165.200.225
- *puerto-global* = 8080

Cuando no se utiliza un número de puerto bien conocido, el cliente debe especificar el número de puerto de la aplicación.

Al igual que otros tipos de NAT, el reenvío de puertos requiere que se configuren las interfaces NAT interna y externa.

Como en el caso de la NAT estática, se puede utilizar el comando **show ip nat translations** para verificar el reenvío de puertos, como se muestra en la figura 3.

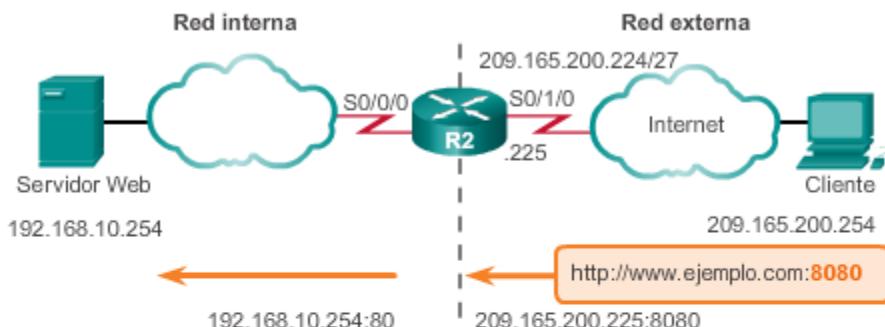
En el ejemplo, cuando el router recibe el paquete con la dirección IPv4 global interna 209.165.200.225 y un puerto TCP de destino 8080, el router realiza una búsqueda en la tabla de NAT con la dirección IPv4 de destino y el puerto de destino como claves. A continuación, el router traduce la dirección a la dirección local interna del host 192.168.10.254 y el puerto de destino 80. Luego, el R2 reenvía el paquete al servidor web. En el caso de los paquetes de retorno del servidor web al cliente, este proceso se invierte.

Reenvío de puertos con IOS

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]}
```

Parámetro	Descripción
tcp o udp	Indica si este es un número de puerto TCP o UDP.
<i>ip-local</i>	Esta es la dirección IPv4 asignada al host en la red interna, generalmente, del espacio de direcciones privadas definido en RFC 1918.
<i>puerto-local</i>	Establece el puerto local TCP/UDP en un rango de 1 a 65535. Este es el número de puerto en el que escucha el servidor.
<i>ip-global</i>	Esta es la dirección IPv4 globalmente única de un host interno. Esta es la dirección IP que utilizan los clientes externos para llegar al servidor interno.
<i>puerto-global</i>	Establece el puerto global TCP/UDP en un rango de 1 a 65535. Este es el número de puerto que utilizan los clientes externos para llegar al servidor interno.
extendable	La opción extendable se aplica de forma automática. La palabra clave extendable permite que el usuario configure varias traducciones estáticas ambiguas, es decir, traducciones con la misma dirección local o global. Permite que el router extienda la traducción a más de un puerto, en caso de ser necesario.

Ejemplo de reenvío de puertos con IOS



Establece la traducción estática entre una dirección local interna y un puerto local, y entre una dirección global interna y un puerto global.

```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

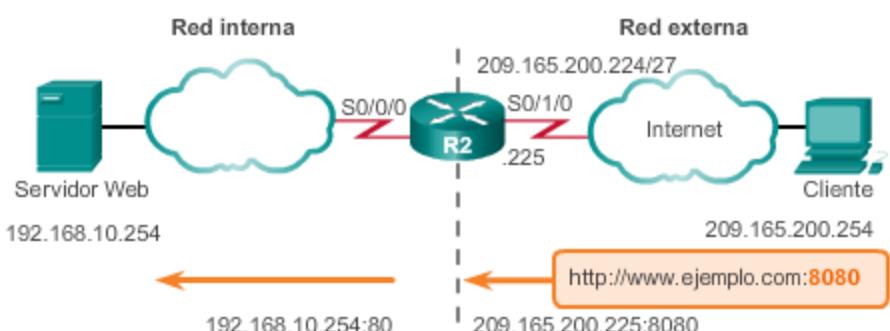
Identifica la interfaz serial 0/0/0 como interfaz NAT interna.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifica la interfaz serial 0/1/0 como interfaz NAT externa.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

Verificación del reenvío de puertos



```
R2# show ip nat translations
Pro Inside global           Inside local           Outside local
tcp 209.165.200.225:8080  192.168.10.254:80   209.165.200.254:461
tcp 209.165.200.225:8080  192.168.10.254:80   ---
```

11.3.4 Configuración de NAT e IPv6

La cuestión del agotamiento del espacio de direcciones IPv4 es una prioridad para el IETF desde principios de la década de los noventa. La combinación de las direcciones IPv4 privadas definidas en RFC 1918 y de NAT cumple un papel decisivo para retrasar este agotamiento. NAT presenta desventajas considerables, y en enero de 2011, la IANA asignó sus últimas direcciones IPv4 a los RIR.

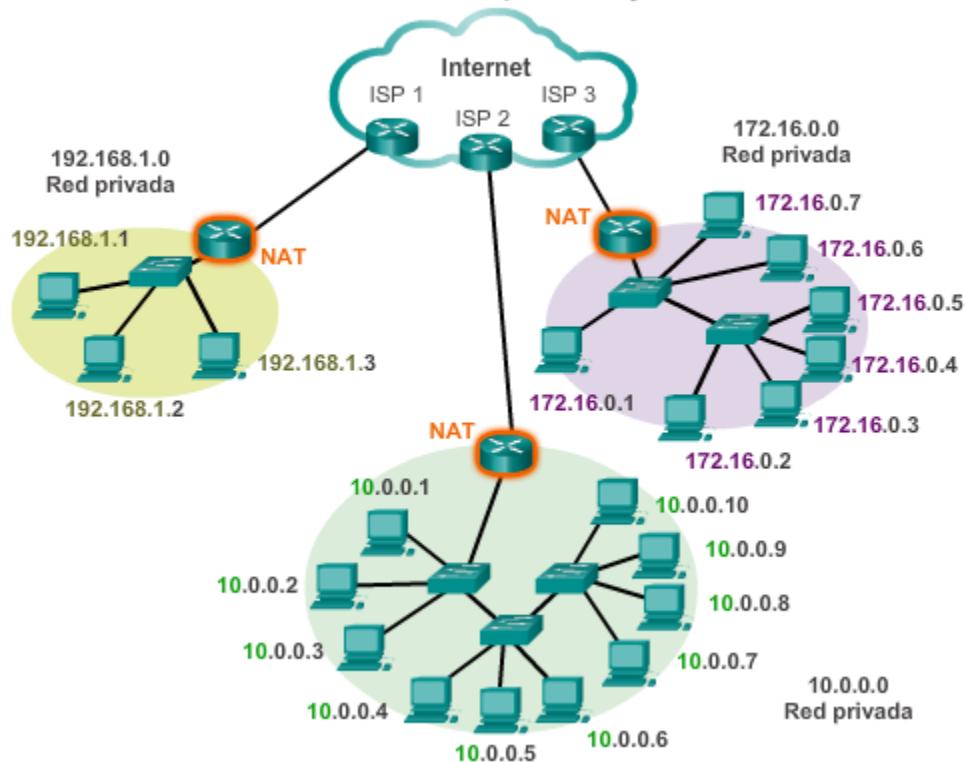
Uno de los beneficios de NAT para IPv4 que no fueron intencionales es que oculta la red privada de Internet pública. NAT tiene la ventaja de que ofrece un nivel de seguridad considerable al denegar el acceso de las computadoras que se encuentran en Internet pública a los hosts internos. Sin embargo, no debe considerarse como un sustituto de la seguridad de red adecuada, como la que proporciona un firewall.

En RFC 5902, el Consejo de Arquitectura de Internet (IAB) incluyó la siguiente cita sobre la traducción de direcciones de red IPv6:

“En general, se cree que una caja NAT proporciona un nivel de protección porque los hosts externos no pueden iniciar directamente una comunicación con los hosts detrás de una NAT. No obstante, no se deben confundir las cajas NAT con los firewalls. Como se analizó en [RFC4864], sección 2.2, el acto de traducción en sí mismo no proporciona seguridad. La función de filtrado con estado puede proporcionar el mismo nivel de protección sin requerir una función de traducción”.

Con una dirección de 128 bits, IPv6 proporciona 340 sextillones de direcciones. Por lo tanto, el espacio de direcciones no es un problema. IPv6 se desarrolló con la intención de que la NAT para IPv4 con su traducción entre direcciones IPv4 públicas y privadas resulte innecesaria. Sin embargo, IPv6 implementa una forma de NAT. IPv6 incluye su propio espacio de direcciones IPv6 privadas y NAT, que se implementan de manera distinta de como se hace para IPv4.

Direcciones IPv4 privadas y NAT



Las direcciones IPv6 locales únicas (ULA) se asemejan a las direcciones privadas en IPv4 definidas en RFC 1918, pero también existen diferencias considerables. El objetivo de las ULA es proporcionar espacio de direcciones IPv6 para las comunicaciones dentro de un sitio local, no tienen el propósito de proporcionar espacio adicional de direcciones IPv6 ni un nivel de seguridad.

Como se muestra en la ilustración, las ULA tienen el prefijo FC00::/7, lo que produce un rango de primer hexteto que va desde FC00 hasta FDFF. El bit siguiente se establece en 1 si el prefijo se asigna localmente. Es posible que en el futuro se pueda establecer en 0. Los 40 bits siguientes corresponden a una ID global seguida de una ID de subred de 16 bits. Estos primeros 64 bits se combinan para crear el prefijo de la ULA. Esto permite que los 64 bits restantes se utilicen para la ID de interfaz o, en términos de IPv4, la porción de host de la dirección.

Las direcciones locales únicas se definen en RFC 4193. Las ULA también se conocen como “direcciones IPv6 locales” (no se deben confundir con las direcciones IPv6 link-local) y tienen varias características, incluidas las siguientes:

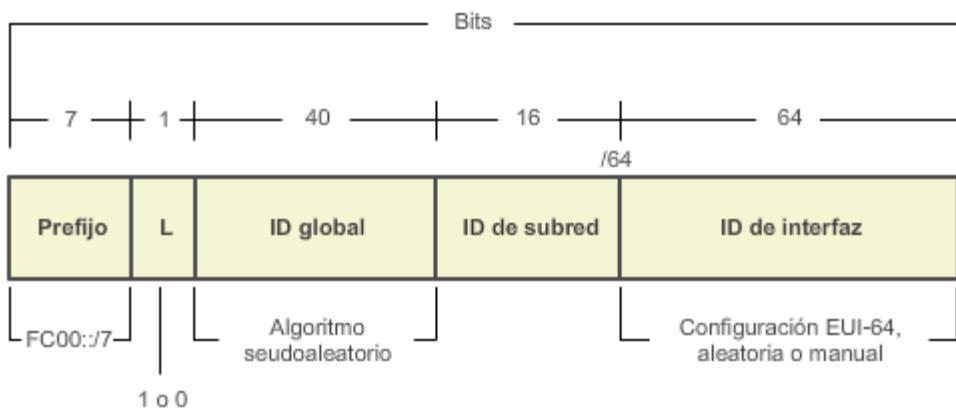
- Permiten que los sitios se combinen o se interconecten de manera privada, sin generar conflictos entre direcciones y sin necesidad de volver a numerar las interfaces que usan estos prefijos.
- Son independientes de cualquier ISP y se pueden usar para las comunicaciones dentro de un sitio sin tener conectividad a Internet.
- No se pueden enrutar a través de Internet; sin embargo, si se filtran por routing o DNS, no existe conflicto con otras direcciones.

Las ULA no son tan sencillas como las direcciones definidas en RFC 1918. A diferencia de las direcciones IPv4 privadas, el IETF no tenía la intención de utilizar una forma de NAT para traducir entre las direcciones locales únicas y las direcciones IPv6 de unidifusión global.

La comunidad de Internet continúa analizando la implementación y los posibles usos de las direcciones IPv6 locales únicas. Por ejemplo, el IETF considera permitir la opción de crear el prefijo de la ULA de forma local con FC00::/8, o de que lo asigne un tercero de forma automática y que empiece con FD00::/8.

Nota: la especificación original de IPv6 asignaba el espacio de direcciones para las direcciones locales de sitio, definidas en RFC 3513. El IETF dejó en desuso las direcciones locales de sitio en RFC 3879 porque el término “sitio” resultaba algo ambiguo. Las direcciones locales de sitio tenían el rango de prefijos FEC0::/10 y todavía pueden encontrarse en documentos antiguos de IPv6.

Dirección IPv6 local única

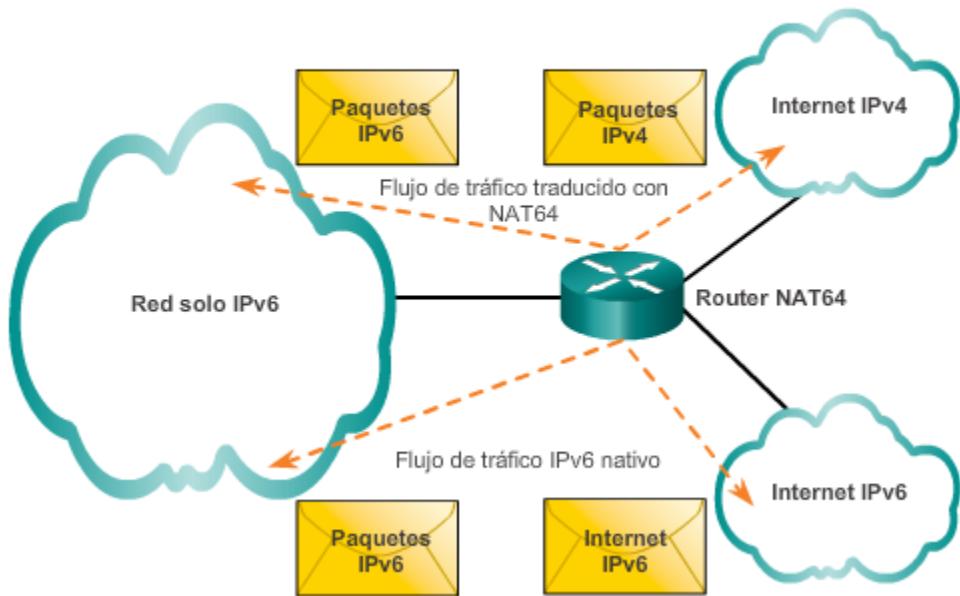


NAT para IPv6 se usa en un contexto muy distinto al de NAT para IPv4. Las variedades de NAT para IPv6 se usan para proporcionar acceso de manera transparente entre redes solo IPv6 y redes solo IPv4. No se utiliza como forma de traducción de IPv6 privada a IPv6 global.

Lo ideal es que IPv6 se ejecute de forma nativa siempre que sea posible. Es decir, en dispositivos IPv6 que se comunican entre sí a través de redes IPv6. No obstante, para colaborar en el cambio de IPv4 a IPv6, el IETF elaboró varias técnicas de transición que admiten una variedad de situaciones de IPv4 a IPv6, como dual-stack, tunneling y traducción.

Dual-stack es cuando los dispositivos ejecutan protocolos asociados a IPv4 y a IPv6. Tunneling para IPv6 es el proceso de encapsulación de un paquete IPv6 dentro de un paquete IPv4. Esto permite que el paquete IPv6 se transmita a través de una red solo IPv4.

La NAT para IPv6 no se debe usar como una estrategia a largo plazo, sino como un mecanismo temporal para contribuir a la migración de IPv4 a IPv6. Con el correr de los años, hubo varios tipos de NAT para IPv6, incluida la traducción de direcciones de red/traducción de protocolos (NAT-PT). El IETF dejó en desuso NAT-PT en favor de su reemplazo, NAT64. NAT64 excede el ámbito de este currículo.

NAT64**11.4 Resolución de problemas de NAT**

En la figura 1, se muestra el R2 habilitado para PAT, que usa el rango de direcciones de 209.165.200.226 a 209.165.200.240.

Cuando hay problemas de conectividad IPv4 en un entorno NAT, suele ser difícil determinar la causa del problema. El primer paso para resolverlo es descartar que la causa sea NAT. Siga estos pasos para verificar que NAT funcione como se espera:

Paso 1. En función de la configuración, defina claramente lo que debe lograr la NAT. Esto puede revelar un problema con la configuración.

Paso 2. Verifique que las traducciones de la tabla sean correctas con el comando `show ip nat translations`.

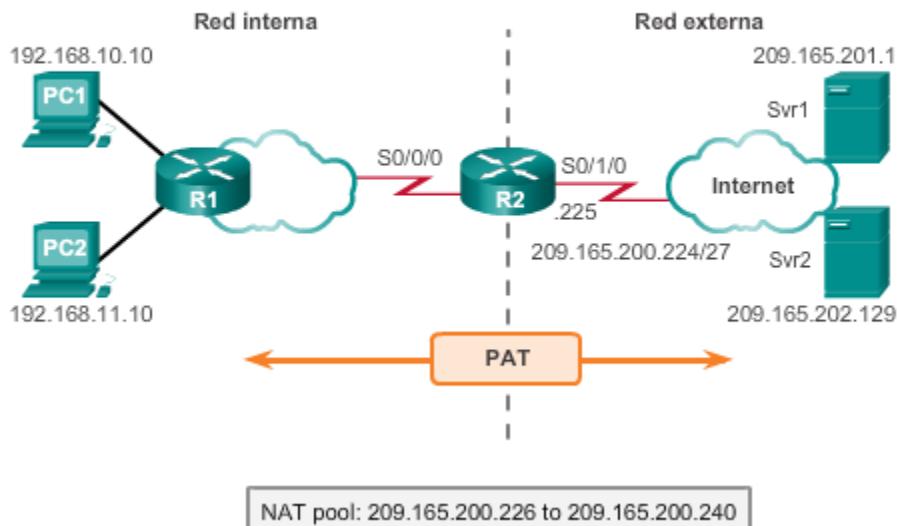
Paso 3. Utilice los comandos `clear ydebug` para verificar que NAT funcione como se espera. Verifique si se vuelven a crear las entradas dinámicas después de borrarlas.

Paso 4. Revise en detalle lo que sucede con el paquete y verifique que los routers tengan la información de routing correcta para trasladar el paquete.

En la figura 2, se muestra el resultado de los comandos `show ip nat statistics` y `show ip nat translations`. Antes de utilizar los comandos `show`, se eliminan las estadísticas y entradas de NAT de la tabla de NAT con los comandos `clear ip nat statistics` y `clear ip nat translation *`. Una vez que el host en 192.168.10.10 accede mediante Telnet al servidor en 209.165.201.1, se muestran las estadísticas de NAT y la tabla de NAT para verificar que NAT funcione como se espera.

En un entorno de red simple, es útil controlar las estadísticas de NAT con el comando `show ip nat statistics`. El comando `show ip nat statistics` muestra información sobre la cantidad total de traducciones activas, los parámetros de configuración NAT, la cantidad de direcciones en el conjunto y la cantidad que se asignó. Sin embargo, en un entorno NAT más complejo, con varias traducciones en curso, es posible que este comando no identifique el problema de forma clara. Es posible que se deban ejecutar los comandos `debug` en el router.

Resolución de problemas de NAT



Para verificar el funcionamiento de la característica de NAT, utilice el comando `debug ip nat`, que muestra información sobre cada paquete que traduce el router. El comando `debug ip nat detailed` genera una descripción de cada paquete que se tiene en cuenta para traducir. Este comando también proporciona información sobre determinados errores o condiciones de excepción, como la falla para asignar una dirección global. El comando `debug ip nat detailed` genera más sobrecarga que el comando `debug ip nat`, pero puede proporcionar el detalle necesario para resolver el problema de NAT. Desactive siempre la depuración al finalizar.

En la figura 1, se muestra un resultado de ejemplo de `debug ip nat`. Este resultado muestra que el host interno (192.168.10.10) inició el tráfico hacia el host externo (209.165.201.1) y que la dirección de origen se tradujo a la dirección 209.165.200.226.

Cuando decodifique el resultado de este comando, observe los significados de los siguientes símbolos y valores:

- * (asterisco): el asterisco junto a NAT indica que la traducción se realiza en la ruta de switching rápido. Al primer paquete en una conversación siempre se aplica el switching de procesos, que es más lento. Si existe una entrada de caché, el resto de los paquetes atraviesan la ruta de switching rápido.
- s=: este símbolo se refiere a la dirección IP de origen.
- a.b.c.d--->w.x.y.z: este valor indica que la dirección de origen a.b.c.d se traduce a w.x.y.z.

- **d=:** este símbolo se refiere a la dirección IP de destino.
- **[xxxx]:** el valor entre corchetes es el número de identificación IP. Esta información puede ser útil para la depuración, ya que habilita la correlación con otros seguimientos de paquetes realizados por los analizadores de protocolos.

Nota: verifique que la ACL mencionada en la referencia de comandos de NAT permita todas las redes necesarias. En la figura 2, solo las direcciones 192.168.0.0/16 se pueden traducir. El R2 no traduce los paquetes de la red interna destinados a Internet con direcciones de origen que la ACL 1 no permita de forma explícita.

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2817]
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4180]
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2818]
*Feb 15 20:01:311.702: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2819]
*Feb 15 20:01:311.710: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2820]
*Feb 15 20:01:311.710: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4181]
*Feb 15 20:01:311.722: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4182]
*Feb 15 20:01:311.726: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2821]
*Feb 15 20:01:311.730: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4183]
*Feb 15 20:01:311.734: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2822]
*Feb 15 20:01:311.734: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4184]
<resultado omitido>
```

Caso práctico 1

En la figura 1, se muestra que los hosts de las LAN 192.168.0.0/16, la PC1 y la PC2, no pueden hacer ping a los servidores en la red externa, el Srv1 y el Srv2.

Para iniciar la resolución de problemas, utilice el comando **show ip nat translations** a fin de verificar si actualmente hay alguna traducción en la tabla de NAT. El resultado de la figura 1 muestra que no hay traducciones en la tabla.

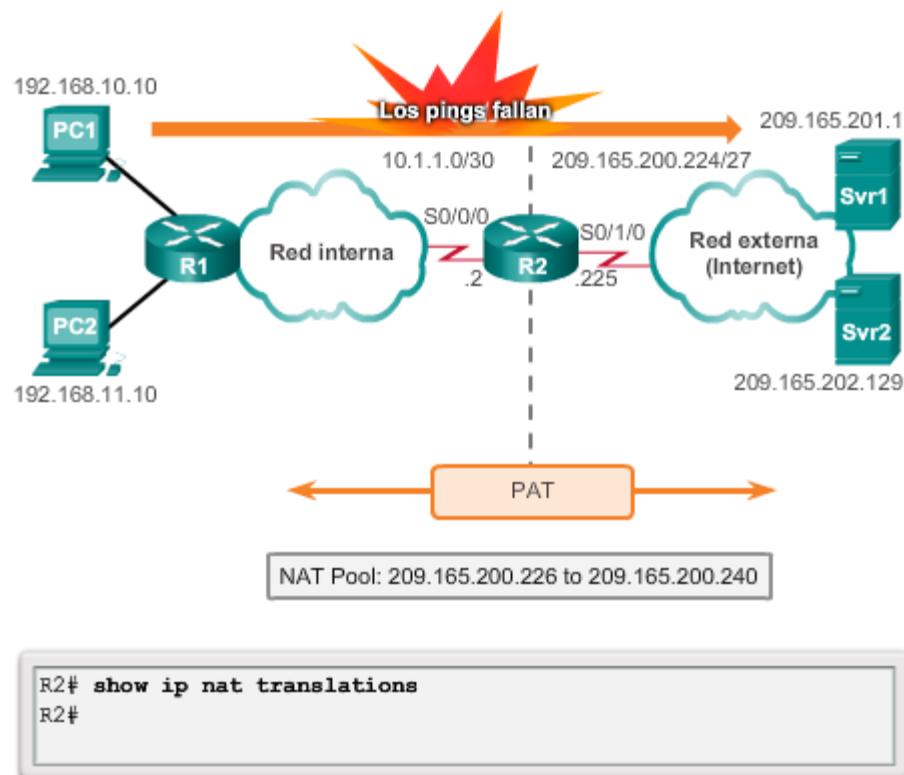
El comando **show ip nat statistics** se utiliza para determinar si se realizaron traducciones. También identifica las interfaces entre las que debe ocurrir la traducción. Como se muestra en el resultado de la figura 2, los contadores de NAT están en 0, lo que verifica que no se realizó ninguna traducción. Al comparar el resultado con la topología de la figura 1, observe que las interfaces del router están definidas de forma incorrecta como NAT interna o NAT externa. También es posible verificar una configuración incorrecta con el comando **show running-config**.

Se debe eliminar la configuración NAT actual de las interfaces antes de aplicar la configuración correcta.

Luego de definir correctamente las interfaces NAT interna y externa, otro ping de la PC1 al Srv1 falla. El uso de los comandos **show ip nat translations** y **show ip nat statistics** nuevamente verifica que no hay traducciones en curso.

Como se muestra en la figura 3, el comando `show access-lists` se utiliza para determinar si la ACL a la que hace referencia el comando NAT permite todas las redes necesarias. Al examinar el resultado, se comprueba que se utilizó una máscara de bits wildcard incorrecta en la ACL que define las direcciones que se deben traducir. La máscara wildcard solo permite la subred 192.168.0.0/24. Primero se elimina la lista de acceso y después se reconfigura con la máscara wildcard correcta.

Una vez corregidas las configuraciones, se genera otro ping de la PC1 al Srv1, y esta vez el ping es correcto. Como se muestra en la figura 4, los comandos `show ip nat translations` y `show ip nat statistics` se utilizan para verificar que se produzca la traducción NAT.



```
R2# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  Serial0/1/0
Hits: 0 Misses: 0
<resultado omitido>

R2(config)# interface serial 0/0/0
R2(config-if)# no ip nat outside
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# no ip nat inside
R2(config-if)# ip nat outside
```

```
R2# show access-lists
Standard IP access list 1
  10 permit 192.168.0.0, wildcard bits 0.0.0.255
R2#
R2(config)# no access-list 1
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:37:58 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 20 Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 1
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
  pool NAT-POOL2: netmask 255.255.255.224
  start 209.165.200.226 end 209.165.200.240
  type generic, total addresses 15, allocated 1 (6%), misses 0
<resultado omitido>

R2# show ip nat translations
Pro Inside global      Inside local      Outside local      Ou
icmp 209.165.200.226:38 192.168.10.10:38  209.165.201.1:38  20
R2#
```

11.5 Resumen

En este capítulo, se explicó cómo se utiliza NAT para contribuir a mitigar el agotamiento del espacio de direcciones IPv4. La NAT para IPv4 permite que los administradores de red utilicen el espacio de direcciones privadas definido en RFC 1918, a la vez que proporciona conectividad a Internet, mediante una única dirección pública o una cantidad limitada de estas.

NAT conserva el espacio de direcciones públicas y reduce la sobrecarga administrativa de forma considerable al administrar las adiciones, los movimientos y las modificaciones. NAT y PAT se pueden implementar para ahorrar espacio de direcciones públicas y armar intranets privadas seguras sin afectar la conexión al ISP. Sin embargo, NAT presenta desventajas en términos de sus efectos negativos en el rendimiento de los dispositivos, la seguridad, la movilidad y la conectividad de extremo a extremo, y se debe considerar como una implementación a corto plazo para el agotamiento de direcciones, cuya solución a largo plazo es IPv6.

En este capítulo, se analizó la NAT para IPv4, incluido lo siguiente:

- Las características, la terminología y las operaciones generales de NAT
- Los diferentes tipos de NAT, incluidas la NAT estática, la NAT dinámica y PAT
- Las ventajas y las desventajas de NAT
- La configuración, la verificación y el análisis de la NAT estática, la NAT dinámica y PAT
- La forma en que se puede usar el reenvío de puertos para acceder a los dispositivos internos desde Internet
- La resolución de problemas de NAT mediante los comandos `show` y `debug`



Frontera de NAT