Principios básicos de enrutamiento y switching.

CCNA1 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 Akin Ramirez, revisado por Nicolás Contador.

Agradecimientos a la comunidad de elprofederedes.wordpress.com

Contenido

Capítulo 1: Exploración de la red 1.0.1.1 Introducción

Introducción

Nos encontramos en un momento decisivo respecto del uso de la tecnología para extender y potenciar nuestra capacidad de comunicarnos. La globalización de Internet se ha producido más rápido de lo que cualquiera hubiera imaginado. El modo en que se producen las interacciones sociales, comerciales, políticas y personales cambia en forma continua para estar al día con la evolución de esta red global. En la próxima etapa de nuestro desarrollo, los innovadores usarán Internet como punto de inicio para sus esfuerzos, lo que generará nuevos productos y servicios diseñados específicamente para aprovechar las capacidades de la red. A medida que los programadores impulsen los límites de lo posible, las capacidades de las redes interconectadas que crean la Internet jugarán un papel cada vez más grande en el éxito de estos proyectos.

Este capítulo presenta la plataforma de redes de datos de la cual dependen cada vez más nuestras relaciones sociales y comerciales. El material presenta las bases para explorar los servicios, las tecnologías y los problemas que enfrentan los profesionales de red mientras diseñan, desarrollan y mantienen la red moderna.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Explicar cómo afectan las redes la forma en que interactuamos, aprendemos, trabajamos y jugamos.
- Describir la forma en que las redes permiten la comunicación.
- Explicar el concepto de red convergente.
- Describir los cuatro requisitos básicos de una red confiable.
- Explicar el uso de los dispositivos de red.
- Comparar los dispositivos y las topologías de una LAN con los dispositivos y las topologías de una WAN.
- Explicar la estructura básica de Internet.
- Explicar la forma en que las LAN y las WAN se interconectan a Internet.
- Describir el impacto de BYOD, de la colaboración en línea, del video y de la computación en la nube en una red empresarial.
- Explicar la forma en que las tecnologías de red están cambiando el entorno doméstico.
- Identificar algunas amenazas y soluciones de seguridad básicas para redes pequeñas y de gran tamaño.
- Explicar cómo operan las tres arquitecturas empresariales de Cisco para satisfacer las necesidades del entorno de red en constante evolución.

Capítulo 1: Exploración de la red 1.1.1.1 Las redes en nuestra vida cotidiana

Entre todos los elementos esenciales para la existencia humana, la necesidad de interactuar está justo después de la necesidad de sustentar la vida. La comunicación es casi tan importante para nosotros como el aire, el agua, los alimentos y un lugar para vivir.

Los métodos que utilizamos para comunicarnos están en constante cambio y evolución. Si bien en el pasado nos limitábamos a interactuar cara a cara, los avances en tecnología extendieron significativamente el alcance de las comunicaciones. Desde las pinturas rupestres hasta la imprenta, la radio y la televisión, cada nuevo descubrimiento mejoró nuestra capacidad de conectarnos y comunicarnos.

La creación y la interconexión de redes de datos sólidas tuvieron un efecto profundo en la comunicación y se convirtieron en la nueva plataforma en la que se producen las comunicaciones modernas.

En el mundo actual, estamos conectados como nunca antes gracias al uso de redes. Las personas que tienen alguna idea pueden comunicarse de manera instantánea con otras personas para hacer esas ideas realidad. Las noticias y los descubrimientos se conocen en todo el mundo en cuestión de segundos. Incluso, las personas pueden conectarse y jugar con amigos que estén del otro lado del océano y en otros continentes.

Las redes conectan a las personas y promueven la comunicación libre. Todos pueden conectarse, compartir y hacer una diferencia.

Capítulo 1: Exploración de la red 1.1.1.2 La tecnología antes y ahora

Imagine un mundo sin Internet, sin Google, YouTube, mensajería instantánea, Facebook, Wikipedia, juegos en línea, Netflix, iTunes ni fácil acceso a información de actualidad. Un mundo sin sitios Web de comparación de precios, donde no podríamos evitar hacer fila ya que no podríamos comprar en línea y tampoco podríamos buscar rápidamente números de teléfono ni indicaciones en mapas para llegar a diversos lugares con solo un clic.

¿Cuán diferentes serías nuestras vidas sin todo esto? Vivíamos en ese mundo hace apenas 15 o 20 años. Sin embargo, con el correr de los años, las redes de datos se expandieron y transformaron lentamente para mejorar la calidad de vida de las personas en todo el mundo.

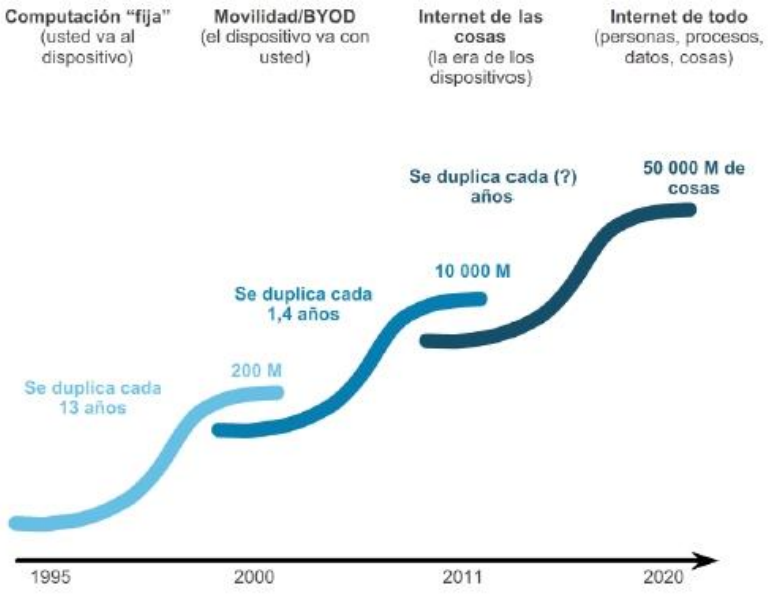
En el transcurso de un día, los recursos disponibles en Internet pueden ayudarlo a llevar a cabo las siguientes tareas:

- Enviar y compartir sus fotografías, videos hechos en casa y experiencias con amigos o con el mundo.
- Acceder a trabajos curriculares y entregarlos.
- Comunicarse con amigos, familiares y pares mediante correo electrónico, mensajería instantánea o llamadas de teléfono a través de Internet.
- Mirar videos, películas o capítulos de programas de televisión a petición.
- Jugar en línea con amigos.
- Decidir cómo vestirse al consultar en línea las condiciones actuales del clima.
- Buscar el camino menos congestionado hacia su destino al observar videos de cámaras Web que muestran el clima y el tráfico.
- Consultar su estado de cuenta bancario y pagar electrónicamente las facturas.

Los innovadores buscan formas de utilizar Internet aún más cada día. A medida que los desarrolladores amplían los límites de lo posible, las capacidades de Internet y la función que Internet desempeña en nuestras vidas se expanden cada vez más. Piense en los cambios que se produjeron desde 1995, descritos en la ilustración. Ahora, considere qué cambios sucederán en el transcurso de los próximos 25 años. Lo que este futuro depara es Internet de todo (IdT).

IdT reúne personas, procesos, datos y demás cosas para hacer que las conexiones mediante redes sean más relevantes y tengan mayor valor. IdT transforma la información en acciones que crean nuevas capacidades y proporcionan experiencias más enriquecedoras y oportunidades económicas sin precedentes a personas, empresas y países.

¿Qué más considera que podremos hacer si utilizamos la red como plataforma?



Capítulo 1: Exploración de la red 1.1.1.3 La comunidad mundial

Los avances en tecnologías de red son, quizá, los agentes de cambio más significativos en el mundo actual. Gracias a estos avances, podemos crear un mundo en el que las fronteras nacionales, las distancias geográficas y las limitaciones físicas se vuelven menos importantes y se convierten en obstáculos cada vez más fáciles de sortear.

Internet cambió la manera en la que se producen las interacciones sociales, comerciales, políticas y personales. La naturaleza inmediata de las comunicaciones por Internet alienta la creación de comunidades globales. Estas comunidades permiten una interacción social que no depende de la ubicación ni de la zona horaria. La creación de comunidades en línea para el intercambio de ideas e información tiene el potencial de aumentar las oportunidades de productividad en todo el planeta.

Para Cisco, esto se denomina "red humana". La red humana se enfoca en el impacto que tienen Internet y las redes en las personas y las empresas.

¿Cómo lo afecta la red humana?

Capítulo 1: Exploración de la red 1.1.1.4 Las redes respaldan la forma en que aprendemos

Las redes e Internet cambiaron todo lo que hacemos, desde la forma en que aprendemos hasta la forma en que nos comunicamos, cómo trabajamos e, incluso, cómo jugamos.

Cambio en la forma en que aprendemos

Comunicación, colaboración y compromiso son los componentes básicos de la educación. Las instituciones se esfuerzan continuamente para mejorar estos procesos y maximizar la diseminación del conocimiento. Los métodos de capacitación tradicionales proporcionan principalmente dos fuentes de conocimientos de las cuales los estudiantes pueden obtener información: el libro de texto y el instructor. Estas dos fuentes son limitadas, tanto en el formato como en la temporización de la presentación.

Las redes cambiaron la forma en que aprendemos. Redes confiables y sólidas respaldan y enriquecen las experiencias de aprendizaje de los estudiantes.

Mediante las redes, se ofrece material educativo en una amplia variedad de formatos, que incluye actividades, evaluaciones y comentarios. Como se muestra en la figura 1, en la actualidad las redes tienen las siguientes características:

- Admiten la creación de aulas virtuales.
- Proporcionan video a petición.
- Dan lugar a espacios de aprendizaje cooperativos.
- Permiten el aprendizaje móvil.

El acceso a la enseñanza de alta calidad ya no está restringido para los estudiantes que viven en las inmediaciones de donde dicha enseñanza se imparte. El aprendizaje a distancia en línea eliminó las barreras geográficas y mejoró la oportunidad de los estudiantes. Ahora, los cursos en línea (e-learning) se pueden dictar a través de una red. Estos cursos pueden contener datos (texto, enlaces), voz y video disponibles para los estudiantes en cualquier momento y desde cualquier lugar. Los foros o grupos de discusión permiten al estudiante colaborar con el instructor, con otros estudiantes de la clase e incluso con estudiantes de todo el mundo. Los cursos combinados pueden mezclar las clases dirigidas por instructores y software educativo para proporcionar lo mejor de ambos estilos. En la figura 2, se muestra un video sobre las formas en las que se expandió el aula.

Además de los beneficios para el estudiante, las redes han mejorado la gestión y la administración de los cursos también. Algunas de estas funciones en línea incluyen la inscripción de alumnos, la entrega de evaluaciones y el seguimiento del progreso.

Capítulo 1: Exploración de la red 1.1.1.5 Las redes respaldan la forma en que nos comunicamos

Cambio en la forma en que nos comunicamos

La globalización de Internet conduce a nuevas formas de comunicación que les dan a las personas la capacidad de crear información a la que puede acceder una audiencia mundial.

Algunas formas de comunicación incluyen las siguientes:

- IM/mensajería de texto: tanto la mensajería instantánea (IM, Instant Messaging) como la mensajería de texto permiten que dos o más personas se comuniquen de forma instantánea y en tiempo real. Muchas de las aplicaciones de IM y de mensajería de texto incorporan características como la transferencia de archivos. Las aplicaciones de IM pueden ofrecer funciones adicionales, como comunicación por voz y por video.

- Medios sociales: consisten en sitios Web interactivos en los que las personas y las comunidades crean y comparten contenido generado por los usuarios con amigos, familiares, pares y el mundo.

- Herramientas de colaboración:estas herramientas permiten que las personas puedan trabajar en forma conjunta con documentos compartidos. Las personas conectadas a un sistema compartido pueden comunicarse y hablar, generalmente a través de video interactivo en tiempo real, sin limitaciones de ubicación o de zona horaria. A través de la red, pueden compartir texto y gráficos, además de editar documentos en forma conjunta. Con las herramientas de colaboración siempre disponibles, las organizaciones pueden compartir información rápidamente y lograr los objetivos. La amplia distribución de las redes de datos permite que las personas en ubicaciones remotas puedan contribuir de igual manera con las personas ubicadas en los centros de gran población.

- Weblogs (blogs): los weblogs son páginas Web fáciles de actualizar y editar. A diferencia de los sitios Web comerciales, creados por expertos profesionales en comunicación, los blogs proporcionan a todas las personas un medio para comunicar sus opiniones a una audiencia mundial sin tener conocimientos técnicos sobre diseño Web. Hay blogs de casi todos los temas que uno se pueda imaginar y con frecuencia se forman comunidades de gente alrededor de los autores de blogs populares.

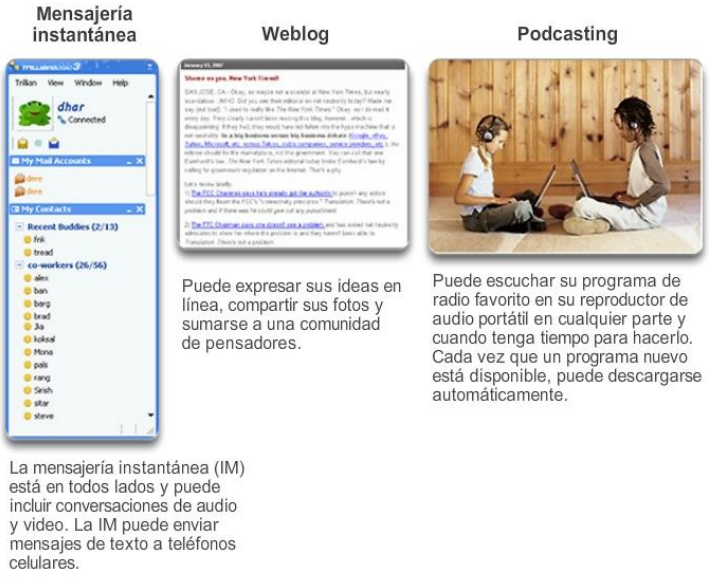
- Wikis: las wikis son páginas Web que grupos de personas pueden editar y ver juntos. Mientras un blog es más como un diario individual y personal, una wiki es una creación de grupo. Como tal, puede estar sujeta a una revisión y edición más extensa. Al igual que los blogs, las wikis pueden crearse en etapas, por cualquier persona, sin el patrocinio de una importante empresa comercial. Wikipedia se convirtió en un recurso muy completo, una enciclopedia en línea de temas aportados por el público. Las personas y organizaciones privadas también pueden crear sus propias wikis para capturar la información recopilada sobre un tema en particular. Muchas empresas utilizan wikis como herramienta de colaboración interna. Ahora con el Internet mundial, gente de cualquier ámbito de la sociedad puede participar en las wikis y añadir sus propias ideas y conocimientos a un recurso compartido.

- Podcasting: se trata de un medio basado en audio que originalmente permitía a las personas grabar audio y convertirlo para utilizarlo. El podcasting permite a las personas difundir sus grabaciones entre un público amplio. El archivo de audio se coloca en un sitio Web (o un blog o wiki) donde otros pueden descargarlo y reproducirlo en sus PC, computadoras portátiles y otros dispositivos móviles.

- Intercambio de archivos P2P: el intercambio de archivos punto a punto (P2P, Peer-to-Peer) permite a las personas compartir archivos entre sí sin tener que almacenarlos en un servidor central ni descargarlos de un servidor tal. Para incorporarse a la red P2P, el usuario simplemente debe instalar un software P2P. Esto les permite localizar archivos y compartirlos con otros usuarios de la red P2P.

  La extensa digitalización de los archivos de medios, como archivos de música y video, aumentó el interés en el intercambio de archivos P2P. Sin embargo, no todos adoptaron el intercambio de archivos P2P. Hay muchas personas a las que les preocupa infringir las leyes sobre materiales protegidos por derechos de autor.

¿Qué otros sitios o herramientas utiliza para compartir lo que piensa?



Capítulo 1: Exploración de la red 1.1.1.6 Las redes respaldan la forma en que trabajamos

Cambio en la forma en que trabajamos

En el ámbito empresarial, al comienzo las empresas utilizaban las redes de datos para registrar y administrar internamente información financiera, información de clientes y los sistemas de nómina de pagos de los

empleados. Estas redes empresariales evolucionaron para permitir la transmisión de muchos tipos de servicios de información diferentes, incluidos correo electrónico, video, mensajería y telefonía.

El uso de redes para capacitar a los empleados de forma eficaz y rentable tiene una aceptación cada vez mayor. Las oportunidades de aprendizaje en línea pueden disminuir el transporte costoso y prolongado, e incluso asegurar que todos los empleados estén correctamente capacitados para realizar sus tareas de manera productiva y segura.

Hay muchas historias de éxito que muestran formas innovadoras en las que las redes se utilizan para hacernos más exitosos en el lugar de trabajo. Algunas de esas situaciones se encuentran disponibles en el sitio Web de Cisco, http://www.cisco.com.

Capítulo 1: Exploración de la red 1.1.1.7 Las redes respaldan la forma en que jugamos

Cambio en la forma en que jugamos

La adopción generalizada de Internet por las industrias de viaje y entretenimiento mejora la posibilidad de disfrutar y compartir diferentes formas de recreación, sin importar la ubicación. Es posible explorar lugares, en forma interactiva, que antes soñábamos visitar, así como también ver con anticipación los destinos reales antes de realizar un viaje. Los viajeros pueden publicar en línea detalles y fotografías de sus experiencias para que los vean otras personas.

Además, Internet se utiliza para formas tradicionales de entretenimiento. Escuchamos a artistas de sellos discográficos, vemos avances y películas, leemos libros completos y descargamos material para acceder sin conexión en otro momento. Los eventos deportivos y conciertos en vivo se pueden sentir en el momento en que ocurren, o se pueden grabar y ver en cualquier momento.

Las redes permiten la creación de nuevas formas de entretenimiento, tales como juegos en línea. Los jugadores participan en cualquier clase de competencia en línea que los diseñadores de juegos puedan imaginar. Competimos contra amigos y enemigos de todo el mundo como si estuviéramos en la misma habitación.

Incluso las actividades fuera de línea se fortalecen con el uso de servicios de colaboración de red. Las comunidades mundiales de interés han crecido rápidamente. Compartimos experiencias comunes y hobbies

fuera de nuestro vecindario, ciudad o región. Los fanáticos del deporte comparten opiniones y hechos sobre sus equipos favoritos. Los coleccionistas muestran valiosas colecciones y reciben comentarios de expertos.

Los mercados y los sitios de subastas en línea permiten comprar, vender y comercializar todo tipo de mercancía.

Las redes mejoran nuestra experiencia, independientemente de la forma de diversión que disfrutemos en la red humana.

¿Cómo se juega en Internet?

Capítulo 1: Exploración de la red 1.1.2.1 Redes de varios tamaños

Hay redes de todo tamaño. Pueden ir desde redes simples, compuestas por dos PC, hasta redes que conectan millones de dispositivos.

Las redes simples que se instalan en hogares permiten compartir recursos, como impresoras, documentos, imágenes y música, entre algunas PC locales.

Con frecuencia, las personas que trabajan desde una oficina doméstica o remota y necesitan conectarse a una red corporativa u otros recursos centralizados configuran redes de oficinas domésticas y de oficinas pequeñas. Además, muchos emprendedores independientes utilizan redes de oficinas domésticas y de oficinas pequeñas para publicitar y vender productos, hacer pedidos y comunicarse con clientes. La comunicación a través de una red normalmente es más eficaz y económica que las formas de comunicación tradicionales, como puede ser el correo estándar o las llamadas telefónicas de larga distancia.

En las empresas y grandes organizaciones, las redes se pueden utilizar incluso de manera más amplia para permitir que los empleados proporcionen consolidación y almacenamiento de la información en los servidores de red, así como acceso a dicha información. Las redes también proporcionan formas de comunicación rápida, como el correo electrónico y la mensajería instantánea, y permiten la colaboración entre empleados.

Además de las ventajas que perciben en el nivel interno, muchas organizaciones utilizan sus redes para ofrecer productos y servicios a los clientes a través de su conexión a Internet.

Internet es la red más extensa que existe. De hecho, el término Internet significa “red de redes”. Internet es, literalmente, una colección de redes privadas y públicas interconectadas, como las que se describen más arriba. Por lo general, las redes de empresas, de oficinas pequeñas e incluso las redes domésticas proporcionan una conexión a Internet compartida.

Es increíble la rapidez con la que Internet se convirtió en una parte integral de nuestras rutinas diarias.

Redes domésticas pequeñas

Redes de oficinas pequeñas y oficinas hogareñas

Redes medianas a grandes

Redes mundiales

Redes domésticas pequeñas

Las redes domésticas pequeñas conectan algunas PC entre sí y a Internet.

Redes de oficinas pequeñas y oficinas hogareñas

Las redes de oficinas pequeñas y oficinas domésticas, o redes SOHO (Small Office/Home Office), permiten que las PC de una oficina doméstica o una oficina remota se conecten a una red corporativa y tengan acceso a recursos compartidos centralizados.

Redes medianas a grandes

Las redes medianas a grandes, como las que se utilizan en corporaciones e instituciones educativas, pueden tener muchas ubicaciones con cientos o miles de PC interconectadas.

Redes mundiales

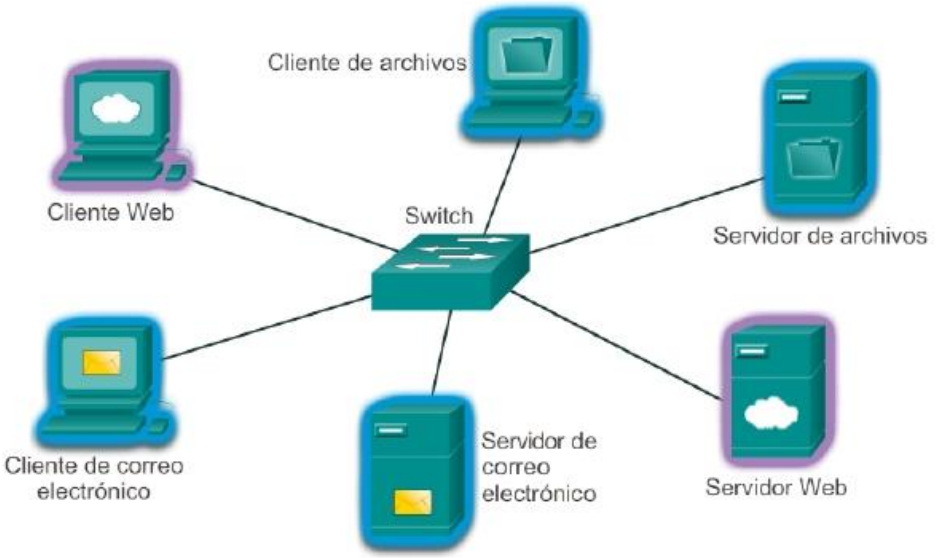
Internet es una red de redes que conecta cientos de millones de PC en todo el mundo.

Capítulo 1: Exploración de la red 1.1.2.2 Clientes y servidores

Todas las PC conectadas a una red que participan directamente en las comunicaciones de red se clasifican como hosts o dispositivos finales. Los hosts pueden enviar y recibir mensajes a través de la red. En las redes modernas, los dispositivos finales pueden funcionar como clientes, servidores o ambos. El software instalado en la computadora determina cuál es la función que cumple la computadora.

Los servidores son hosts con software instalado que les permite proporcionar información, por ejemplo correo electrónico o páginas Web, a otros hosts de la red. Cada servicio requiere un software de servidor diferente. Por ejemplo, para proporcionar servicios Web a la red, un host necesita un software de servidor Web.

Los clientes son computadoras host que tienen instalado un software que les permite solicitar información al servidor y mostrar la información obtenida. Un explorador Web, como Internet Explorer, es un ejemplo de software cliente.



Servidor y cliente Web

El servidor Web ejecuta software de servidor, mientras que los clientes utilizan software de explorador, como Windows Internet Explorer, para obtener acceso a las páginas Web que se encuentran en el servidor.

Servidor y cliente de archivos

El servidor de archivos almacena los archivos, mientras que el dispositivo cliente obtiene acceso a ellos mediante software cliente, como el Explorador de Windows.

Servidor y cliente de correo electrónico

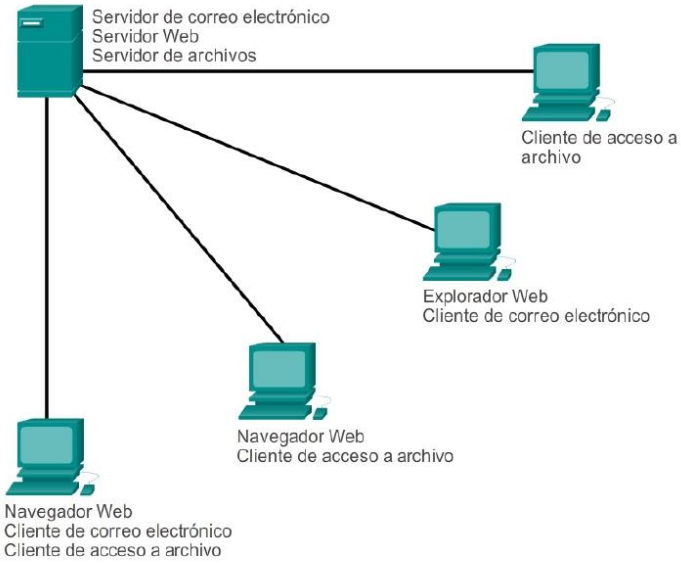
El servidor de correo electrónico ejecuta software de servidor, mientras que los clientes utilizan software cliente de correo electrónico, como Microsoft Outlook, para obtener acceso a los mensajes de correo electrónico que se encuentran en el servidor.

Capítulo 1: Exploración de la red 1.1.2.3 Clientes y servidores (cont.)

Una computadora con software de servidor puede prestar servicios a uno o varios clientes simultáneamente.

Además, una sola computadora puede ejecutar varios tipos de software de servidor. En una oficina pequeña u hogareña, puede ser necesario que una computadora actúe como servidor de archivos, servidor Web y servidor de correo electrónico.

Una sola computadora también puede ejecutar varios tipos de software cliente. Debe haber un software cliente por cada servicio requerido. Si un host tiene varios clientes instalados, puede conectarse a varios servidores de manera simultánea. Por ejemplo, un usuario puede leer su correo electrónico y ver una página Web mientras utiliza el servicio de mensajería instantánea y escucha la radio a través de Internet.



Capítulo 1: Exploración de la red 1.1.2.4 Punto a punto

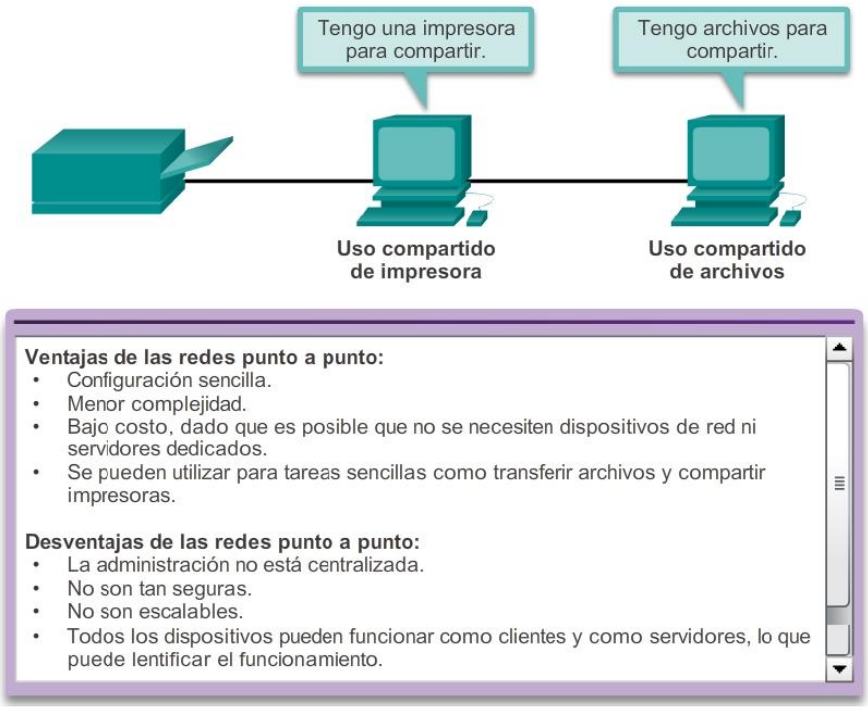
El software de servidor y el de cliente normalmente se ejecutan en computadoras distintas, pero también es posible que una misma computadora cumpla las dos funciones a la vez. En pequeñas empresas y hogares, muchas computadoras funcionan como servidores y clientes en la red. Este tipo de red se denomina red entre pares (peer-to-peer).

La red punto a punto más sencilla consiste en dos computadoras conectadas directamente mediante una conexión por cable o inalámbrica.

También es posible conectar varias PC para crear una red punto a punto más grande, pero para hacerlo se necesita un dispositivo de red, como un hub, para interconectar las computadoras.

La principal desventaja de un entorno punto a punto es que el rendimiento de un host puede verse afectado si éste actúa como cliente y servidor a la vez.

En empresas más grandes, en las que el tráfico de red puede ser intenso, con frecuencia es necesario tener servidores dedicados para poder responder a la gran cantidad de solicitudes de servicio.



Capítulo 1: Exploración de la red 1.2.1.1 Componentes de la red

La ruta que toma un mensaje desde el origen hasta el destino puede ser tan sencilla como un solo cable que conecta una computadora con otra o tan compleja como una red que literalmente abarca el mundo. Esta infraestructura de red es la plataforma que da soporte a la red. Proporciona el canal estable y confiable por el cual se producen las comunicaciones.

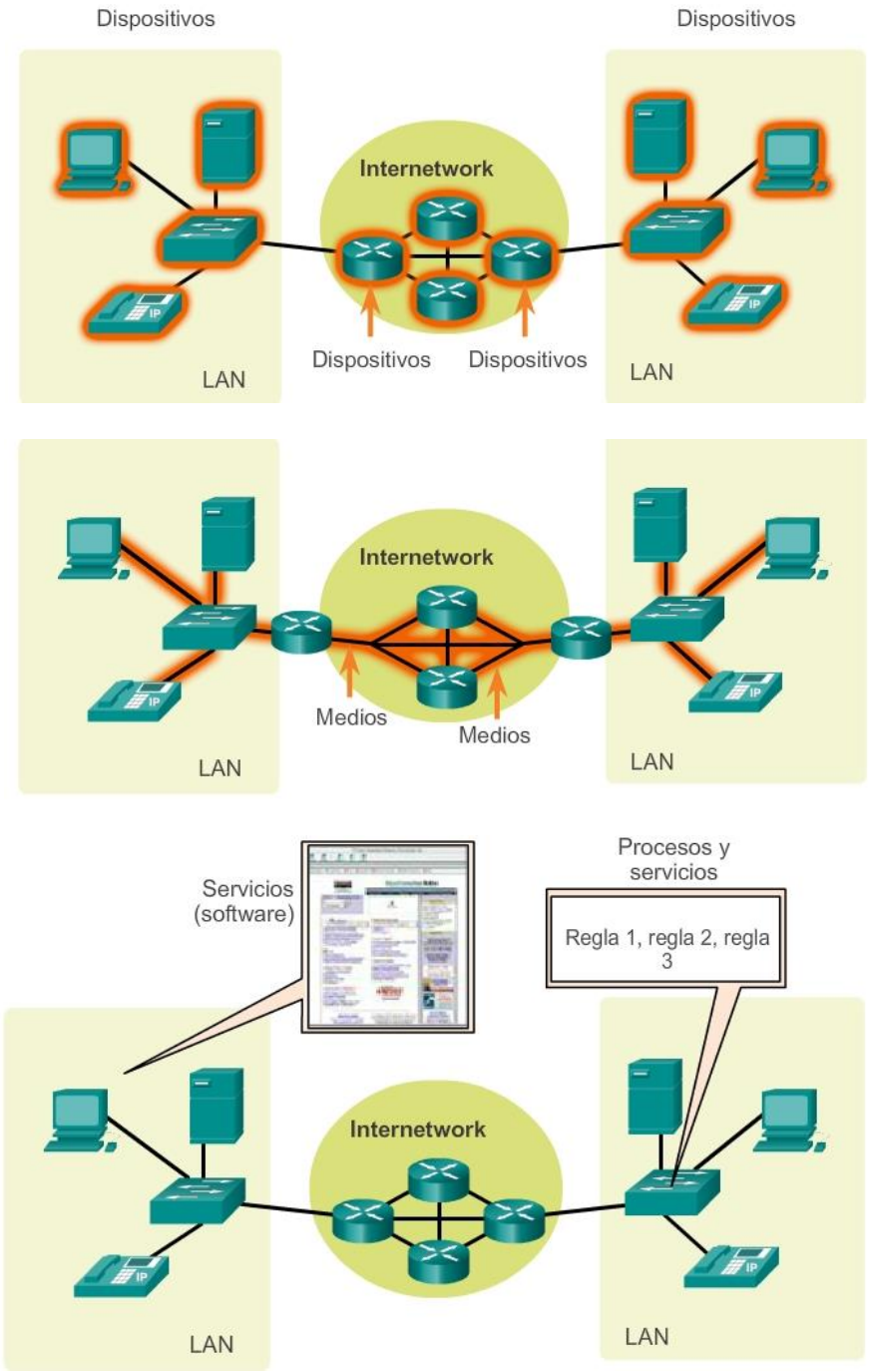
La infraestructura de red contiene tres categorías de componentes de red:

- Dispositivos
- Medios
- Servicios

Los dispositivos y los medios son los elementos físicos o el hardware, de la red. Por lo general, el hardware está compuesto por los componentes visibles de la plataforma de red, como una computadora portátil, una PC, un switch, un router, un punto de acceso inalámbrico o el cableado que se utiliza para conectar esos dispositivos. A veces, puede que algunos componentes no sean visibles. En el caso de los medios inalámbricos, los mensajes se transmiten a través del aire mediante radio frecuencias invisibles u ondas infrarojas.

Los componentes de red se utilizan para proporcionar servicios y procesos, que son los programas de comunicación, denominados “software”, que se ejecutan en los dispositivos conectados en red. Un servicio de red proporciona información en respuesta a una solicitud. Los servicios incluyen muchas de las aplicaciones de red comunes que utilizan las personas a diario, como los servicios de hosting de correo electrónico y web hosting.

Los procesos proporcionan la funcionalidad que direcciona y traslada mensajes a través de la red. Los procesos son menos obvios para nosotros, pero son críticos para el funcionamiento de las redes.



Capítulo 1: Exploración de la red 1.2.1.2 Dispositivos finales

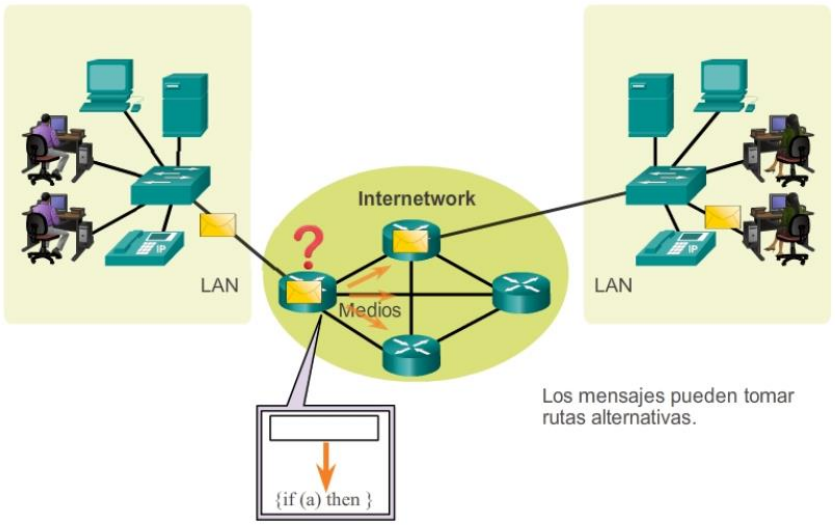
Los dispositivos de red con los que las personas están más familiarizadas se denominan “dispositivos finales” o “hosts”. Estos dispositivos forman la interfaz entre los usuarios y la red de comunicación subyacente.

Algunos ejemplos de dispositivos finales son:

- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)
- Impresoras de red
- Teléfonos VoIP
- Terminales de TelePresence

- Cámaras de seguridad
- Dispositivos portátiles móviles (como smartphones, tablet PC, PDA y lectores inalámbricos de tarjetas de débito y crédito, y escáneres de códigos de barras)

Un dispositivo host es el origen o el destino de un mensaje transmitido a través de la red, tal como se muestra en la animación. Para distinguir un host de otro, cada host en la red se identifica por una dirección. Cuando un host inicia la comunicación, utiliza la dirección del host de destino para especificar a dónde se debe enviar el mensaje.



Los datos se originan con un dispositivo final, fluyen por la red y llegan a un dispositivo final.

Capítulo 1: Exploración de la red 1.2.1.3 Dispositivos de red intermediarios

Los dispositivos intermediarios interconectan dispositivos finales. Estos dispositivos proporcionan conectividad y operan detrás de escena para asegurar que los datos fluyan a través de la red, como se muestra en la animación. Los dispositivos intermediarios conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork.

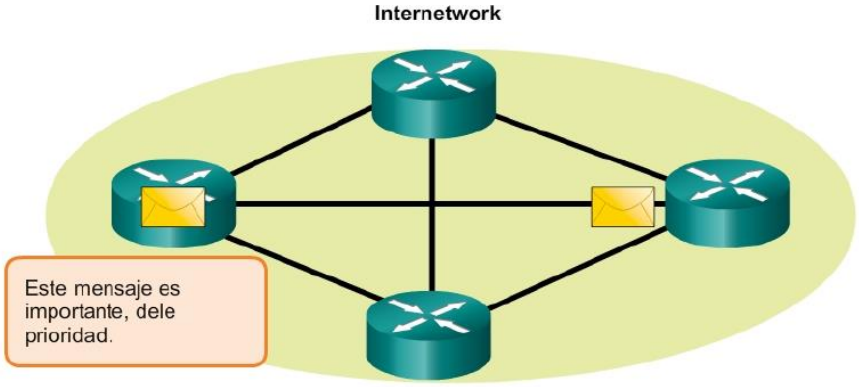
Los siguientes son ejemplos de dispositivos de red intermediarios:

- Acceso a la red (switches y puntos de acceso inalámbrico)
- Internetworking (routers)
- Seguridad (firewalls)

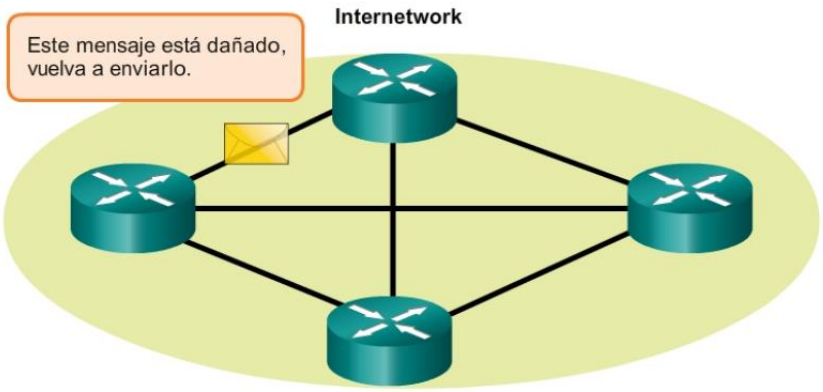
La administración de datos, así como fluye en la red, es también una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red para determinar la ruta que deben tomar los mensajes a través de la red.

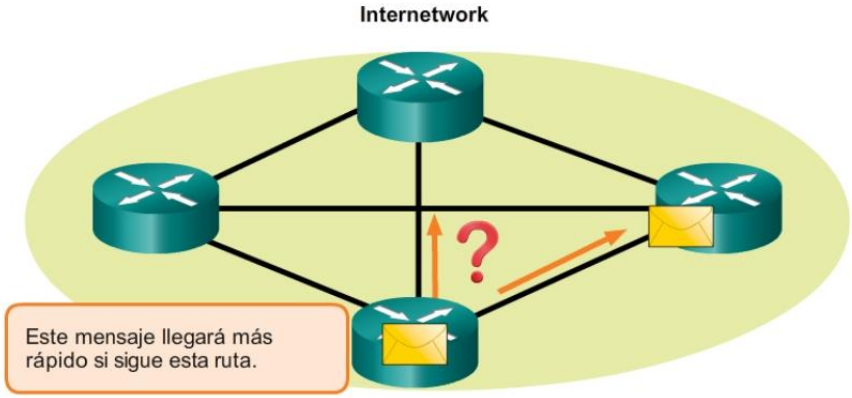
Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones:

- Volver a generar y transmitir las señales de datos.
- Conservar información acerca de las rutas que existen a través de la red y de internetwork.
- Notificar a otros dispositivos los errores y las fallas de comunicación.
- Dirigir los datos a lo largo de rutas alternativas cuando hay una falla en el enlace.
- Clasificar y dirigir los mensajes según las prioridades de calidad de servicio (QoS, Quality of Service).
- Permitir o denegar el flujo de datos de acuerdo con la configuración de seguridad.



Los dispositivos intermediarios dirigen la ruta de los datos, pero no generan contenido de datos ni lo modifican.





Capítulo 1: Exploración de la red 1.2.1.4 Medios de red

La comunicación a través de una red es transportada por un medio. El medio proporciona el canal por el cual viaja el mensaje desde el origen hasta el destino.

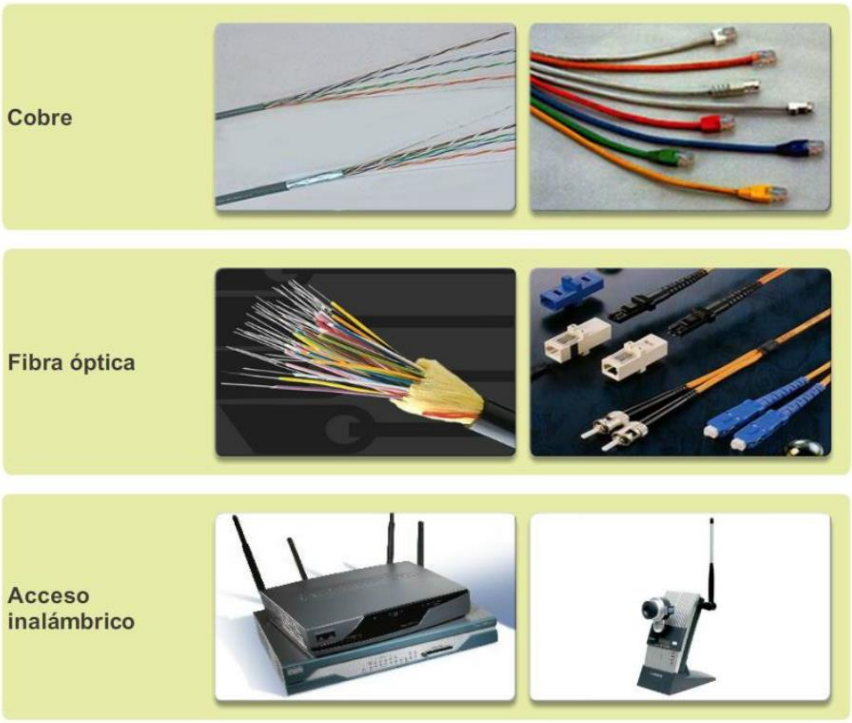
Las redes modernas utilizan principalmente tres tipos de medios para interconectar los dispositivos y proporcionar la ruta por la cual pueden transmitirse los datos. Como se muestra en la ilustración, estos medios son los siguientes:

- Hilos metálicos dentro de cables
- Fibras de vidrio o plástico (cable de fibra óptica)
- Transmisión inalámbrica

La codificación de la señal que se debe realizar para que se transmita el mensaje es diferente para cada tipo de medio. En los hilos metálicos, los datos se codifican dentro de impulsos eléctricos que coinciden con patrones específicos. Las transmisiones por fibra óptica dependen de pulsos de luz, dentro de intervalos de luz visible o infrarroja. En las transmisiones inalámbricas, los patrones de ondas electromagnéticas muestran los distintos valores de bits.

Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin. Los criterios para elegir medios de red son los siguientes:

- La distancia por la que los medios pueden transportar una señal correctamente
- El entorno en el que se instalarán los medios
- La cantidad de datos y la velocidad a la que se deben transmitir
- El costo del medio y de la instalación



Capítulo 1: Exploración de la red 1.2.1.5 Representaciones de red

Para transmitir información compleja, como la presentación de todos los dispositivos y el medio en una internetwork grande, es conveniente utilizar representaciones visuales. Los diagramas permiten comprender fácilmente la forma en la que se conectan los dispositivos en una red grande. Estos diagramas utilizan símbolos para representar los diferentes dispositivos y conexiones que componen una red. Este tipo de representación de una red se denomina “diagrama de topología”.

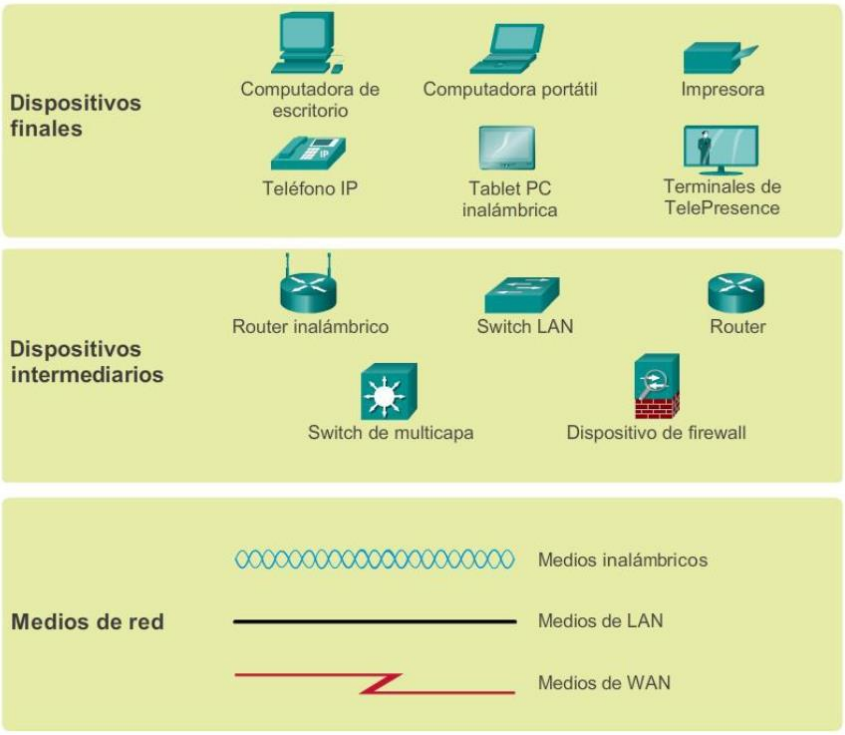
Como cualquier otro lenguaje, el lenguaje de las redes se compone de un conjunto común de símbolos que se utilizan para representar los distintos dispositivos finales, dispositivos de red y medios, como se muestra en la ilustración. La capacidad de reconocer las representaciones lógicas de los componentes físicos de red es fundamental para poder visualizar la organización y el funcionamiento de una red. A lo largo de este curso y de estos laboratorios, aprenderá cómo operan estos dispositivos y cómo realizar tareas de configuración básica en los mismos.

Además de estas representaciones, se utiliza terminología especializada al hablar sobre cómo se conectan estos dispositivos y los medios unos a otros. Algunos términos importantes para recordar son:

- Tarjeta de interfaz de red: una NIC, o adaptador LAN, proporciona la conexión física a la red para la PC u otro dispositivo host. Los medios que realizan la conexión de la PC al dispositivo de red se conectan en la NIC.

- Puerto físico: se trata de un conector o una boca en un dispositivo de red donde se conectan los medios a un host u otro dispositivo de red.

- Interfaz: puertos especializados en un dispositivo de internetworking que se conectan a redes individuales. Puesto que los routers se utilizan para interconectar redes, los puertos de un router se conocen como interfaces de red.



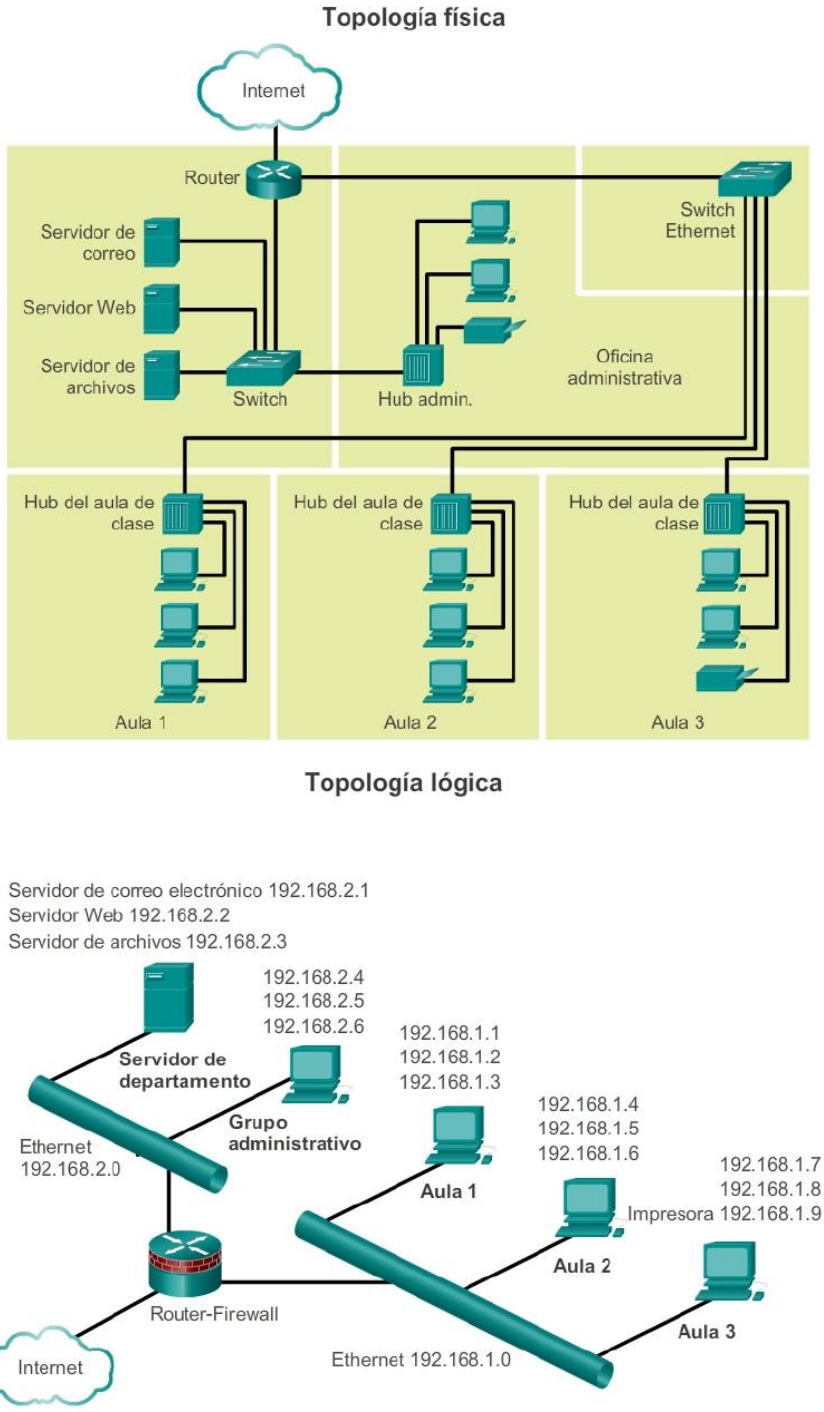
Capítulo 1: Exploración de la red 1.2.1.6 Diagramas de topología

Los diagramas de topología son obligatorios para todos los que trabajan con redes. Estos diagramas proporcionan un mapa visual que muestra cómo está conectada la red.

Existen dos tipos de diagramas de topología:

- Diagramas de topología física: identifican la ubicación física de los dispositivos intermediarios, los puertos configurados y la instalación de los cables.

- Diagramas de topología lógica: identifican dispositivos, puertos y el esquema de direccionamiento IP.



Capítulo 1: Exploración de la red 1.2.2.1 Tipos de red

Las infraestructuras de red pueden variar en gran medida en los siguientes aspectos:

- El tamaño del área que abarcan.
- La cantidad de usuarios conectados.
- La cantidad y los tipos de servicios disponibles.

En la ilustración, se muestran dos de los tipos de infraestructuras de red más comunes:

- Red de área local: las redes de área local (LAN, Local Area Network) son infraestructuras de red que proporcionan acceso a los usuarios y a los dispositivos finales en un área geográfica pequeña.

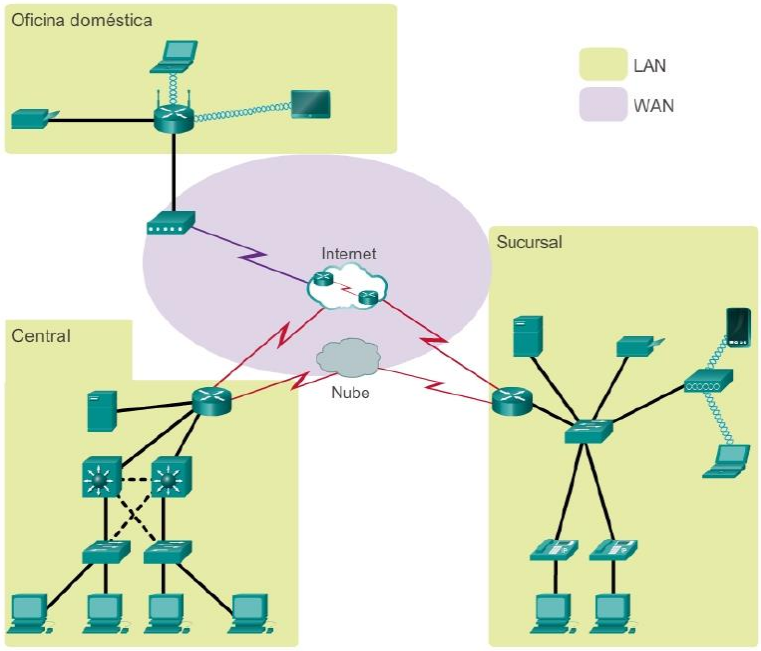
- Red de área extensa: las redes de área extensa (WAN, Wide Area Network) son infraestructuras de red que proporcionan acceso a otras redes en un área geográfica extensa.

Otros tipos de redes incluyen los siguientes:

- Red de área metropolitana: las redes de área metropolitana (MAN, Metropolitan Area Network) son infraestructuras de red que abarcan un área física mayor que la de una LAN pero menor que la de una WAN (por ejemplo, una ciudad). Por lo general, la operación de MAN está a cargo de una única entidad, como una organización de gran tamaño.

- LAN inalámbrica: las LAN inalámbricas (WLAN, Wireless LAN) son similares a las LAN, solo que interconectan de forma inalámbrica a los usuarios y los extremos en un área geográfica pequeña.

- Red de área de almacenamiento: las redes de área de almacenamiento (SAN, Storage area network) son infraestructuras de red diseñadas para admitir servidores de archivos y proporcionar almacenamiento, recuperación y replicación de datos. Estas incluyen los servidores de tecnología avanzada, matrices de varios discos (denominadas “bloques”) y la tecnología de interconexión de canal de fibra.



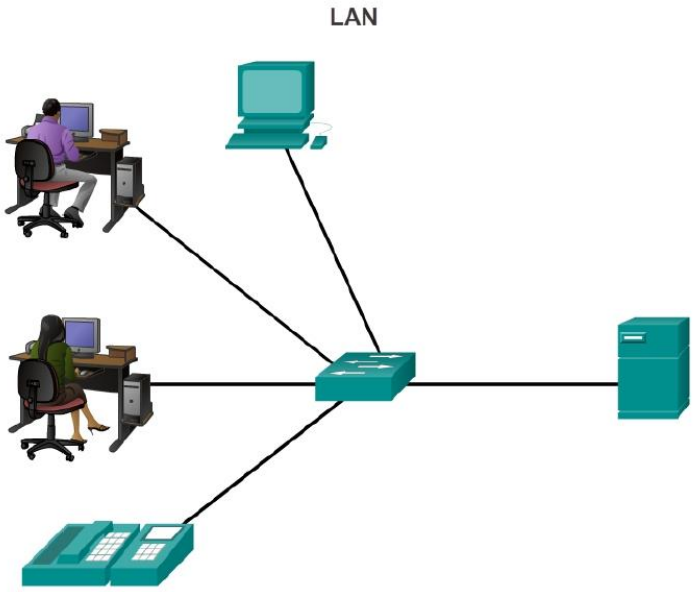
Capítulo 1: Exploración de la red 1.2.2.2 Redes de área local

Las redes de área local (LAN, Local Area Networks) son infraestructuras de red que abarcan un área geográfica pequeña. Las características específicas de las LAN incluyen lo siguiente:

- Las LAN interconectan dispositivos finales en un área limitada, como una casa, un lugar de estudios, un edificio de oficinas o un campus.

- Por lo general, la administración de las LAN está a cargo de una única organización o persona. El control administrativo que rige las políticas de seguridad y control de acceso está implementado en el nivel de red.

- Las LAN proporcionan un ancho de banda de alta velocidad a los dispositivos finales internos y a los dispositivos intermediarios.



Una red que proporciona conectividad a un hogar, un edificio o un campus se considera una LAN.

Capítulo 1: Exploración de la red 1.2.2.3 Redes de área amplia

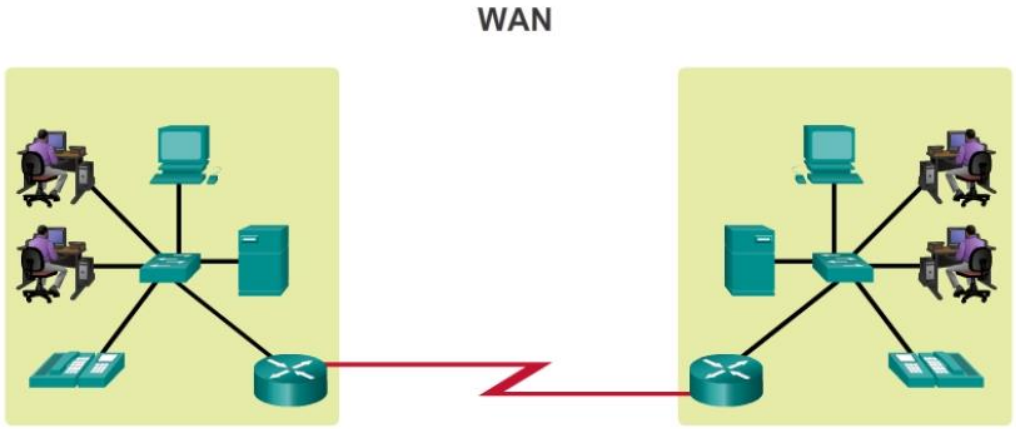
Las redes de área extensa (WAN, Wide Area Networks) son infraestructuras de red que abarcan un área geográfica extensa. Normalmente, la administración de las WAN está a cargo de proveedores de servicios (SP) o proveedores de servicios de Internet (ISP).

Las características específicas de las WAN incluyen lo siguiente:

- Las WAN interconectan LAN a través de áreas geográficas extensas, por ejemplo, entre ciudades, estados, provincias, países o continentes.

- Por lo general, la administración de las WAN está a cargo de varios proveedores de servicios.

- Normalmente, las WAN proporcionan enlaces de velocidad más lenta entre redes LAN.



Las LAN que están separadas por una distancia geográfica se conectan mediante una red conocida como WAN.

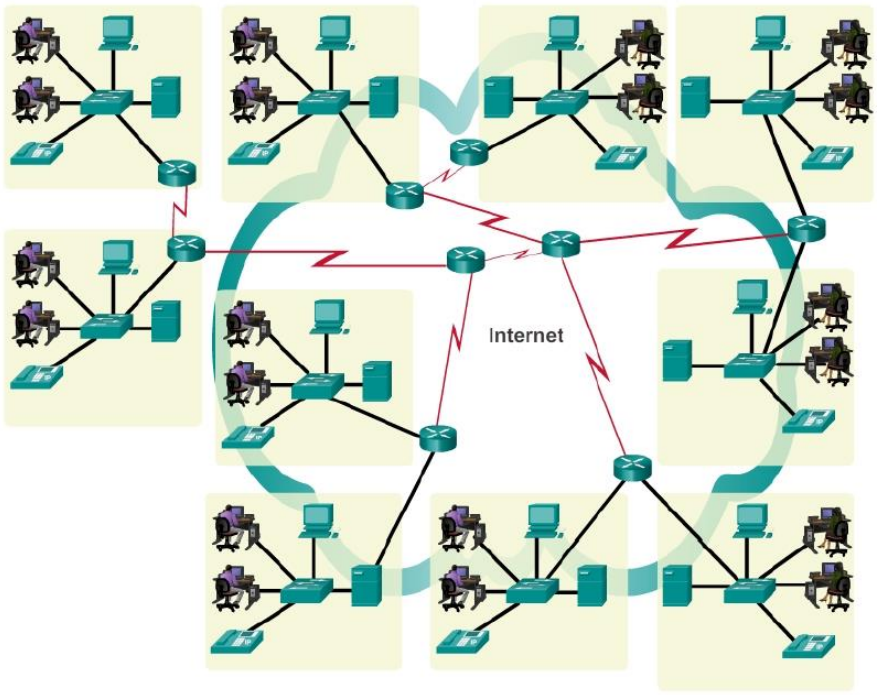
Capítulo 1: Exploración de la red 1.2.3.1 Internet

Aunque el uso de redes LAN o WAN tiene ventajas, la mayoría de las personas necesitan comunicarse con un recurso ubicado en otra red, fuera de la red local del hogar, el campus o la organización. Esto se logra mediante el uso de Internet.

Como se muestra en la ilustración, Internet es una colección mundial de redes interconectadas (abreviado: internetworks o internet), que colaboran para intercambiar información sobre la base de estándares comunes. A través de cables telefónicos, cables de fibra óptica, transmisiones inalámbricas y enlaces satelitales, los usuarios de Internet pueden intercambiar información de diversas formas.

Internet es un conglomerado de redes que no es propiedad de ninguna persona ni de ningún grupo. Para garantizar una comunicación eficaz en esta infraestructura heterogénea, se requiere la aplicación de tecnologías y estándares coherentes y comúnmente reconocidos, así como la cooperación de muchas entidades de administración de redes. Existen organizaciones que se desarrollaron con el fin de ayudar a mantener la estructura y la estandarización de los protocolos y los procesos de Internet. Entre estas organizaciones, se encuentran Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN) e Internet Architecture Board (IAB), entre muchas otras.

Nota: el término “internet” (con “i” minúscula) se utiliza para describir un conjunto de redes interconectadas. Para referirse al sistema global de redes de computadoras interconectadas, o World Wide Web, se utiliza el término “Internet” (con “I” mayúscula).



Las redes LAN y WAN se pueden conectar en internetworks.

Capítulo 1: Exploración de la red 1.2.3.2 Intranets y extranets

Hay otros dos términos que son similares al término “Internet”:

- Intranet
- Extranet

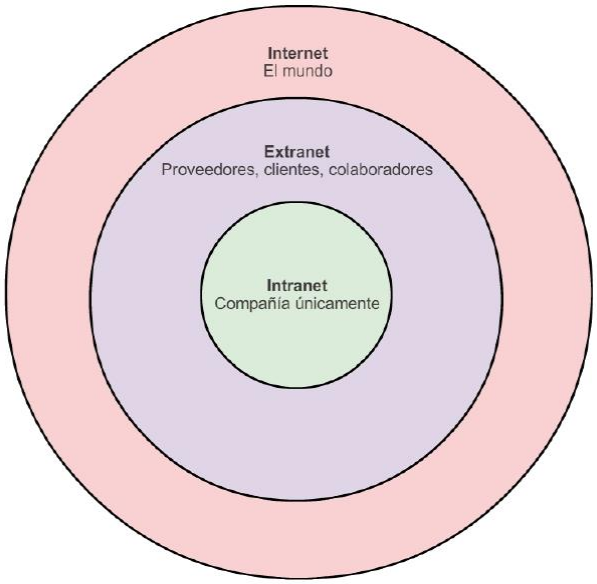
El término “intranet” se suele utilizar para hacer referencia a una conexión privada de redes LAN y WAN que pertenece a una organización y que está diseñada para que solo accedan a ella los miembros y los empleados de la organización u otras personas autorizadas. Básicamente, las intranets son internets a la que solamente se puede acceder desde dentro de la organización.

Las organizaciones pueden publicar en una intranet páginas Web sobre eventos internos, políticas de higiene y seguridad, boletines de personal y directorios telefónicos del personal. Por ejemplo, los lugares de estudios pueden tener intranets que incluyan información sobre los programas de clases, currículos en línea y foros de discusión. Generalmente, las intranets ayudan a eliminar el papeleo y aceleran los flujos de trabajo. El personal que trabaja fuera de la organización puede tener acceso a la intranet mediante conexiones seguras a la red interna.

Es posible que una organización utilice una extranet para proporcionar acceso seguro a las personas que trabajan para otra organización, pero requieren datos de la compañía. Entre los ejemplos de extranets, se incluyen los siguientes:

- Una compañía que proporciona acceso a proveedores y contratistas externos.
- Un hospital que cuenta con un sistema de registro para que los médicos puedan cargar citas con sus pacientes.

- Una secretaría de educación local que proporciona información sobre presupuesto y personal a las escuelas del distrito.



Capítulo 1: Exploración de la red 1.2.4.1 Tecnologías de acceso a Internet

Existen varias formas diferentes de conectar a usuarios y organizaciones a Internet.

Generalmente, los usuarios domésticos, los trabajadores a distancia y las oficinas pequeñas requieren una conexión a un proveedor de servicios de Internet (ISP, Internet Service Provider) para acceder a Internet. Las opciones de conexión varían considerablemente según los ISP y la ubicación geográfica. Sin embargo, las opciones más utilizadas incluyen la banda ancha por cable, la banda ancha por línea de suscriptor digital (DSL, digital subscriber line), las redes WAN inalámbricas y los servicios móviles.

Normalmente, las organizaciones necesitan acceder a otros sitios corporativos y a Internet. Para admitir servicios empresariales, como telefonía IP, videoconferencias y el almacenamiento en centros de datos, se requieren conexiones rápidas.

Por lo general, los proveedores de servicios (SP, service providers) son quienes proporcionan interconexiones de nivel empresarial. Los servicios de nivel empresarial más comunes son DSL empresarial, las líneas arrendadas y la red Metro Ethernet.

Capítulo 1: Exploración de la red 1.2.4.2 Conexión de usuarios remotos a Internet

En la ilustración, se muestran opciones de conexión comunes para los usuarios de oficinas pequeñas y oficinas domésticas, que incluyen las siguientes:

- Cable: por lo general, es un servicio ofrecido por proveedores de servicios de televisión por cable. La señal de datos de Internet se transmite a través del mismo cable coaxial que transporta la señal de televisión por cable. Esta opción proporciona una conexión a Internet permanente y de un ancho de banda elevado. Se utiliza un módem por cable especial que separa la señal de datos de Internet de las otras señales que transporta el cable y proporciona una conexión Ethernet a un equipo host o a una LAN.

- DSL: proporciona una conexión a Internet permanente y de un ancho de banda elevado. Requiere un módem de alta velocidad especial que separa la señal DSL de la señal telefónica y proporciona una conexión Ethernet a un equipo host o a una LAN. La señal DSL se transmite a través de una línea telefónica, que está dividida en tres canales. Uno de los canales se utiliza para llamadas telefónicas de voz. Este canal permite que una persona reciba llamadas telefónicas sin desconectarse de Internet. El segundo es un canal de descarga más rápido y se utiliza para recibir información de Internet.

  El tercer canal se utiliza para enviar o subir información. Por lo general, este canal es un poco más lento que el canal de descarga. La calidad y la velocidad de la conexión DSL dependen principalmente de la calidad de la línea telefónica y de la distancia a la que se encuentra la oficina central de la compañía telefónica. Cuanto más lejos esté de la oficina central, más lenta será la conexión.

- Datos móviles: el acceso a Internet por datos móviles se logra mediante una red de telefonía celular. Puede obtener acceso a Internet por datos móviles en cualquier lugar donde tenga cobertura de telefonía móvil. El rendimiento se verá limitado por las capacidades del teléfono y la torre de telefonía móvil a la que se conecte. La disponibilidad del acceso a Internet por datos móviles es una gran ventaja para las áreas que no tienen acceso a otro tipo de conectividad a Internet, o para personas que van de un lado a otro.

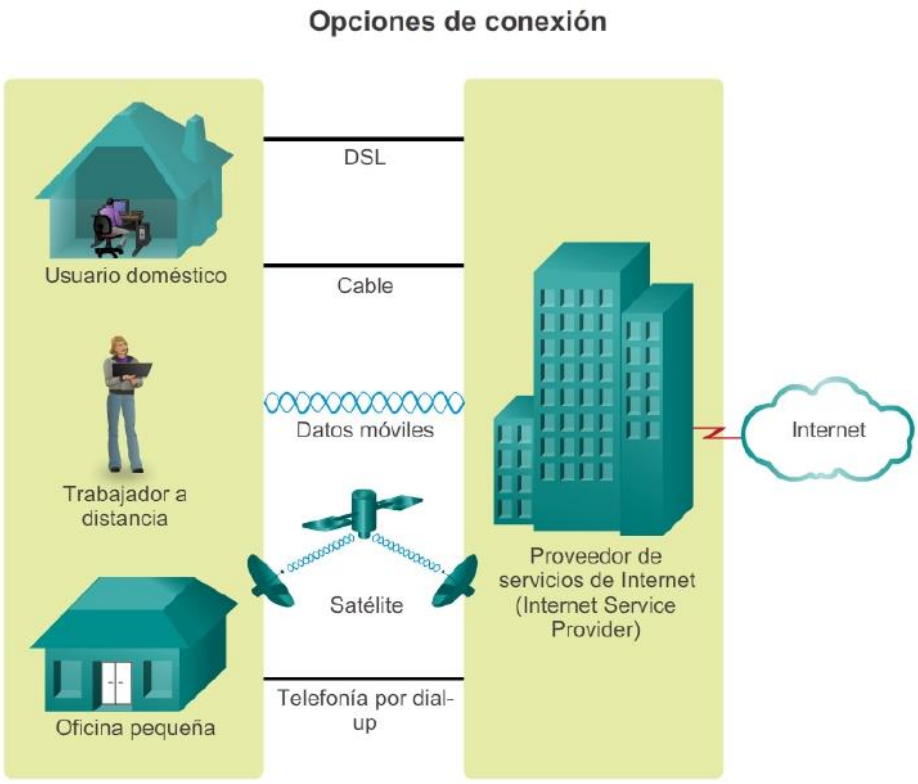
- Satelital: el servicio satelital es una buena opción para los hogares o las oficinas que no tienen acceso a DSL o cable. Las antenas parabólicas requieren una línea de vista despejada al satélite, por lo que no son adecuadas para zonas muy boscosas o lugares que posean algún otro tipo de obstrucción aérea. Las velocidades varían según el contrato, pero suelen ser buenas. Los costos de equipos e instalación pueden ser elevados (consulte con el proveedor para conocer las ofertas especiales) y luego se paga una tarifa mensual módica. La disponibilidad de acceso a Internet satelital es una gran ventaja para las áreas que no tienen acceso a otro tipo de conectividad a Internet.

- Telefónica por dial-up: es una opción de bajo costo que funciona con cualquier línea telefónica y un módem. Para conectar al ISP, el usuario llama al número telefónico de acceso del ISP. El ancho de banda que proporciona una conexión por módem dial-up es bajo y, por lo general, no es suficiente para trasferencias de datos masivas, si bien es útil para acceso móvil durante viajes. La opción de conexión por módem dial-up solo se debe considerar cuando no haya opciones de conexión más veloces disponibles.

Cada vez es más común que los hogares y las oficinas pequeñas se conecten directamente mediante cables de fibra óptica. Esto permite que los proveedores de servicios de Internet proporcionen velocidades de ancho de banda más elevadas y admitan más servicios, como Internet, teléfono y TV.

La oferta de opciones de conexión varía según la ubicación geográfica y la disponibilidad de proveedores de servicios.

¿Con qué opciones cuenta para conectarse a Internet?



Capítulo 1: Exploración de la red 1.2.4.3 Conexión de empresas a Internet

Las opciones de conexión corporativas difieren de las opciones que tienen los usuarios domésticos. Es posible que las empresas requieran un ancho de banda mayor y dedicado, además de servicios administrados. Las opciones de conexión disponibles varían según la cantidad de proveedores de servicios que haya en las cercanías.

En la ilustración, se muestran las opciones de conexión comunes para las organizaciones, que incluyen las siguientes:

- Línea arrendada dedicada: se trata de una conexión dedicada que va del proveedor de servicios a las instalaciones del cliente. Las líneas arrendadas son circuitos reservados reales que conectan oficinas que están separadas geográficamente para propósitos de comunicaciones por voz o redes de datos privados. Normalmente, los circuitos se alquilan por una tarifa mensual o anual, por lo que suele ser una opción costosa.

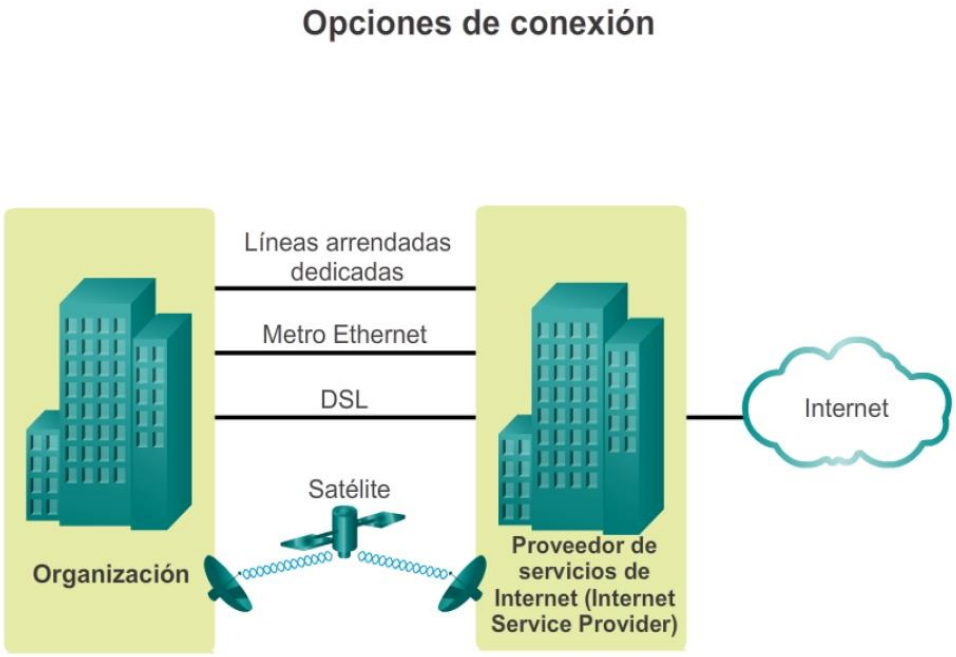
  En Norteamérica, los circuitos comunes de línea arrendada incluyen las opciones T1 (1,54 Mb/s) y T3 (44,7 Mb/s), mientras que, en otras partes del mundo, están disponibles las opciones E1 (2 Mb/s) y E3 (34 Mb/s).

- Red Metro Ethernet: normalmente, Metro Ethernet es un servicio disponible desde el proveedor a las instalaciones del cliente mediante una conexión dedicada de cable de cobre o de fibra óptica que proporciona velocidades de ancho de banda de 10 Mb/s a 10 Gb/s. En muchos casos, la opción de Ethernet por cobre (EoC, Ethernet over Copper) es más económica que el servicio de Ethernet por fibra óptica, es de amplia disponibilidad y alcanza velocidades de hasta 40 Mbps. Sin embargo, el servicio de Ethernet por cobre se ve limitado por la distancia. El servicio de Ethernet por fibra óptica ofrece las conexiones más rápidas que hay disponibles por un precio por megabit económico. Desafortunadamente, todavía hay muchas áreas donde el servicio no está disponible.

- DSL: el servicio de DSL empresarial está disponible en diversos formatos. Una opción muy utilizada es la línea de suscriptor digital simétrica (SDSL, Symmetric Digital Subscriber Lines), que es similar a la DSL asimétrica (ADSL, Asymmetric Digital Subscriber Line), pero proporciona las mismas velocidades de subida y descarga. El servicio ADSL está diseñado para proporcionar un ancho de banda con velocidades descendentes y ascendentes diferentes. Por ejemplo, un cliente con acceso a Internet puede tener velocidades descendentes de 1,5 Mbps a 9 Mbps, mientras que el ancho de banda ascendente varía de 16 kbps a 640 kbps. Las transmisiones por ADSL funcionan a distancias de hasta 18 000 pies (5488 metros) a través de un único par trenzado de cobre.

- Satelital: el servicio satelital puede proporcionar una conexión cuando no hay soluciones de conexión por cable disponibles. Las antenas parabólicas requieren una línea de vista despejada al satélite. Los costos de equipos e instalación pueden ser elevados y luego se paga una tarifa mensual módica. Las conexiones suelen ser más lentas y menos confiables que las de vía terrestre, lo que la convierte en una alternativa menos atractiva.

La oferta de opciones de conexión varía según la ubicación geográfica y la disponibilidad de proveedores de servicios.



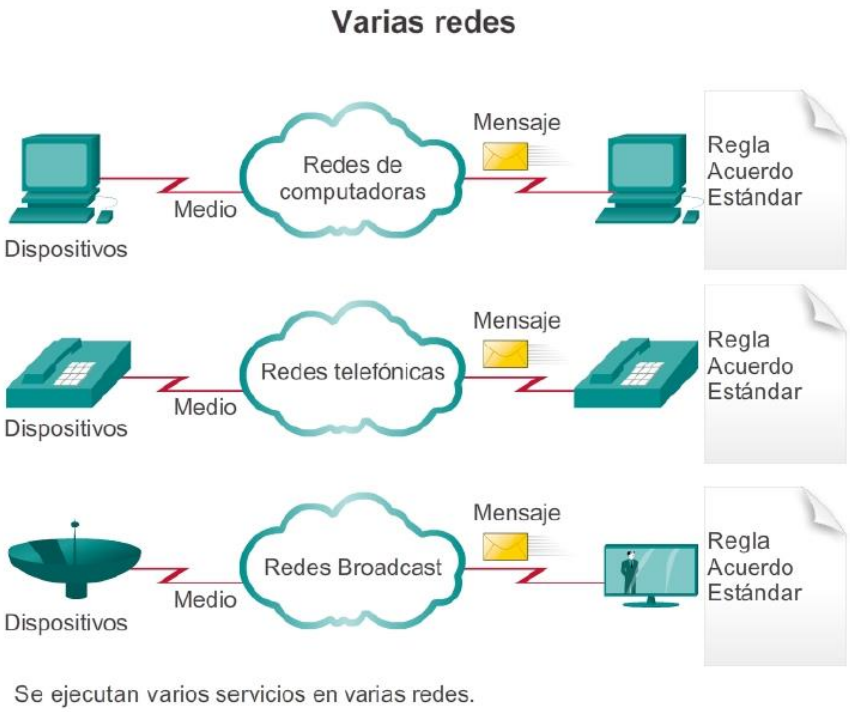
Capítulo 1: Exploración de la red 1.3.1.1 La red convergente

Las redes modernas están en constante evolución para satisfacer las demandas de los usuarios. Las primeras redes de datos estaban limitadas a intercambiar información con base en caracteres entre sistemas informáticos conectados. Las redes tradicionales de teléfono, radio y televisión se mantenían separadas de las redes de datos. En el pasado, cada uno de estos servicios necesitaba una red dedicada, con distintos canales de comunicación y diferentes tecnologías para transportar una señal de comunicación específica. Cada servicio tenía su propio conjunto de reglas y estándares para asegurar la comunicación satisfactoria.

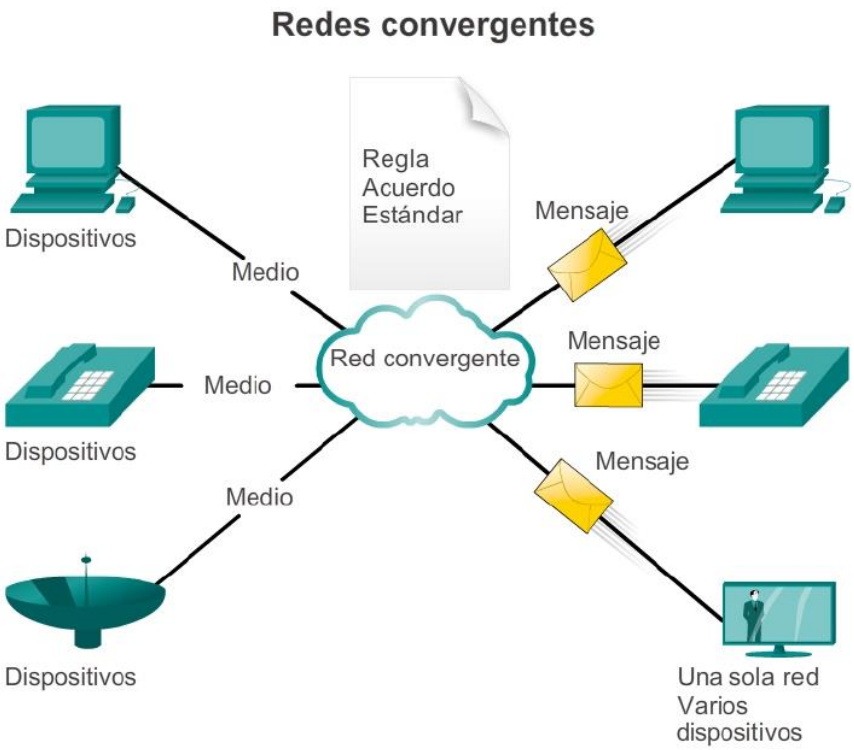
Piense en una escuela construida hace cuarenta años. En ese entonces, las aulas contaban con conexiones por cable para la red de datos, la red telefónica y la red de video para los televisores. Estas redes separadas eran dispares; es decir, no podían comunicarse entre sí, como se muestra en la figura 1.

Los avances en la tecnología nos permiten consolidar estos tipos de redes diferentes en una plataforma conocida como “red convergente”. A diferencia de las redes dedicadas, las redes convergentes pueden transmitir voz, streams de video, texto y gráficos entre diferentes tipos de dispositivos utilizando el mismo canal de comunicación y la misma estructura de red, como se muestra en la figura 2. Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona accesos a una amplia variedad de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

En las redes convergentes, sigue habiendo muchos puntos de contacto y muchos dispositivos especializados, como computadoras personales, teléfonos, televisores y tablet PC, pero hay una infraestructura de red común. Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación.



Se ejecutan varios servicios en varias redes.



Las redes de datos convergentes transportan varios servicios en una red.

Capítulo 1: Exploración de la red 1.3.1.2 Planificación para el futuro

La convergencia de los diferentes tipos de redes de comunicación en una plataforma representa la primera fase en la creación de la red inteligente de información. En la actualidad nos encontramos en esta fase de evolución de la red. La próxima fase será consolidar no sólo los diferentes tipos de mensajes en una única red, sino también consolidar las aplicaciones que generan, transmiten y aseguran los mensajes en los dispositivos de red integrados.

No sólo la voz y el video se transmitirán mediante la misma red, sino que los dispositivos que realizan la conmutación de teléfonos y el broadcasting de videos serán los mismos dispositivos que enrutan los mensajes en la red. La plataforma de comunicaciones que resulta brinda una funcionalidad de alta calidad de las aplicaciones a un costo reducido.

El paso al que avanza el desarrollo de nuevas y emocionantes aplicaciones de red convergentes se puede atribuir al rápido crecimiento y expansión de Internet. Con apenas unos 10 000 millones de elementos actualmente conectados en todo el mundo —de un total de 1,5 billones—, hay un gran potencial para conectar aquello que está desconectado a través de IdT. Esta expansión creó un público más amplio para cualquier mensaje, producto o servicio que se pueda entregar.

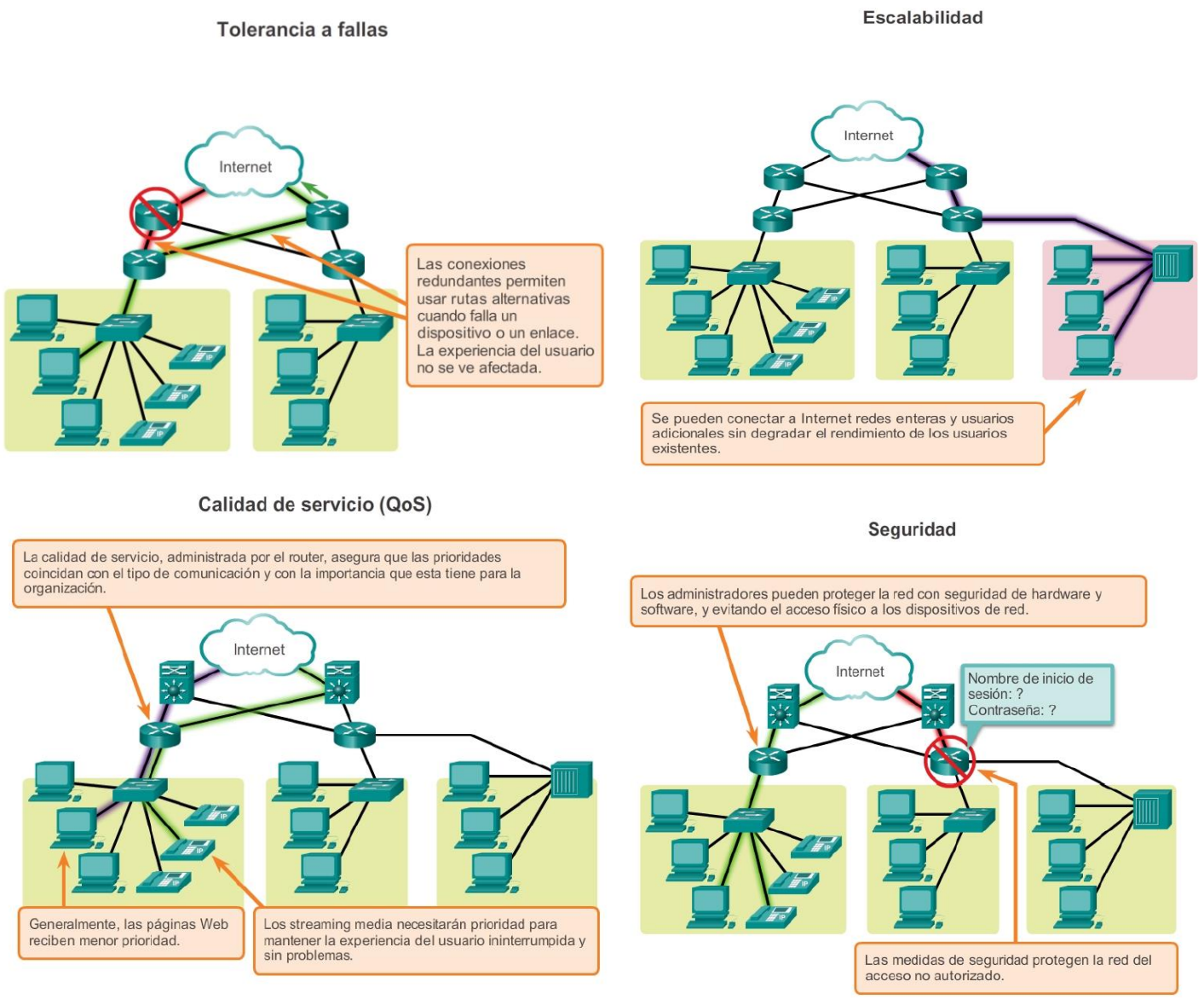
Los mecanismos y procesos subyacentes que impulsan este crecimiento explosivo dieron lugar a una arquitectura de red que es capaz tanto de admitir cambios como de crecer. Como plataforma tecnológica que se puede aplicar a la vida, al aprendizaje, al trabajo y al juego en la red humana, la arquitectura de red de Internet se debe adaptar a los constantes cambios en los requisitos de seguridad y de servicio de alta calidad.

Capítulo 1: Exploración de la red 1.3.2.1 La arquitectura de la red que da soporte

Las redes deben admitir una amplia variedad de aplicaciones y servicios, así como funcionar a través de los distintos tipos de cables y dispositivos que componen la infraestructura física. En este contexto, el término “arquitectura de red” se refiere a las tecnologías que dan soporte a la infraestructura y a los servicios y las reglas, o protocolos, programados que trasladan los mensajes a través de la red.

A medida que las redes evolucionan, descubrimos que existen cuatro características básicas que las arquitecturas subyacentes necesitan para cumplir con las expectativas de los usuarios:

- Tolerancia a fallas (figura 1)
- Escalabilidad (figura 2)
- Calidad de servicio (QoS) (figura 3)
- Seguridad (figura 4)



Capítulo 1: Exploración de la red 1.3.2.2 Tolerancia a fallas en redes conmutadas por circuitos

Tolerancia a fallas

Se espera que Internet esté siempre disponible para los millones de usuarios que confían en ese servicio. Para lograrlo, se requiere una arquitectura de red desarrollada para tener tolerancia a fallas. Una red con tolerancia a fallas es una que limita el impacto de las fallas, de modo que la cantidad de dispositivos afectados sea la menor posible. Además, se arma de forma tal que permita una recuperación rápida cuando se produce una falla. Estas redes dependen de varias rutas entre el origen y el destino del mensaje. Si falla una ruta, los mensajes se pueden enviar inmediatamente por otro enlace. El hecho de que haya varias rutas que conducen a un destino se denomina “redundancia”.

Redes orientadas a la conexión y conmutadas por circuitos

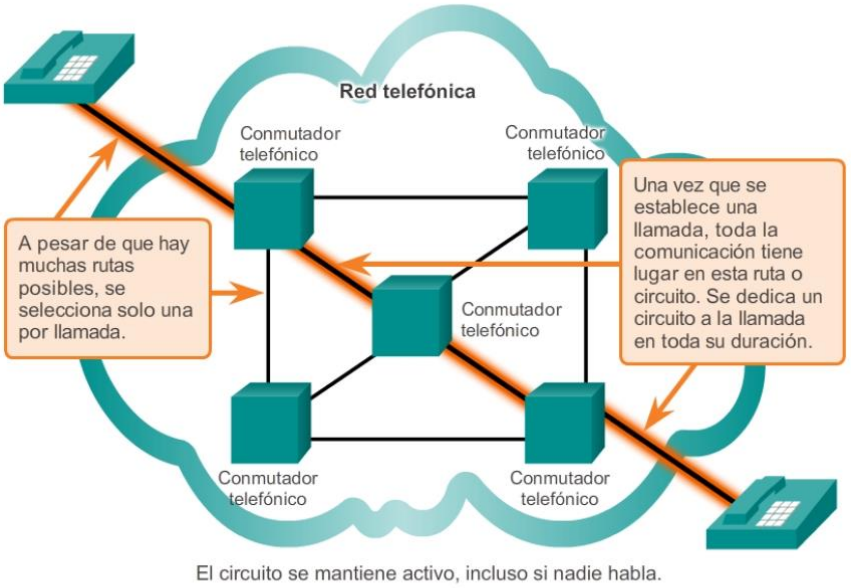
Para comprender la necesidad de redundancia, podemos tomar como ejemplo el funcionamiento de los primeros sistemas telefónicos. Cuando se realizaba una llamada con un teléfono tradicional, esta primero se sometía un proceso de configuración. Este proceso identificaba las ubicaciones de conmutación telefónica de la persona que realizaba la llamada (origen) y del teléfono que recibía la llamada (destino). Se creaba una ruta temporal, o circuito, para el tiempo que durara la llamada telefónica.

Si fallaba un enlace o un dispositivo en el circuito, la llamada se interrumpía. Para volver a establecer la conexión, se debía realizar una nueva llamada con un nuevo circuito.

Este proceso de conexión se conoce como “proceso de conmutación por circuitos” y se muestra en la ilustración.

Muchas redes conmutadas por circuitos dan prioridad a las conexiones de circuitos existentes, a expensas de las solicitudes de nuevos circuitos. Una vez establecido el circuito, este permanece conectado y los recursos se utilizan hasta que una de las partes desconecta la llamada, aunque no exista comunicación entre las personas en ningún extremo de la llamada. Debido a que solo se puede crear una cantidad finita de circuitos, es posible recibir un mensaje que indique que todos los circuitos están ocupados y que no se puede realizar una llamada. La razón por la que la tecnología de conmutación por circuitos no es óptima para Internet radica en el costo de crear varias rutas alternativas con suficiente capacidad para admitir una gran cantidad de circuitos simultáneos y las tecnologías necesarias para recrear de forma dinámica los circuitos interrumpidos en caso de falla.

Conmutación por circuitos en una red telefónica



Existen muchísimos circuitos, pero son una cantidad finita. Durante los períodos de demanda pico, es posible que se denieguen algunas llamadas.

Capítulo 1: Exploración de la red 1.3.2.3 Tolerancia a fallas en redes conmutadas por paquetes

Packet-Switched Networks

Durante la búsqueda de una red con mayor tolerancia a fallas, los primeros diseñadores de Internet investigaron las redes conmutadas por paquetes. La premisa para este tipo de red es que un único mensaje se puede dividir en varios bloques de mensajes. Cada bloque contiene información de direccionamiento que indica el punto de origen y el destino final. Con esta información incorporada, estos bloques de mensajes, llamados “paquetes”, se pueden enviar a través de la red mediante varias rutas y se pueden volver a unir para formar el mensaje original al llegar a destino, como se muestra en la ilustración.

Los dispositivos que están dentro de la red normalmente desconocen el contenido de los paquetes individuales. La única información visible son las direcciones de origen y destino final. Por lo general, a estas

direcciones se las conoce como “direcciones IP” y se expresan en formato decimal punteado, por ejemplo, 10.10.10.10. Cada paquete se envía en forma independiente desde una ubicación a otra.

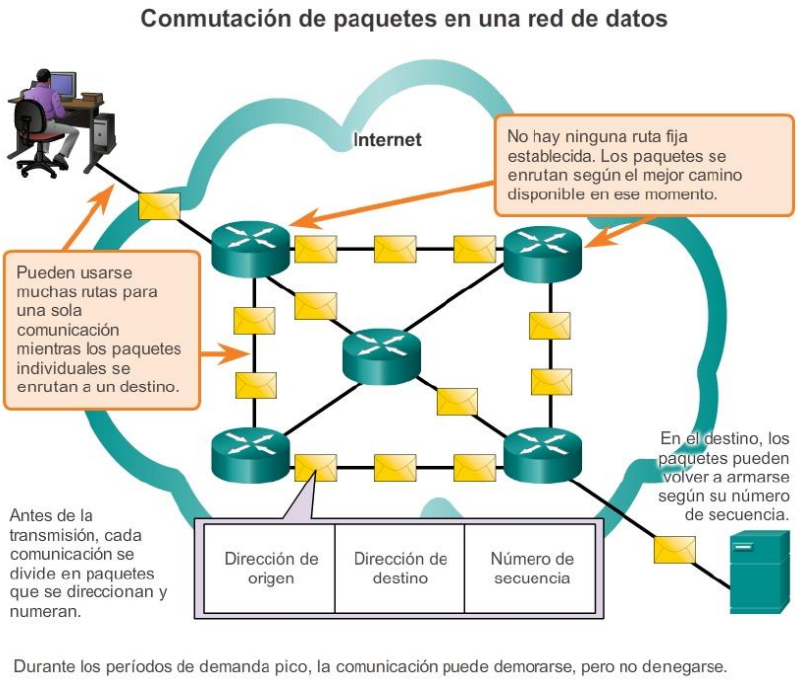
En cada ubicación, se decide qué ruta utilizar para enviar el paquete al destino final. Esto se asemeja a escribirle un mensaje largo a un amigo, dividido en diez postales. Cada postal tiene la dirección de destino del destinatario. A medida que las postales avanzan a través del sistema de correo postal, se utiliza la dirección de destino para determinar la siguiente ruta que deben seguir. Finalmente, se entregarán en la dirección que figura en las postales.

Si una ruta utilizada anteriormente ya no está disponible, la función de enrutamiento puede elegir en forma dinámica la próxima ruta disponible. Debido a que los mensajes se envían por partes, en lugar de hacerlo como un único mensaje completo, los pocos paquetes que pueden perderse pueden volverse a transmitir al destino por una ruta diferente. En muchos casos, el dispositivo de destino desconoce si ocurrió una falla o un enrutamiento. Siguiendo la analogía de la postal, si una de las postales se pierde en el camino, solo es necesario volver a enviar esa tarjeta.

En una red conmutada por paquetes no existe la necesidad de un circuito reservado y simple de extremo a extremo. Cualquier parte del mensaje puede enviarse a través de la red utilizando una ruta disponible. Además, los paquetes que contienen las partes de los mensajes de diferentes orígenes pueden viajar por la red al mismo tiempo.

Al proporcionar una forma dinámica de utilizar rutas redundantes sin la intervención del usuario, Internet se convirtió en un método de comunicación con tolerancia a fallas. En nuestra analogía del correo, mientras la postal viaja a través del sistema de correo postal, comparte el transporte con otras postales, cartas y paquetes. Por ejemplo, es posible que se coloque una de las postales en un avión, junto con otros paquetes y cartas que se transportan hacia su destino final.

Aunque las redes de conmutación por paquetes sin conexión son la principal infraestructura de Internet en la actualidad, los sistemas orientados a la conexión, como el sistema de telefonía de conmutación por circuitos, tienen ciertas ventajas. Debido a que los recursos de las diferentes ubicaciones de conmutación están destinados a proporcionar un número determinado de circuitos, pueden garantizarse la calidad y la consistencia de los mensajes transmitidos en una red orientada a la conexión. Otro beneficio es que el proveedor del servicio puede cobrar a los usuarios de la red durante el periodo de tiempo en que la conexión se encuentra activa. La capacidad de cobrar a los usuarios para conexiones activas a través de la red es una premisa fundamental de la industria del servicio de telecomunicaciones.



Capítulo 1: Exploración de la red 1.3.2.4 Redes escalables

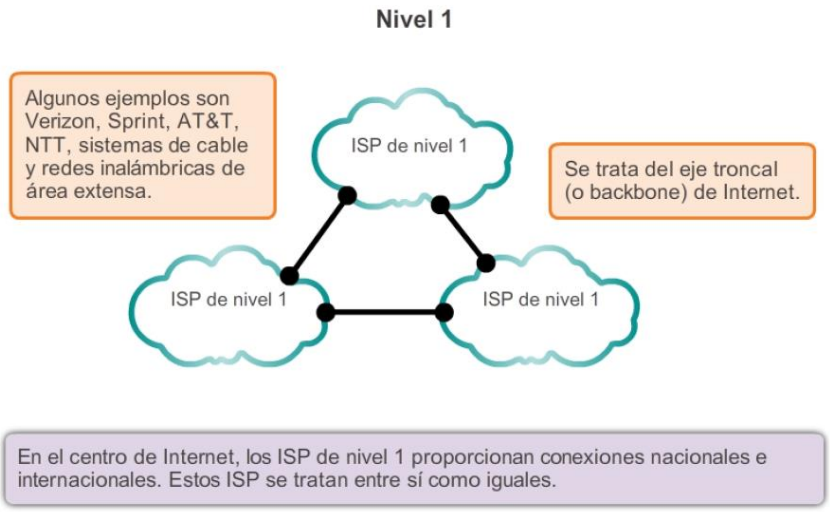
Escalabilidad

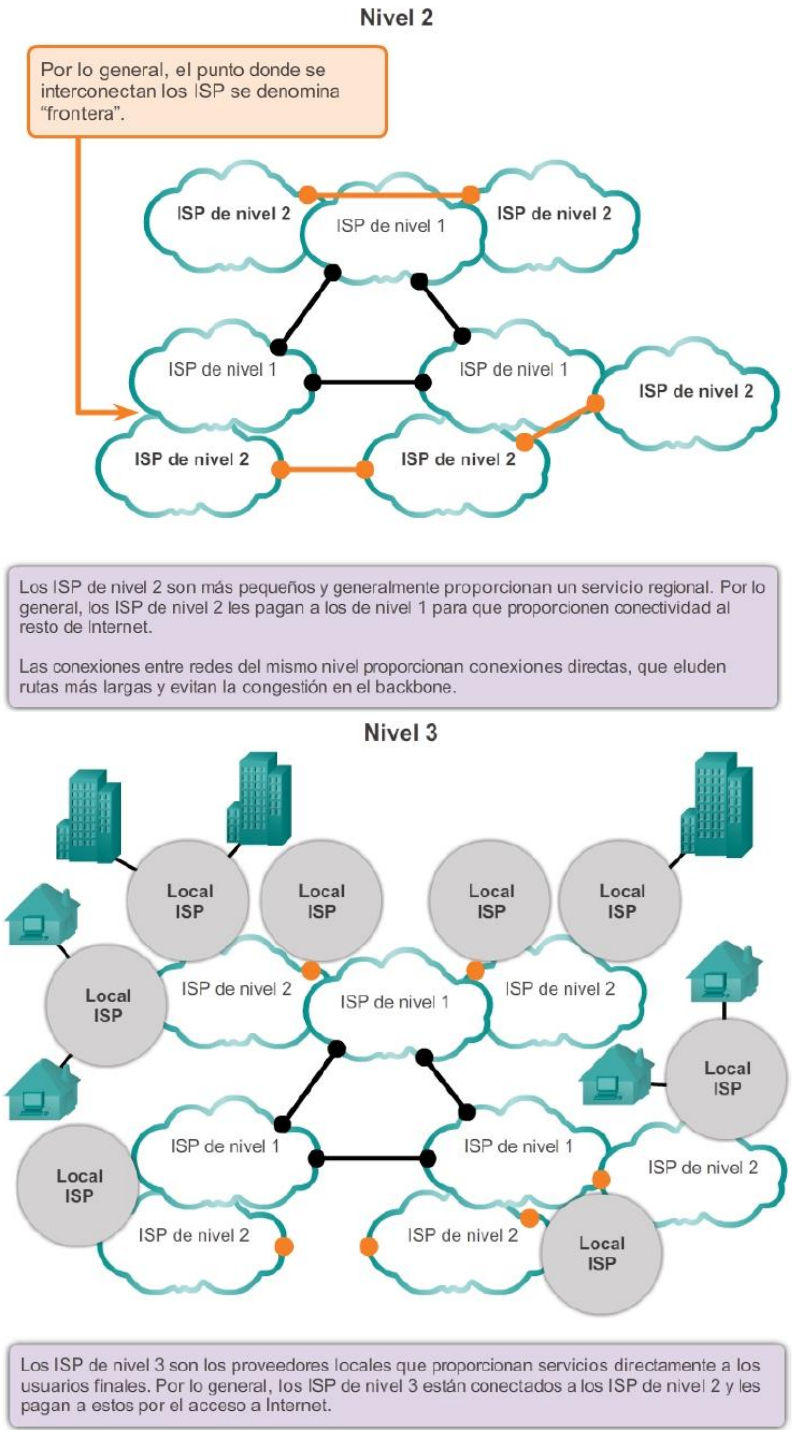
Miles de nuevos usuarios y proveedores de servicio se conectan a Internet cada semana. Para que Internet admita esta cantidad de usuarios en rápido crecimiento, debe ser escalable. Una red escalable puede expandirse rápidamente para admitir nuevos usuarios y aplicaciones sin afectar el rendimiento del servicio enviado a los usuarios actuales. En las ilustraciones, se muestra la estructura de Internet.

El hecho de que Internet se expanda a esta velocidad, sin afectar seriamente el rendimiento de usuarios individuales, es una función del diseño de los protocolos y de las tecnologías subyacentes sobre la cual se construye. Internet tiene una estructura jerárquica en capas para brindar servicios de direccionamiento, nomenclatura y conectividad. Como resultado, el tráfico de redes destinado para servicios regionales y locales no necesita cruzar a un punto central para su distribución. Los servicios comunes se pueden duplicar en diferentes regiones, por ello mantienen fuera el tráfico de las redes backbone de alto nivel.

La escalabilidad también se refiere a la capacidad de admitir nuevos productos y aplicaciones. Aunque no hay una organización única que regule Internet, las numerosas redes individuales que proporcionan conectividad a Internet y cooperan para cumplir con los estándares y protocolos aceptados. La observancia de los estándares permite a los fabricantes de hardware y software concentrarse en el desarrollo de productos y la mejora en las áreas de rendimiento y capacidad, con la certeza de que los nuevos productos pueden integrarse a la infraestructura existente y mejorarla.

La arquitectura de Internet actual, altamente escalable, no siempre puede mantener el ritmo de la demanda del usuario. Los nuevos protocolos y estructuras de direccionamiento están en desarrollo para cumplir con el ritmo acelerado al cual se agregan los servicios y aplicaciones de Internet.


Nivel 1
Algunos ejemplos son Verizon, Sprint, AT&T, NTT, sistemas de cable y redes inalámbricas de área extensa.
ISP de nivel 1
Se trata del eje troncal (o backbone) de Internet.
ISP de nivel 1
ISP de nivel 1
En el centro de Internet, los ISP de nivel 1 proporcionan conexiones nacionales e internacionales. Estos ISP se tratan entre sí como iguales.



Capítulo 1: Exploración de la red 1.3.2.5 Provisión de QoS

Calidad de servicio

La calidad de servicio (QoS, Quality of Service) también es un requisito cada vez más importante para las redes hoy en día. Las nuevas aplicaciones disponibles para los usuarios en internetworks, como las transmisiones de voz y de video en vivo, que se muestran en la figura 1, generan expectativas más altas sobre la calidad de los servicios que se proporcionan. ¿Alguna vez intentó mirar un video con interrupciones y pausas constantes?

Las redes deben proporcionar servicios predecibles, mensurables y, en ocasiones, garantizados. La arquitectura de red conmutada por paquetes no garantiza que todos los paquetes que conforman un mensaje en particular lleguen a tiempo y en el orden correcto, ni tampoco garantiza la llegada.

Las redes también necesitan mecanismos para administrar el tráfico de redes congestionado. El ancho de banda es la medida de la capacidad de transmisión de datos de la red. En otras palabras, ¿cuánta información se puede transmitir en un lapso determinado? El ancho de banda de la red es la medida de la cantidad de bits que se pueden transmitir en un segundo, es decir, bits por segundo (bps). Cuando se producen intentos de comunicaciones simultáneas a través de la red, la demanda de ancho de banda puede exceder su disponibilidad, lo que provoca congestión en la red. Simplemente, la red tiene más bits para transmitir que lo que el ancho de banda del canal de comunicación puede entregar.

En la mayoría de los casos, cuando el volumen de los paquetes es mayor que lo que se puede transportar a través de la red, los dispositivos colocan los paquetes en cola, o en espera, en la memoria hasta que haya recursos disponibles para transmitirlos, como se muestra en la figura 2. Los paquetes en cola causan retrasos, dado que los nuevos paquetes no se pueden transmitir hasta que no se hayan procesado los anteriores. Si el número de paquetes en cola continúa aumentando, las colas de la memoria se llenan y los paquetes se descartan.

El secreto para ofrecer una solución de calidad de aplicación de extremo a extremo exitosa es lograr la QoS necesaria mediante la administración de los parámetros de retraso y de pérdida de paquetes en una red. Una de las formas en que esto se puede lograr es mediante la clasificación. Para crear clasificaciones de QoS de datos, utilizamos una combinación de características de comunicación y la importancia relativa que se asigna a la aplicación, como se muestra en la figura 3. Luego, incluimos todos los datos en la misma clasificación sobre la base de las mismas reglas. Por ejemplo, el tipo de comunicaciones en las que el tiempo es un factor importante, como las transmisiones de voz, se clasificaría de forma distinta que las comunicaciones que pueden tolerar retrasos, como la transferencia de archivos.

Algunas de las decisiones prioritarias para una organización pueden ser:

- Comunicaciones dependientes del factor tiempo: aumento de la prioridad para servicios como la telefonía o la distribución de videos.
- Comunicaciones independientes del factor tiempo: disminución de la prioridad para la recuperación de páginas Web o correos electrónicos.
- Suma importancia a la organización: aumento de la prioridad de los datos de control de producción o transacciones comerciales.
- Comunicaciones no deseadas: disminución de la prioridad o bloqueo de la actividad no deseada, como intercambio de archivos punto a punto o entretenimiento en vivo.

Redes convergentes

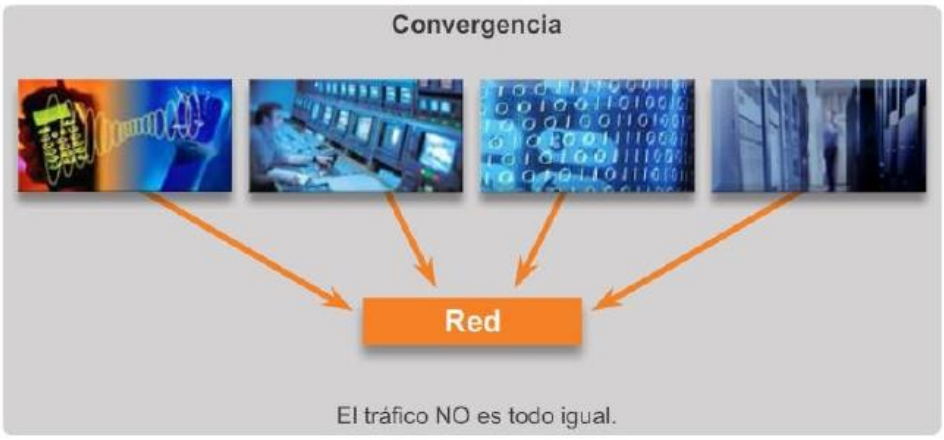
Tráfico en tiempo real
- Voz sobre IP (VOIP)
- Videoconferencia

Contenido Web
- Explorar
- Hacer compras

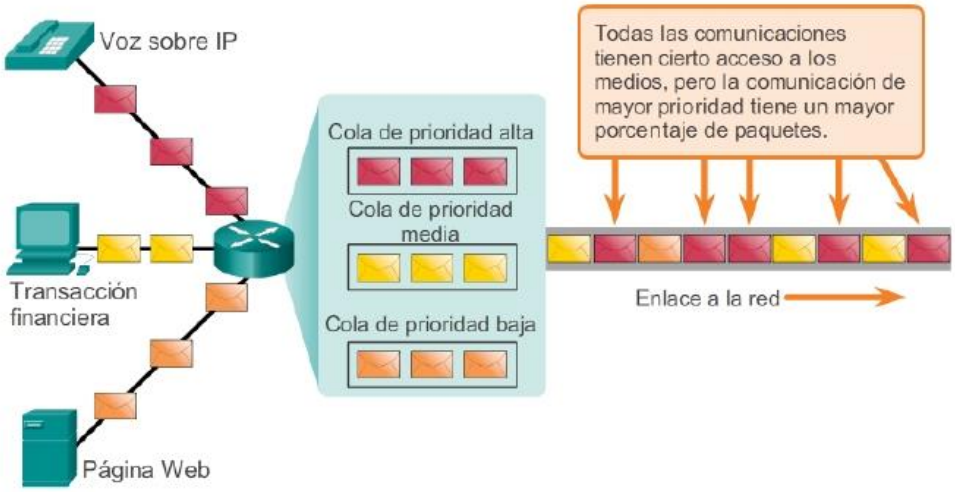
Tráfico de transacciones
- Procesamiento de pedidos y facturación
- Inventario e informes
- Contabilidad e informes

Tráfico de streaming
- Video a petición (VoD)
- Películas

Tráfico masivo
- Correo electrónico
- Copias de seguridad de datos
- Archivos de impresión



Uso de colas para priorizar la comunicación



La puesta en cola según los tipos de datos permite que los datos de voz tengan prioridad sobre los datos de transacción, los que a su vez tienen prioridad sobre los datos Web.

La calidad de servicio importa

Tipo de comunicación	Sin QoS	Con QoS
Streaming video o streaming audio	 Imagen entrecortada que comienza y se detiene.	 Servicio nítido y continuo.
Transacciones de importancia crítica	Tiempo/Precio 02:14:05 : $1,54 Solo un segundo antes.	Tiempo/Precio 02:14:04 : $1,52 El precio podría ser mejor.
Descarga de páginas web (a menudo, de prioridad baja)	 Las páginas web tardan un poco más en llegar.	 El resultado final es el mismo.

Capítulo 1: Exploración de la red 1.3.2.6 Prestación de seguridad de la red

Seguridad

Internet ha evolucionado y ha pasado de ser una internetwork de organizaciones educativas y gubernamentales fuertemente controlada a ser un medio accesible para todos para la transmisión de comunicaciones comerciales y personales. Como resultado, cambiaron los requerimientos de seguridad de la red. La infraestructura de red, los servicios y los datos contenidos en los dispositivos conectados a la red son activos comerciales y personales muy importantes. Si se pone en peligro la integridad de esos recursos, esto podría traer consecuencias graves, como las siguientes:

- Interrupciones de la red que impidan la comunicación y la realización de transacciones, lo que puede provocar pérdidas de negocios.
- Robo de propiedad intelectual (ideas de investigación, patentes y diseños) y uso por parte de la competencia.
- Información personal o privada que se pone en riesgo o se hace pública sin el consentimiento de los usuarios.
- Mala orientación y pérdida de recursos personales y comerciales.
- Pérdida de datos importantes cuyo reemplazo requiere un gran trabajo o que son irreemplazables.

Existen dos tipos de problemas de seguridad de red que se deben tratar: la seguridad de la infraestructura de red y la seguridad de la información.

La seguridad de una infraestructura de red incluye el aseguramiento físico de los dispositivos que proporcionan conectividad de red y prevenir el acceso no autorizado al software de administración que reside en ellos.

La seguridad de la información se refiere a proteger la información que contienen los paquetes que se transmiten por la red y la información almacenada en los dispositivos conectados a la red. Las medidas de seguridad que se deben tomar en una red son:

- Prevenir la divulgación no autorizada.
- Prevenir el robo de información (figura 1).
- Evitar la modificación no autorizada de la información.
- Prevenir la denegación de servicio (DoS).

Para alcanzar los objetivos de seguridad de red, hay tres requisitos principales, que se muestran en la figura 2:

- Asegurar la confidencialidad: la confidencialidad de los datos se refiere a que solamente los destinatarios deseados y autorizados (personas, procesos o dispositivos) pueden acceder a los datos y leerlos.

  Esto se logra mediante la implementación de un sistema sólido de autenticación de usuarios, el establecimiento de contraseñas que sean difíciles de adivinar y la solicitud a los usuarios de que las cambien con frecuencia. La encriptación de datos con el fin de que solamente el destinatario deseado pueda leerlos también forma parte de la confidencialidad.

- Mantener la integridad de la comunicación: la integridad de los datos se relaciona con tener la seguridad de que la información no se alteró durante la transmisión desde el origen hasta el destino. La integridad de los datos se puede poner en riesgo si se daña la información, ya sea voluntaria o accidentalmente. Se puede asegurar la integridad de los datos mediante la solicitud de validación del emisor así como por medio del uso de mecanismos para validar que el paquete no se modificó durante la transmisión.

- Asegurar la disponibilidad: la disponibilidad se relaciona con tener la seguridad de que los usuarios autorizados contarán con acceso a los servicios de datos en forma confiable y oportuna. Los dispositivos de firewall de red, junto con el software antivirus de los equipos de escritorio y de los servidores pueden asegurar la confiabilidad y la solidez del sistema para detectar, repeler y resolver esos ataques. Crear infraestructuras de red totalmente redundantes, con pocos puntos de error únicos, puede reducir el impacto de estas amenazas.

El uso no autorizado de nuestros datos de comunicaciones puede tener consecuencias graves.

Las comunicaciones y la información que deseamos mantener privadas están protegidas de quienes las utilizarían sin autorización.

Capítulo 1: Exploración de la red 1.4.1.1 Nuevas tendencias

Cuando observamos la forma en la que Internet cambió tantas de las cosas que las personas hacen a diario, es difícil creer que hace solo alrededor de 20 años que la mayoría tiene acceso a este servicio. Internet realmente transformó la manera en la que las personas y las organizaciones se comunican. Por ejemplo, antes de que Internet estuviera tan ampliamente disponible, las compañías y las pequeñas empresas dependían principalmente de material de marketing impreso para que los consumidores conocieran sus productos. Era difícil para las empresas determinar qué hogares eran posibles clientes, por lo que utilizaban programas masivos de marketing impreso. Esos programas eran costosos y su eficacia era variada. Compare ese método con los que se utilizan actualmente para llegar a los consumidores. La mayoría de las empresas están presentes en Internet, donde los consumidores pueden obtener información sobre sus productos, leer comentarios de otros clientes y pedir productos directamente desde los sitios Web. Los sitios de redes sociales se asocian a las empresas para promocionar productos y servicios. Los blogueros se asocian a las empresas para destacar y respaldar productos y servicios. La mayor parte de esta publicidad no tradicional está dirigida al consumidor potencial, y no a las masas. En la ilustración 1, se muestran varias predicciones sobre Internet para el futuro cercano.

A medida que se lanzan al mercado nuevas tecnologías y dispositivos para usuarios finales, las empresas y los consumidores deben continuar adaptándose a este entorno en constante evolución. La función de la red es transformarse para permitir que las personas, los dispositivos y la información estén conectados. Existen muchas nuevas tendencias de red que afectarán a organizaciones y consumidores. Algunas de las tendencias principales incluyen las siguientes:

- Cualquier dispositivo, a cualquier contenido, de cualquier forma
- Colaboración en línea
- Video
- Computación en la nube

Estas tendencias están interconectadas y seguirán creciendo al respaldarse entre ellas en los próximos años. Se tratarán estas tendencias con mayor detalle en los siguientes temas.

Sin embargo, debe recordar que a diario se imaginan y concretan nuevas tendencias. ¿Cómo piensa que cambiará Internet en los próximos 10 años?, ¿y en los próximos 20 años?

Considere algunas de las siguientes predicciones:

- Para el año 2014, el tráfico de los dispositivos inalámbricos excederá el tráfico de los dispositivos conectados por cable.
- Para el año 2015, la cantidad de contenido que fluya anualmente por Internet será 540 000 veces la cantidad que se transmitió en 2003.
- Para el año 2015, el 90% de todo el contenido en Internet estará basado en video.
- Para el año 2015, un millón de minutos de video atravesarán Internet por segundo.
- Para el año 2016, el tráfico IP global anual superará el umbral del zettabyte (1 180 591 620 717 411 303 424 bytes).
- Para el año 2016, la cantidad de dispositivos conectados a redes IP será aproximadamente tres veces la población mundial.
- Para el año 2016, 1,2 millones de minutos de contenido de video atravesarán la red por segundo.
- Para el año 2020, habrá 50 000 millones de dispositivos conectados a Internet.

Capítulo 1: Exploración de la red 1.4.1.2 BYOD

Bring Your Own Device (BYOD)

El concepto de “cualquier dispositivo, a cualquier contenido, de cualquier forma” es una importante tendencia global que requiere cambios significativos en la forma en que se utilizan los dispositivos. Esta tendencia se conoce como “Bring Your Own Device” (BYOD) o Traiga su propio dispositivo.

La tendencia BYOD les da a los usuarios finales la libertad de utilizar herramientas personales para acceder a información y comunicarse a través de una red comercial o de campus. Con el crecimiento de los dispositivos para consumidores —y la consiguiente caída en los costos—, se espera que los empleados y estudiantes cuenten con algunas de las herramientas más avanzadas de computación y de redes para uso personal. Entre estas herramientas personales, se incluyen computadoras portátiles, equipos ultraportátiles, tablet PC, smartphones y lectores de libros electrónicos. Estos dispositivos pueden ser propiedad de la compañía o el lugar de estudios, de una persona, o una combinación de ambas.

BYOD significa que se puede usar cualquier dispositivo, de cualquier persona, en cualquier lugar. Por ejemplo, en el pasado, un estudiante que necesitaba acceder a la red del campus o a Internet debía usar una de las PC del lugar de estudios. Por lo general, estos dispositivos eran limitados y se los veía como herramientas que servían únicamente para trabajar en el aula o en la biblioteca. La conectividad extendida mediante acceso móvil y remoto a la red del campus les da a los estudiantes una enorme flexibilidad y más oportunidades de aprendizaje.

BYOD es una tendencia influyente que afecta o afectará a todas las organización de TI.

Capítulo 1: Exploración de la red 1.4.1.3 Colaboración en línea

Colaboración en línea

Las personas no quieren conectarse a la red solo para acceder a aplicaciones de datos, sino también para colaborar entre sí. La colaboración se define como “el acto de trabajar con otras personas en un proyecto conjunto”.

Para las empresas, la colaboración es una prioridad esencial y estratégica. Para seguir siendo competitivas, las organizaciones deben responder tres preguntas principales sobre la colaboración:

- ¿Cómo se puede lograr que todos compartan los mismos criterios?
- ¿Cómo se pueden equilibrar los recursos para llegar a más lugares al mismo tiempo con recortes de presupuesto y de personal?
- ¿Cómo se pueden mantener relaciones cara a cara con una creciente red de colegas, clientes, socios y pares en un entorno que depende más de la conectividad las 24 horas?

La colaboración también es una prioridad en la educación. Los estudiantes necesitan colaborar para ayudarse mutuamente con el aprendizaje, para desarrollar las habilidades de trabajo en equipo que se utilizan en la fuerza laboral y para trabajar juntos en proyectos en equipo.

Una forma de responder a estas preguntas y de satisfacer estas demandas en el entorno actual es a través de herramientas de colaboración en línea. En los espacios de trabajo tradicionales, así como en los entornos de BYOD, las personas aprovechan las ventajas de los servicios de voz, video y conferencias en sus proyectos de colaboración.

La capacidad de colaborar en línea modifica los procesos comerciales. Las nuevas herramientas de colaboración y las que están en expansión permiten que las personas colaboren de forma rápida y sencilla, independientemente de su ubicación física. Las organizaciones tienen mucha más flexibilidad en cuanto a la forma en que se organizan. Las personas ya no se ven limitadas por la ubicación física. Acceder al conocimiento experto es más fácil que nunca. La expansión de la colaboración permite que las organizaciones

mejoren la recopilación de información, innovación y productividad. En la ilustración, se enumeran algunos de los beneficios de la colaboración en línea.

Las herramientas de colaboración proporcionan a empleados, estudiantes, docentes, clientes y socios una manera instantánea de conectarse, interactuar y hacer negocios, por el canal de comunicación que prefieran y de alcanzar así sus objetivos.

Los beneficios de incorporar herramientas de colaboración a una estrategia empresarial incluyen los siguientes:

- **Mejorar la satisfacción del cliente** : aumentar la calidad de la experiencia del cliente a través de un mecanismo instantáneo de presencia y comunicación en línea.
- **Aumentar las opciones de comunicación** : proporcionar una gama más amplia de canales de comunicación y, al mismo tiempo, reducir costos y mejorar la satisfacción del cliente.
- **Optimizar el desempeño del equipo** : generar confianza y compartir información entre grupos, negocios y puntos geográficos distribuidos para mejorar la agilidad comercial.
- **Permitir que haya usuarios móviles** : proporcionar flexibilidad y satisfacción a los empleados al permitirles trabajar desde cualquier lugar, con el dispositivo que prefieran.
- **Mejorar las comunicaciones de la organización** : comunicarse de forma eficaz con toda la organización a través de foros en línea o de reuniones en línea de toda la compañía que permiten que todos los niveles de la empresa participen y se sientan incluidos.
- **Transformar la administración de capacitaciones y eventos** : proporcionar una estrategia interactiva para lograr un alto rendimiento comercial mediante la capacitación, sin tener costos adicionales de viajes para interacciones cara a cara.
- **Mejorar la administración de las instalaciones** : crear un nuevo espacio laboral que ofrezca opciones de trabajo seguras y flexibles para mejorar el trabajo en equipo y aumentar la productividad y, al mismo tiempo, reducir el costo de los requisitos inmobiliarios y físicos del lugar de trabajo.

Capítulo 1: Exploración de la red 1.4.1.4 Comunicación por video

Comunicación por video

Otra tendencia de red que tiene una importancia crítica en lo que respecta a la comunicación y el trabajo en colaboración es el video. El video se utiliza actualmente para propósitos de comunicación, colaboración y

entretenimiento. Las videollamadas son cada vez más populares, ya que facilitan las comunicaciones como parte de la red humana. Las videollamadas se pueden hacer desde cualquier lugar que cuente con una conexión a Internet, incluso desde el hogar o en el trabajo.

Las videollamadas y las videoconferencias han demostrado ser particularmente eficaces en los procesos de ventas y para hacer negocios. El video es una herramienta útil para realizar negocios a distancia, tanto en el ámbito local como global. Hoy en día, las empresas utilizan el video para transformar la forma en que hacen negocios. El video ayuda a las empresas a crear una ventaja competitiva, a bajar costos y a minimizar el impacto ambiental al reducir la necesidad de viajar. En la figura 1, se muestra la tendencia de video en la comunicación.

Tanto los consumidores como las empresas impulsan este cambio. A medida que las organizaciones se extienden más allá de los límites geográficos y culturales, el video se convierte en un requisito clave para una colaboración eficaz. Ahora, los usuarios de video requieren la capacidad de ver cualquier contenido, en cualquier dispositivo, en cualquier lugar.

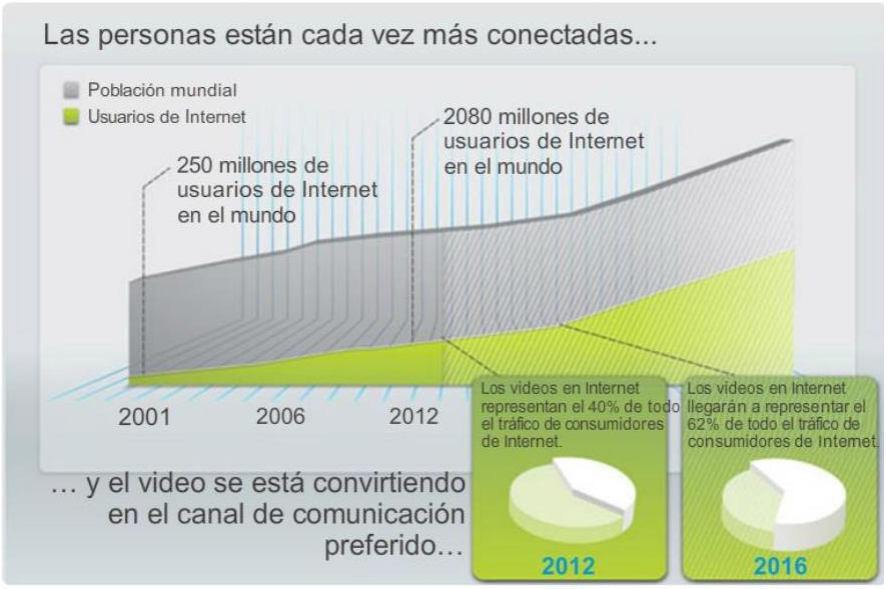
Las empresas también reconocen la función que desempeña el video en el mejoramiento de la red humana. El crecimiento de los medios y las nuevas aplicaciones que se les dan impulsan la necesidad de integrar audio y video en muchas formas de comunicación. La audioconferencia coexistirá con la videoconferencia.

Las herramientas de colaboración diseñadas para conectar a los empleados distribuidos integrarán el servicio de video de escritorio para salvar distancias entre los equipos.

Existen varios factores y beneficios que impulsan la inclusión de una estrategia para utilizar video. Cada organización es única. La combinación exacta y la naturaleza de los motivos para utilizar el video varían según la organización y la función empresarial. El marketing, por ejemplo, puede enfocarse en la globalización y en los gustos en constante cambio de los consumidores, mientras el enfoque del director ejecutivo de información (CIO) puede estar en la reducción de costos mediante el recorte de los gastos de viajes de los empleados que necesitan reunirse en persona. En la ilustración 2, se enumeran algunos de los motivos por los que las organizaciones deciden desarrollar e implementar una estrategia de soluciones de video.

En la figura 3, se muestra un video que explica detalladamente cómo se puede incorporar TelePresence a la vida y los negocios de todos los días mediante el uso de video.

Otra tendencia en video es el video a petición y el streaming video en vivo. La transmisión de video a través de la red nos permite ver películas y programas de televisión cuando y donde queremos.



Motivos para implementar una estrategia de video:

- **Una fuerza laboral global y la necesidad de colaboración en tiempo real**: permite la creación de equipos de colaboración que atraviesan los límites corporativos, nacionales y geográficos.
- **Reducción de costos y TI ecológica**: al evitar los viajes, se reducen los costos y las emisiones de carbono.
- **Nuevas oportunidades para la convergencia IP**: las aplicaciones de video convergentes, como la colaboración por video de alta definición, los sistemas de vigilancia por video y la publicidad por video, remiten a una única red IP.
- **Explosión de los medios**: gracias a la caída de los precios de las cámaras de video y a una nueva generación de dispositivos económicos de alta calidad, los usuarios se convirtieron en aspirantes a productores de películas.
- **Redes sociales**: el fenómeno de las redes sociales puede ser tan eficaz para los negocios como lo es en el contexto social. Por ejemplo, los empleados cada vez filman más videos cortos para compartir las prácticas recomendadas con sus colegas y para informar a sus pares sobre proyectos e iniciativas.
- **Demanda de acceso universal a los medios**: los usuarios demandan tener acceso a aplicaciones de medios enriquecidos dondequiera que estén y desde cualquier dispositivo. La participación en videoconferencias, la capacidad de ver las últimas comunicaciones ejecutivas y la colaboración con compañeros de trabajo son aplicaciones que deben ser accesibles para los empleados, independientemente de su sitio de trabajo.

Capítulo 1: Exploración de la red 1.4.1.5 Computación en la nube

Computación en la nube

La computación en la nube consiste en el uso de recursos informáticos (hardware y software) que se proveen como servicio a través de una red. Una compañía utiliza el hardware y software de la nube y se le cobra un precio por el servicio.

Las PC locales ya no tienen que hacer el “trabajo pesado” cuando se trata de ejecutar aplicaciones de red. En cambio, la red de PC que componen la nube es la que ocupa de ejecutarlas. Esto disminuye los requisitos de hardware y software del usuario. La PC del usuario debe interactuar con la nube mediante software, que puede ser un explorador Web, mientras que la red de la nube se encarga del resto.

La computación en la nube es otra tendencia global que cambia el modo en que accedemos a los datos y los almacenamos. Esta tendencia abarca todos los servicios de suscripción o de pago según el uso en tiempo real en Internet. Este sistema nos permite almacenar archivos personales e incluso crear copias de seguridad de nuestra unidad de disco duro completa en servidores a través de Internet. Mediante la nube, se puede acceder a aplicaciones de procesamiento de texto y edición de fotografías, entre otras.

Para las empresas, la computación en la nube expande las capacidades de TI sin necesidad de invertir en infraestructura nueva, en capacitación de personal nuevo ni en licencias de software nuevo. Estos servicios están disponibles a petición y se proporcionan de forma económica a cualquier dispositivo en cualquier lugar del mundo, sin comprometer la seguridad ni el funcionamiento.

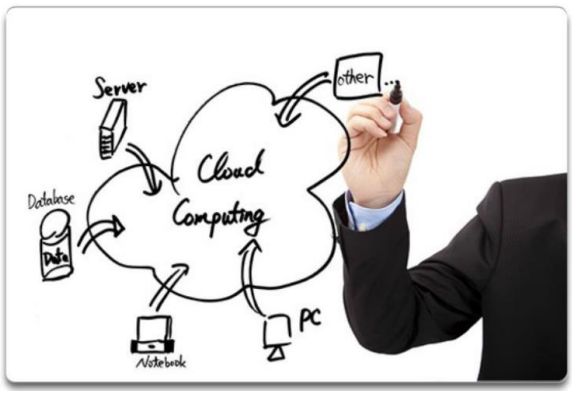
El término “computación en la nube” se refiere concretamente a computación basada en la Web. Los servicios bancarios, las tiendas de venta minorista y la descarga de música en línea son ejemplos de computación en la nube.

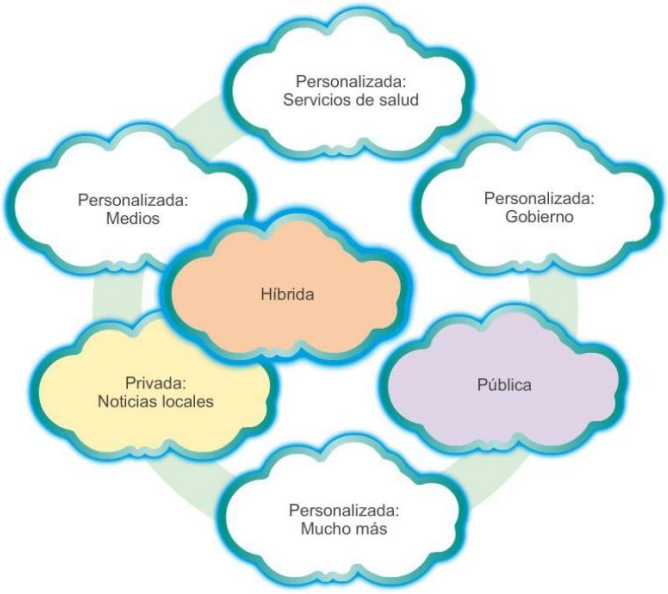
Generalmente, los usuarios pueden acceder a las aplicaciones en la nube a través de un explorador Web y no necesitan instalar ningún tipo de software en su dispositivo final. Esto permite que se puedan conectar muchos tipos de dispositivos diferentes a la nube.

La computación en la nube ofrece los siguientes beneficios potenciales:

- Flexibilidad en la organización: los usuarios pueden acceder a la información en cualquier momento y lugar mediante un explorador Web.
- Agilidad e implementación rápida: el departamento de TI puede concentrarse en la provisión de herramientas para extraer, analizar y compartir información y conocimientos de bases de datos, archivos y personas.
- Menor costo de infraestructura: la tecnología pasa de estar en el sitio a estar en un proveedor en la nube, lo que elimina el costo de hardware y aplicaciones.
- Nuevo enfoque de los recursos de TI: lo que se ahorra en costos de hardware y de aplicaciones se puede utilizar para otro fin.
- Creación de nuevos modelos empresariales: se puede acceder a las aplicaciones y los recursos fácilmente, para que las empresas puedan reaccionar rápidamente a las necesidades de los clientes. Esto les permite establecer estrategias para promover la innovación al entrar potencialmente en nuevos mercados.

Existen cuatro tipos principales de nubes, como se muestra en la figura 2. Haga clic en cada nube para obtener más información.





Nubes personalizadas

Estas son nubes creadas para satisfacer las necesidades de un sector específico, como salud o medios. Las nubes personalizadas pueden ser privadas o públicas.

Nubes públicas

Las aplicaciones y los servicios basados en la nube que se ofrecen en una nube pública están a disposición de la población en general. Los servicios pueden ser gratuitos u ofrecerse en el formato de pago según el uso, como el pago de almacenamiento en línea. La nube pública utiliza Internet para proporcionar servicios.

Nubes privadas

Las aplicaciones y los servicios basados en la nube que se ofrecen en una nube privada están destinados a una organización o una entidad específica, como el gobierno. Se puede configurar una nube privada utilizando la red privada de la organización, si bien el armado y el mantenimiento pueden ser costosos. Una organización externa que cuente con una seguridad de acceso estricta también puede administrar una nube privada.

Nubes híbridas

Una nube híbrida consta de dos o más nubes (por ejemplo, una parte personalizada y otra parte pública); ambas partes son objetos separados, pero están conectadas mediante una única arquitectura. En una nube híbrida, las personas podrían tener grados de acceso a diversos servicios según los derechos de acceso de los usuarios.

Capítulo 1: Exploración de la red 1.4.1.6 Centros de datos

La computación en la nube es posible gracias a los centros de datos. Un centro de datos es una instalación utilizada para alojar sistemas de computación y componentes relacionados, entre los que se incluyen los siguientes:

- Conexiones de comunicaciones de datos redundantes
- Servidores virtuales de alta velocidad (en ocasiones, denominados “granjas de servidores” o “clústeres de servidores”)
- Sistemas de almacenamiento redundante (generalmente utilizan tecnología SAN)

- Fuentes de alimentación redundantes o de respaldo
- Controles ambientales (p. ej., aire acondicionado, extinción de incendios)
- Dispositivos de seguridad

Un centro de datos puede ocupar una habitación en un edificio, un piso o más, o un edificio entero. Los centros de datos modernos utilizan la computación en la nube y la virtualización para administrar de forma eficaz las transacciones de grandes cantidades de datos. La virtualización es la creación de una versión virtual de un elemento, como una plataforma de hardware, un sistema operativo (OS, operating system), un dispositivo de almacenamiento o recursos de red.

Mientras que una PC física es un dispositivo independiente y real, una máquina virtual consiste en un conjunto de archivos y programas que se ejecutan en un sistema físico real. A diferencia de la multitarea, que incluye la ejecución de varios programas en el mismo SO, en la virtualización se ejecutan varios SO en forma paralela en una misma CPU. Esto reduce drásticamente los costos administrativos e indirectos.

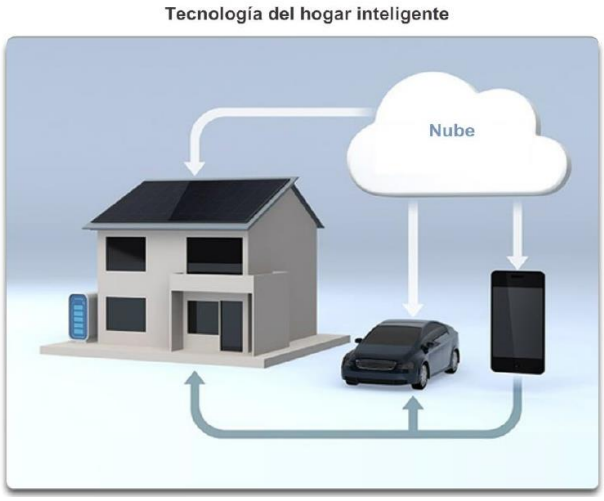
Por lo general, la creación y el mantenimiento de centros de datos son muy costosos. Por esta razón, solo las grandes organizaciones utilizan centros de datos privados creados para alojar sus datos y proporcionar servicios a los usuarios. Por ejemplo, es posible que un hospital grande posea un centro de datos separado donde se guardan las historias clínicas de los pacientes en formato electrónico. Las organizaciones más pequeñas, que no pueden costear el mantenimiento de un centro propio de datos privado, pueden reducir el costo total de propiedad mediante el alquiler de servicios de servidor y almacenamiento a una organización en la nube con un centro de datos más grande.

Capítulo 1: Exploración de la red 1.4.2.1 Tendencias tecnológicas en el hogar

Las tendencias de red no solo afectan la forma en que nos comunicamos en el trabajo y en el lugar de estudios, sino que también están cambiando prácticamente cada aspecto del hogar.

Las nuevas tendencias del hogar incluyen la “tecnología del hogar inteligente”. La tecnología del hogar inteligente se integra a los dispositivos que se utilizan a diario, lo que permite que se interconecten con otros dispositivos y que se vuelvan más “inteligentes” o automatizados. Por ejemplo, imagine poder preparar un plato y colocarlo en el horno para cocinarlo antes de irse de su casa para no regresar en todo el día. Imagine si el horno “reconociera” el plato que cocina y estuviese conectado a su “calendario de eventos” para determinar cuándo debería estar listo para comer y pudiera ajustar la hora de inicio y la duración de la cocción de acuerdo con esos datos. Incluso podría ajustar el tiempo y la temperatura de cocción sobre la base de los cambios en su agenda. Además, una conexión mediante smartphone o tablet PC permite al usuario conectarse al horno directamente para realizar los cambios que desee. Cuando el plato está “disponible”, el horno envía un mensaje de alerta al dispositivo para usuarios finales especificado en el que indica que el plato está listo y se está calentando.

Esta situación no está muy lejos de ser real. De hecho, actualmente se desarrolla tecnología del hogar inteligente para todas las habitaciones de un hogar. La tecnología del hogar inteligente se volverá más real a medida que las redes domésticas y la tecnología de Internet de alta velocidad lleguen a más hogares. Se desarrollan nuevas tecnologías de red a diario para cumplir con estos tipos de necesidades crecientes de tecnología.

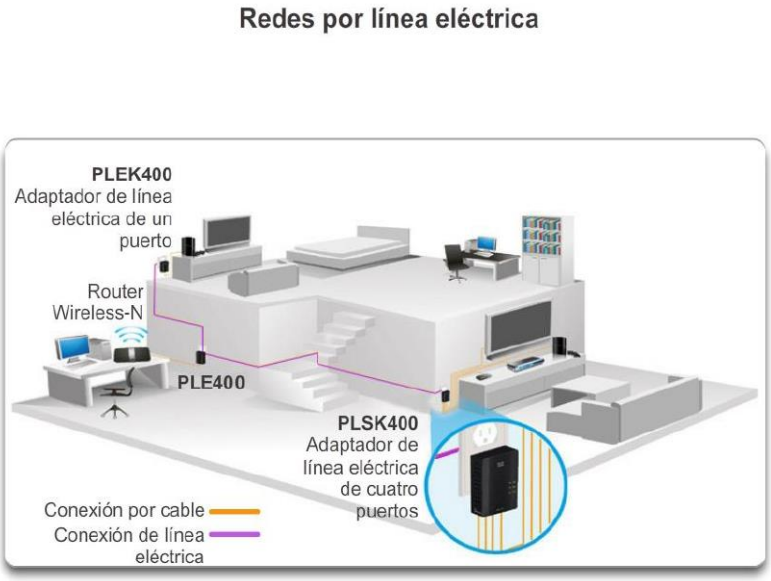


Capítulo 1: Exploración de la red 1.4.2.2 Redes por línea eléctrica

Las redes por línea eléctrica son una tendencia emergente para redes domésticas que utilizan los cables eléctricos existentes para conectar dispositivos, como se muestra en la ilustración. El concepto “sin nuevos cables” se refiere a la capacidad de conectar un dispositivo a la red donde haya un tomacorriente. Esto ahorra el costo de instalar cables de datos y no genera ningún costo adicional en la factura de electricidad.

Mediante el uso de los mismos cables que transmiten electricidad, las redes por línea eléctrica transmiten información mediante el envío de datos en ciertas frecuencias similares a las de la tecnología que se utiliza para DSL.

Mediante un adaptador estándar de línea eléctrica HomePlug, los dispositivos pueden conectarse a la LAN donde haya un tomacorriente. Las redes por línea eléctrica son particularmente útiles en el caso de que no se puedan utilizar puntos de acceso inalámbrico o de que estos no lleguen a todos los dispositivos del hogar, pero no están diseñadas para reemplazar el cableado dedicado para redes de datos. Sin embargo, es una alternativa cuando los cables de red o las comunicaciones inalámbricas no son una opción viable.



Capítulo 1: Exploración de la red 1.4.2.3 Banda ancha inalámbrica

La conexión a Internet es fundamental para la tecnología del hogar inteligente. DSL y cable son tecnologías comunes que se utilizan para conectar hogares y pequeñas empresas a Internet. Sin embargo, la red inalámbrica puede ser otra opción en muchas áreas.

Proveedor de servicios de Internet inalámbrico (WISP)

El proveedor de servicios de Internet inalámbrico (WISP, Wireless Internet Service Provider) es un ISP que conecta a los suscriptores a un punto de acceso designado o una zona activa mediante tecnologías inalámbricas similares a las que se encuentran en las redes de área local inalámbrica (WLAN, Wireless Local Area Network). Los WISP se encuentran con mayor frecuencia en entornos rurales donde los servicios de cable o DSL no están disponibles.

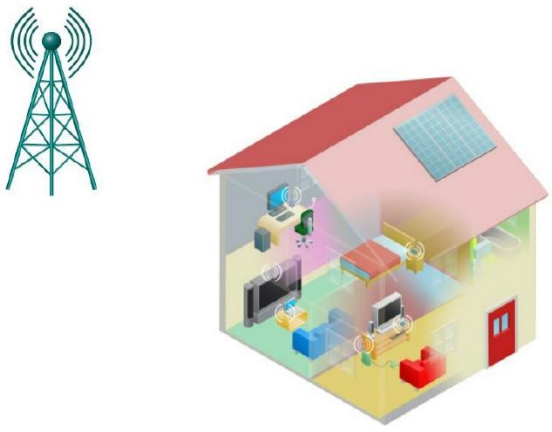
Aunque se puede instalar una torre de transmisión separada para la antena, comúnmente la antena se conecta a una estructura elevada existente, como una torre de agua o una torre de radio. Se instala una pequeña antena en el techo del suscriptor, al alcance del transmisor del WISP.

La unidad de acceso del suscriptor se conecta a la red conectada por cable dentro del hogar. Desde la perspectiva del usuario doméstico, la configuración no es muy diferente de la de DSL o el servicio de cable. La diferencia principal es que la conexión del hogar al ISP es inalámbrica, en lugar de establecerse mediante un cable físico.

Servicio de banda ancha inalámbrico

Otra solución inalámbrica para los hogares y las pequeñas empresas es la banda ancha inalámbrica. Esta opción utiliza la misma tecnología de datos móviles que se utiliza para acceder a Internet con un smartphone o una tablet PC. Se instala una antena fuera del hogar, que proporciona conectividad inalámbrica o por cable a los dispositivos en el hogar. En muchas zonas, la banda ancha inalámbrica doméstica compite directamente con los servicios de DSL y cable.

Servicio de banda ancha inalámbrico



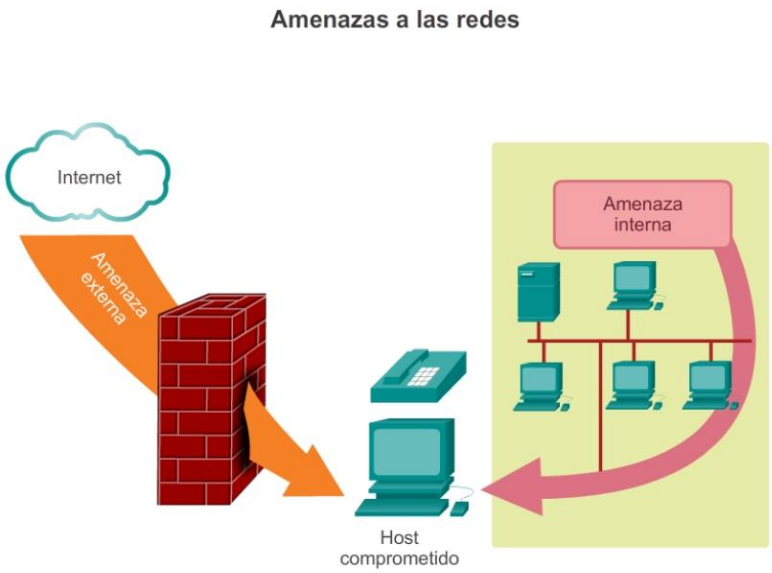
Capítulo 1: Exploración de la red 1.4.3.1 Amenazas de seguridad

La seguridad de redes es una parte integral de las redes de computadoras, independientemente de si la red está limitada a un entorno doméstico con una única conexión a Internet o si es tan extensa como una empresa con miles de usuarios. La seguridad de red implementada debe tomar en cuenta el entorno, así como las herramientas y los requisitos de la red. Debe poder proteger los datos y, al mismo tiempo, mantener la calidad de servicio que se espera de la red.

La protección de la red incluye protocolos, tecnologías, dispositivos, herramientas y técnicas para proteger los datos y mitigar amenazas. En la actualidad, muchas amenazas de seguridad de red externas se expanden por Internet. Las amenazas externas más comunes a las redes incluyen las siguientes:

- Virus, gusanos y caballos de Troya: se trata de softwares malintencionados y códigos arbitrarios que se ejecutan en un dispositivo de usuario.
- Spyware y adware: software instalado en un dispositivo de usuario que recopila información sobre el usuario de forma secreta.
- Ataques de día cero, también llamados “ataques de hora cero”: ataque que ocurre el mismo día en que se hace pública una vulnerabilidad.
- Ataques de piratas informáticos: ataque de una persona experta a los dispositivos de usuario o recursos de red.
- Ataques por denegación de servicio: ataques diseñados para reducir o para bloquear aplicaciones y procesos en un dispositivo de red.
- Interceptación y robo de datos: ataque para capturar información privada en la red de una organización.
- Robo de identidad: ataque para robar las credenciales de inicio de sesión de un usuario a fin de acceder a datos privados.

También es importante tener en cuenta las amenazas internas. Se llevaron a cabo numerosos estudios que muestran que las infracciones de seguridad de datos más comunes suceden a causa de los usuarios internos de la red. Esto se puede atribuir a dispositivos perdidos o robados o al mal uso accidental por parte de los empleados, y dentro del entorno empresarial, incluso a empleados malintencionados. Con las estrategias de BYOD en desarrollo, los datos corporativos son mucho más vulnerables. Por lo tanto, cuando se desarrolla una política de seguridad, es importante abordar tanto las amenazas de seguridad externas como las internas.



Capítulo 1: Exploración de la red 1.4.3.2 Soluciones de seguridad

No hay una solución única que pueda proteger una red contra la variedad de amenazas que existen. Por este motivo, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad. Si un componente de seguridad no puede identificar ni proteger la red, hay otros que pueden hacerlo.

La implementación de seguridad en redes domésticas generalmente es muy básica. Por lo general, se implementa en los dispositivos host de conexión así como en el punto de conexión a Internet e incluso puede depender de servicios contratados al ISP.

Por otra parte, la implementación de seguridad de red en redes corporativas normalmente consiste en la integración de numerosos componentes a la red para controlar y filtrar el tráfico. Lo ideal es que todos los componentes funcionen juntos, lo que minimiza la necesidad de mantenimiento y aumenta la seguridad.

Los componentes de seguridad de red para redes domésticas o de oficinas pequeñas deben incluir, como mínimo, lo siguiente:

- Software antivirus y antispyware: para proteger los dispositivos de usuario contra software malintencionado.

- Filtrado de firewall: para bloquear accesos no autorizados a la red.

  Esto puede incluir un sistema de firewall basado en host que se implemente para impedir el acceso no autorizado al dispositivo host o un servicio de filtrado básico en el router doméstico para impedir el acceso no autorizado del mundo exterior a la red.

Además de lo anterior, las redes más grandes y las redes corporativas generalmente tienen otros requisitos de seguridad:

- Sistemas de firewall dedicados: para proporcionar capacidades de firewall más avanzadas que puedan filtrar una gran cantidad de tráfico con mayor granularidad.

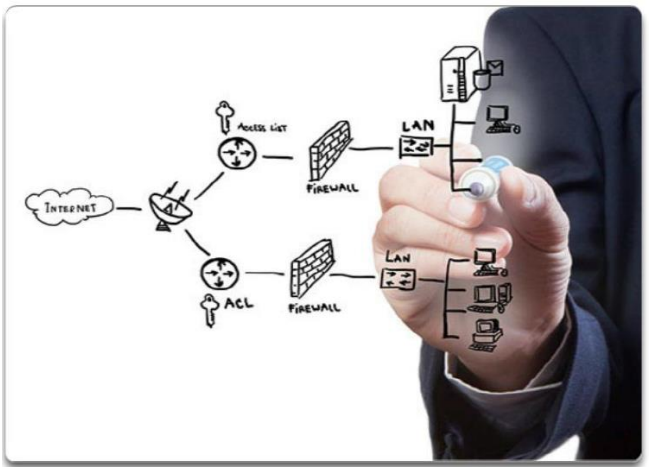
- Listas de control de acceso: las listas de control de acceso (ACL, Access control list) filtran el acceso y el reenvío de tráfico.

- Sistemas de prevención de intrusión: los sistemas de prevención de intrusión (IPS) identifican amenazas de rápida expansión, como ataques de día cero o de hora cero.

- Redes privadas virtuales: las redes privadas virtuales (VPN, Virtual private networks) proporcionan un acceso seguro a los trabajadores remotos.

Los requisitos de seguridad de la red deben tomar en cuenta el entorno de red, así como las diversas aplicaciones y los requisitos informáticos. Tanto los entornos domésticos como las empresas deben poder proteger sus datos y, al mismo tiempo, mantener la calidad de servicio que se espera de cada tecnología. Además, la solución de seguridad implementada debe poder adaptarse a las crecientes tendencias de red, en constante cambio.

El estudio de las amenazas de seguridad de red y de las técnicas de mitigación comienza con una comprensión clara de la infraestructura de conmutación y enrutamiento subyacente utilizada para organizar los servicios de red.



Capítulo 1: Exploración de la red 1.4.4.1 Arquitecturas de red de Cisco

La función de la red cambió de una red únicamente de datos a un sistema que permite conectar personas, dispositivos e información en un entorno de red convergente y con gran variedad de medios. Para que las redes funcionen eficazmente y crezcan en este tipo de entorno, se deben crear sobre la base de una arquitectura de red estándar.

La arquitectura de red se refiere a los dispositivos, las conexiones y los productos que se integran para admitir las tecnologías y aplicaciones necesarias.

Una arquitectura de tecnología de red bien planificada ayuda a asegurar la conexión de cualquier dispositivo en cualquier combinación de redes. Además de garantizar la conectividad, también aumenta la rentabilidad al integrar la seguridad y la administración de la red, y mejora los procesos comerciales. En la base de todas las arquitecturas de red —y de hecho, en la base de Internet propiamente dicha—, se encuentran los routers y los switches. Los routers y los switches transportan datos y comunicaciones de voz y video, además de permitir acceso inalámbrico y proporcionar seguridad.

La creación de redes que admitan nuestras necesidades actuales y las necesidades y las tendencias del futuro comienza con una clara comprensión de la infraestructura de conmutación y enrutamiento subyacente.

Una vez que se establece una infraestructura de red básica de conmutación y enrutamiento, las personas, las pequeñas empresas y las organizaciones pueden ampliar la red con el tiempo mediante el agregado de características y funcionalidades a una solución integrada.

Teleconferencias en el lugar de trabajo

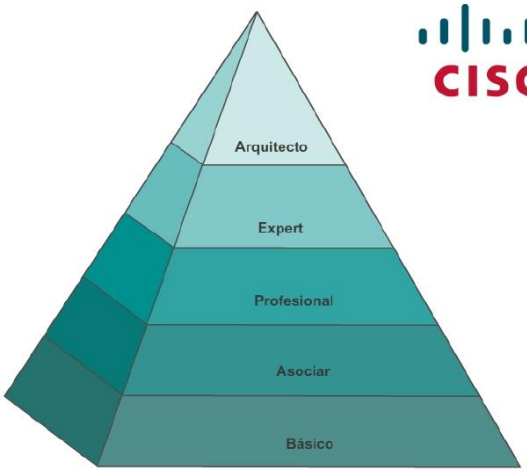
Capítulo 1: Exploración de la red 1.4.4.2 CCNA

A medida que aumenta el uso de estas redes integradas y en expansión, también aumenta la necesidad de capacitación para las personas que implementan y administran soluciones de red. Esta capacitación debe comenzar con las bases de la conmutación y el enrutamiento. Obtener la certificación de Cisco Certified Network Associate (CCNA) es el primer paso para ayudar a una persona a prepararse para una carrera en redes.

La certificación CCNA valida la capacidad de una persona para instalar, configurar y operar redes medianas enrutadas y conmutadas, y solucionar problemas en estas redes, incluidas la implementación y la verificación de conexiones a sitios remotos en una WAN.

El currículo de CCNA también incluye la mitigación básica de amenazas a la seguridad, una introducción a conceptos y terminología de redes inalámbricas y capacidades basadas en el desempeño. Este currículo de CCNA incluye el uso de diferentes protocolos, por ejemplo: IP, Open Shortest Path First (OSPF), protocolo de interfaz de línea serial, Frame Relay, VLAN, Ethernet y listas de control de acceso (ACL), entre otros.

Este curso ayuda a crear el marco para los conceptos de redes y las configuraciones básicas de enrutamiento y conmutación, además de ser un inicio en su camino para obtener la certificación CCNA.



Capítulo 1: Exploración de la red 1.5.1.2 Resumen

Las redes e Internet cambiaron el modo en que nos comunicamos, aprendemos, trabajamos e incluso la forma en que jugamos.

Hay redes de todo tamaño. Pueden ir desde redes simples, compuestas por dos computadoras, hasta redes que conectan millones de dispositivos.

Internet es la red más extensa que existe. De hecho, el término Internet significa “red de redes”. Internet proporciona los servicios que nos permiten conectarnos y comunicarnos con nuestra familia, nuestros amigos, nuestro trabajo y nuestros intereses.

La infraestructura de red es la plataforma que da soporte a la red. Proporciona el canal estable y confiable por el cual pueden producirse las comunicaciones. Consta de componentes de red, incluidos dispositivos finales, dispositivos intermediarios y medios de red.

Las redes deben ser confiables. Esto significa que las redes deben ser tolerantes a fallas, escalables, proporcionar calidad de servicio y garantizar la seguridad de la información y de los recursos en ellas. La seguridad de redes es una parte integral de las redes de computadoras, independientemente de si la red está limitada a un entorno doméstico con una única conexión a Internet o si es tan extensa como una empresa con miles de usuarios. No hay una solución única que pueda proteger una red contra la variedad de amenazas que existen. Por este motivo, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad.

La infraestructura de red puede variar ampliamente en términos de tamaño, cantidad de usuarios, y cantidad y tipo de servicios que admite.

La infraestructura de red debe crecer y ajustarse para admitir la forma en que se utiliza la red. La plataforma de routing y switching es la base de toda infraestructura de red.

Este capítulo se centró en las redes como plataforma principal para permitir la comunicación. En el capítulo siguiente, se presentará el Sistema operativo Internetwork (IOS) de Cisco utilizado para permitir el enrutamiento y la conmutación en entornos de red de Cisco.

Capítulo 2: Configuración de un sistema operativo de red 2.0.1.1 Introducción a Cisco IOS

Por lo general, las redes domésticas interconectan una amplia variedad de dispositivos finales, como computadoras portátiles y de escritorio, tablet PC, smartphones, televisores inteligentes y reproductores de medios de red que cumplen con los requisitos de la Digital Living Network Alliance (DLNA), como las consolas Xbox 360 o Playstation 3, entre otros.

Por lo general, todos estos dispositivos finales están conectados a un router doméstico. En realidad, los routers domésticos son cuatro dispositivos en uno:

- Router: reenvía paquetes de datos a Internet y recibe paquetes de datos de ella.
- Switch: conecta dispositivos finales mediante cables de red.
- Punto de acceso inalámbrico: consta de un transmisor de radio que puede conectar dispositivos finales en forma inalámbrica.
- Dispositivo de firewall: protege el tráfico saliente y restringe el tráfico entrante.

En las redes empresariales más grandes, con muchos más dispositivos y mucho más tráfico, estos se suelen incorporar como dispositivos independientes y autónomos que proporcionan un servicio dedicado. Los dispositivos finales, como las computadoras portátiles y de escritorio, se conectan a los switches de red mediante conexiones por cable. Para enviar paquetes más allá de la red local, los switches de red se conectan a routers de red. Entre los demás dispositivos de infraestructura en una red, se incluyen los puntos de acceso inalámbrico y los dispositivos de seguridad dedicados, como los firewalls.

Cada dispositivo es muy diferente en lo que respecta al hardware, el uso y la capacidad. Sin embargo, en todos los casos, el sistema operativo es lo que permite que el hardware funcione.

Prácticamente en todos los dispositivos para usuarios finales y de red conectados a Internet se utilizan sistemas operativos. Entre los dispositivos para usuarios finales, se incluyen los dispositivos como smartphones, tablet PC y computadoras portátiles y de escritorio. Los dispositivos de red, o intermediarios, se utilizan para transportar datos a través de la red.

Entre estos se incluyen los switches, los routers, los puntos de acceso inalámbrico y los firewalls. El sistema operativo de un dispositivo de red se conoce como “sistema operativo de red”.

Sistema operativo Internetwork (IOS, Internetwork Operating System) de Cisco es un término genérico para la colección de sistemas operativos de red que se utilizan en los dispositivos de red Cisco. Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o el tipo de dispositivo.

En este capítulo, se hace referencia a una topología de red básica que consta de dos switches y dos PC, a fin de demostrar el uso de Cisco IOS.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Explicar el propósito de Cisco IOS.
- Explicar cómo acceder a Cisco IOS y cómo explorarlo para configurar los dispositivos de red.
- Describir la estructura de comandos del software Cisco IOS.
- Configurar nombres de host en un dispositivo Cisco IOS mediante la CLI.
- Utilizar los comandos de Cisco IOS para limitar el acceso a las configuraciones de dispositivos.
- Utilizar los comandos de Cisco IOS para guardar la configuración en ejecución.
- Explicar la forma en que se comunican los dispositivos a través de los medios de red.
- Configurar un dispositivo host con una dirección IP.
- Verificar la conectividad entre dos dispositivos finales.

Capítulo 2: Configuración de un sistema operativo de red 2.1.1.1 Sistemas operativos

Todos los dispositivos finales y de red conectados a Internet requieren un sistema operativo (SO) que los ayude a realizar sus funciones.

Al encender una computadora se carga el SO, por lo general desde una unidad de disco, en la RAM. La parte del código del SO que interactúa directamente con el hardware de la computadora se conoce como núcleo. La porción que interactúa con las aplicaciones y el usuario se conoce como “shell”. El usuario puede interactuar con el shell mediante la interfaz de línea de comandos (CLI, command-line interface) o la interfaz gráfica de usuario (GUI, graphical user interface).

Al emplear la CLI, el usuario interactúa directamente con el sistema en un entorno basado en texto introduciendo comandos con el teclado en una ventana de petición de entrada de comandos. El sistema ejecuta el comando y, por lo general, proporciona una respuesta en forma de texto. La interfaz GUI permite que el usuario interactúe con el sistema en un entorno que utiliza imágenes gráficas, formatos multimedia y texto. Las acciones se llevan a cabo al interactuar con las imágenes en la pantalla. La GUI es más fácil de usar y requiere un menor conocimiento de la estructura de comandos para utilizar el sistema.

Por este motivo, muchas personas prefieren los entornos GUI. Muchos sistemas operativos ofrecen tanto una GUI como una CLI.

Haga clic en las porciones de Hardware, Núcleo y Shell de la ilustración para obtener más información.

A la mayoría de los sistemas operativos de los dispositivos finales, incluidos MS Windows, MAC OS X, Linux, Apple iOS y Android, entre otros, se accede mediante una GUI.

El sistema operativo de los routers domésticos generalmente se denomina “firmware”. El método más frecuente para configurar un router doméstico consiste en utilizar un explorador Web para acceder a una GUI fácil de usar. La mayoría de los routers domésticos habilitan la actualización del firmware a medida que se detectan nuevas características o vulnerabilidades de seguridad.

Los dispositivos de red de infraestructura utilizan un sistema operativo de red. El sistema operativo de red que se utiliza en los dispositivos Cisco se denomina Sistema operativo Internetwork (IOS, Internetwork Operating System). “Cisco IOS” es un término genérico para la colección de sistemas operativos de red que se utilizan en los dispositivos de red Cisco. Cisco IOS se utiliza en la mayoría de los dispositivos Cisco, independientemente del tamaño o el tipo de dispositivo. El método más frecuente para acceder a estos dispositivos consiste en utilizar una CLI.

Este capítulo se centra en la topología de switch de la red de una pequeña empresa. La topología consta de dos switches y dos PC, y se utilizará para demostrar el uso de Cisco IOS mediante la CLI.

Haga clic en Hardware, Núcleo y Shell para obtener más información.

Capítulo 2: Configuración de un sistema operativo de red 2.1.1.2 Propósito de los OS

Los sistemas operativos de red se asemejan en gran medida a los sistemas operativos de PC. Los sistemas operativos realizan una serie de funciones técnicas “detrás de escena” que habilitan a los usuarios a hacer lo siguiente:

- Utilizar un mouse.
- Ver resultados en un monitor.
- Introducir comandos de texto.
- Seleccionar opciones en una ventana de cuadro de diálogo.

Las funciones “detrás de escena” de los switches y los routers son muy similares. El IOS de un switch o un router proporciona una interfaz a los técnicos de red. El técnico puede introducir comandos para configurar o programar el dispositivo a fin de que lleve a cabo diversas funciones de redes. Los detalles operativos de los IOS en los dispositivos de internetworking varían según el propósito del dispositivo y las características que admite.

Cisco IOS es un término que abarca diferentes sistemas operativos que se ejecutan en diversos dispositivos de redes. Existen muchas variaciones distintas de Cisco IOS:

- IOS para switches, routers y otros dispositivos de red Cisco
- Versiones numeradas de IOS para un dispositivo de red Cisco determinado
- Conjuntos de características de IOS que proporcionan paquetes específicos de características y servicios

Al igual que una PC puede ejecutar Microsoft Windows 8 y una MacBook puede ejecutar OS X, un dispositivo de red Cisco ejecuta una versión específica de Cisco IOS. La versión de IOS depende del tipo de dispositivo que se utilice y de las características necesarias. Si bien todos los dispositivos traen un IOS y un conjunto de características predeterminados, es posible actualizar el conjunto de características o la versión de IOS para obtener capacidades adicionales.

En este curso, se concentrará principalmente en Cisco IOS, versión 15.x. En la figura 1, se muestra una lista de las versiones del software IOS para un switch Cisco Catalyst 2960. En la figura 2, se muestra una lista de las versiones del software IOS para un router de servicios integrados (ISR, Integrated Services Router) Cisco 2911.

Capítulo 2: Configuración de un sistema operativo de red 2.1.1.3 Ubicación de Cisco IOS

El archivo IOS en sí tiene un tamaño de varios megabytes y se encuentra almacenado en un área de memoria semipermanente llamada flash. En la ilustración, se muestra una tarjeta Compact Flash. La memoria flash provee almacenamiento no volátil. Esto significa que los contenidos de la memoria no se pierden cuando el dispositivo se apaga. Si bien el contenido de la memoria flash no se pierde durante un corte de la alimentación, puede modificarse o sobrescribirse si es necesario.

Esto permite actualizar el IOS a una versión más reciente o agregarle nuevas características sin reemplazar el hardware. Además, se puede utilizar la memoria flash para almacenar varias versiones del software IOS al mismo tiempo.

En muchos dispositivos Cisco, el IOS de la memoria flash se copia a la memoria de acceso aleatorio (RAM, random access memory) cuando se enciende el dispositivo. Luego, cuando el dispositivo está en funcionamiento, el IOS se ejecuta desde la RAM. La RAM tiene muchas funciones, incluido el almacenamiento de los datos que utiliza el dispositivo para admitir las operaciones de la red. La ejecución del IOS en la RAM aumenta el rendimiento del dispositivo. Sin embargo, la RAM se considera memoria volátil dado que los datos se pierden durante un reinicio. Un reinicio consiste en apagar y volver a encender un dispositivo, ya sea a propósito o por accidente.

La cantidad de memoria flash y RAM requerida para un IOS determinado varía notablemente. A los efectos del mantenimiento y la planificación de redes, es importante determinar los requisitos de memoria flash y RAM para cada dispositivo, incluidas las configuraciones máximas de estos tipos de memoria.

Es posible que los requisitos de las versiones más recientes de IOS exijan más memoria RAM y flash de la que puede instalarse en algunos dispositivos.

Capítulo 2: Configuración de un sistema operativo de red 2.1.1.4 Funciones de IOS

Los routers y switches en los que se utiliza Cisco IOS realizan funciones de las cuales dependen los profesionales de red para hacer que sus redes funcionen de la forma esperada. Las funciones principales que realizan o habilitan los routers y switches Cisco incluyen las siguientes:

- Prestación de seguridad de la red
- Direccionamiento IP de interfaces virtuales y físicas
- Habilitación de configuraciones específicas de la interfaz para optimizar la conectividad de los respectivos medios
- Enrutamiento
- Habilitación de tecnologías de calidad de servicio (QoS)
- Compatibilidad con tecnologías de administración de red

Cada característica o servicio tiene asociado un conjunto de comandos de configuración que permite su implementación por parte de los técnicos de red.

Por lo general, se accede a los servicios que proporciona Cisco IOS mediante una CLI.

Capítulo 2: Configuración de un sistema operativo de red 2.1.2.1 Método de acceso a la consola

Existen varias formas de acceder al entorno de la CLI. Los métodos más comunes son los siguientes:

Consola

Telnet o SSH

Puerto auxiliary

Consola

El puerto de consola es un puerto de administración que proporciona acceso fuera de banda a los dispositivos Cisco. El acceso fuera de banda se refiere al acceso mediante un canal de administración dedicado que se utiliza únicamente para el mantenimiento del dispositivo.

La ventaja de utilizar un puerto de consola es que es posible acceder al dispositivo incluso si no se configuró ningún servicio de red, por ejemplo, cuando se realiza la configuración inicial del dispositivo de red. Al realizar la configuración inicial, una PC con software de emulación de terminal se conecta al puerto de consola del dispositivo mediante un cable especial. Los comandos de configuración para el switch o el router se pueden introducir en la PC conectada.

El puerto de consola también puede utilizarse cuando fallan los servicios de red y no es posible acceder al dispositivo Cisco IOS de manera remota. Si esto ocurre, una conexión a la consola puede habilitar a una PC para determinar el estado del dispositivo.

En forma predeterminada, la consola comunica el inicio del dispositivo, la depuración y los mensajes de error. Una vez que el técnico de red se conecta al dispositivo, puede ejecutar cualquier comando de configuración necesario mediante la sesión de consola.

Para muchos dispositivos IOS, el acceso de consola no requiere ningún tipo de seguridad, en forma predeterminada. Sin embargo, la consola debe estar configurada con contraseñas para evitar el acceso no autorizado al dispositivo. En caso de que se pierda una contraseña, existe un conjunto especial de procedimientos para eludir la contraseña y acceder al dispositivo. También se debe colocar el dispositivo en una habitación bajo llave o en un bastidor de equipos para evitar el acceso físico no autorizado.

Puerto de consola

Capítulo 2: Configuración de un sistema operativo de red 2.1.2.2 Métodos de acceso mediante Telnet, SSH y puerto auxiliar

Telnet

Telnet es un método para establecer una sesión de CLI de un dispositivo en forma remota, mediante una interfaz virtual, a través de una red. A diferencia de la conexión de consola, las sesiones de Telnet requieren servicios de redes activos en el dispositivo. El dispositivo de red debe tener, por lo menos, una interfaz activa configurada con una dirección de Internet, por ejemplo una dirección IPv4. Los dispositivos Cisco IOS incluyen un proceso de servidor Telnet que permite a los usuarios introducir comandos de configuración desde un cliente Telnet. Además de admitir el proceso de servidor Telnet, el dispositivo Cisco IOS también contiene un cliente Telnet. Esto permite que los administradores de red accedan mediante Telnet a cualquier otro dispositivo que admita un proceso de servidor Telnet desde la CLI del dispositivo Cisco.

SSH

El protocolo de Shell seguro (SSH) proporciona un inicio de sesión remoto similar al de Telnet, excepto que utiliza servicios de red más seguros. El SSH proporciona autenticación de contraseña más potente que Telnet y usa encriptación cuando transporta datos de la sesión. De esta manera se mantienen en privado la ID del usuario, la contraseña y los detalles de la sesión de administración. Se recomienda utilizar el protocolo SSH en lugar de Telnet, siempre que sea posible.

La mayoría de las versiones de Cisco IOS incluyen un servidor SSH. En algunos dispositivos, este servicio se activa en forma predeterminada. Otros dispositivos requieren que el servidor SSH se habilite en forma manual. Los dispositivos IOS también incluyen un cliente SSH que puede utilizarse para establecer sesiones SSH con otros dispositivos.

AUX

Una antigua forma de establecer una sesión de CLI de manera remota era mediante una conexión telefónica de dial-up con un módem conectado al puerto auxiliar (AUX) de un router, el cual aparece resaltado en la ilustración. Al igual que la conexión de consola, el método de puerto auxiliar también es una conexión fuera de banda y no requiere la configuración ni la disponibilidad de ningún servicio de red en el dispositivo.

En caso de que los servicios de red fallen, es posible que un administrador remoto acceda al switch o al router mediante una línea telefónica.

El puerto auxiliar también puede usarse en forma local, como el puerto de consola, con una conexión directa a una computadora que ejecute un programa de emulación de terminal. No obstante, se prefiere el puerto de consola al puerto auxiliar para la resolución de problemas, ya que el primero muestra mensajes de inicio, depuración y error de manera predeterminada.

Nota: los switches Cisco Catalyst no admiten conexiones auxiliares.

Capítulo 2: Configuración de un sistema operativo de red 2.1.2.3 Programas de emulación de terminal

Existen varios programas excelentes de emulación de terminales disponibles para conectarse a un dispositivo de red mediante una conexión serial por un puerto de consola o mediante una conexión Telnet o SSH. Algunos de estos programas incluyen los siguientes:

PuTTY (figura 1)

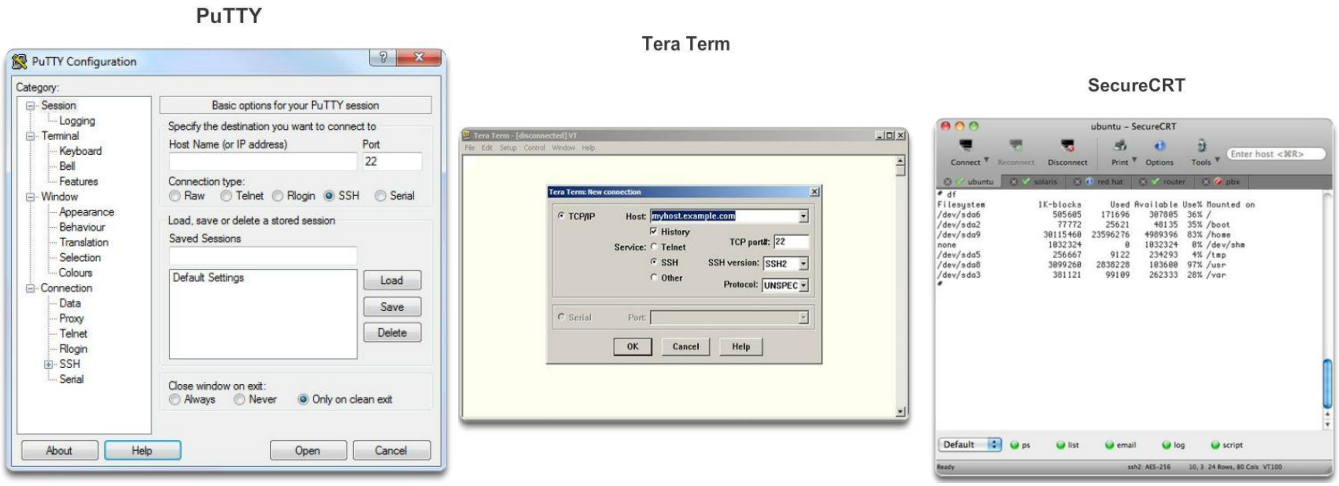
Tera Term (figura 2)

SecureCRT (figura 3)

HyperTerminal

OS X Terminal

Estos programas le permiten aumentar la productividad mediante ajustes del tamaño de la ventana, modificaciones de los tamaños de fuente y cambios en los esquemas de colores.



Capítulo 2: Configuración de un sistema operativo de red 2.1.3.1 Modos de funcionamiento de Cisco IOS

Una vez que un técnico de red se conecta a un dispositivo, puede configurarlo. El técnico de red debe navegar a través de diversos modos del IOS. Los modos de Cisco IOS para los switches y los routers son muy similares. La CLI utiliza una estructura jerárquica para los modos.

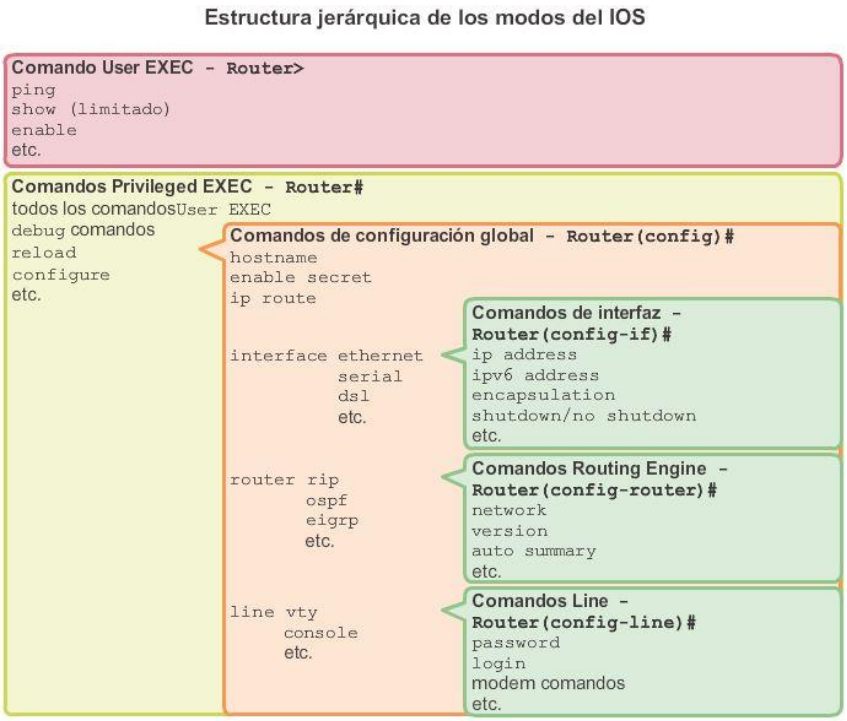
En orden jerárquico desde el más básico hasta el más especializado, los modos principales son los siguientes:

- Modo de usuario (EXEC de usuario)
- Modo de ejecución privilegiado (EXEC privilegiado)
- Modo de configuración global
- Otros modos de configuración específicos, como el modo de configuración de interfaz

Cada modo tiene una petición de entrada distinta y se utiliza para realizar tareas determinadas con un conjunto específico de comandos que están disponibles solo para el modo en cuestión. Por ejemplo, el modo de configuración global permite que los técnicos configuren los parámetros del dispositivo que lo afectan en su conjunto, como la configuración del nombre de dispositivo. Sin embargo, se requiere un modo diferente si el técnico de red desea configurar los parámetros de seguridad en un puerto específico de un switch, por ejemplo. En ese caso, el técnico de red debe ingresar al modo de configuración de interfaz para ese puerto específico. Todas las configuraciones que se introducen en el modo de configuración de interfaz se aplican solo a ese puerto.

Se puede configurar la estructura jerárquica para proporcionar seguridad. Puede requerirse una autenticación diferente para cada modo jerárquico. Así se controla el nivel de acceso que puede concederse al personal de red.

En la ilustración, se muestra la estructura de los modos de IOS con sus peticiones de entrada y características típicas.



Capítulo 2: Configuración de un sistema operativo de red 2.1.3.2 Modos principales

Los dos modos de funcionamiento principales son el modo EXEC del usuario y el modo EXEC privilegiado. Como característica de seguridad, el software Cisco IOS divide las sesiones de EXEC en dos niveles de acceso. Como se muestra en la ilustración, el modo EXEC privilegiado tiene un mayor nivel de autoridad con respecto a lo que permite que realicen los usuarios en el dispositivo.

Modo EXEC del usuario

El modo EXEC del usuario tiene capacidades limitadas, pero es útil para algunas operaciones básicas. El modo EXEC del usuario se encuentra en el nivel más básico de la estructura jerárquica modal. Este es el primer modo que se encuentra al entrar a la CLI de un dispositivo IOS.

El modo EXEC del usuario permite sólo una cantidad limitada de comandos de monitoreo básicos. A menudo se le describe como un modo de visualización solamente. El nivel EXEC del usuario no permite la ejecución de ningún comando que podría cambiar la configuración del dispositivo.

En forma predeterminada, no se requiere autenticación para acceder al modo EXEC del usuario desde la consola. Sin embargo, siempre conviene asegurarse de que se configure la autenticación durante la configuración inicial.

El modo EXEC del usuario se puede reconocer por la petición de entrada de la CLI que termina con el símbolo >. Este es un ejemplo que muestra el símbolo > en la petición de entrada:

Switch>

Modo EXEC privilegiado

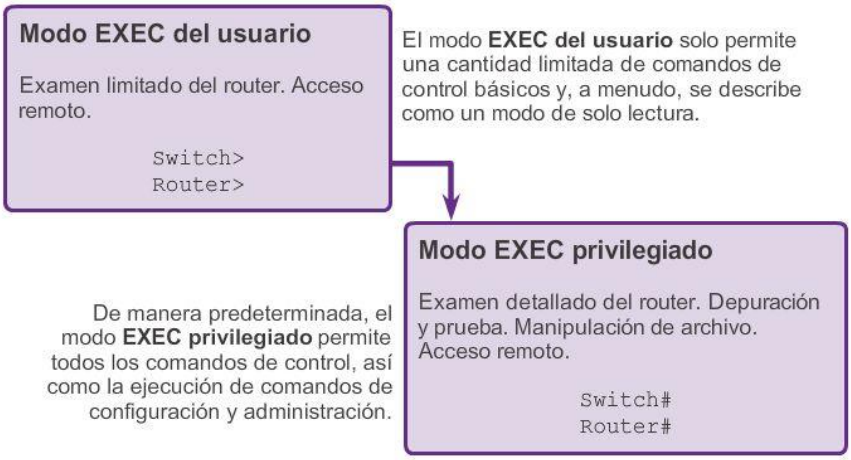
La ejecución de los comandos de configuración y administración requiere que el administrador de red utilice el modo EXEC privilegiado o un modo más específico en la jerarquía. Esto significa que los usuarios deben ingresar primero al modo EXEC del usuario y, desde allí, acceder al modo EXEC privilegiado.

El modo EXEC privilegiado se puede reconocer por la petición de entrada que termina con el símbolo #.

Switch#

De manera predeterminada, el modo EXEC privilegiado no requiere autenticación. Siempre conviene asegurarse de que la autenticación esté configurada.

Para ingresar al modo de configuración global y a todos los demás modos de configuración más específicos, es necesario entrar al modo EXEC privilegiado. En una sección posterior de este capítulo, analizaremos la configuración de dispositivos y algunos de los modos de configuración.



Capítulo 2: Configuración de un sistema operativo de red 2.1.3.3 Modo y submodos de configuración global

Solo se puede ingresar al modo de configuración global y a los modos de configuración de interfaz por medio del modo EXEC privilegiado.

Modo de configuración global

El modo de configuración principal recibe el nombre de configuración global o global config. En el modo de configuración global, se realizan cambios en la configuración de la CLI que afectan el funcionamiento del dispositivo en su totalidad. Antes de acceder a los modos de configuración específicos, se accede al modo de configuración global.

El siguiente comando de la CLI se usa para cambiar el dispositivo del modo EXEC privilegiado al modo de configuración global y para permitir la entrada de comandos de configuración desde una terminal:

Switch# configure terminal

Una vez que se ejecuta el comando, la petición de entrada cambia para mostrar que el switch está en el modo de configuración global.

Switch(config)#

Modos de configuración específicos

En el modo de configuración global, el usuario puede ingresar a diferentes modos de subconfiguración. Cada uno de estos modos permite la configuración de una parte o función específica del dispositivo IOS. La lista que se presenta a continuación muestra algunos de ellos:

Modo de interfaz: para configurar una de las interfaces de red (Fa0/0, S0/0/0).

Modo de línea: para configurar una de las líneas físicas o virtuales (consola, auxiliar, VTY).

En la figura 1, se muestran las peticiones de entrada de algunos de estos modos. Para salir de un modo de configuración específico y volver al modo de configuración global, escriba exit (salir) en la petición de entrada.

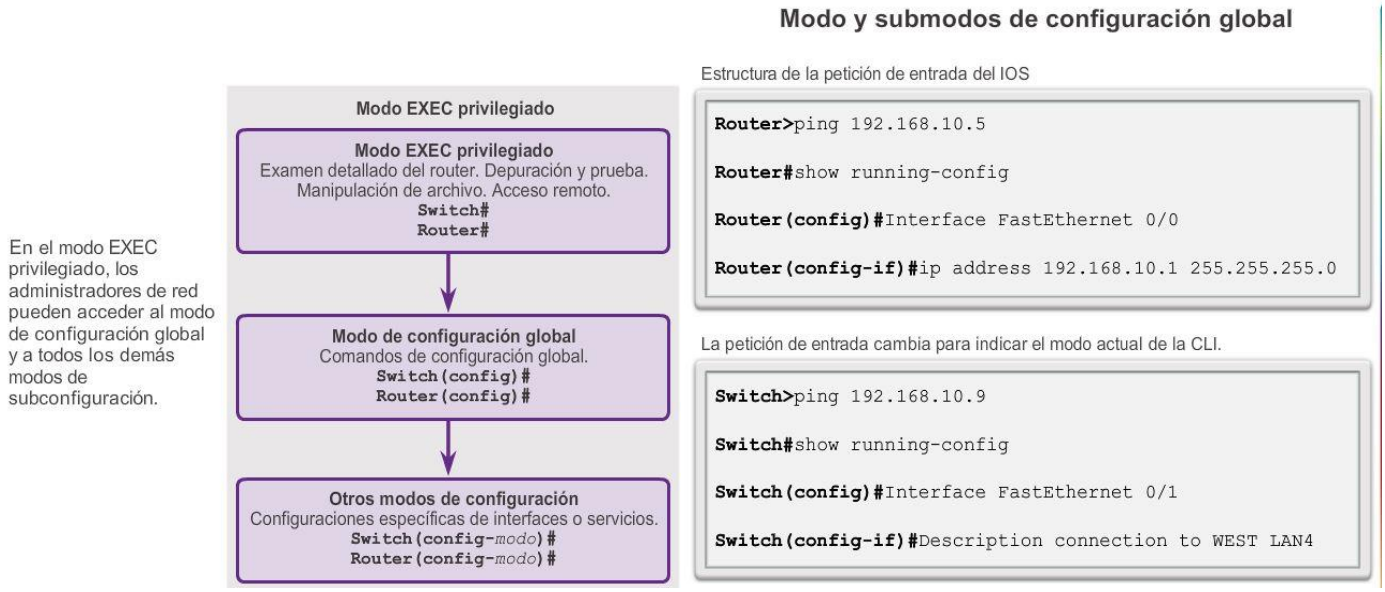
Para salir completamente del modo de configuración y volver al modo EXEC privilegiado, ingrese end o use la secuencia de teclas Ctrl-Z.

Indicadores del sistema

Cuando se usa la CLI, el modo se identifica mediante la petición de entrada de línea de comandos que es exclusiva de ese modo. De manera predeterminada, cada petición de entrada empieza con el nombre del dispositivo. Después del nombre, el resto de la petición de entrada indica el modo. Por ejemplo, la petición de entrada predeterminada del modo de configuración global en un switch sería la siguiente:

Switch(config)#

A medida que se utilizan los comandos y se cambian los modos, la petición de entrada cambia para reflejar el contexto actual, como se muestra en la figura 2.



Capítulo 2: Configuración de un sistema operativo de red 2.1.3.4 Navegación entre los modos de IOS

Cómo alternar entre los modos EXEC del usuario y privilegiado

Los comandos enable y disable se usan para cambiar la CLI entre el modo EXEC del usuario y el modo EXEC privilegiado, respectivamente.

Para acceder al modo EXEC privilegiado, use el comando enable. El modo EXEC privilegiado en ocasiones se denomina modo enable.

La sintaxis para ingresar el comando enable es:

Switch> enable

Este comando se ejecuta sin la necesidad de un argumento o una palabra clave. Una vez que se presiona la tecla Entrar, la petición de entrada pasa a ser la siguiente:

Switch#

El símbolo # al final de la petición de entrada indica que el switch está ahora en el modo EXEC privilegiado.

Si se configuró la autenticación de contraseña para el modo EXEC privilegiado, el IOS solicita la contraseña.

Por ejemplo:

Switch> enable

Password:

Switch#

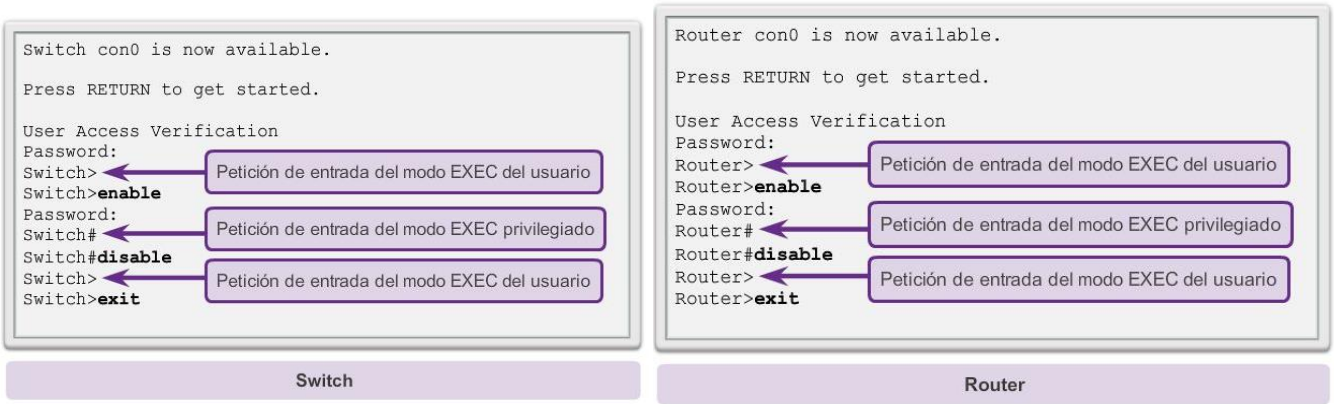
El comando disable se usa para volver del modo EXEC privilegiado al modo EXEC del usuario.

Por ejemplo:

Switch# disable

Switch>

Como se muestra en la ilustración, los comandos para acceder al modo EXEC privilegiado y para regresar al modo EXEC del usuario en un router Cisco son idénticos a los que se utilizan en un switch Cisco.



Capítulo 2: Configuración de un sistema operativo de red 2.1.3.5 Navegación entre los modos de IOS (cont.)

Cómo alternar entre el modo y los submodos de configuración global

Para salir del modo de configuración global y volver al modo EXEC privilegiado, introduzca el comando exit.

Tenga en cuenta que, al introducir el comando exit en el modo EXEC privilegiado, la sesión de consola finaliza. Es decir que, al introducir exit en el modo EXEC privilegiado, aparece la pantalla que se ve cuando se inicia una sesión de consola. En esta pantalla, se debe presionar la tecla Entrar para ingresar al modo EXEC del usuario.

Para pasar de cualquier submodo del modo de configuración global al modo que se encuentra un nivel más arriba en la jerarquía de modos, introduzca el comando exit. En la figura 1, se muestra cómo pasar del modo EXEC del usuario al modo EXEC privilegiado, cómo ingresar luego al modo de configuración global y al modo de configuración de interfaz, cómo volver al modo de configuración global y cómo regresar al modo EXEC privilegiado utilizando el comando exit.

Para pasar de cualquier submodo del modo EXEC privilegiado al modo EXEC privilegiado, introduzca el comando end o presione la combinación de teclas Ctrl+Z. En la figura 2, se muestra cómo pasar del modo de configuración de VLAN al modo EXEC privilegiado utilizando el comando end.

Para pasar de cualquier submodo del modo de configuración global a otro submodo “inmediato” de dicho modo, solo debe introducir el comando correspondiente que normalmente se introduce en el modo de configuración global. En la ilustración 3, se muestra cómo pasar del modo de configuración de línea, Switch(config-line)#, al modo de configuración de interfaz, Switch(config-if)#, sin tener que salir del modo de configuración de línea.

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# line vty 0 4
Switch(config-line)# interface fastethernet 0/1
Switch(config-if)# end
Switch#
```

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# interface vlan 1
Switch(config-if)# exit
Switch(config)# exit
Switch#
```

```
Switch# configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)# vlan 1
Switch(config-vlan)# end
Switch#
```

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.1 Estructura de los comandos de IOS

Estructura básica de comandos de IOS

Los dispositivos Cisco IOS admiten muchos comandos. Cada comando de IOS tiene una sintaxis o formato específico y puede ejecutarse solamente en el modo adecuado. La sintaxis general para un comando es el comando seguido de las palabras clave y los argumentos correspondientes.

Algunos comandos incluyen un subconjunto de palabras clave y argumentos que proporcionan funcionalidad adicional. Los comandos se utilizan para ejecutar una acción y las palabras clave se utilizan para identificar dónde o cómo ejecutar el comando.

Como se muestra en la figura 1, el comando es la palabra o las palabras iniciales que se introducen en la línea de comandos a continuación de la petición de entrada. Los comandos no distinguen mayúsculas de minúsculas. A continuación del comando siguen una o más palabras clave y argumentos. Una vez que introduzca cada comando completo, incluidos cualquier palabra clave y argumento, presione la tecla Entrar para enviar el comando al intérprete de comandos.

Las palabras clave describen parámetros específicos al intérprete de comandos. Por ejemplo, el comando show se usa para mostrar información sobre el dispositivo.

Este comando tiene varias palabras clave que deben utilizarse para definir el resultado específico que se debe mostrar. Por ejemplo:

Switch# show running-config

El comando show va seguido de la palabra clave running-config. La palabra clave especifica que se mostrará la configuración en ejecución como resultado.

Convenciones de los comandos de IOS

Un comando podría requerir uno o más argumentos. A diferencia de una palabra clave, generalmente un argumento no es una palabra predefinida. Un argumento es un valor o una variable definida por el usuario. Para determinar cuáles son las palabras clave y los argumentos requeridos para un comando, consulte la sintaxis de comandos. La sintaxis proporciona el patrón o el formato que se debe utilizar cuando se introduce un comando.

Por ejemplo, la sintaxis para utilizar el comando description es la siguiente:

Switch(config-if)# description *cadena*

Como se muestra en la figura 2, el texto en negrita indica los comandos y las palabras clave que se escriben como se muestran, y el texto en cursiva indica un argumento para el que el usuario proporciona el valor. Para el comandodescription, el argumento es un valor de cadena. El valor de cadena puede ser cualquier cadena de texto de hasta 80 caracteres.

En consecuencia, al aplicar una descripción a una interfaz con el comandodescription, se debe introducir una línea como la siguiente:

Switch(config-if)# description Switch de oficina central

El comando es description, y el argumento definido por el usuario esSwitch de oficina central.

Los siguientes ejemplos muestran algunas convenciones utilizadas para registrar y usar comandos de IOS.

Para el comando ping:

Sintaxis:

Switch> ping *dirección IP*

Ejemplo con valores:

Switch> ping 10.10.10.5

El comando es ping, y el argumento definido por el usuario es la dirección IP10.10.10.5.

De manera similar, la sintaxis para ingresar el comando traceroute es:

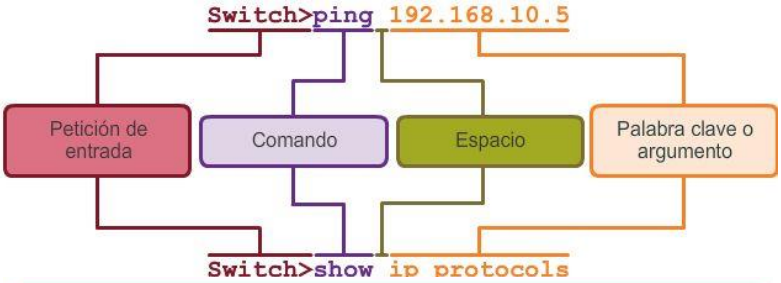
Sintaxis:

Switch> traceroute *dirección IP*

Ejemplo con valores:

Switch> traceroute 192.168.254.254

El comando es traceroute, y el argumento definido por el usuario es la dirección IP 192.168.254.254.



Cuando se describe el uso de comandos, se suelen utilizar estas convenciones.

Convención	Descripción
Negrita	El texto en negrita indica los comandos y las palabras clave que se introducen literalmente como se muestran.
Cursiva	El texto en cursiva indica los argumentos para los cuales el usuario proporciona el valor.
[x]	Los corchetes indican un elemento optativo (palabra clave o argumento).
{x}	Las llaves indican un elemento obligatorio (palabra clave o argumento).
[x {y | z}]	Las llaves y las líneas verticales dentro de corchetes indican una opción obligatoria dentro de un elemento optativo.

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.2 Referencia de comandos de Cisco IOS

Cisco IOS Command Reference (Referencia de comandos de Cisco IOS) es una colección de documentos en línea que describen en detalle los comandos de IOS utilizados en los dispositivos Cisco. La referencia de comandos es la mejor fuente de información sobre comandos de IOS específicos, de la misma manera en que un diccionario es la mejor fuente para obtener información sobre una palabra específica.

La referencia de comandos es un recurso fundamental que los ingenieros de redes utilizan para revisar diversas características de un comando de IOS determinado. Algunas de las características más frecuentes son las siguientes:

- Sintaxis: la versión más detallada de la sintaxis para un comando que se puede encontrar.
- Predeterminado: la manera en que el comando se implementa en un dispositivo con una configuración predeterminada.
- Modo: el modo de configuración del dispositivo en el que se introduce el comando.
- Historial: descripciones de cómo se implementa el comando en relación con la versión de IOS.
- Pautas de uso: pautas que describen específicamente cómo implementar el comando.
- Ejemplos: ejemplos útiles que muestran situaciones en las que se utiliza el comando con frecuencia.

Para navegar hasta la referencia de comandos y buscar un comando específico, siga los pasos que se indican a continuación:

Paso 1. Acceda a www.cisco.com.
Paso 2. Haga clic en Support (Soporte).
Paso 3. Haga clic en Networking Software (Software de redes) (IOS e NX-OS).
Paso 4. Haga clic en 15.2M&T, (por ejemplo).
Paso 5. Haga clic en Reference Guides (Guías de referencia).
Paso 6. Haga clic en Command References (Referencias de comandos).
Paso 7. Haga clic en la tecnología específica que abarca el comando al que hace referencia.
Paso 8. Haga clic en el enlace de la izquierda que coincida alfabéticamente con el comando al que hace referencia.
Paso 9. Haga clic en el enlace del comando.

Por ejemplo, el comando description se encuentra en *Cisco IOS Interface and Hardware Component Command Reference* (Referencia de comandos de componentes de hardware y de interfaz de Cisco IOS), en el enlace para el rango alfabético *D through E* (D a E).

Nota: se pueden descargar versiones completas de las referencias de comandos para una tecnología determinada en formato PDF mediante los enlaces que se encuentran en la página a la que se llega después de completar el paso 7 mencionado anteriormente.

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.3 Ayuda contextual

El IOS ofrece varias formas de ayuda:

- Ayuda contextual
- Verificación de la sintaxis del comando
- Teclas de acceso rápido y métodos abreviados

Ayuda contextual

La ayuda contextual proporciona una lista de comandos y los argumentos asociados con esos comandos dentro del contexto del modo actual. Para acceder a la ayuda contextual, introduzca un signo de interrogación, ?, en cualquier petición de entrada. Aparece una respuesta inmediata sin necesidad de utilizar la tecla Entrar.

Uno de los usos de la ayuda contextual es para la obtención de una lista de los comandos disponibles. Dicha lista puede utilizarse cuando existen dudas sobre el nombre de un comando o se desea verificar si el IOS admite un comando específico en un modo determinado.

Por ejemplo, para obtener una lista de los comandos disponibles en el nivel EXEC del usuario, introduzca un signo de interrogación, ?, en la petición de entrada Switch>.

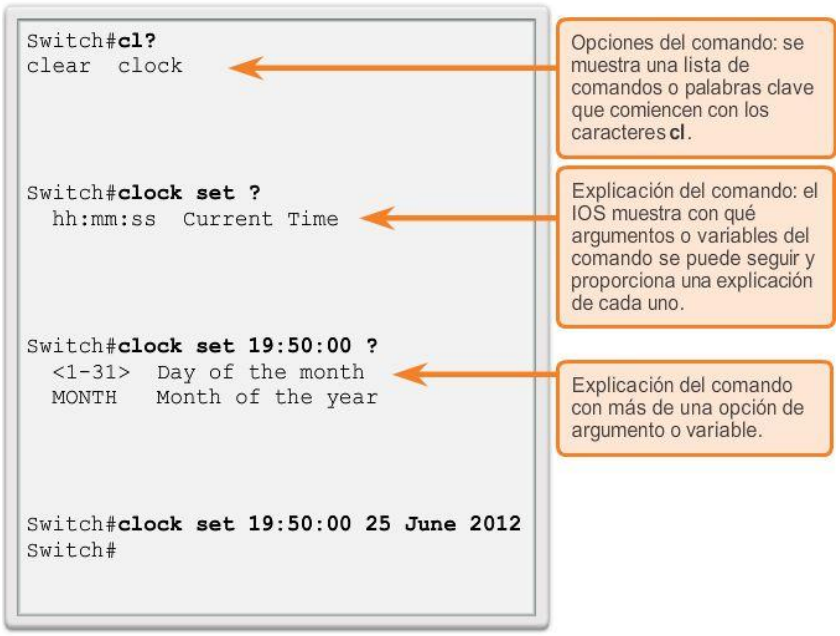
Otro de los usos de la ayuda contextual es visualizar una lista de los comandos o palabras clave que empiezan con uno o varios caracteres específicos. Si se introduce un signo de interrogación, sin espacio, inmediatamente después de introducir una secuencia de caracteres, el IOS muestra una lista de comandos o palabras clave para el contexto que comienzan con los caracteres introducidos.

Por ejemplo, introduzca sh? para obtener una lista de los comandos que comienzan con la secuencia de caracteres sh.

Un último tipo de ayuda contextual se utiliza para determinar qué opciones, palabras clave o argumentos coinciden con un comando específico. Al introducir un comando, introduzca un espacio seguido de un ? para determinar qué puede o debe introducirse a continuación.

Como se muestra en la ilustración, después de introducir el comando clock set 19:50:00, se puede introducir el signo? para determinar las demás opciones o palabras clave disponibles para este comando.

Ayuda contextual



Capítulo 2: Configuración de un sistema operativo de red 2.1.4.4 Verificación de la sintaxis del comando

Verificación de la sintaxis del comando

Cuando se emite un comando presionando la tecla Entrar, el intérprete de la línea de comandos analiza la sintaxis del comando de izquierda a derecha para determinar qué acción se solicitó. En general, el IOS solo proporciona comentarios negativos, como se muestra en la figura 1. Si el intérprete comprende el comando, la acción requerida se ejecuta y la CLI vuelve a la petición de entrada correspondiente. Sin embargo, si el intérprete no puede comprender el comando que se ingresa, mostrará un comentario que describe el error del comando.

En la figura 2, se muestran tres tipos distintos de mensajes de error:

Ambiguous command (comando ambiguo)

Incomplete command (comando incompleto)

Incorrect command (comando incorrecto)

El comando de IOS clock set es ideal para experimentar con los distintos mensajes de ayuda de la revisión de sintaxis de comandos, como se muestra en la figura 1. En la figura 2, se proporciona ayuda sobre los tres tipos de mensajes de error.

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.5 Teclas de acceso rápido y métodos abreviados

Teclas de acceso rápido y métodos abreviados

La interfaz de línea de comandos IOS proporciona teclas de acceso rápido y métodos abreviados que facilitan la configuración, el monitoreo y la resolución de problemas.

En la ilustración se muestran la mayoría de los métodos abreviados. Merece la pena tener en cuenta de manera especial los siguientes:

Flecha abajo: permite al usuario desplazarse hacia delante a través de los comandos anteriores.

Flecha arriba: permite al usuario desplazarse hacia atrás a través de los comandos anteriores.

Tabulación: completa el resto de un comando o de una palabra clave que se escribió parcialmente.

Ctrl-A: se traslada al comienzo de la línea.

Ctrl-E: se traslada al final de la línea.

Ctrl-R: vuelve a mostrar una línea

Ctrl-Z: sale del modo de configuración y vuelve al modo EXEC del usuario.

Ctrl-C: sale del modo de configuración o cancela el comando actual.

Ctrl-Mayús-6: permite al usuario interrumpir un proceso de IOS, como ping o traceroute.

Análisis más detallado de algunos de ellos:

Tabulación

La tecla de tabulación se utiliza para completar el resto de los comandos y los parámetros abreviados, siempre que la abreviatura contenga suficientes letras para diferenciarse de cualquier otro comando o parámetro actualmente disponible.

Cuando se ha ingresado una parte suficiente del comando o la palabra clave como para que sean únicos, presione la tecla Tab y la CLI mostrará el resto del comando o palabra clave.

Esta es una buena técnica para usar cuando se está aprendiendo porque permite ver la palabra completa utilizada para el comando o palabra clave.

Ctrl-R

La función de volver a mostrar la línea actualiza la línea que se acaba de escribir. Use Ctrl-R para volver a mostrar la línea. Por ejemplo, puede ocurrir que el IOS esté reenviando un mensaje a la CLI justo cuando se está escribiendo una línea. Puede usar Ctrl-R para actualizar la línea y evitar tener que volver a escribirla.

En este ejemplo, aparece en medio de un comando un mensaje sobre una falla en una interfaz.

Switch# show mac-

16w4d: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down

16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to down

Para volver a mostrar la línea que estaba escribiendo, utilice Ctrl-R:

Switch# show mac

Ctrl-Z

Esta combinación de teclas permite salir de cualquier modo de configuración y volver al modo EXEC privilegiado. Dado que el IOS tiene una estructura de modos jerárquica, el usuario puede encontrarse varios niveles hacia abajo. En lugar de salir de cada modo en forma individual, utilice Ctrl-Z para volver directamente a la petición de entrada de EXEC privilegiado en el nivel superior.

Flechas arriba y abajo

Las teclas de comandos anteriores recuerdan el historial de comandos introducidos. El software IOS de Cisco almacena temporalmente varios caracteres y comandos anteriores de manera tal que las entradas puedan recuperarse. El búfer es útil para volver a introducir comandos sin tener que volver a escribirlos.

Existen secuencias clave para desplazarse a través de estos comandos almacenados en el búfer. Use la tecla flecha arriba (Ctrl-P) para mostrar los comandos introducidos anteriormente. Cada vez que se presiona esta tecla, se mostrará el siguiente comando sucesivo anterior. Use la tecla flecha abajo(Ctrl-N) para desplazarse hacia delante en el historial y mostrar los comandos más recientes.

Ctrl-Mayús-6

La secuencia de escape interrumpe cualquier proceso en ejecución. Cuando se inicia un proceso del IOS desde la CLI, como un ping o traceroute, el comando se ejecuta hasta que se termina o interrumpe. Mientras el proceso está en ejecución, la CLI no responde. Para interrumpir el resultado e interactuar con la CLI, presione Ctrl-Mayús-6.

Ctrl-C

Interrumpe la entrada de un comando y sale del modo de configuración, lo que resulta útil después de introducir un comando que se necesita cancelar.

Abreviación de comandos o palabras clave

Los comandos y las palabras clave pueden abreviarse a la cantidad mínima de caracteres que identifiquen una selección única. Por ejemplo, el comandoconfigure puede abreviarse en conf ya que configure es el único comando que empieza con conf. La abreviatura con no dará resultado ya que hay más de un comando que empieza con con.

Las palabras clave también pueden abreviarse.

Otro ejemplo podría ser show interfaces, que se puede abreviar de la siguiente manera:

Switch# show interfaces

Switch# show int

Se puede abreviar tanto el comando como las palabras clave, por ejemplo:

Switch# sh int

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.6 Comandos de examen de IOS

Para verificar y resolver problemas en la operación de la red, debemos examinar la operación de los dispositivos. El comando básico de examen es el comando show.

Existen muchas variantes diferentes de este comando. A medida que el usuario adquiera más conocimientos sobre IOS, aprenderá a usar e interpretar el resultado de los comandos show. Utilice el comando show ? para obtener una lista de los comandos disponibles en un modo o contexto determinado.

Un comando show típico puede proporcionar información sobre la configuración, el funcionamiento y el estado de las partes de un switch o un router Cisco. En la ilustración, se destacan algunos de los comandos de IOS frecuentes.

En este curso, la atención se centra principalmente en los comandos showbásicos.

Un comando show de uso frecuente es show interfaces. Este comando muestra estadísticas de todas las interfaces del dispositivo. Para ver las estadísticas de una interfaz específica, introduzca el comando show interfaces seguido del tipo de interfaz específico y el número de ranura o de puerto. Por ejemplo:

Switch# show interfaces fastethernet 0/1

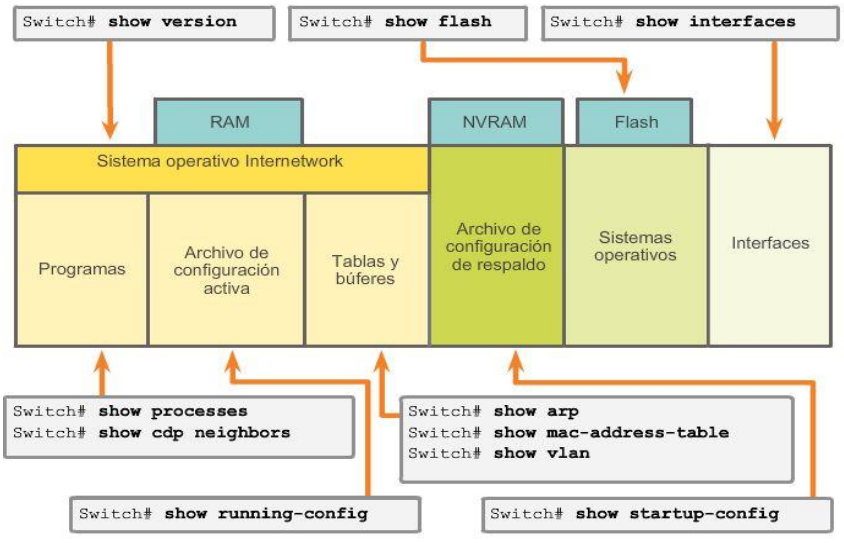
Algunos otros comandos show que los técnicos de red utilizan con frecuencia incluyen los siguientes:

show startup-config: muestra la configuración guardada ubicada en la NVRAM.

show running-config: muestra el contenido del archivo de configuración en ejecución actual.

La petición de entrada More

Cuando un comando devuelve más resultados de los que pueden mostrarse en una sola pantalla, aparece la petición de entrada --More-- en la parte inferior de la pantalla. Cuando aparezca la petición de entrada --More--, presione la barra espaciadora para ver el siguiente tramo del resultado. Para visualizar sólo la siguiente línea, presione la tecla Intro. Si se presiona cualquier otra tecla, se cancela el resultado y se vuelve a la petición de entrada.



Los comandos **show** del IOS pueden proporcionar información sobre la configuración, el funcionamiento y el estado de las partes de un switch o router Cisco.

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.7 El comando show versión

Uno de los comandos de uso más frecuente en un switch o un router es el siguiente:

Switch# show version

Este comando muestra información sobre la versión de IOS cargada actualmente, además de información sobre el hardware y los dispositivos. Si inició sesión en un router o un switch de manera remota, el comando show version es un medio excelente para obtener rápidamente un resumen de información útil sobre el dispositivo específico al cual está conectado. Algunos de los datos que se obtienen a partir de este comando son los siguientes:

Versión del software: versión del software IOS (almacenada en la memoria flash).

Versión de bootstrap: versión de bootstrap (almacenada en la ROM de arranque).

Tiempo de actividad del sistema: tiempo transcurrido desde la última vez que se reinició.

Información de reinicio del sistema: método de reinicio (por ejemplo, apagado y encendido, colapso).

Nombre de la imagen del software: nombre del archivo de IOS almacenado en la memoria flash.

Tipo de router y tipo de procesador: número de modelo y tipo de procesador.

Tipo y asignación de memoria (compartida/principal): memoria RAM del procesador principal y almacenamiento en búfer de E/S de paquetes compartidos.

Características del software: protocolos y conjuntos de características admitidos.

Interfaces de hardware: interfaces disponibles en el dispositivo.

Registro de configuración: establece especificaciones de arranque, la configuración de velocidad de la consola y parámetros relacionados.

En la figura 1, se muestra el resultado para un ISR Cisco 1941, mientras que en la figura 2 se muestra el resultado para un switch Cisco Catalyst 2960.

```
Router# show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version
15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

cisco1941 uptime is 41 minutes
System returned to ROM by power-on
System image file is ""flash0:c1900-universalk9-mz.SPA.152-
4.M1.bin""
Last reload type: Normal Reload
Last reload reason: power-on



This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
```

```
Switch# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3,
RELEASE SOFTWARE (fc1)

Switch uptime is 44 minutes
System returned to ROM by power-on
System image file is ""flash:/c2960-lanbasek9-mz.150-2.SE.bin""


This product contains cryptographic features and is subject to
United
States and local country laws governing import, export, transfer
and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use
encryption.
```

Capítulo 2: Configuración de un sistema operativo de red 2.1.4.8 Packet Tracer: Navegación de IOS

En esta actividad, practicará las habilidades necesarias para navegar dentro de Cisco IOS, incluidos distintos modos de acceso de usuario, diversos modos de configuración y comandos comunes que utiliza

habitualmente. También practicará el acceso a la ayuda contextual mediante la configuración del comando clock.

Capítulo 2: Configuración de un sistema operativo de red 2.2.1.1 Por qué elegir un switch

Según lo analizado, los switches y los routers 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 durante su implementación en una red son idénticos para ambos dispositivos.

Sin embargo, un switch Cisco IOS es uno de los dispositivos más simples que se pueden configurar en una red. Esto se debe a que no se requiere ninguna configuración antes de poner en funcionamiento el dispositivo. En su versión más básica, se puede conectar un switch sin ninguna configuración, y de todas maneras conmutará los datos entre los dispositivos conectados.

Un switch también es uno de los dispositivos fundamentales que se utilizan para crear una red pequeña. Al conectar dos PC a un switch, esas PC tienen conectividad mutua en forma inmediata.

Por lo tanto, el resto de este capítulo se centra en la creación de una pequeña red de dos PC conectada mediante un switch configurado con los parámetros iniciales. Los parámetros iniciales incluyen la configuración de un nombre para el switch, la limitación del acceso a la configuración del dispositivo, la configuración de mensajes de aviso y guardar la configuración.

Capítulo 2: Configuración de un sistema operativo de red 2.2.1.2 Nombres de dispositivos

Al configurar un dispositivo de red, uno de los primeros pasos es la configuración de un nombre de dispositivo único o “nombre de host”. Los nombres de host aparecen en las peticiones de entrada de la CLI, pueden utilizarse en varios procesos de autenticación entre dispositivos y deben utilizarse en los diagramas de topologías.

Los nombres de host se configuran en el dispositivo de red activo. Si el nombre del dispositivo no se configura explícitamente, Cisco IOS utiliza un nombre de dispositivo predeterminado de fábrica. El nombre predeterminado de los switches Cisco IOS es “Switch”.

Imagine si una internetwork tuviera varios switches con el nombre predeterminado “Switch” (como se muestra en la ilustración). Esto generaría una gran confusión durante la configuración y el mantenimiento de la red. Al acceder a un dispositivo remoto mediante SSH, es importante tener la confirmación de que se está conectado al dispositivo correcto. Si se dejara el nombre predeterminado en todos los dispositivos, sería difícil determinar que el dispositivo correcto está conectado.

Al elegir nombres adecuados, resulta más fácil recordar, analizar, registrar e identificar los dispositivos de red. Para nombrar los dispositivos de manera uniforme y provechosa, es necesario el establecimiento de una convención de denominación que se extienda por toda la empresa o, al menos, por la división.

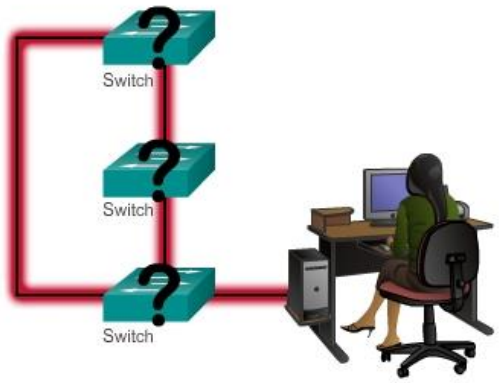
A fin de permitir la continuidad dentro de una organización, siempre conviene crear la convención de nomenclatura al mismo tiempo que el esquema de direccionamiento.

Según ciertas pautas de convenciones de denominación, los nombres deberían:

- Comenzar con una letra.
- No contener espacios.
- Finalizar con una letra o dígito.
- Utilizar solamente letras, dígitos y guiones.
- Tener menos de 64 caracteres de longitud.

Los nombres de host utilizados en el IOS del dispositivo conservan el uso de caracteres en mayúscula y minúscula. Por lo tanto, es posible escribir un nombre con mayúsculas como se haría normalmente. Esto contrasta con la mayoría de los esquemas de denominación de Internet, donde los caracteres en mayúsculas y minúsculas reciben igual trato.

Configuración básica mediante Cisco IOS



Sin nombres, es difícil identificar los dispositivos de red para propósitos de configuración.

Capítulo 2: Configuración de un sistema operativo de red 2.2.1.3 Nombres de host

Los nombres de host permiten que los administradores de red identifiquen dispositivos a través de una red o de Internet.

Ejemplo de aplicación de nombres

Utilicemos un ejemplo de tres switches conectados en una red que abarca tres pisos diferentes.

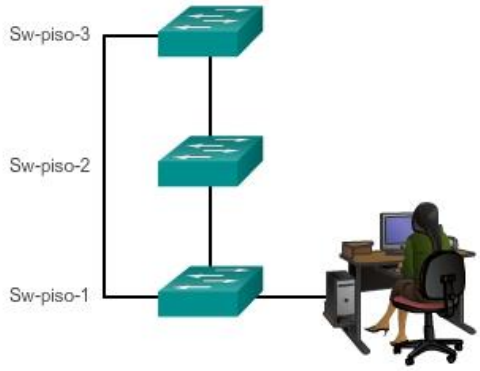
A fin de crear una convención de nomenclatura para los switches, se debe tener en cuenta la ubicación y el propósito de los dispositivos.

Por ejemplo, en la ilustración se denominó a los tres switches como Sw-piso-1, Sw-piso-2 y Sw-piso-3.

En la documentación de la red, se incluirán estos nombres y los motivos de su elección, a fin de asegurar la continuidad de nuestra convención de denominación a medida que se agregan dispositivos.

Una vez que se identifica la convención de nomenclatura, el paso siguiente es aplicar los nombres a los dispositivos usando la CLI.

Configuración de nombres de dispositivos



Con nombres, es fácil identificar los dispositivos de red para propósitos de configuración.

Capítulo 2: Configuración de un sistema operativo de red 2.2.1.4 Configuración de nombres de host

Configuración del nombre de host de IOS

En el modo EXEC privilegiado, acceda al modo de configuración global introduciendo el comando configure terminal:

Switch# configure terminal

Después de que se ejecuta el comando, la petición de entrada cambiará a:

Switch(config)#

Introduzca el nombre de host en el modo de configuración global, como se muestra en la ilustración:

Switch(config)# hostname Sw-piso-1

Después de que se ejecuta el comando, la petición de entrada cambiará a:

Sw-piso-1 (config)#

Observe que el nombre de host aparece en la petición de entrada. Para salir del modo de configuración global, utilice el comando exit.

Siempre asegúrese de que la documentación esté actualizada cada vez que se agrega o modifica un dispositivo. Identifique los dispositivos en la documentación por su ubicación, propósito y dirección.

Nota: para deshacer los efectos de un comando, escriba la palabra clave noantes del comando.

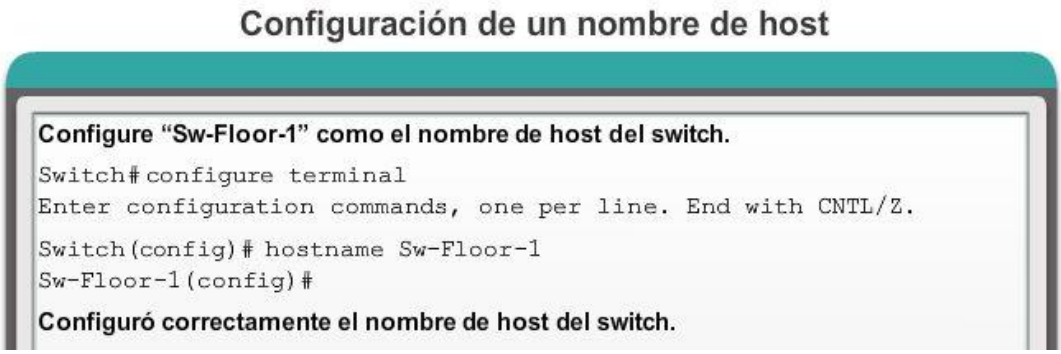
Por ejemplo, para eliminar el nombre de un dispositivo, utilice:

Sw-piso-1 (config)# no hostname

Switch(config)#

Observe que el comando no hostname provocó que el switch volviera a usar el nombre de host predeterminado “Switch”.

En la ilustración, practique la introducción de un nombre de host en un switch.



Capítulo 2: Configuración de un sistema operativo de red 2.2.2.1 Protección del acceso a los dispositivos

La limitación física del acceso a los dispositivos de red mediante su colocación en armarios y bastidores bajo llave es aconsejable; sin embargo, las contraseñas son la principal defensa contra el acceso no autorizado a los dispositivos de red. Todos los dispositivos, incluso los routers domésticos, deben tener contraseñas configuradas en forma local para limitar el acceso. Más adelante, se presentará la forma de reforzar la seguridad mediante la solicitud de un nombre de usuario junto con una contraseña. Por ahora, presentaremos precauciones de seguridad básicas mediante el uso de contraseñas únicamente.

Como se comentó anteriormente, el IOS usa modos jerárquicos para colaborar con la seguridad del dispositivo. Como parte de este cumplimiento de seguridad, el IOS puede aceptar diversas contraseñas para permitir diferentes privilegios de acceso al dispositivo.

Las contraseñas ingresadas aquí son:

- Contraseña de enable: limita el acceso al modo EXEC privilegiado.
- Contraseña secreta de enable: es una contraseña encriptada que limita el acceso al modo EXEC privilegiado.
- Contraseña de consola: limita el acceso a los dispositivos mediante la conexión de consola.
- Contraseña de VTY: limita el acceso a los dispositivos a través de Telnet.

Siempre conviene utilizar contraseñas de autenticación diferentes para cada uno de estos niveles de acceso. Si bien no es práctico iniciar sesión con varias contraseñas diferentes, es una precaución necesaria para proteger adecuadamente la infraestructura de la red ante accesos no autorizados.

Además, utilice contraseñas seguras que no se descubran fácilmente El uso de contraseñas simples o fáciles de adivinar continúa siendo un problema de seguridad en muchas facetas del mundo empresarial.

Considere estos puntos clave cuando elija contraseñas:

- Use contraseñas que tengan más de 8 caracteres.
- Utilice una combinación de letras mayúsculas y minúsculas, números, caracteres especiales o secuencias numéricas en las contraseñas.
- Evite el uso de la misma contraseña para todos los dispositivos.
- Evite el uso de palabras comunes como contraseña o administrador, porque se descubren fácilmente.

Nota: en la mayoría de las prácticas de laboratorio de este curso, se utilizan contraseñas simples como cisco o class. Estas contraseñas se consideran no seguras y fáciles de adivinar, y deben evitarse en un entorno laboral. Estas contraseñas solo se utilizan por comodidad en el aula o para ilustrar ejemplos de configuración.

Capítulo 2: Configuración de un sistema operativo de red 2.2.2.2 Protección del acceso a EXEC privilegiado

Para proteger el acceso a EXEC privilegiado, utilice el comando enable secret*contraseña*. Una variación más antigua y menos segura de este comando es el comando enable password *contraseña*. Si bien puede utilizarse cualquiera de estos comandos para establecer la autenticación antes de permitir el acceso al modo EXEC privilegiado (enable), se recomienda utilizar el comando enable secret. El comando enable secret proporciona mayor seguridad, dado que la contraseña está encriptada.

Comando de ejemplo para establecer contraseñas:

Switch(config)# enable secret class

El ejemplo de la ilustración muestra que no se solicita una contraseña cuando se utiliza el comando enable por primera vez. A continuación, se configura el comando enable secret class, y el acceso a EXEC privilegiado ahora queda protegido. Observe que, por motivos de seguridad, la contraseña no se muestra cuando se introduce.

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Capítulo 2: Configuración de un sistema operativo de red 2.2.2.3 Protección del acceso a EXEC del usuario

El puerto de consola de dispositivos de red debe estar asegurado, como mínimo, mediante el pedido de una contraseña segura al usuario. Así se reducen las posibilidades de que personal no autorizado conecte físicamente un cable al dispositivo y obtenga acceso a éste.

Los siguientes comandos se usan en el modo de configuración global para establecer una contraseña para la línea de consola:

Switch(config)# line console 0

Switch(config-line)# password cisco

Switch(config-line)# login

En el modo de configuración global, se usa el comando line console 0 para ingresar al modo de configuración de línea de la consola. El cero se utiliza para representar la primera (y en la mayoría de los casos la única) interfaz de consola.

El segundo comando, password cisco, especifica una contraseña para la línea de consola.

El comando login configura el switch para que requiera autenticación al iniciar sesión. Cuando se habilita el inicio de sesión y se establece una contraseña, se solicita al usuario de la consola que introduzca una contraseña antes de darle acceso a la CLI.

Contraseña de VTY

Las líneas vty permiten el acceso a un dispositivo Cisco a través de Telnet. De manera predeterminada, muchos switches Cisco admiten hasta 16 líneas vty que se numeran del 0 al 15. El número de líneas vty que admite un router Cisco varía según el tipo de router y la versión de IOS. No obstante, la cantidad más frecuente de líneas vty configuradas es cinco. Estas líneas se numeran del 0 al 4 de manera predeterminada, aunque se pueden configurar líneas adicionales. Es necesario establecer una contraseña para todas las líneas vty disponibles. Puede configurarse la misma contraseña para todas las conexiones. Sin embargo, con frecuencia conviene configurar una única contraseña para una línea a fin de proporcionar un recurso secundario para el ingreso administrativo al dispositivo si las demás conexiones están en uso.

Comandos de ejemplo utilizados para establecer una contraseña en las líneas vty:

Switch(config)# line vty 0 15

Switch(config-line)# password cisco

Switch(config-line)# login

De manera predeterminada, el IOS incluye el comando login en las líneas VTY. Esto impide el acceso al dispositivo mediante Telnet sin autenticación. Si por error se establece el comando no login, que elimina el requisito de autenticación, personas no autorizadas podrían conectarse a la línea a través de la red utilizando Telnet. Esto representaría un riesgo importante para la seguridad.

En la ilustración, se muestra la protección del acceso a EXEC del usuario en las líneas de consola y las líneas Telnet.

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

Capítulo 2: Configuración de un sistema operativo de red 2.2.2.4 Visualización de contraseñas de encriptación

Existe otro comando de utilidad que impide que las contraseñas aparezcan como texto no cifrado cuando se visualizan los archivos de configuración: se trata del comando service password-encryption.

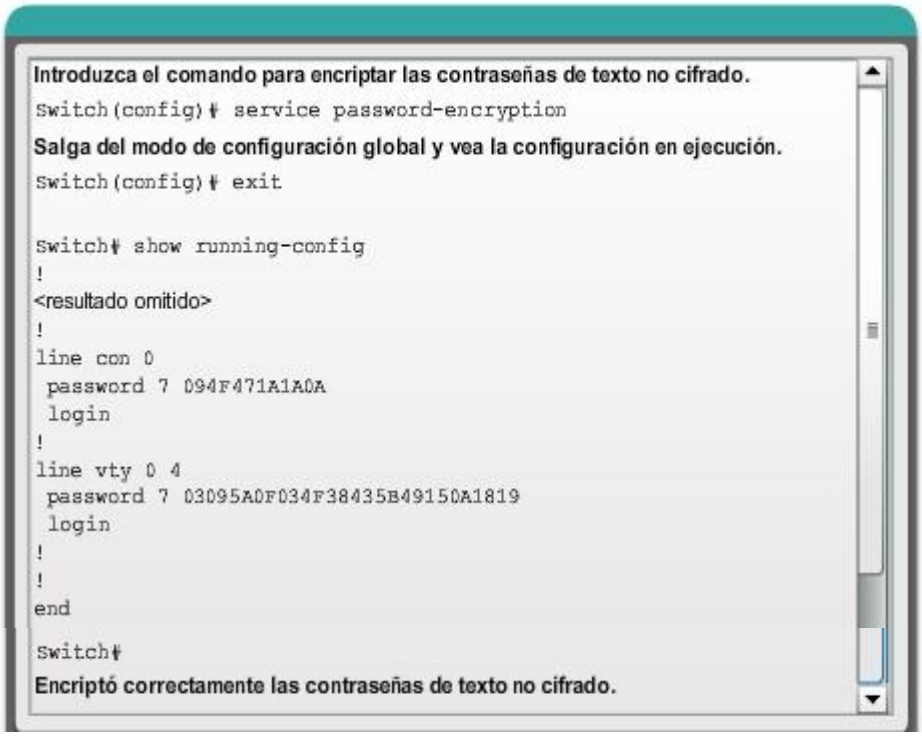
Este comando provee la encriptación de la contraseña cuando ésta se configura.

El comando service password-encryption aplica una encriptación mínima a todas las contraseñas sin encriptar. Esta encriptación solo se aplica a las contraseñas del archivo de configuración; no a las contraseñas mientras se envían a través de los medios. El propósito de este comando es evitar que individuos no autorizados vean las contraseñas en el archivo de configuración.

Si se ejecuta el comando show running-config o show startup-configantes de ejecutar el comando service password-encryption, las contraseñas sin encriptar resultan visibles en el resultado de configuración. El comando service password-encryption puede entonces ejecutarse y se aplicará la encriptación a las contraseñas. Una vez que se ha aplicado la encriptación, la cancelación del servicio de encriptación no revierte la encriptación.

En la ilustración, practique la introducción del comando para configurar la encriptación de contraseñas.

Configuración de la encriptación de contraseñas



Capítulo 2: Configuración de un sistema operativo de red 2.2.2.5 Mensajes de aviso

Aunque el pedido de contraseñas es un modo de impedir el acceso a la red de personas no autorizadas, resulta vital proveer un método para informar que sólo el personal autorizado debe intentar obtener acceso al dispositivo. Para hacerlo, agregue un aviso a la salida del dispositivo.

Los avisos pueden ser una parte importante en los procesos legales en el caso de una demanda por el ingreso no autorizado a un dispositivo. Algunos sistemas legales no permiten la acusación, y ni siquiera el monitoreo de los usuarios, a menos que haya una notificación visible.

El contenido o las palabras exactas de un aviso dependen de las leyes locales y de las políticas de la empresa. A continuación se muestran algunos ejemplos de información que se debe incluir en un aviso:

- “El uso del dispositivo es exclusivo del personal autorizado”.
- “Es posible que se esté controlando la actividad”.
- “Se iniciarán acciones legales en caso de uso no autorizado”.

Ya que cualquier persona que intenta iniciar sesión puede ver los avisos, se debe redactar el mensaje cuidadosamente. Es inapropiada toda redacción que implique que "se acepta" o "se invita" al usuario a iniciar sesión. Si una persona causa problemas en la red luego de obtener acceso no autorizado, será difícil probar la responsabilidad si hay algún indicio de invitación.

La creación de avisos es un proceso simple; sin embargo, éstos deben usarse en forma apropiada. Cuando se utiliza un aviso, este nunca debe invitar a un usuario al dispositivo. Debe aclarar que sólo el personal autorizado tiene permitido el acceso al dispositivo. Asimismo, el aviso puede incluir cierres programados del sistema y demás información que afecte a todos los usuarios de la red.

El IOS proporciona varios tipos de avisos. Un aviso común es el mensaje del día (MOTD). Con frecuencia se usa para notificaciones legales ya que se visualiza en todos los terminales conectados.

Configure el MOTD con el comando banner motd del modo de configuración global.

El comando banner motd requiere el uso de delimitadores para identificar el contenido del mensaje de aviso. El comando banner motd va seguido de un espacio y un carácter delimitador. Luego, se ingresan una o más líneas de texto para representar el mensaje del aviso. Una segunda ocurrencia del carácter delimitador denota el final del mensaje. El carácter delimitador puede ser cualquier carácter siempre que no aparezca en el mensaje. Por este motivo, a menudo se usan símbolos como "#".

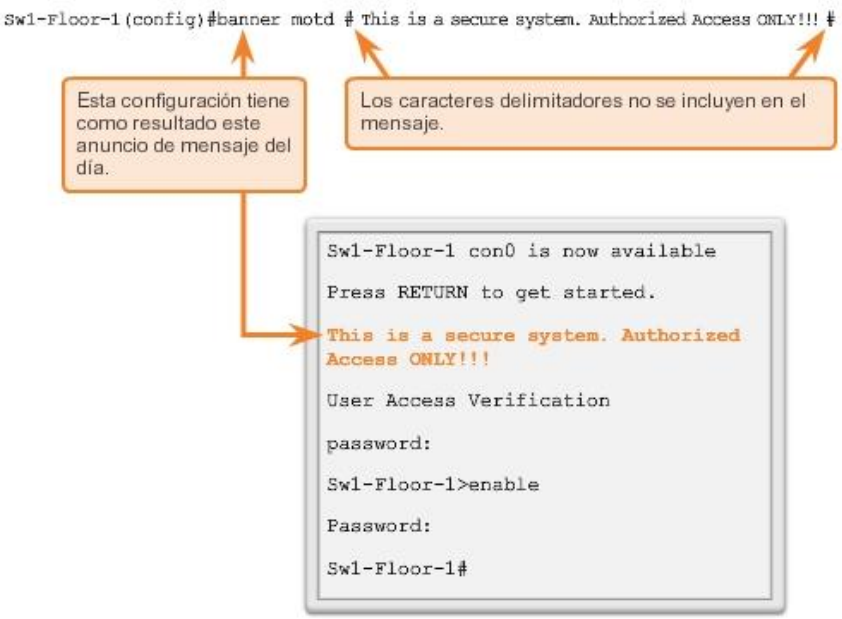
La sintaxis para configurar un MOTD en el modo de configuración global es la siguiente:

Switch(config)# banner motd # *Mensaje* #

Una vez que se ha ejecutado el comando, aparecerá el aviso en todos los intentos posteriores de acceso al dispositivo hasta que el aviso se elimine.

El ejemplo de la ilustración muestra un anuncio configurado con el símbolo delimitador “#”. Observe cómo aparece ahora el anuncio cuando se accede al switch.

Limitación del acceso a los dispositivos: MOTD



Capítulo 2: Configuración de un sistema operativo de red 2.2.3.1 Archivos de configuración

El archivo de configuración en ejecución refleja la configuración actual aplicada a un dispositivo Cisco IOS. Contiene los comandos utilizados para determinar cómo funciona el dispositivo en la red, tal como se muestra en la figura 1. La modificación de la configuración en ejecución afecta el funcionamiento de un dispositivo Cisco de inmediato.

El archivo de configuración en ejecución se almacena en la memoria de trabajo del dispositivo o memoria de acceso aleatorio (RAM). Esto significa que el archivo de configuración en ejecución está temporalmente activo

mientras el dispositivo Cisco está en funcionamiento (encendido). Sin embargo, si se corta la alimentación al dispositivo o se lo reinicia, se pierden todos los cambios de configuración, a menos que se hayan guardado.

Después de realizar cambios a un archivo de configuración en ejecución, tenga en cuenta estas distintas opciones:

- Volver a la configuración original del dispositivo.
- Eliminar todas las configuraciones del dispositivo.
- Convertir la configuración cambiada en la nueva configuración de inicio.

El archivo de configuración de inicio refleja la configuración que utilizará el dispositivo cuando se lo reinicie. El archivo de configuración de inicio se almacena en NVRAM. Cuando se configura un dispositivo de red y se modifica la configuración en ejecución, es importante guardar esos cambios en el archivo de configuración de inicio. Esto evita que los cambios se pierdan debido a cortes de energía o a un reinicio intencional.

Antes de asignar los cambios, use los correspondientes comandos show para verificar la operación del dispositivo. Como se muestra en la ilustración, se puede utilizar el comando show running-config para ver un archivo de configuración en ejecución.

Cuando se verifica que los cambios son correctos, utilice el comando copy running-config startup-config en la petición de entrada del modo EXEC privilegiado. El comando para guardar la configuración en ejecución en el archivo de configuración de inicio es:

```
Switch# copy running-config startup-config
```

Una vez que se ejecuta, el archivo de configuración en ejecución actualiza el archivo de configuración de inicio.

Si los cambios realizados en la configuración en ejecución no tienen el efecto deseado, puede ser necesario volver a la configuración previa del dispositivo. Suponiendo que no se ha sobreescrito la configuración de inicio con los cambios, se puede reemplazar la configuración en ejecución por la configuración de inicio. La mejor manera de hacerlo es reiniciando el dispositivo con el comando reload ante la petición de entrada del modo EXEC privilegiado.

Cuando se inicia una recarga, el IOS detectará que la configuración en ejecución tiene cambios que no se guardaron en la configuración de inicio. Aparecerá una petición de entrada para preguntar si se desean guardar los cambios realizados. Para descartar los cambios, ingrese n o no.

Aparecerá otra petición de entrada para confirmar la recarga. Para confirmar, presione Entrar. Si se presiona cualquier otra tecla, se cancelará el proceso.

Por ejemplo:

```
Switch# reload

System configuration has been modified. Save? [yes/no]: n
```

Proceed with reload? [confirm]

*Apr 13 01:34:15.758: %SYS-5-RELOAD: Reload requested by console. Reload Reason:

Reload Command.

System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

Soporte técnico: http://www.cisco.com/techsupport

Derechos de autor © 2004 por Cisco Systems, Inc.

PLD version 0x10

GIO ASIC version 0x127

c1841 processor with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled

Si se guardan cambios no deseados en la configuración de inicio, posiblemente sea necesario eliminar todas las configuraciones. Esto requiere borrar la configuración de inicio y reiniciar el dispositivo.

La configuración de inicio se elimina mediante el comando erase startup-config.

Para borrar el archivo de configuración de inicio, utilice erase NVRAM:startup-config o erase startup-config en la petición de entrada del modo EXEC privilegiado:

Switch# erase startup-config

Una vez que se emite el comando, el switch le solicita confirmación:

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

Confirm es la respuesta predeterminada. Para confirmar y borrar el archivo de configuración de inicio, presione la tecla Entrar. Si se presiona cualquier otra tecla, se cancelará el proceso.

Precaución: tenga cuidado al utilizar el comando erase. Este comando puede utilizarse para borrar cualquier archivo del dispositivo. El uso incorrecto del comando puede borrar el IOS mismo u otro archivo esencial.

En un switch, también se debe emitir el comando delete vlan.dat además del comando erase startup-config, a fin de devolver el dispositivo a la configuración predeterminada inicial (similar a un restablecimiento de la configuración predeterminada de fábrica):

Switch# delete vlan.dat

Delete filename [vlan.dat]?

Delete flash:vlan.dat? [confirm]

Switch# erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]

[OK]

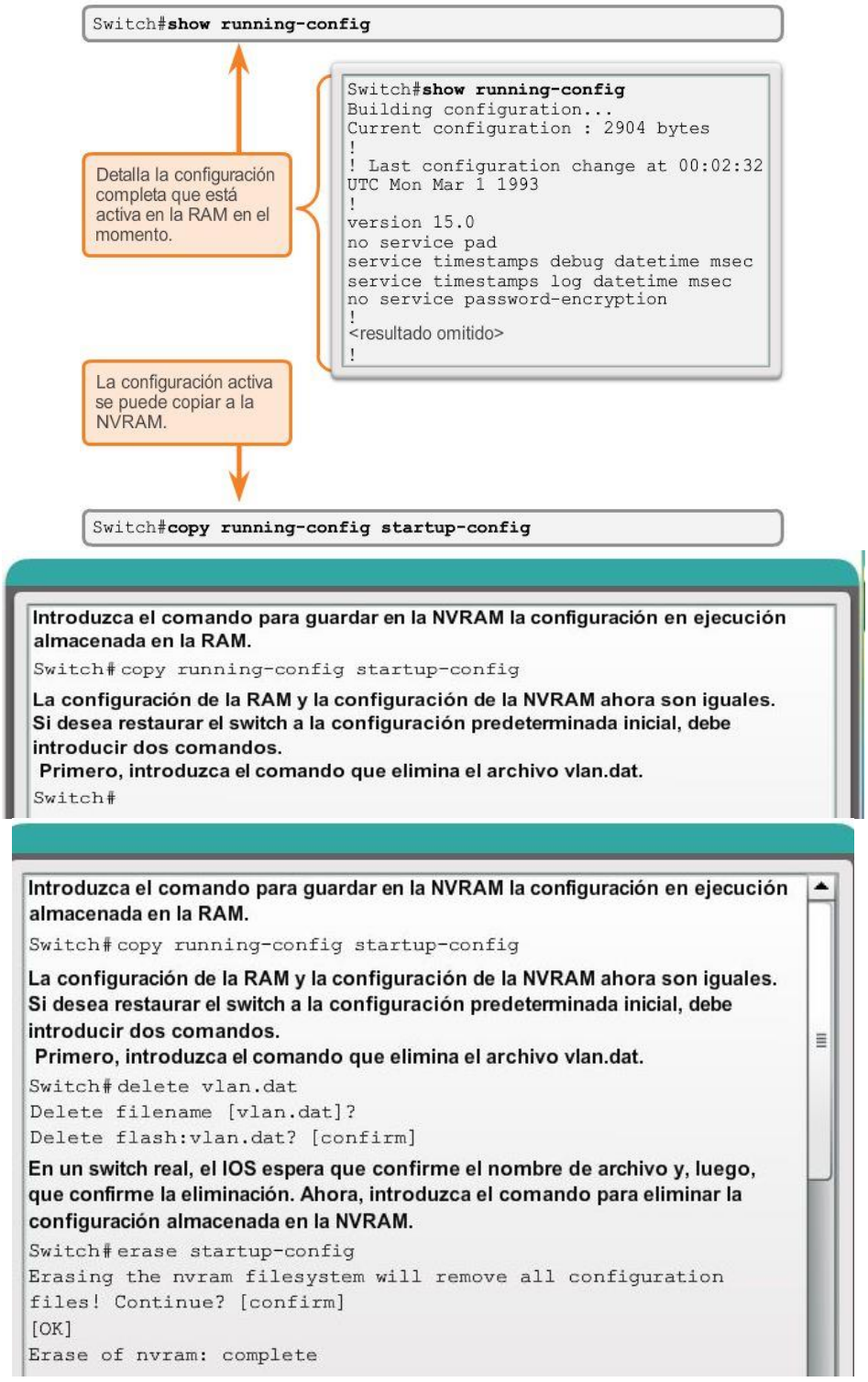
Erase of nvram: complete

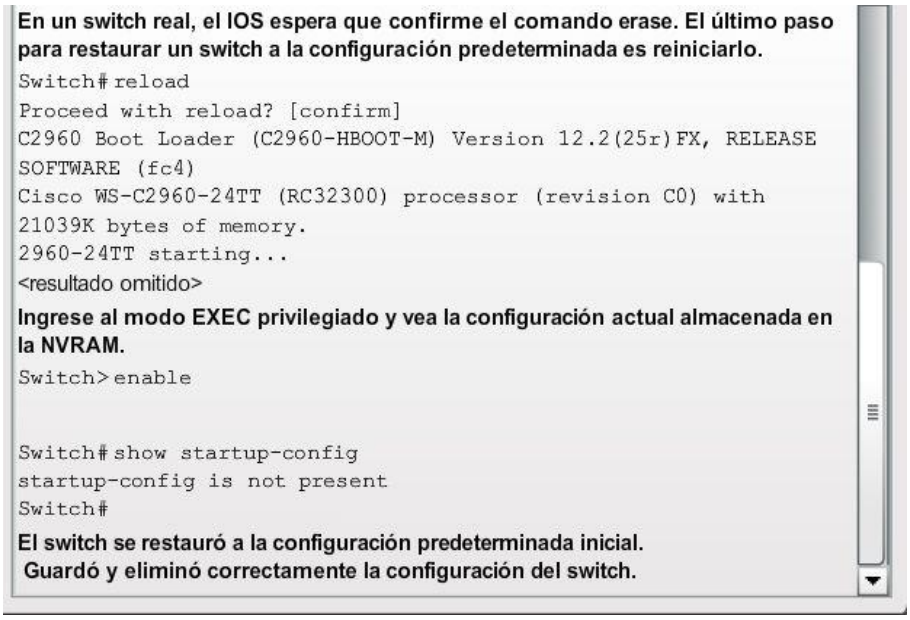
Switch#

Después de eliminar la configuración de inicio de la NVRAM (y de borrar el archivo vlan.dat en el caso de un switch), vuelva a cargar el dispositivo para eliminar el archivo de configuración actual en ejecución de la RAM. El dispositivo cargará entonces la configuración de inicio predeterminada que se envió originalmente con el dispositivo en la configuración en ejecución.

En la figura 2, practique la introducción de comandos para guardar la configuración en ejecución de la RAM en la NVRAM.

Cómo guardar y borrar la configuración





Capítulo 2: Configuración de un sistema operativo de red 2.2.3.2 Captura de texto

Copia de seguridad de las configuraciones mediante captura de texto

Además de guardar las configuraciones en ejecución en la configuración de inicio, los archivos de configuración también se pueden guardar y archivar en documentos de texto. Esta secuencia de pasos asegura la disponibilidad de una copia utilizable de los archivos de configuración para su modificación o reutilización en otra oportunidad.

En la figura 1, los archivos de configuración se pueden guardar y archivar en un documento de texto utilizando Tera Term.

Los pasos son los siguientes:

- En el menú File, haga clic en Log.
- Elija la ubicación. Tera Term comenzará a capturar texto.
- Una vez que comienza la captura, ejecute el comando show running-config o show startup-config en la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.
- Cuando la captura haya finalizado, seleccione Close (Cerrar) en la ventana Log (Registro) de TeraTerm.
- Observe el resultado para verificar que no esté dañado.

De manera similar, en la figura 2, se muestra cómo se pueden guardar y archivar los archivos en un documento de texto utilizando HyperTerminal.

Restauración de las configuraciones de texto

Se puede copiar un archivo de configuración desde el almacenamiento a un dispositivo. Cuando se copia en la terminal, el IOS ejecuta cada línea del texto de configuración como un comando. Es posible que deba editar el archivo antes de copiarlo.

Se recomienda cambiar las contraseñas encriptadas a texto no cifrado y eliminar el parámetro, ya sea el número 5 o 7, que especifica que la contraseña está encriptada. Los mensajes de IOS y el texto que no represente comandos, como “--More--”, se deben eliminar. Este proceso se analiza en la práctica de laboratorio.

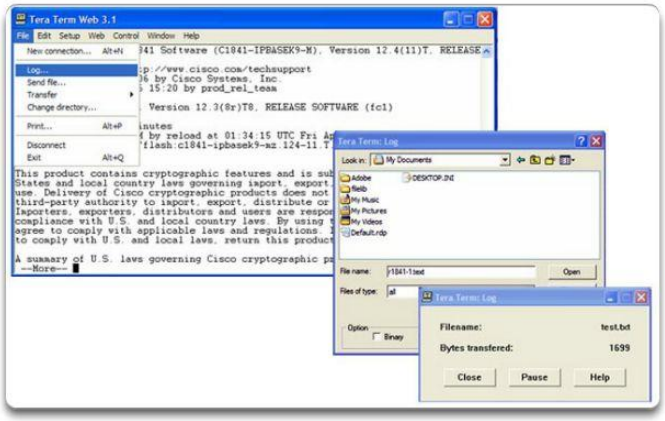
A su vez, en la CLI, el dispositivo debe establecerse en el modo de configuración global para recibir los comandos del archivo de texto que se copia.

Cuando se usa Tera Term, los pasos son los siguientes:

- Edite el texto para eliminar lo que no represente comandos y guarde los cambios.
- En el menú File haga clic en Send para enviar el archivo.
- Ubique el archivo que debe copiar en el dispositivo y haga clic en Open.
- Tera Term pegará el archivo en el dispositivo.

El texto en el archivo estará aplicado como comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo. Este método es conveniente para configurar dispositivos en forma manual.

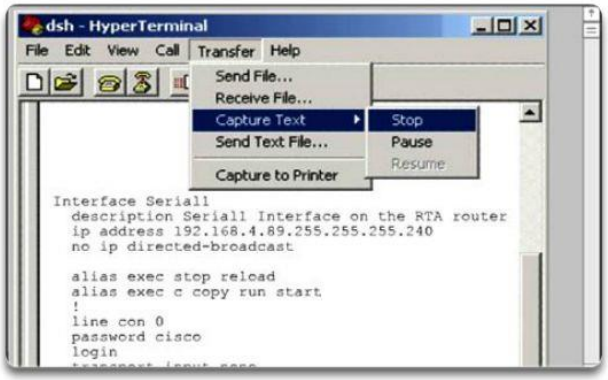
Cómo guardar en un archivo de texto en Tera Term



En la sesión de terminal:

1. Inicie el proceso de registro.
2. Emita un comando **show running-config**
3. Cierre el registro.

Cómo guardar en un archivo de texto en HyperTerminal



En la sesión de terminal:

1. Inicie el proceso de captura de texto
2. Emita un comando **show running-config**
3. Detenga el proceso de captura
4. Guarde el archivo de texto.

Capítulo 2: Configuración de un sistema operativo de red 2.3.1.1 Direccionamiento IP de dispositivos

El uso de direcciones IP, ya sean IPv4 o IPv6, es el principal medio para permitir que los dispositivos se ubiquen entre sí y para establecer la comunicación de extremo a extremo en Internet. De hecho, en cualquier internetwork, las direcciones IP son fundamentales para que los dispositivos se comuniquen de origen a destino y viceversa.

Cada dispositivo final en una red se debe configurar con direcciones IP. Algunos ejemplos de dispositivos finales son:

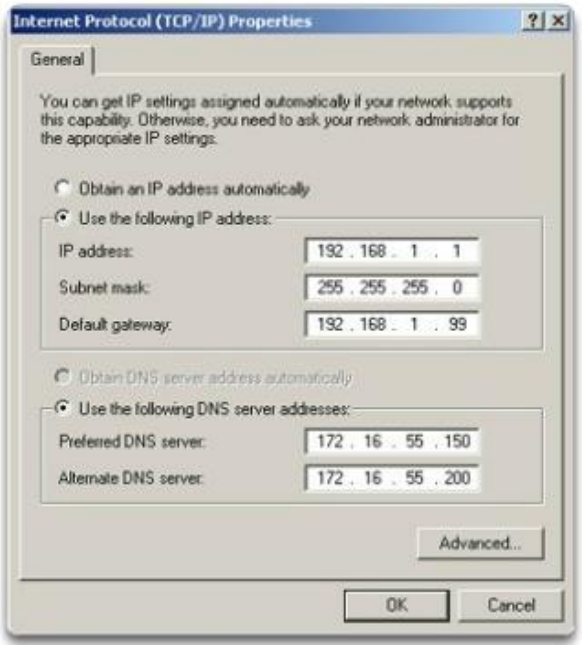
- Computadoras (estaciones de trabajo, computadoras portátiles, servidores de archivos, servidores web)

- Impresoras de red
- Teléfonos VoIP
- Cámaras de seguridad
- Smartphones
- Dispositivos portátiles móviles (como los escáneres inalámbricos para códigos de barras)

La estructura de una dirección IPv4 se denomina “notación decimal punteada” y se representa con cuatro números decimales entre 0 y 255. Las direcciones IPv4 son números asignados a los dispositivos individuales conectados a una red. Son de naturaleza lógica, ya que proporcionan información sobre la ubicación del dispositivo.

Con la dirección IP, también se necesita una máscara de subred. Las máscaras de subred son un tipo especial de direcciones IPv4 que, combinadas con las direcciones IP, determinan de qué subred específica de una red más grande forma parte el dispositivo.

Las direcciones IP se pueden asignar tanto a los puertos físicos como a las interfaces virtuales de los dispositivos. Una interfaz virtual significa que no hay hardware físico en el dispositivo asociado a ella.



Capítulo 2: Configuración de un sistema operativo de red 2.3.1.2 Interfaces y puertos

Las comunicaciones de red dependen de las interfaces de los dispositivos para usuarios finales, las interfaces de los dispositivos de red y los cables que las conectan.

Cada interfaz física tiene especificaciones o estándares que la definen. Los cables que se conectan a la interfaz deben estar diseñados para cumplir con los estándares físicos de la interfaz. Los tipos de medios de red incluyen los cables de cobre de par trenzado, los cables de fibra óptica, los cables coaxiales y la tecnología inalámbrica. Los diferentes tipos de medios de red tienen diferentes características y beneficios. No todos los medios de red tienen las mismas características ni son adecuados para el mismo fin.

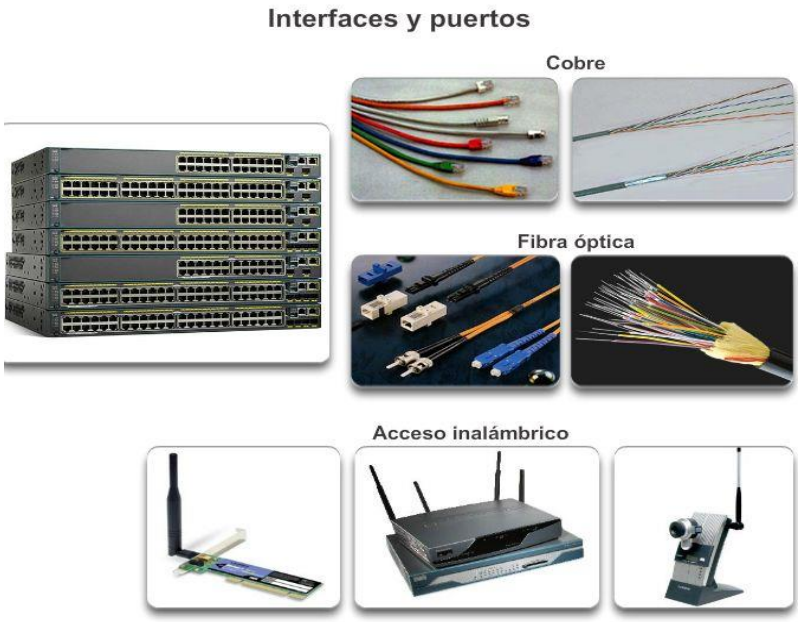
Algunas de las diferencias entre los distintos tipos de medios incluyen las siguientes:

- La distancia a través de la cual los medios pueden transportar una señal correctamente.
- El entorno en el que se instalarán los medios.

- La cantidad de datos y la velocidad a la que se deben transmitir.
- El costo de los medios y de la instalación.

Cada enlace de Internet no solo requiere un tipo específico de medio de red, sino que también requiere una determinada tecnología de red. Ethernet es la tecnología de red de área local (LAN) de uso más frecuente en la actualidad. Hay puertos Ethernet en los dispositivos para usuarios finales, en los dispositivos de switch y en otros dispositivos de red que se pueden conectar físicamente a la red mediante un cable. Para que un cable conecte dispositivos mediante un puerto Ethernet, este debe tener el conector correcto: un conector RJ-45.

Los switches Cisco IOS tienen puertos físicos a los que se pueden conectar los dispositivos, pero también cuentan con una o más interfaces virtuales de switch (SVI, switch virtual interfaces). Son interfaces virtuales porque no hay hardware físico en el dispositivo asociado a ellas; las SVI se crean en el software. La interfaz virtual proporciona un medio para administrar un switch de manera remota a través de una red usando IPv4. Cada switch viene con una SVI que aparece en la configuración predeterminada inicial. La SVI predeterminada es interface VLAN1.



Capítulo 2: Configuración de un sistema operativo de red 2.3.2.1 Configuración de una interfaz virtual de switch

Para acceder al switch de manera remota, se deben configurar una dirección IP y una máscara de subred en la SVI:

- Dirección IP: junto con la máscara de subred, identifica el dispositivo final en la internetwork de manera exclusiva.

- Máscara de subred: determina qué parte de una red más grande utiliza una dirección IP.

Por el momento, se mantendrá el enfoque en IPv4; más adelante, se explorará IPv6.

Pronto aprenderá el sentido detrás de todas estas direcciones IP; por el momento, el objetivo es configurar rápidamente el switch para admitir el acceso remoto. En la ilustración, se muestra el comando para habilitar la conectividad IP del S1 mediante la dirección IP 192.168.10.2:

- interface vlan 1: se utiliza para navegar hasta el modo de configuración de interfaz desde el modo de configuración global.

- ip address 192.168.10.2 255.255.255.0: configura la dirección IP y la máscara de subred del switch (esta es solo una de muchas combinaciones posibles de una dirección IP y una máscara de subred).

- no shutdown: habilita administrativamente el estado activo de la interfaz.

Una vez que se configuran estos comandos, el switch tiene todos los elementos IP listos para la comunicación a través de la red.

Nota: todavía se deben configurar uno o más puertos físicos en el switch, así como las líneas VTY, para completar la configuración que permite la administración remota del switch.

Practique la configuración de una interfaz virtual de switch introduciendo comandos en la ilustración.

Configuración de una interfaz virtual de switch

Capítulo 2: Configuración de un sistema operativo de red 2.3.2.2 Configuración manual de dirección IP para dispositivos finales

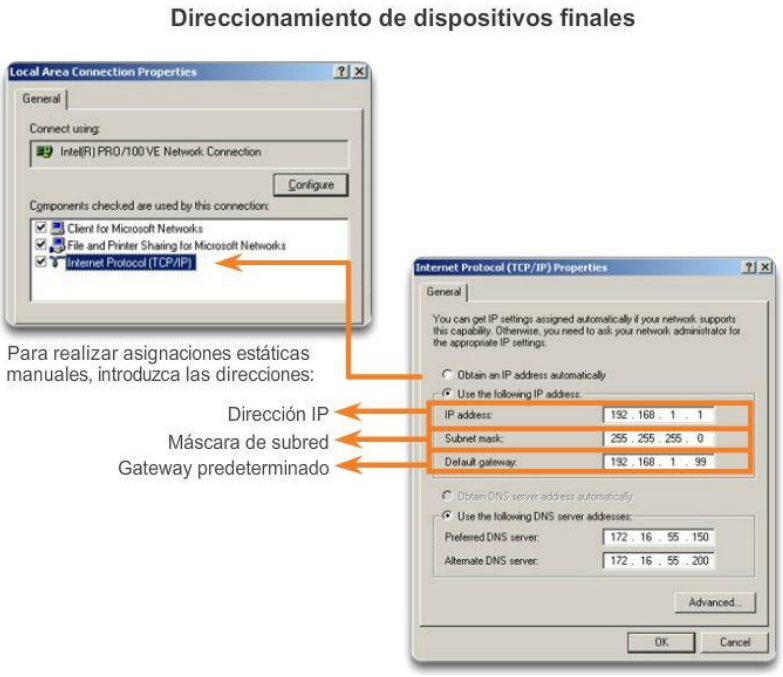
Para que un dispositivo final se comunique a través de la red, se debe configurar con la información de dirección IP correcta. De modo similar al de una SVI, el dispositivo final se debe configurar con una dirección IP y una máscara de subred. Esta información se configura en los parámetros de la PC.

Para que un dispositivo final se conecte correctamente a la red, se deben configurar todos estos parámetros. Esta información se configura en los parámetros de red de la PC. Además de la información de dirección IP y máscara de subred, es posible configurar la información del gateway predeterminado y del servidor DNS, como se muestra en la ilustración.

La dirección de gateway predeterminado es la dirección IP de la interfaz del router que se utiliza para que el tráfico de la red salga de la red local. El gateway predeterminado es una dirección IP que, por lo general, asigna el administrador de red y se utiliza cuando se debe enrutar tráfico a otra red.

La dirección del servidor DNS es la dirección IP del servidor del Sistema de nombres de dominios (DNS, Domain Name System), que se utiliza para traducir direcciones IP a direcciones Web, como www.cisco.com.

A todos los dispositivos de Internet se les asigna una dirección IP, mediante la cual se accede a ellos. Sin embargo, resulta más fácil recordar nombres que números. Por lo tanto, los sitios Web tienen nombres para simplificar el proceso. El servidor DNS se utiliza para mantener la asignación entre las direcciones IP y los nombres de los diversos dispositivos.



Capítulo 2: Configuración de un sistema operativo de red 2.3.2.3 Configuración automática de direcciones IP para dispositivos finales

La información de dirección IP se puede introducir en la PC en forma manual o mediante el Protocolo de configuración dinámica de host (DHCP). El protocolo DHCP permite configurar la información de IP de los dispositivos finales de manera automática.

DHCP es una tecnología que se utiliza en casi todas las redes comerciales. Para comprender mejor por qué DHCP es tan popular, tenga en cuenta todo el trabajo adicional que habría que realizar sin este protocolo.

DHCP permite la configuración automática de direcciones IPv4 para cada dispositivo final de una red con DHCP habilitado. Imagine la cantidad de tiempo que le llevaría si cada vez que se conectara a la red tuviera que introducir manualmente la dirección IP, la máscara de subred, el gateway predeterminado y el servidor DNS. Multiplique eso por cada usuario y cada uno de los dispositivos en la red, y se dará cuenta del problema.

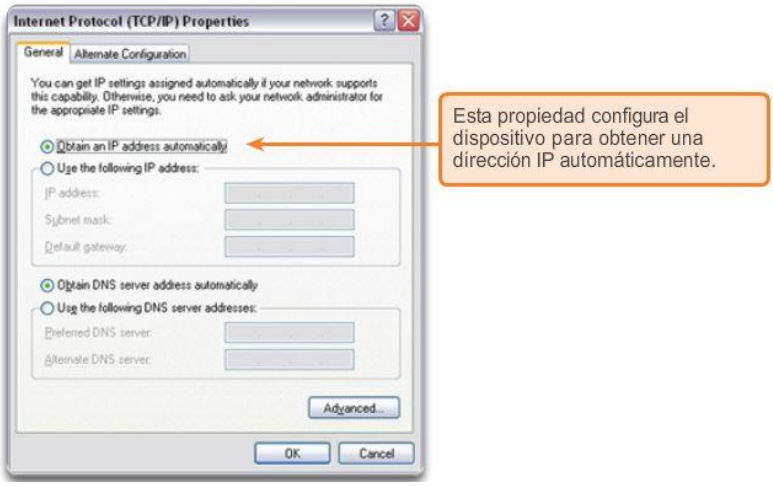
DHCP es un ejemplo de la tecnología en su máxima expresión. Uno de los propósitos principales de cualquier tecnología es facilitar las tareas que se desean o se deben realizar. Con DHCP, el usuario final ingresa al área que abarca una red determinada, conecta un cable Ethernet o habilita una conexión inalámbrica e, inmediatamente, se le asigna la información de IPv4 necesaria para comunicarse de manera correcta a través de la red.

Como se muestra en la figura 1, para configurar el protocolo DHCP en un equipo Windows, solo debe seleccionar “Obtener una dirección IP automáticamente” y “Obtener la dirección del servidor DNS automáticamente”. Se asigna información de un grupo de direcciones IP a la PC y se configura la información de IP relacionada en el servidor de DHCP.

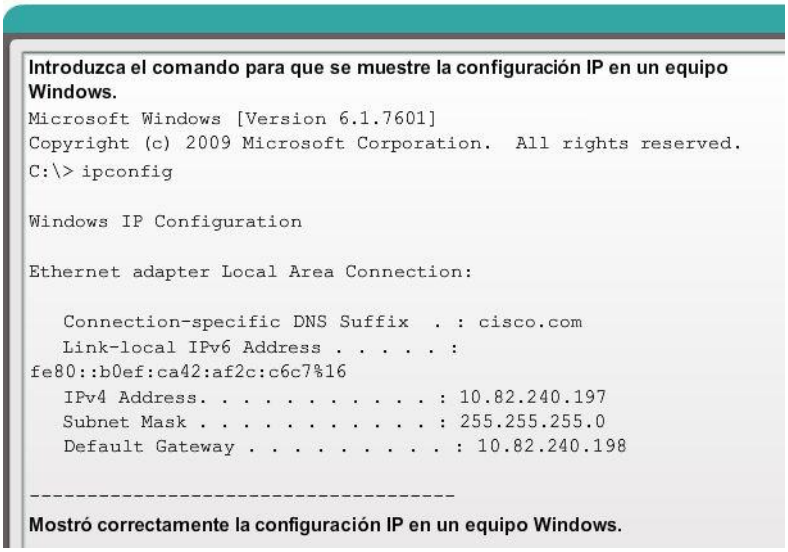
Es posible mostrar las opciones de configuración IP en un equipo Windows usando el comando ipconfig en el símbolo del sistema. El resultado muestra la dirección IP, la máscara de subred y el gateway que la PC recibió del servidor de DHCP.

Practique cómo mostrar la dirección IP de un equipo Windows introduciendo comandos en la figura 2.

Asignación de direcciones dinámicas



Verificación de la configuración IP de un equipo Windows



Capítulo 2: Configuración de un sistema operativo de red 2.3.2.4 Conflictos de dirección IP

Si se define una dirección IP estática (manual) para un dispositivo de red; por ejemplo, una impresora, y luego se instala un servidor de DHCP, pueden ocurrir conflictos de direcciones IP duplicadas entre el dispositivo de red y una PC que obtiene información de direccionamiento IP automático del servidor de DHCP. También puede ocurrir un conflicto si se define manualmente una dirección IP estática para un dispositivo de red durante una falla de red relacionada con el servidor de DHCP; una vez que se resuelve la falla de red y se puede acceder al servidor de DHCP a través de la red, surge el conflicto.

Para resolver tales conflictos de direccionamiento IP, convierta el dispositivo de red con la dirección IP estática en cliente DHCP o excluya la dirección IP estática para el dispositivo final del ámbito de DHCP en el servidor de DHCP.

La segunda solución requiere privilegios de nivel administrativo en el servidor de DHCP y que esté familiarizado con la configuración de DHCP en un servidor.

También puede encontrar conflictos de direccionamiento IP al realizar manualmente la configuración de IP en un dispositivo final de una red que solo utiliza direcciones IP estáticas. En este caso, debe determinar qué direcciones IP están disponibles en la subred IP específica y realizar la configuración según corresponda.

Este caso muestra por qué es tan importante que un administrador de red mantenga un registro detallado de los dispositivos finales que incluya las asignaciones de direcciones IP.

Nota: por lo general, en redes de pequeñas o medianas empresas, se utilizan direcciones IP estáticas en los servidores e impresoras, mientras que los dispositivos de los empleados utilizan información de dirección IP asignada mediante DHCP.

Conflictos de dirección IP

Capítulo 2: Configuración de un sistema operativo de red 2.3.3.1 Prueba de la dirección de bucle invertido en un dispositivo final

Prueba de loopback

En la ilustración, se muestra el primer paso de la secuencia de prueba. El comando ping se utiliza para verificar la configuración IP interna en un host local. Esta prueba se realiza utilizando el comando ping en una dirección reservada denominada “dirección de loopback” (127.0.0.1). El protocolo TCP/IP define la dirección de loopback, 127.0.0.1, como una dirección reservada que permite enrutar los paquetes de regreso al host.

Los comandos ping se introducen en una línea de comandos en el host local con la siguiente sintaxis:

C:\> ping 127.0.0.1

La respuesta de este comando se parecería a ésta:

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 127.0.0.1:

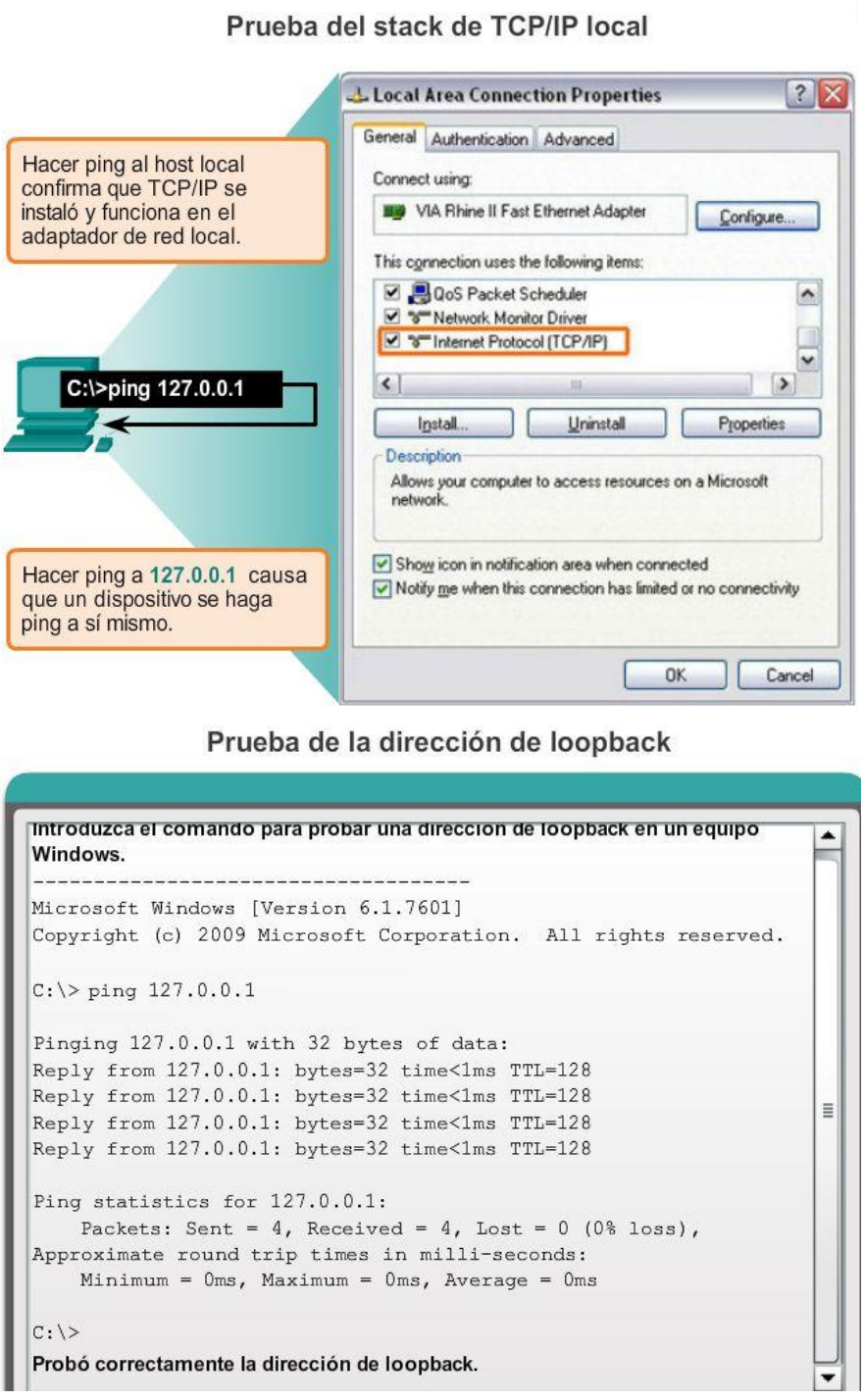
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),

Tiempo aproximado de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms

El resultado indica que se enviaron cuatro paquetes de prueba de 32 bytes cada uno desde el host 127.0.0.1 y se devolvieron a este en un tiempo de menos de 1 ms. Esta solicitud de ping correcta verifica que la tarjeta de interfaz de red, los controladores y la implementación del protocolo TCP/IP funcionan correctamente.

Practique la prueba de una dirección de loopback introduciendo comandos en la figura 2.



Capítulo 2: Configuración de un sistema operativo de red 2.3.3.2 Prueba de la asignación de interfaz

Así como se utilizan comandos y utilidades para verificar una configuración de host, también se utilizan comandos para verificar las interfaces de dispositivos intermediarios. El IOS proporciona comandos para verificar el funcionamiento de interfaces de router y switch.

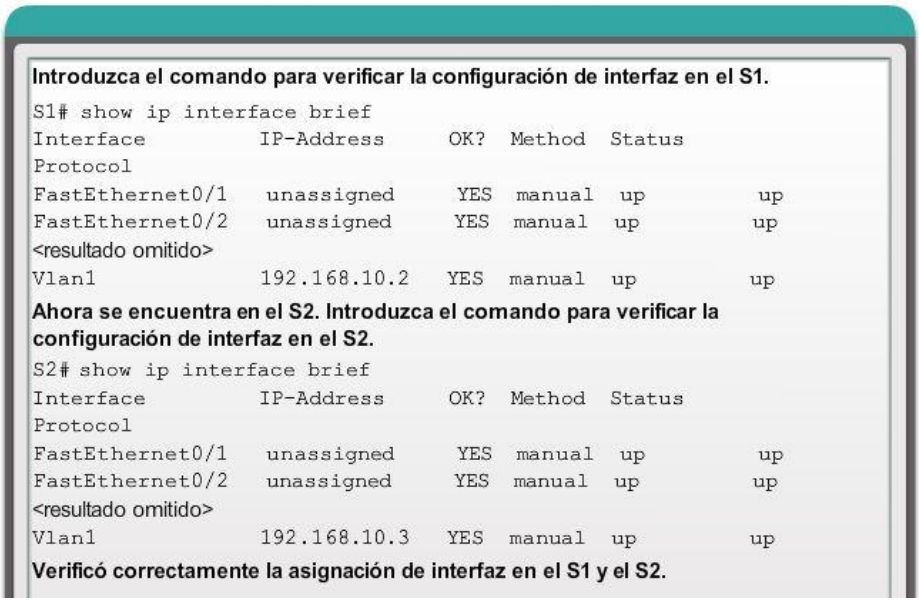
Verificación de las interfaces del switch

Al examinar el S1 y el S2, se utiliza el comando show ip interface brief para verificar la condición de las interfaces del switch, como se muestra en la ilustración.

La dirección IP asignada a la interfaz VLAN 1 en el S1 es 192.168.10.2. La dirección IP asignada a la interfaz VLAN 1 en el S2 es 192.168.10.3. Las interfaces físicas F0/1 y F0/2 en el S1 funcionan, al igual que las interfaces físicas F0/1 y F0/2 en el S2.

Practique la verificación de una interfaz VLAN introduciendo comandos en la ilustración.

Verificación de la asignación de interfaz VLAN



Capítulo 2: Configuración de un sistema operativo de red 2.3.3.3 Prueba de la conectividad de extremo a extremo

Prueba de la conectividad de PC a switch

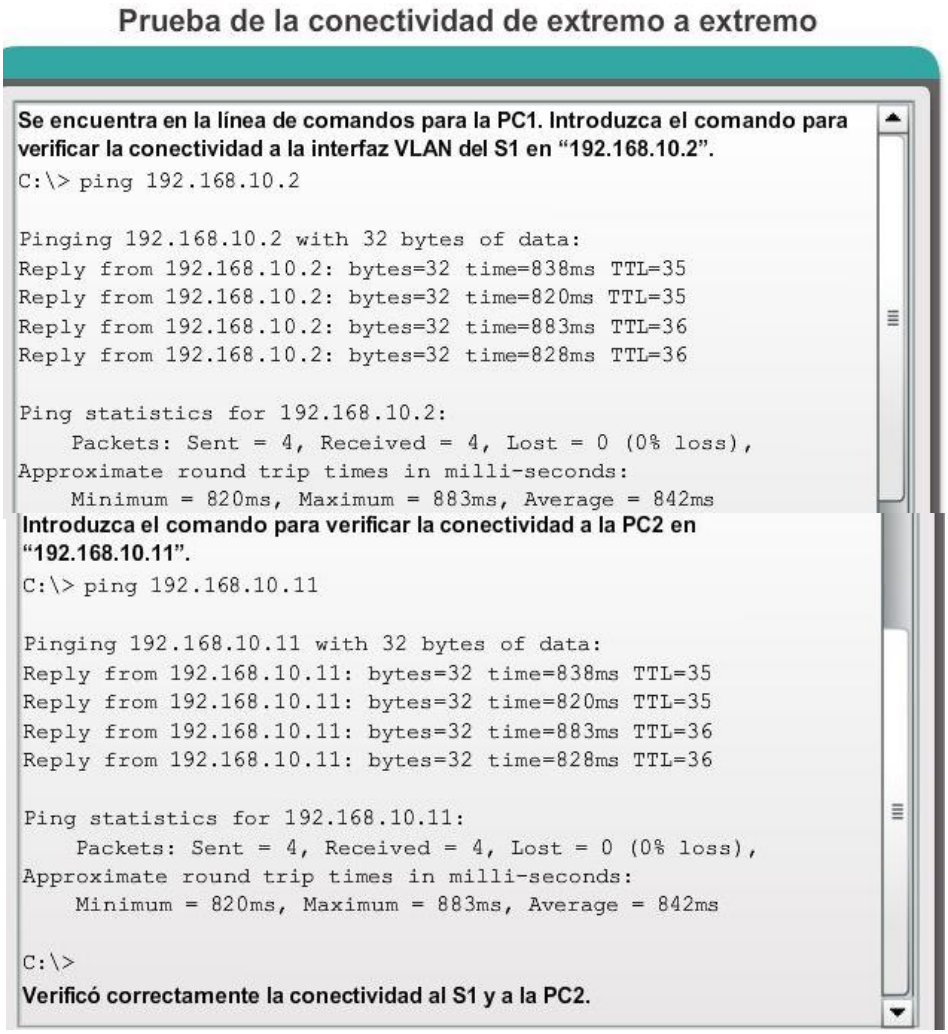
El comando ping se puede utilizar en una PC de la misma forma que en un dispositivo Cisco IOS. En la ilustración, se muestra que el ping de la PC1 a la dirección IP de la interfaz VLAN 1 del S1, 192.168.10.2, debe ser correcto.

Prueba de la conectividad de extremo a extremo

La dirección IP de la PC1 es 192.168.10.10, con una máscara de subred 255.255.255.0 y un gateway predeterminado 192.168.10.1.

La dirección IP de la PC2 es 192.168.10.11, con una máscara de subred 255.255.255.0 y un gateway predeterminado 192.168.10.1.

El ping de la PC1 a la PC2 también debe ser correcto. Si un ping de la PC1 a la PC2 se realiza correctamente, se verifica la conectividad de extremo a extremo en la red.



Capítulo 2: Configuración de un sistema operativo de red 2.4.1.1 Actividad de clase: Enséñeme Resumen

Enséñeme

Los estudiantes trabajarán de a dos. Para esta actividad, se requiere Packet Tracer.

Suponga que un colega nuevo le pidió que lo oriente sobre la CLI de Cisco IOS. Este colega nunca trabajó con dispositivos Cisco.

Usted le explica los comandos y la estructura básicos de la CLI, porque desea que su colega comprenda que la CLI es un lenguaje de comandos simple pero eficaz que se puede comprender y navegar fácilmente.

Utilice Packet Tracer y una de las actividades disponibles en este capítulo como modelo de red simple (por ejemplo, la actividad de laboratorio 2.3.3.5. Práctica de laboratorio: Configuración de una dirección de administración del switch).

Céntrese en estas áreas:

- Si bien los comandos son técnicos, ¿se asemejan a enunciados del lenguaje corriente?
- ¿Cómo se organiza el conjunto de comandos en subgrupos o modos? ¿Cómo sabe un administrador qué modo está utilizando?

- ¿Cuáles son los comandos individuales para configurar los parámetros básicos de un dispositivo Cisco? ¿Cómo explicaría este comando en términos sencillos? Establezca paralelos con la vida real cuando sea adecuado.

Sugiera cómo agrupar distintos comandos según sus modos de manera que se necesite una cantidad mínima de desplazamientos entre modos.

La CLI maneja el Cisco IOS.

Capítulo 2: Configuración de un sistema operativo de red 2.4.1.3 Resumen

Cisco IOS es un término que abarca diferentes sistemas operativos que se ejecutan en diversos dispositivos de redes. El técnico puede introducir comandos para configurar o programar el dispositivo a fin de que lleve a cabo diversas funciones de redes.

Los routers y switches en los que se utiliza Cisco IOS realizan funciones de las cuales dependen los profesionales de red para hacer que sus redes funcionen de la forma esperada.

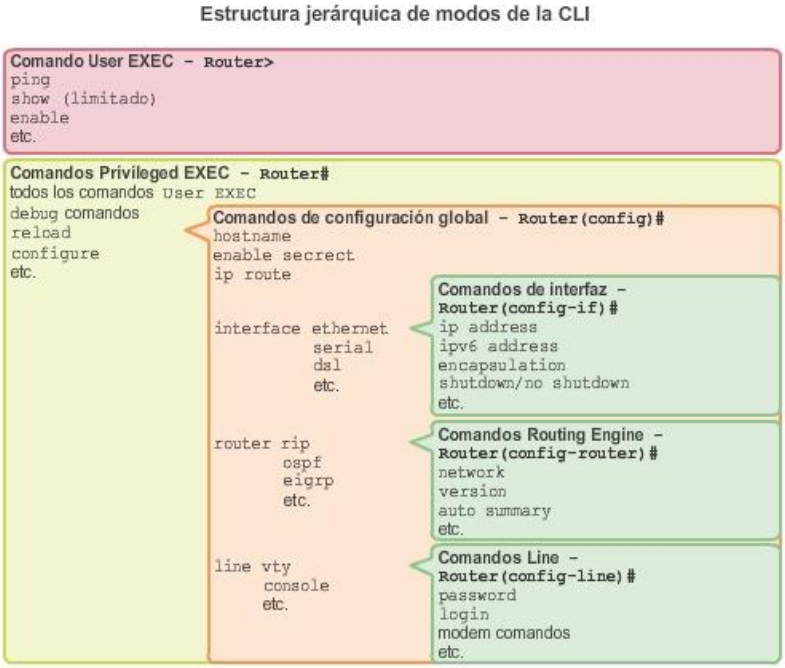
En general, se accede a los servicios que proporciona Cisco IOS mediante una interfaz de línea de comandos (CLI, command-line interface), a la cual se accede a través del puerto de consola, el puerto auxiliar o mediante Telnet o SSH. Una vez que se conectan a la CLI, los técnicos de red pueden realizar cambios de configuración en los dispositivos Cisco IOS. Cisco IOS está diseñado como sistema operativo modal, lo cual significa que los técnicos de red deben navegar a través de diversos modos jerárquicos del IOS. Cada modo admite distintos comandos del IOS.

Cisco IOS Command Reference (Referencia de comandos de Cisco IOS) es una colección de documentos en línea que describen en detalle los comandos de IOS utilizados en los dispositivos Cisco, como los routers y switches Cisco IOS.

Los routers y switches Cisco IOS admiten sistemas operativos modales y estructuras de comandos similares, así como muchos de los mismos comandos. Además, los pasos de configuración inicial durante su implementación en una red son idénticos para ambos dispositivos.

En este capítulo, se presentó Cisco IOS. Se explicaron los diversos modos de Cisco IOS en detalle y se analizó la estructura básica de comandos que se utiliza para configurarlo. También se exploró la configuración inicial de los dispositivos de switch Cisco IOS, la cual incluye la configuración de un nombre, la limitación del acceso a la configuración del dispositivo, la configuración de mensajes de aviso y guardar la configuración.

En el capítulo siguiente, se analiza cómo se desplazan los paquetes a través de la infraestructura de red y se presentan las reglas de comunicación de paquetes.



Capítulo 3: Protocolos y comunicaciones de red 3.0.1.1 Introducción

Las redes nos conectan cada vez más. Las personas se comunican en línea desde cualquier lugar. Las conversaciones que tienen lugar en las aulas pasan a las sesiones de chat de mensajes instantáneos, y los debates en línea continúan en el lugar de estudios. Diariamente, se desarrollan nuevos servicios para aprovechar la red.

En lugar de crear sistemas exclusivos e independientes para la prestación de cada servicio nuevo, el sector de redes en su totalidad adoptó un marco de desarrollo que permite que los diseñadores comprendan las plataformas de red actuales y las mantengan. Al mismo tiempo, este marco se utiliza para facilitar el desarrollo de nuevas tecnologías, a fin de satisfacer las necesidades de las comunicaciones y las mejoras tecnológicas futuras.

Un aspecto fundamental de este marco de desarrollo es el uso de modelos generalmente aceptados que describen reglas y funciones de red.

En este capítulo, obtendrá información sobre estos modelos, sobre los estándares que hacen que las redes funcionen y sobre la forma en que se produce la comunicación a través de una red.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Explicar por qué los protocolos son necesarios en la comunicación.
- Explicar el propósito de adherir a una suite de protocolos.
- Explicar la función de los organismos de estandarización en el establecimiento de protocolos para la interoperabilidad de redes.
- Explicar la forma en que se utilizan los modelos TCP/IP y OSI para facilitar la estandarización en el proceso de comunicación.
- Explicar por qué las RFC se convirtieron en el proceso para establecer estándares.
- Describir el proceso de RFC.
- Explicar la forma en que la encapsulación de datos permite que estos se transporten a través de la red.
- Explicar la forma en que los hosts locales acceden a recursos locales en una red.
- Explicar la forma en que los hosts locales acceden a recursos remotos en una red.

Capítulo 3: Protocolos y comunicaciones de red 3.0.1.2 Actividad de clase: Diseño de un sistema de comunicaciones

Solo hablemos de esto…

Acaba de adquirir un automóvil nuevo para uso personal. Después de conducir el automóvil durante alrededor de una semana, descubre que no funciona correctamente.

Después de analizar el problema con varios de sus pares, decide llevarlo un taller de reparaciones de automóviles muy recomendado. Se trata del único taller de reparaciones que le queda cerca.

Cuando llega al taller de reparaciones, advierte que todos los mecánicos hablan otro idioma. Tiene dificultades para explicar los problemas de funcionamiento del automóvil, pero es realmente necesario realizar las reparaciones. No está seguro de poder conducirlo de regreso a su hogar para buscar otras opciones.

Debe encontrar una manera de trabajar con el taller para asegurarse de que el automóvil se repare correctamente.

¿Cómo se comunicará con los mecánicos de esa empresa? Diseñe un modelo de comunicaciones para asegurar que el vehículo se repare correctamente.

Los protocolos y estándares de red hacen que la comunicación de red sea más fácil.

Capítulo 3: Protocolos y comunicaciones de red 3.1.1.1 ¿Qué es la comunicación?

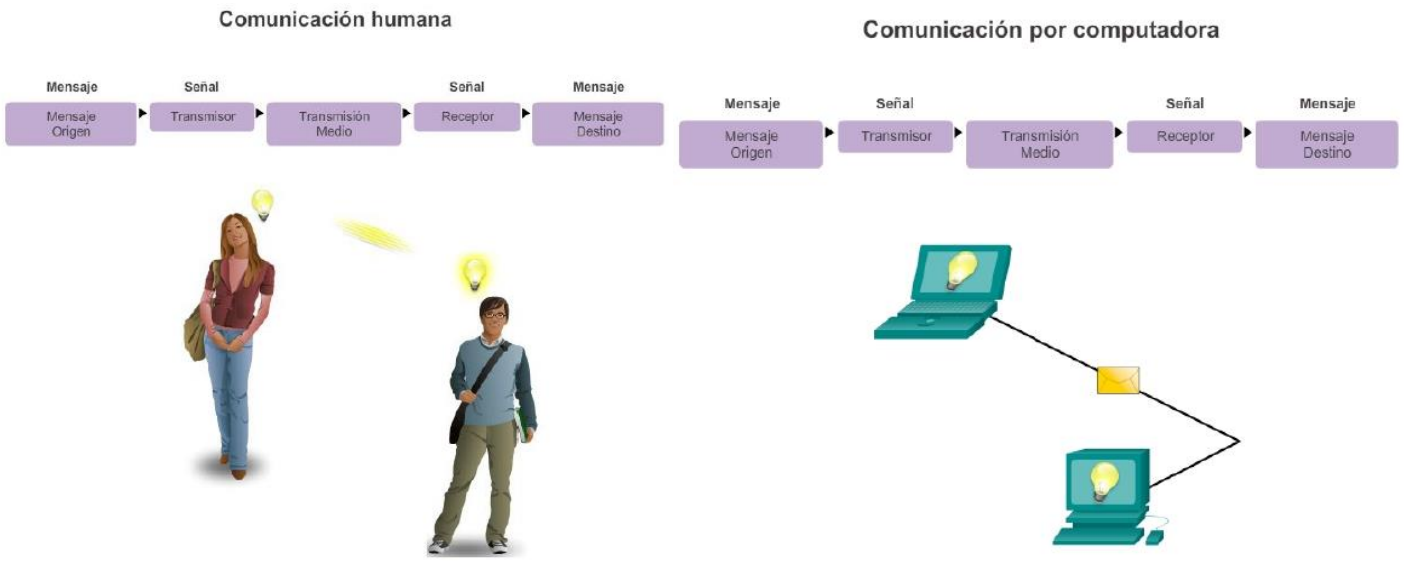
Una red puede ser tan compleja como los dispositivos conectados a través de Internet, o tan simple como dos PC conectadas directamente entre sí mediante un único cable, o puede tener cualquier grado de complejidad intermedia. Las redes pueden variar en lo que respecta al tamaño, la forma y la función. Sin embargo, realizar simplemente la conexión física entre los dispositivos finales no es suficiente para habilitar la comunicación. Para que se produzca la comunicación, los dispositivos deben saber “cómo” comunicarse.

Las personas intercambian ideas mediante diversos métodos de comunicación. Sin embargo, independientemente del método elegido, todos los métodos de comunicación tienen tres elementos en común. El primero de estos elementos es el origen del mensaje, o emisor. Los orígenes de los mensajes son las personas o los dispositivos electrónicos que deben enviar un mensaje a otras personas o dispositivos. El segundo elemento de la comunicación es el destino, o receptor, del mensaje. El destino recibe el mensaje y lo interpreta. Un tercer elemento, llamado “canal”, está formado por los medios que proporcionan el camino por el que el mensaje viaja desde el origen hasta el destino.

La comunicación comienza con un mensaje, o información, que se debe enviar desde un origen hasta un destino. El envío de este mensaje, ya sea mediante comunicación cara a cara o a través de una red, está regido por reglas llamadas “protocolos”. Estos protocolos son específicos del tipo de método de comunicación en cuestión. En nuestra comunicación personal diaria, las reglas que utilizamos para comunicarnos por un medio, como una llamada telefónica, no son necesariamente las mismas que los protocolos para utilizar otro medio, como enviar una carta.

Por ejemplo, piense en dos personas que se comunican cara a cara, como se muestra en la figura 1. Antes de comunicarse, deben acordar cómo hacerlo. Si en la comunicación se utiliza la voz, primero deben acordar el idioma. A continuación, cuando tienen un mensaje que compartir, deben poder dar formato a ese mensaje de una manera que sea comprensible. Por ejemplo, si alguien utiliza el idioma español, pero la estructura de las oraciones es deficiente, el mensaje se puede malinterpretar fácilmente. Cada una de estas tareas describe protocolos implementados para lograr la comunicación. Esto es válido para la comunicación por computadora, como se muestra en la figura 2.

Piense cuántas reglas o protocolos diferentes rigen todos los métodos de comunicación que existen actualmente en el mundo.



Capítulo 3: Protocolos y comunicaciones de red 3.1.1.2 Establecimiento de reglas

Establecimiento de reglas

Antes de comunicarse entre sí, las personas deben utilizar reglas o acuerdos establecidos que rijan la conversación. Por ejemplo, tenga en cuenta la figura 1, donde los protocolos son necesarios para la comunicación eficaz.

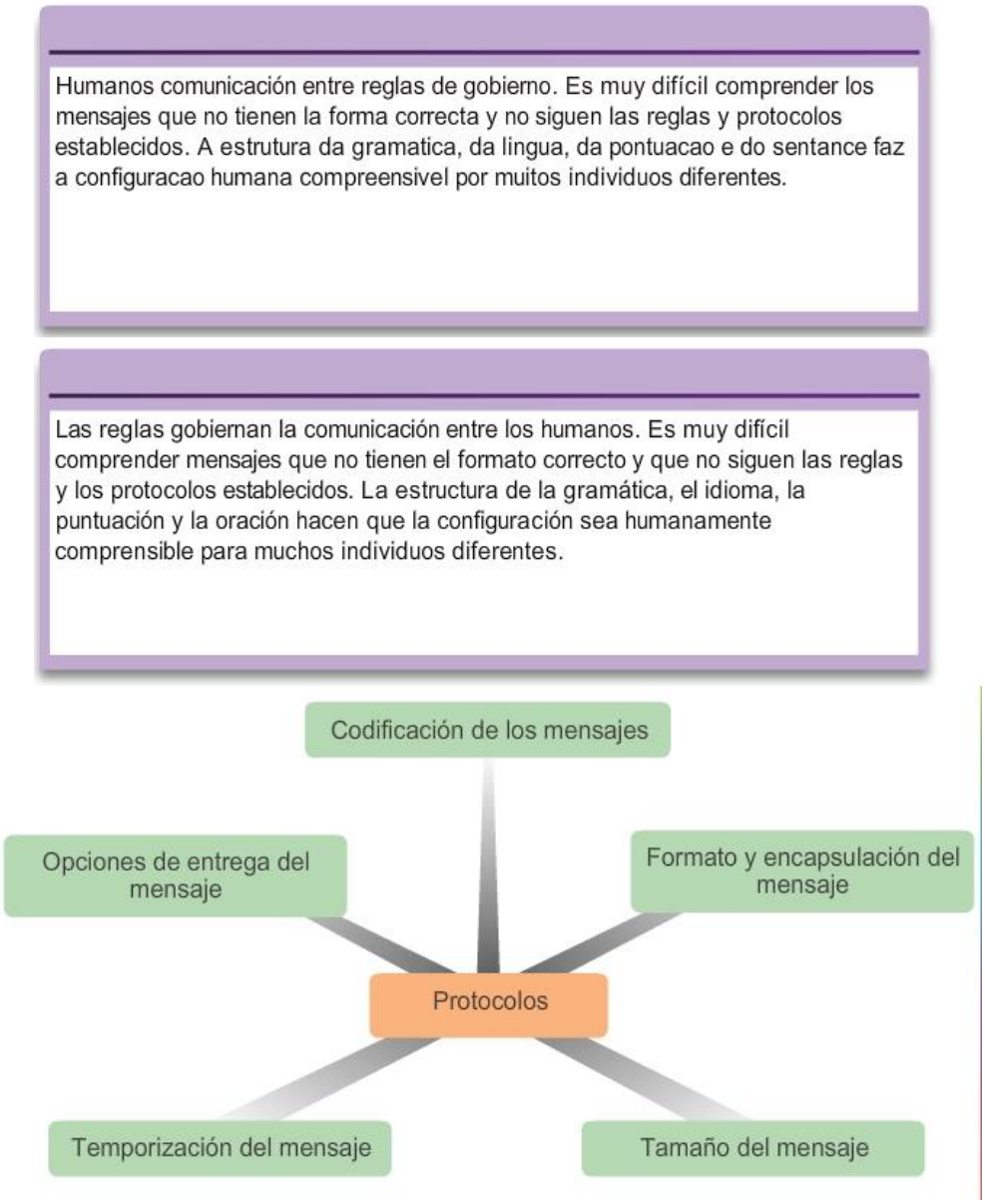
Los protocolos que se utilizan son específicos de las características del método de comunicación, incluidas las características del origen, el destino y el canal. Estas reglas, o protocolos, deben respetarse para que el mensaje se envíe y comprenda correctamente. Se encuentran disponibles muchos protocolos que rigen la comunicación humana correcta. Una vez que se acuerda un método de comunicación (cara a cara, teléfono, carta, fotografía), los protocolos implementados deben contemplar los siguientes requisitos:

- Un emisor y un receptor identificados
- Idioma y gramática común
- Velocidad y temporización de la entrega
- Requisitos de confirmación o acuse de recibo

Los protocolos que se utilizan en las comunicaciones de red comparten muchas de las características fundamentales de los protocolos que se utilizan para regir las conversaciones humanas correctas. Consulte la figura 2. Además de identificar el origen y el destino, los protocolos informáticos y de red definen los detalles sobre la forma en que los mensajes se transmiten a través de una red para cumplir con los requisitos anteriores. Si bien hay muchos protocolos que deben interactuar, entre los protocolos informáticos habituales, se incluyen los siguientes:

- Codificación de los mensajes
- Formato y encapsulación del mensaje
- Tamaño del mensaje
- Temporización del mensaje
- Opciones de entrega del mensaje

A continuación, se analizan más detalladamente cada uno de estos protocolos.



Capítulo 3: Protocolos y comunicaciones de red 3.1.1.3 Codificación de los mensajes

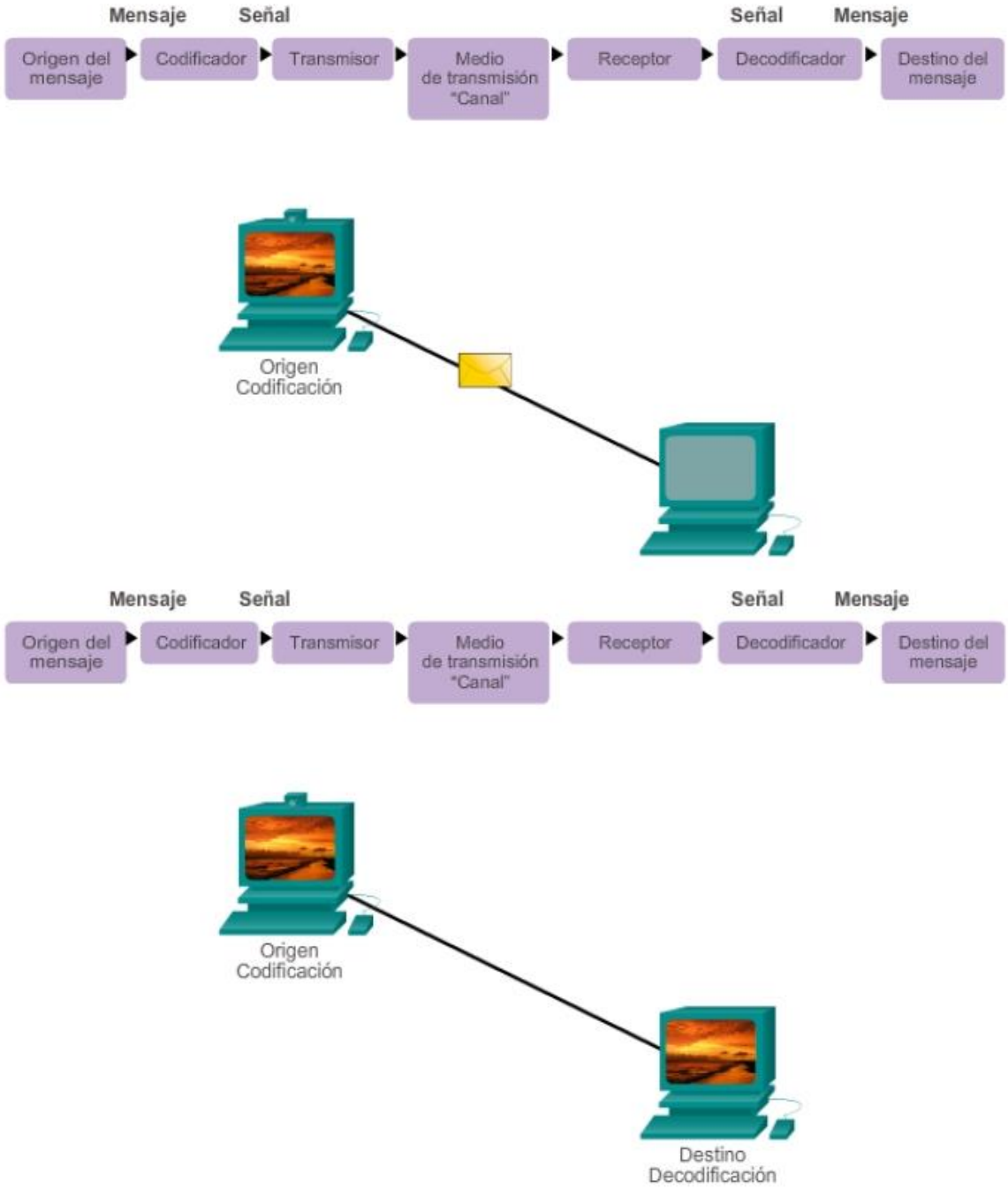
Codificación de los mensajes

Uno de los primeros pasos para enviar un mensaje es codificarlo. La codificación es el proceso mediante el cual la información se convierte en otra forma aceptable para la transmisión. La decodificación invierte este proceso para interpretar la información.

Imagine a una persona que planifica un viaje de vacaciones con un amigo y llama a ese amigo para analizar los detalles respecto de dónde desean ir, como se muestra en la figura 1. Para comunicar el mensaje, el emisor primero debe convertir, o codificar, sus ideas y percepciones acerca del lugar en palabras. Las palabras se articulan a través del teléfono utilizando los sonidos y las inflexiones del lenguaje oral que transmiten el mensaje. En el otro extremo de la línea telefónica, la persona que está escuchando la descripción recibe los sonidos y los decodifica para visualizar la imagen del atardecer descrita por el emisor.

La codificación también tiene lugar en la comunicación por computadora, como se muestra en la figura 2. La codificación entre hosts debe tener el formato adecuado para el medio.

El host emisor, primero convierte en bits los mensajes enviados a través de la red. Cada bit se codifica en un patrón de sonidos, ondas de luz o impulsos electrónicos, según el medio de red a través del cual se transmitan los bits. El host de destino recibe y decodifica las señales para interpretar el mensaje.



Capítulo 3: Protocolos y comunicaciones de red 3.1.1.4 Formato y encapsulación del mensaje

Formato y encapsulación del mensaje

Cuando se envía un mensaje desde el origen hacia el destino, se debe utilizar un formato o estructura específicos. Los formatos de los mensajes dependen del tipo de mensaje y el canal que se utilice para entregar el mensaje.

La escritura de cartas es una de las formas más comunes de comunicación humana por escrito. Durante siglos, el formato aceptado para las cartas personales no ha cambiado. En muchas culturas, una carta personal contiene los siguientes elementos:

- Un identificador del destinatario
- Un saludo
- El contenido del mensaje
- Una frase de cierre
- Un identificador del emisor

Además de tener el formato correcto, la mayoría de las cartas personales también deben colocarse, o encapsularse, en un sobre para la entrega, como se muestra en la figura 1.

El sobre tiene la dirección del emisor y la del receptor, cada una escrita en el lugar adecuado del sobre. Si la dirección de destino y el formato no son correctos, la carta no se entrega. El proceso que consiste en colocar un formato de mensaje (la carta) dentro de otro formato de mensaje (el sobre) se denomina encapsulación. Cuando el destinatario revierte este proceso y quita la carta del sobre se produce la desencapsulación del mensaje.

La persona que escribe la carta utiliza un formato aceptado para asegurarse de que la carta se entregue y de que el destinatario la comprenda. De la misma manera, un mensaje que se envía a través de una red de computadoras sigue reglas de formato específicas para que pueda ser entregado y procesado. De la misma manera en la que una carta se encapsula en un sobre para la entrega, los mensajes de las PC también se encapsulan. Cada mensaje de computadora se encapsula en un formato específico, llamado trama, antes de enviarse a través de la red. Una trama actúa como un sobre: proporciona la dirección del destino propuesto y la dirección del host de origen, como se muestra en la figura 2.

El formato y el contenido de una trama están determinados por el tipo de mensaje que se envía y el canal que se utiliza para enviarlo. Los mensajes que no tienen el formato correcto no se pueden enviar al host de destino o no pueden ser procesados por éste.

Dirección de ubicación del destinatario (destino)	Dirección de ubicación de remitente (origen)	Saludo (indicador de inicio del mensaje)	Identificador del destinatario (destino)	Contenido de la carta (datos encapsulados)	Identificador del emisor (origen)	Fin de la trama (indicador de final del mensaje)
Dirección del sobre		Carta encapsulada				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Florida 34471	Querida	Jane:	Acabo de regresar de mi viaje. Se me ocurrió que te gustaría ver mis fotos.	John	

Destino (dirección física o de hardware)	Origen (dirección física o de hardware)	Indicador de inicio (indicador de inicio del mensaje)	Destinatario (identificador de destino)	Emisor (identificador de origen)	Datos encapsulados (bits)	Fin de la trama (indicador de final del mensaje)
Direccionamiento de la trama		Mensaje encapsulado				

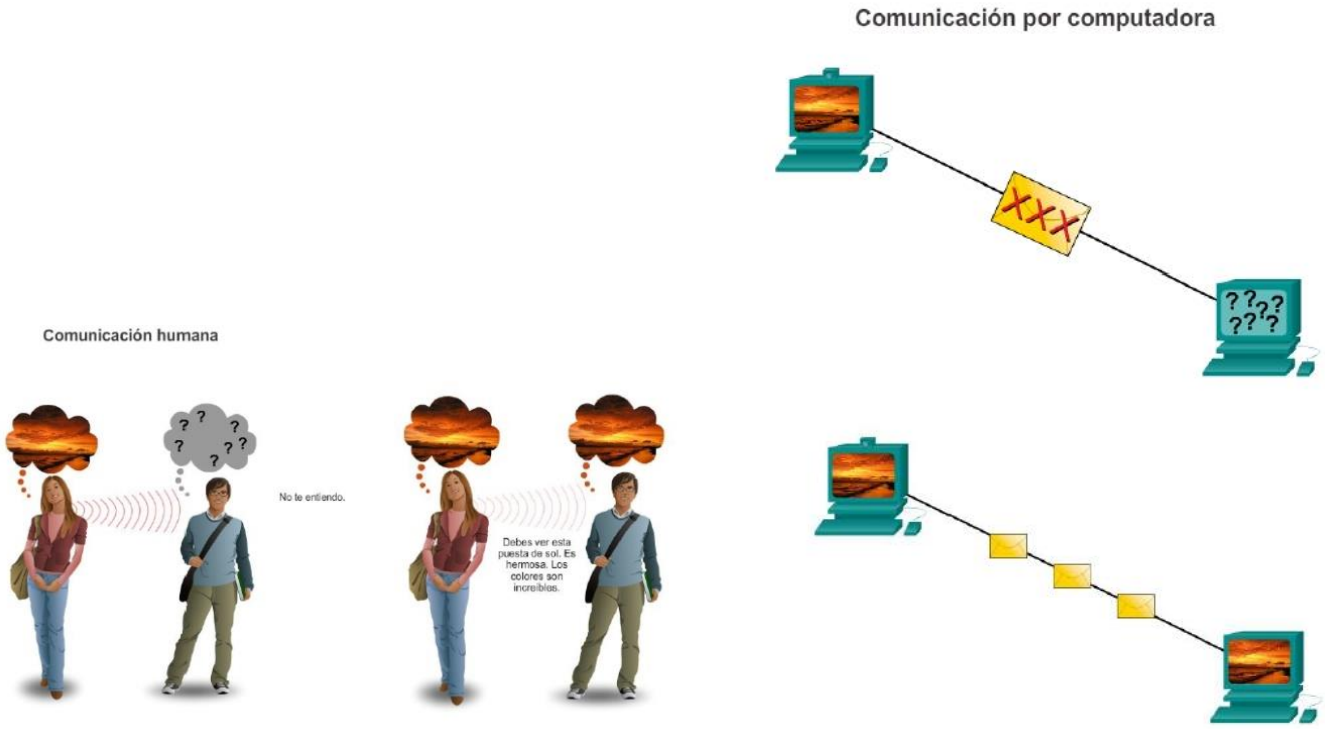
Capítulo 3: Protocolos y comunicaciones de red 3.1.1.5 Tamaño del mensaje

Tamaño del mensaje

Otra regla de comunicación es el tamaño. Cuando las personas se comunican, los mensajes que envían, normalmente, están divididos en fragmentos más pequeños u oraciones. El tamaño de estas oraciones se limita a lo que la persona que recibe el mensaje puede procesar por vez, como se muestra en la figura 1. Una conversación individual puede estar compuesta por muchas oraciones más pequeñas para asegurarse de que cada parte del mensaje sea recibida y comprendida. Imagine cómo sería leer este curso si todo el contenido apareciera como una sola oración larga; no sería fácil de comprender.

De manera similar, cuando se envía un mensaje largo de un host a otro a través de una red, es necesario dividirlo en partes más pequeñas, como se muestra en la figura 2. Las reglas que controlan el tamaño de las partes, o tramas que se comunican a través de la red, son muy estrictas. También pueden ser diferentes, de acuerdo con el canal utilizado. Las tramas que son demasiado largas o demasiado cortas no se entregan.

Las restricciones de tamaño de las tramas requieren que el host de origen divida un mensaje largo en fragmentos individuales que cumplan los requisitos de tamaño mínimo y máximo. Esto se conoce como segmentación. Cada segmento se encapsula en una trama separada con la información de la dirección y se envía a través de la red. En el host receptor, los mensajes se desencapsulan y se vuelven a unir para su procesamiento e interpretación.



Capítulo 3: Protocolos y comunicaciones de red 3.1.1.6 Temporización del mensaje

Temporización del mensaje

Otro factor que afecta la correcta recepción y comprensión del mensaje es la temporización. Las personas utilizan la temporización para determinar cuándo hablar, la velocidad con la que lo harán y cuánto tiempo deben esperar una respuesta. Éstas son las reglas de la participación.

Método de acceso

El método de acceso determina en qué momento alguien puede enviar un mensaje. Estas reglas de temporización se basan en el contexto. Por ejemplo: tal vez usted pueda hablar cada vez que quiera decir algo. En este contexto, una persona debe esperar hasta que nadie más esté hablando antes de comenzar a hablar. Si dos personas hablan a la vez, se produce una colisión de información, y es necesario que ambas se detengan y vuelvan a comenzar, como se muestra en la figura 1. De manera similar, las computadoras deben definir un método de acceso. Los hosts de una red necesitan un método de acceso para saber cuándo comenzar a enviar mensajes y cómo responder cuando se produce algún error.

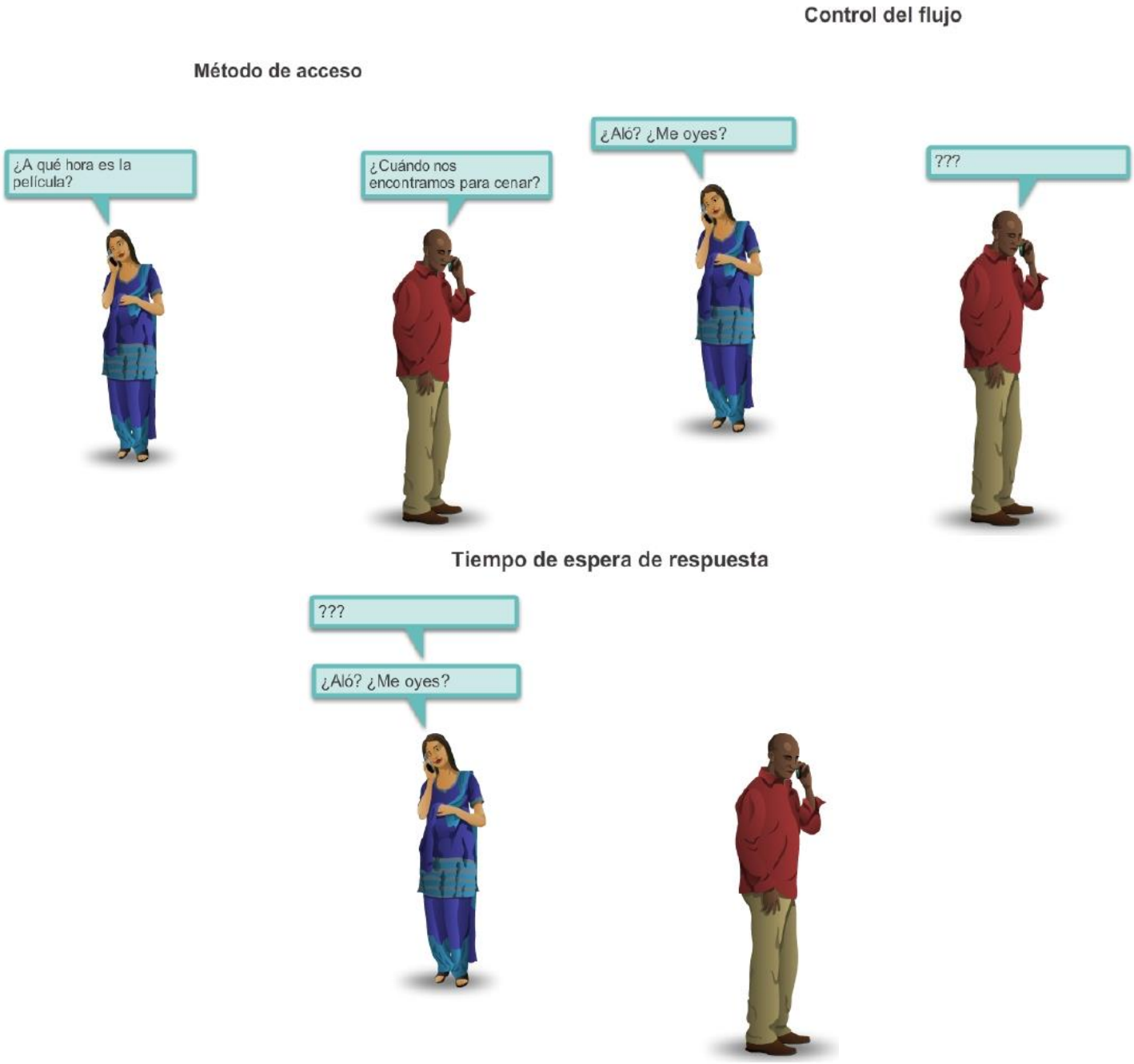
Control de flujo

La temporización también afecta la cantidad de información que se puede enviar y la velocidad con la que puede entregarse. Si una persona habla demasiado rápido, la otra persona tendrá dificultades para escuchar y comprender el mensaje, como se muestra en la figura 2. La persona que recibe el mensaje debe solicitar al emisor que disminuya la velocidad. En las comunicaciones de redes, un host emisor puede transmitir mensajes a una velocidad mayor que la que puede recibir y procesar el host de destino. Los hosts de origen y destino utilizan el control del flujo para negociar la temporización correcta, a fin de que la comunicación sea exitosa.

Tiempo de espera de respuesta

Si una persona hace una pregunta y no escucha una respuesta antes de un tiempo aceptable, supone que no habrá ninguna respuesta y reacciona en consecuencia, como se muestra en la figura 3.

La persona puede repetir la pregunta o puede continuar la conversación. Los hosts de las redes también tienen reglas que especifican cuánto tiempo deben esperar una respuesta y qué deben hacer si se agota el tiempo de espera para la respuesta.



Capítulo 3: Protocolos y comunicaciones de red 3.1.1.7 Opciones de entrega del mensaje

Opciones de entrega del mensaje

Puede ser necesario entregar un mensaje mejor, de distintas maneras, como se muestra en la figura 1. En algunos casos, una persona desea comunicar información a un solo individuo. Otras veces, esa persona puede necesitar enviar información a un grupo de personas simultáneamente o, incluso, a todas las personas de un área. Una conversación entre dos personas constituye un ejemplo de una entrega de uno a uno.

Cuando es necesario que un grupo de destinatarios reciba un mismo mensaje de manera simultánea, se necesita una entrega de mensaje de uno a varios o de uno a todos.

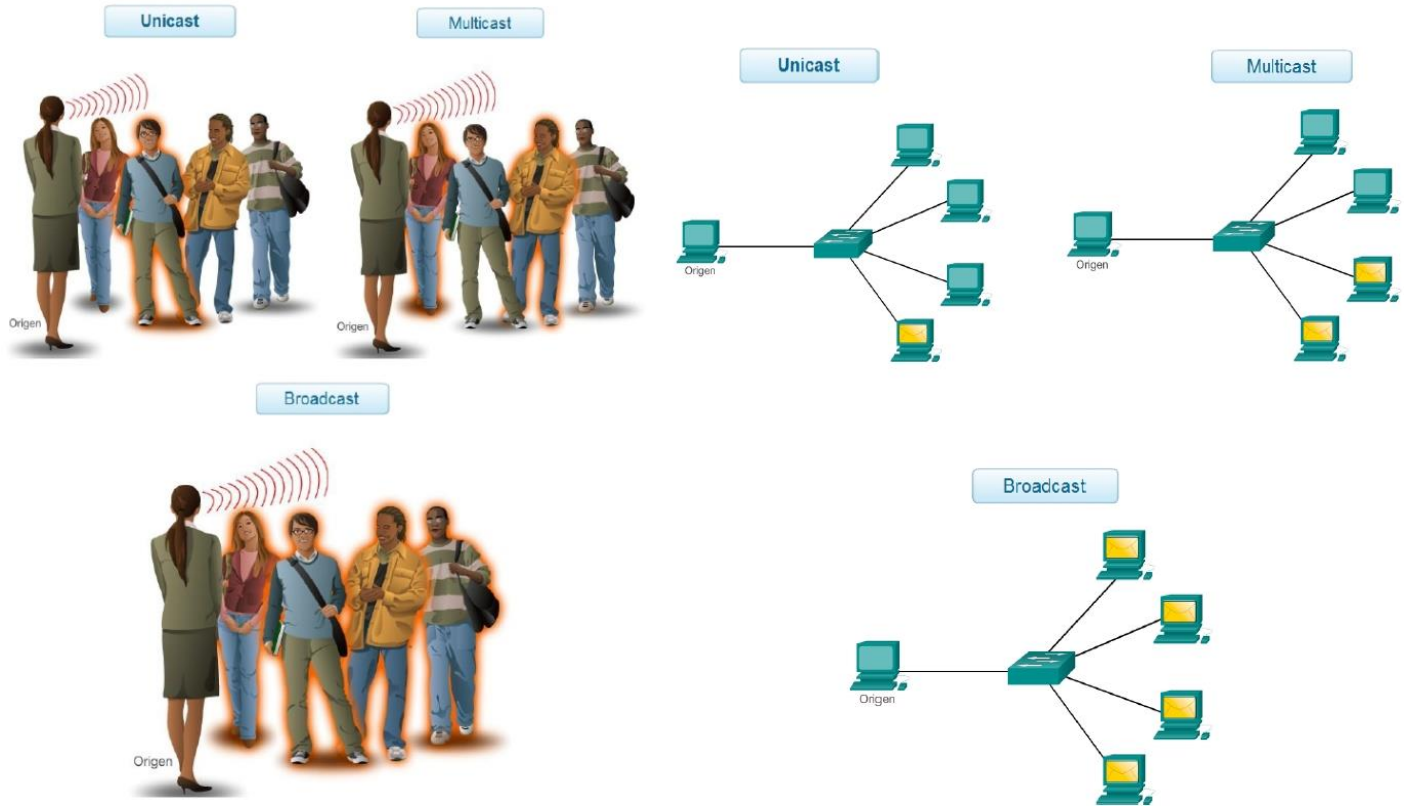
También puede ocurrir que el emisor de un mensaje necesite asegurarse de que el mensaje se haya entregado correctamente al destino. En estos casos, es necesario que el receptor envíe una confirmación al emisor. Si no se necesita ningún acuse de recibo, se dice que el envío del mensaje es sin acuse de recibo.

Los hosts en una red utilizan opciones de entrega similares para comunicarse, como se muestra en la figura 2.

Las opciones de entrega de uno a uno se denominan “unicast”, lo que significa que el mensaje tiene un único destino.

Si un host necesita enviar mensajes utilizando una opción de envío de uno a varios, se denomina “multicast”. Multicasting es el envío de un mismo mensaje a un grupo de hosts de destino de manera simultánea.

Si es necesario que todos los hosts de la red reciban el mensaje a la vez, se utiliza el método de broadcast. El broadcasting representa una opción de entrega de mensaje de uno a todos. Además, los hosts tienen requisitos para los mensajes con confirmación que son diferentes de los requisitos para los mensajes sin confirmación.



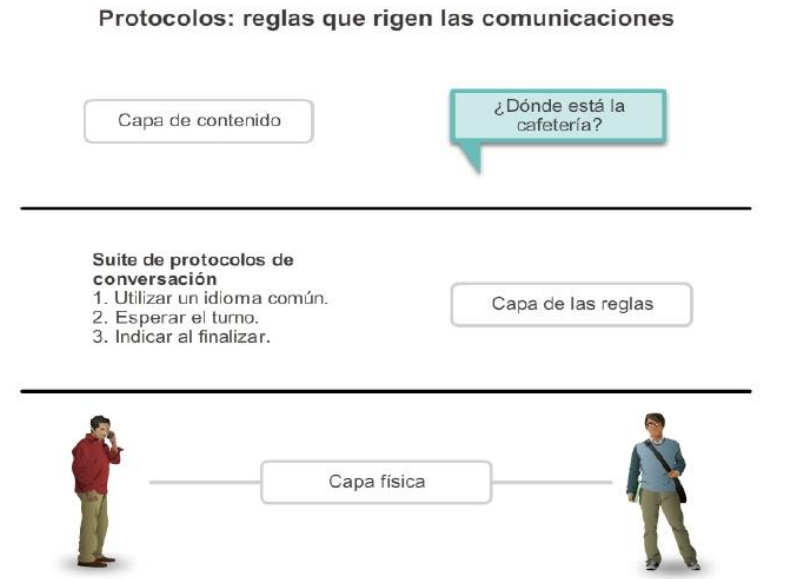
Capítulo 3: Protocolos y comunicaciones de red 3.2.1.1 Protocolos: reglas que rigen las comunicaciones

Al igual que en la comunicación humana, los diversos protocolos informáticos y de red deben poder interactuar y trabajar en conjunto para que la comunicación de red se lleve a cabo correctamente. Un grupo de protocolos interrelacionados que son necesarios para realizar una función de comunicación se denomina “suite de protocolos”. Los hosts y los dispositivos de red implementan las suites de protocolos en software, hardware o ambos.

Una de las mejores formas para visualizar la forma en que los protocolos interactúan dentro de una suite es ver la interacción como un stack. Un stack de protocolos muestra la forma en que los protocolos individuales se implementan dentro de una suite.

Los protocolos se muestran en capas, donde cada servicio de nivel superior depende de la funcionalidad definida por los protocolos que se muestran en los niveles inferiores. Las capas inferiores del stack se encargan del movimiento de datos por la red y proporcionan servicios a las capas superiores, las cuales se enfocan en el contenido del mensaje que se envía. Como se muestra en la ilustración, podemos utilizar capas para describir la actividad que tiene lugar en el ejemplo de comunicación cara a cara. En la capa inferior, la capa física, hay dos personas, cada una con una voz que puede pronunciar palabras en voz alta. En la segunda capa, la capa de las reglas, existe un acuerdo para hablar en un lenguaje común. En la capa superior, la capa de contenido, están las palabras que se pronuncian realmente. Este es el contenido de la comunicación.

Si fuéramos testigos de esta conversación, realmente no veríamos las capas flotando en el lugar. El uso de capas es un modelo que proporciona una forma de dividir convenientemente una tarea compleja en partes y describir cómo funcionan.



Las suites de protocolos son conjuntos de reglas que funcionan en conjunto para ayudar a resolver un problema.

Capítulo 3: Protocolos y comunicaciones de red 3.2.1.2 Protocolos de red

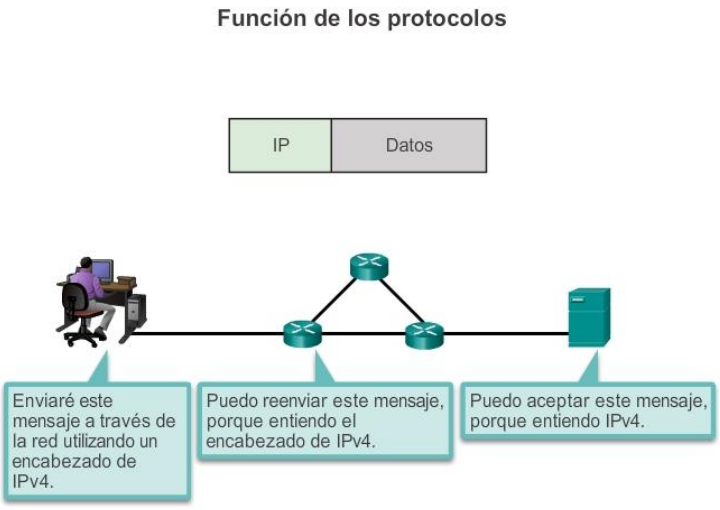
A nivel humano, algunas reglas de comunicación son formales y otras simplemente se sobreentienden, según los usos y costumbres. Para que los dispositivos se puedan comunicar en forma exitosa, un nuevo conjunto de aplicaciones de protocolos debe describir los requerimientos e interacciones precisos.

Los protocolos de red definen un formato y un conjunto de reglas comunes para intercambiar mensajes entre dispositivos. Algunos protocolos de red comunes son IP, HTTP y DHCP.

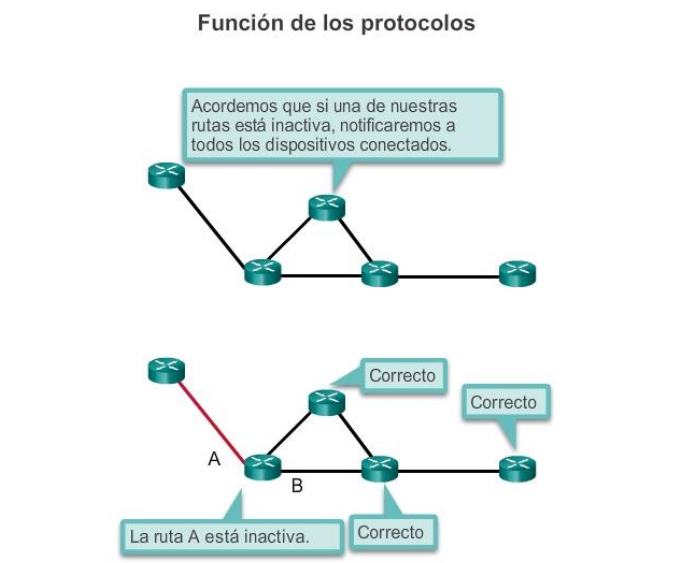
En las ilustraciones, se muestran los protocolos de red que describen los siguientes procesos:

- La manera en que se da formato o se estructura el mensaje, como se muestra en la figura 1.
- El proceso por el cual los dispositivos de red comparten información sobre rutas con otras redes, como se muestra en la figura 2.
- La manera y el momento en que se transmiten mensajes de error y del sistema entre los dispositivos, como se muestra en la figura 3.

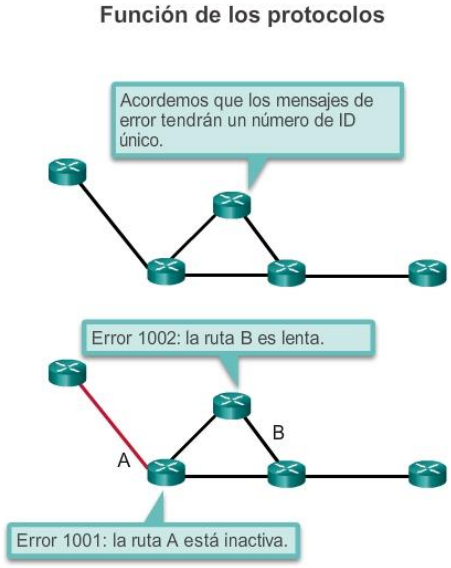
- La configuración y la terminación de sesiones de transferencia de datos, como se muestra en la figura 4



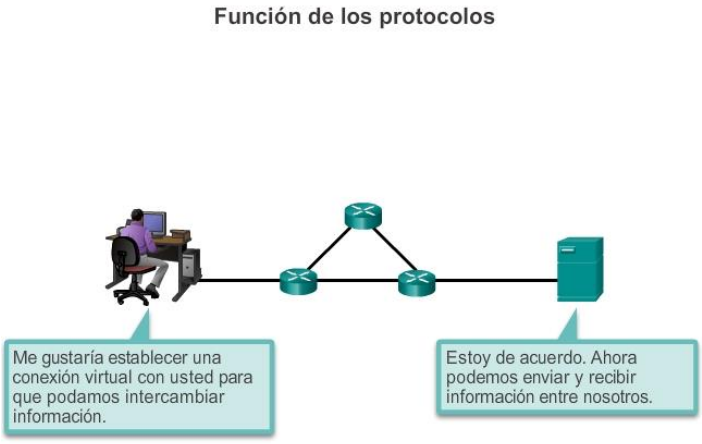
Formato o estructura de las partes de la comunicación



Proceso por el cual los dispositivos de red comparten información sobre rutas a otras redes



Cómo y cuándo se transmiten mensajes de error y del sistema entre los dispositivos



Configuración y terminación de las sesiones de transferencia de datos

Por ejemplo, IP define la forma en que un paquete de datos se entrega dentro de una red o a una red remota. La información del protocolo IPv4 se transmite en un formato específico de modo que el receptor pueda interpretarlo correctamente. Esto no difiere mucho del protocolo utilizado para escribir la dirección en un sobre al enviar una carta. La información debe respetar un determinado formato, ya que, de lo contrario, la oficina de correos no puede entregar la carta en el destino.

Capítulo 3: Protocolos y comunicaciones de red 3.2.1.3 Interacción de protocolos

Un ejemplo del uso de una suite de protocolos en comunicaciones de red es la interacción entre un servidor Web y un cliente Web. Esta interacción utiliza una cantidad de protocolos y estándares en el proceso de intercambio de información entre ellos. Los distintos protocolos trabajan en conjunto para asegurar que ambas partes reciben y entienden los mensajes. Algunos ejemplos de estos protocolos son:

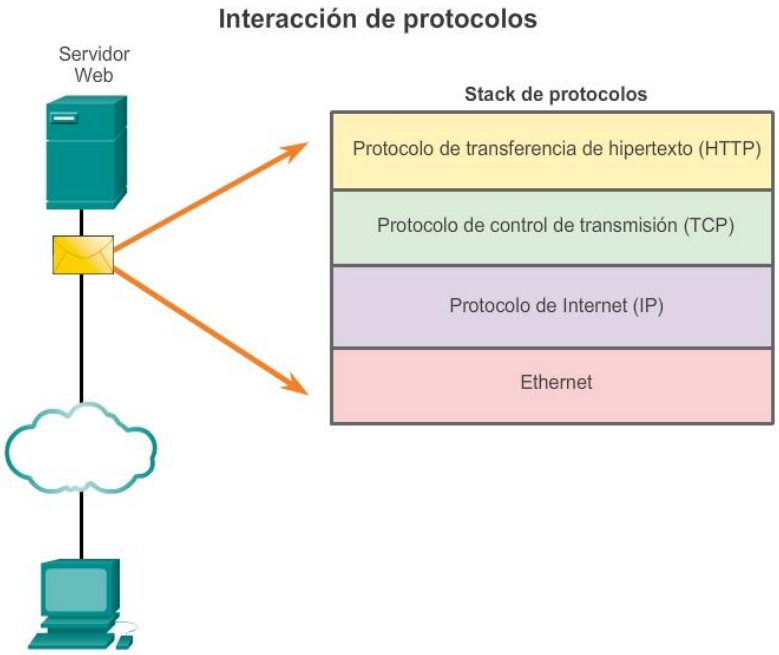
- Protocolo de aplicación: el protocolo de transferencia de hipertexto (HTTP) es un protocolo que rige la forma en que interactúan un servidor Web y un cliente Web. HTTP define el contenido y el formato de las solicitudes y respuestas intercambiadas entre el cliente y el servidor.

  Tanto el cliente como el software del servidor Web implementan el HTTP como parte de la aplicación. HTTP depende de otros protocolos para regular la forma en que los mensajes se transportan entre el cliente y el servidor.

- Protocolo de transporte: el protocolo de control de transmisión (TCP) es el protocolo de transporte que administra las conversaciones individuales entre servidores Web y clientes Web. TCP divide los mensajes HTTP en partes más pequeñas, llamadas “segmentos”. Estos segmentos se envían entre los procesos del servidor y el cliente Web que se ejecutan en el host de destino. TCP también es responsable de controlar el tamaño y la velocidad a los que se intercambian los mensajes entre el servidor y el cliente.

- Protocolo de Internet: IP es responsable de tomar los segmentos con formato de TCP, encapsularlos en paquetes, asignarles las direcciones adecuadas y enviarlos a través del mejor camino hacia el host de destino.

- Protocolos de acceso a la red: los protocolos de acceso a la red describen dos funciones principales, la comunicación a través de un enlace de datos y la transmisión física de datos en los medios de red. Los protocolos de administración de enlace de datos toman los paquetes IP y los formatean para transmitirlos por los medios. Los estándares y protocolos de los medios físicos rigen la forma en que se envían las señales y la forma en que las interpretan los clientes que las reciben. Ethernet constituye un ejemplo de un protocolo de acceso a la red.



Capítulo 3: Protocolos y comunicaciones de red 3.2.2.1 Suites de protocolos y estándares de la industria

Como se indicó anteriormente, una suite de protocolos es un grupo de protocolos que trabajan en forma conjunta para proporcionar servicios integrales de comunicación de red. Las suites de protocolos pueden estar especificadas por un organismo de estandarización o pueden ser desarrolladas por un proveedor.

Los protocolos IP, HTTP y DHCP son todos parte de la suite de protocolos de Internet conocida como protocolo de control de transmisión/IP (TCP/IP).

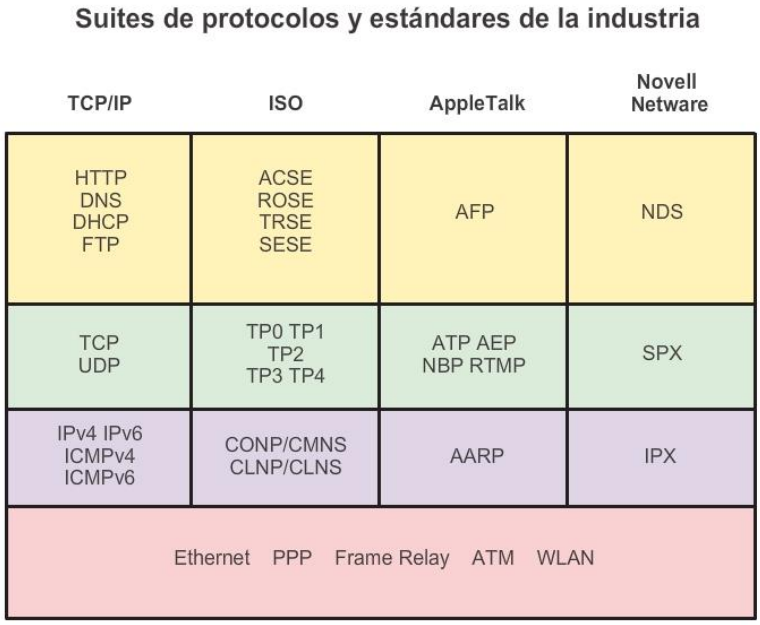
La suite de protocolos TCP/IP es un estándar abierto, lo que significa que estos protocolos están disponibles para el público sin cargo, y cualquier proveedor puede implementar estos protocolos en su hardware o software.

Un protocolo basado en estándares es un proceso o un protocolo que recibió el aval del sector de redes y fue ratificado, o aprobado, por un organismo de estandarización. El uso de estándares en el desarrollo y la implementación de protocolos aseguran que productos de distintos fabricantes puedan interoperar correctamente. Si un fabricante en particular no observa un protocolo estrictamente, es posible que sus equipos o software no puedan comunicarse satisfactoriamente con productos hechos por otros fabricantes.

En las comunicaciones de datos, por ejemplo, si un extremo de una conversación utiliza un protocolo para regir una comunicación unidireccional y el otro extremo adopta un protocolo que describe una comunicación bidireccional, es muy probable que no pueda intercambiarse ningún dato.

Algunos protocolos son exclusivos. Exclusivo, en este contexto, significa que una compañía o un proveedor controlan la definición del protocolo y cómo funciona. Algunos protocolos exclusivos los pueden utilizar distintas organizaciones con permiso del propietario. Otros, solo se pueden implementar en equipos fabricados por el proveedor exclusivo. AppleTalk y Novell Netware constituyen ejemplos de protocolos exclusivos.

Incluso es posible que varias compañías trabajen conjuntamente para crear un protocolo exclusivo. Es común que un proveedor (o grupo de proveedores) desarrolle un protocolo exclusivo para satisfacer las necesidades de sus clientes y posteriormente ayude a hacer de ese protocolo exclusivo un estándar abierto. Por ejemplo, Ethernet fue un protocolo desarrollado inicialmente por Bob Metcalfe en el XEROX Palo Alto Research Center (PARC) en la década de los setenta. En 1979, Bob Metcalfe creó su propia compañía, 3COM, y trabajó junto con Digital Equipment Corporation (DEC), Intel y Xerox para promover el estándar “DIX” para Ethernet. En 1985, el Instituto de Ingenieros en Electricidad y Electrónica (IEEE) publicó el estándar IEEE 802.3, que era casi idéntico a Ethernet. Actualmente, 802.3 es el estándar común que se utiliza en redes de área local (LAN). Otro ejemplo: más recientemente, Cisco abrió el protocolo de enrutamiento EIGRP como RFC informativa para satisfacer las necesidades de los clientes que desean utilizar el protocolo en una red de varios proveedores.



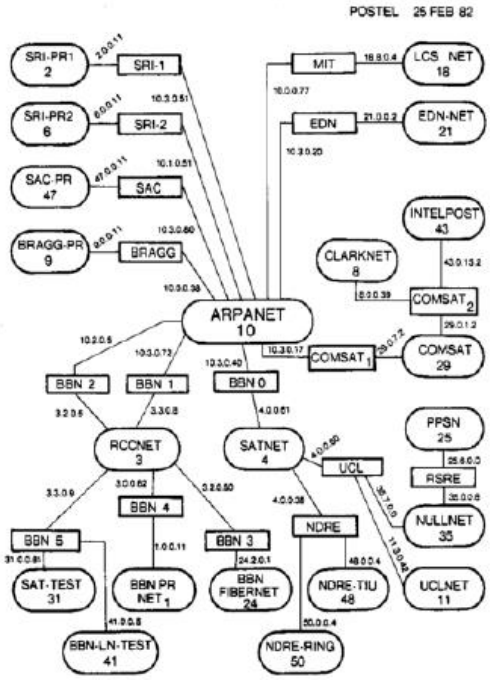
Capítulo 3: Protocolos y comunicaciones de red 3.2.2.2 Creación de Internet y desarrollo de TCP/IP

La suite IP es una suite de protocolos necesaria para transmitir y recibir información mediante Internet. Se conoce comúnmente como TCP/IP, ya que TCP e IP fueron los primeros dos protocolos de red definidos para este estándar. La suite TCP/IP basada en estándares abiertos reemplazó otras suites de protocolos exclusivas de proveedores, como AppleTalk de Apple e Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) de Novell.

La primera red de conmutación de paquetes, antecesora de Internet actual, fue la red Advanced Research Projects Agency Network (ARPANET), que tuvo su origen en 1969 al conectar PC centrales en cuatro ubicaciones. La ARPANET fue fundada por el Departamento de Defensa de los Estados Unidos para que se utilice en universidades y en laboratorios de investigación. Bolt, Beranek and Newman (BBN) fue el contratista que llevó a cabo gran parte del desarrollo inicial de la ARPANET, incluida la creación del primer router conocido como un procesador de mensajes de interfaz (IMP).

En 1973, Robert Kahn y Vinton Cerf comenzaron a trabajar en la suite TCP para desarrollar la siguiente generación de la ARPANET. TCP se diseñó para reemplazar el programa de control de red (NCP) actual de la ARPANET. En 1978, TCP se dividió en dos protocolos: TCP e IP. Posteriormente, se agregaron otros protocolos a la suite de protocolos TCP/IP, entre los que se incluyen Telnet, FTP, DNS y muchos otros.

Haga clic en la línea de tiempo de la ilustración para ver los detalles sobre el desarrollo de otros protocolos y aplicaciones de red.



Capítulo 3: Protocolos y comunicaciones de red 3.2.2.3 Suite de protocolos TCP/IP y proceso de comunicación

Actualmente, la suite incluye decenas de protocolos, como se muestra en la figura 1. Haga clic en cada protocolo para ver su descripción. Están organizados en capas y utilizan el modelo de protocolo TCP/IP. Los protocolos TCP/IP están incluidos en la capa de Internet hasta la capa de aplicación cuando se hace referencia al modelo TCP/IP. Los protocolos de capa inferior de la capa de enlace de datos o de la capa de acceso a la red son responsables de enviar el paquete IP a través del medio físico. Estos protocolos de capa inferior son desarrollados por organismos de estandarización, como el IEEE.

La suite de protocolos TCP/IP se implementa como un stack de TCP/IP tanto en los hosts emisores como en los hosts receptores para proporcionar una entrega de extremo a extremo de las aplicaciones a través de la red. Los protocolos 802.3 o Ethernet se utilizan para transmitir el paquete IP a través de un medio físico que utiliza la LAN.

En las figuras 2 y 3, se muestra el proceso de comunicación completo mediante un ejemplo de servidor Web que transmite datos a un cliente.

Haga clic en el botón Reproducir para ver la demostración animada:

1. La página de lenguaje de marcado de hipertexto (HTML) del servidor Web es el dato que se va a enviar.

2. El encabezado HTTP del protocolo de aplicación se agrega al frente de los datos HTML. El encabezado contiene diversos tipos de información, incluida la versión de HTTP que utiliza el servidor y un código de estado que indica que tiene información para el cliente Web.

3. El protocolo de capa de aplicación HTTP entrega los datos de la página Web con formato HTML a la capa de transporte. El protocolo de la capa de transporte TCP se utiliza para administrar la conversación individual entre el servidor Web y el cliente Web.

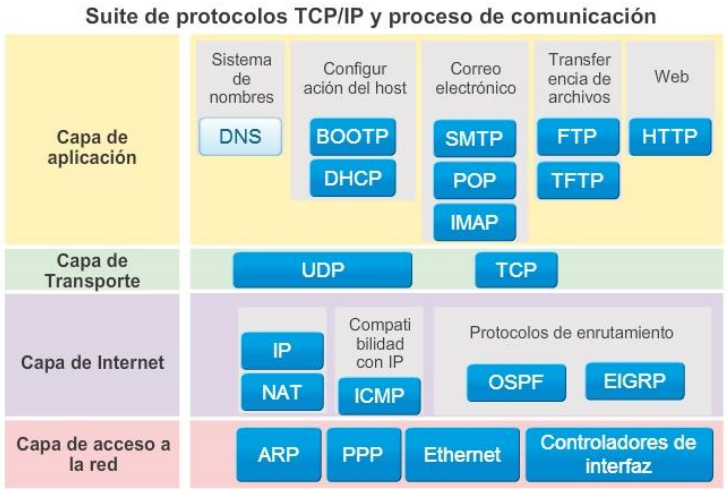
4. Luego, la información IP se agrega al frente de la información TCP. IP asigna las direcciones IP de origen y de destino que corresponden. Esta información se conoce como paquete IP.

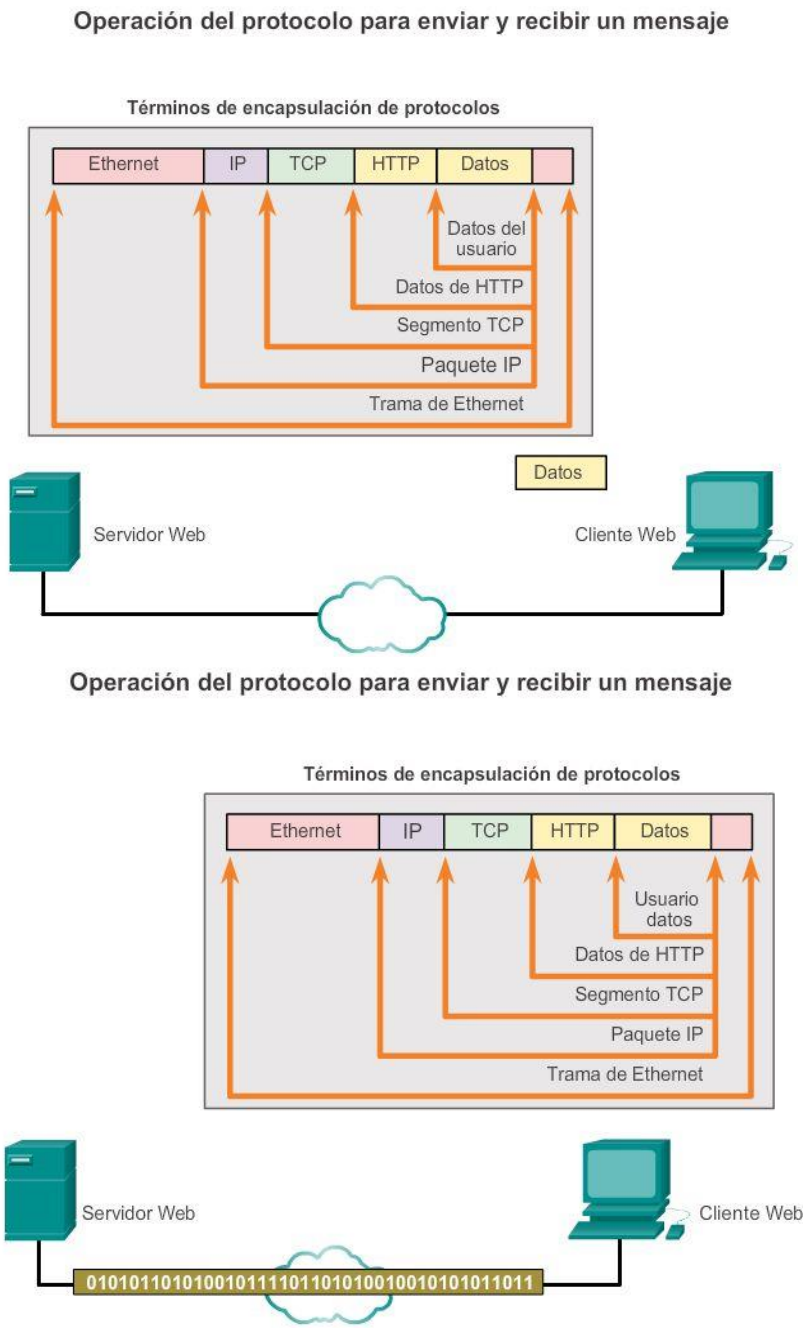
5. El protocolo Ethernet agrega información en ambos extremos del paquete IP, conocidos como la “trama de enlace de datos”. Esta trama se envía al router más cercano a lo largo de la ruta hacia el cliente Web. Este router elimina la información de Ethernet, analiza el paquete IP, determina el mejor camino para el paquete, coloca el paquete en una trama nueva y lo envía al siguiente router vecino hacia el destino. Cada router elimina y agrega información de enlace de datos nueva antes de reenviar el paquete.

6. Estos datos ahora se transportan a través de la internetwork, que consta de medios y dispositivos intermediarios.

7. El cliente recibe las tramas de enlace de datos que contienen los datos, y cada encabezado de protocolo se procesa y, a continuación, se elimina en el orden opuesto al que se agregó. La información de Ethernet se procesa y se elimina, seguida por la información del protocolo IP, luego la información de TCP y, finalmente, la información de HTTP.

8. A continuación, la información de la página Web se transfiere al software de explorador Web del cliente.





Capítulo 3: Protocolos y comunicaciones de red 3.2.3.1 Normas abiertas

Los estándares abiertos fomentan la competencia y la innovación. También garantizan que ningún producto de una sola compañía pueda monopolizar el mercado o tener una ventaja desleal sobre la competencia. La compra de un router inalámbrico para el hogar constituye un buen ejemplo de esto. Existen muchas opciones distintas disponibles de diversos proveedores, y todas ellas incorporan protocolos estándares, como IPv4, DHCP, 802.3 (Ethernet) y 802.11 (LAN inalámbrica). Estos estándares abiertos también permiten que un cliente con el sistema operativo OS X de Apple descargue una página Web de un servidor Web con el sistema operativo Linux. Esto se debe a que ambos sistemas operativos implementan los protocolos de estándar abierto, como los de la suite TCP/IP.

Los organismos de estandarización son importantes para mantener una Internet abierta con especificaciones y protocolos de libre acceso que pueda implementar cualquier proveedor.

Los organismos de estandarización pueden elaborar un conjunto de reglas en forma totalmente independiente o, en otros casos, pueden seleccionar un protocolo exclusivo como base para el estándar. Si se utiliza un protocolo exclusivo, suele participar el proveedor que creó el protocolo.

Los organismos de estandarización generalmente son organismos sin fines de lucro y neutrales en lo que respecta a proveedores, que se establecen para desarrollar y promover el concepto de estándares abiertos.

Entre los organismos de estandarización, se incluyen los siguientes:

- Internet Society (ISOC)
- Internet Architecture Board (IAB)
- Internet Engineering Task Force (IETF)
- Instituto de Ingenieros en Electricidad y Electrónica (IEEE)
- International Organization for Standardization (ISO)

Cada uno de estos organismos se analizará en mayor detalle en las próximas páginas.

En la ilustración, haga clic en cada logotipo para ver la información sobre los estándares.

Capítulo 3: Protocolos y comunicaciones de red 3.2.3.2 ISOC, IAB e IETF

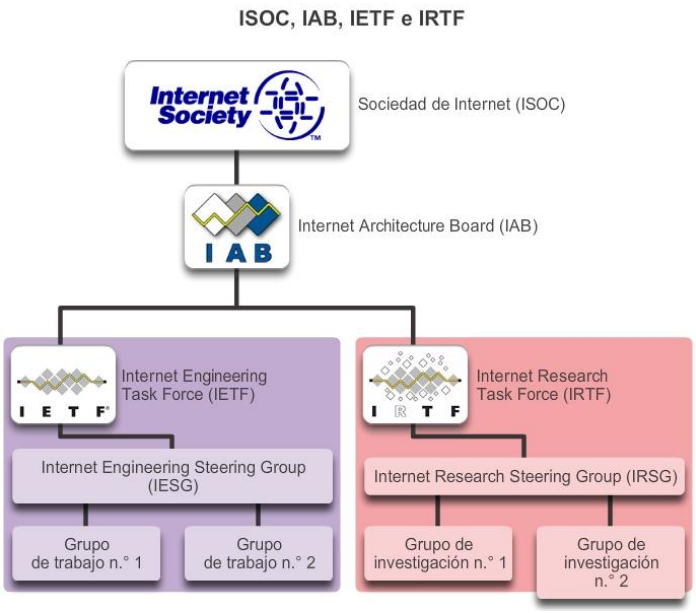
La Internet Society (ISOC) es responsable de promover el desarrollo, la evolución y el uso abiertos de Internet en todo el mundo. ISOC facilita el desarrollo abierto de estándares y protocolos para la infraestructura técnica de Internet, incluida la supervisión del Internet Architecture Board (IAB).

El Internet Architecture Board (IAB) es responsable de la administración y el desarrollo general de los estándares de Internet. El IAB supervisa la arquitectura para los protocolos y los procedimientos que utiliza Internet. El IAB consta de 13 miembros, entre los que se incluye el presidente del Internet Engineering Task Force (IETF). Los miembros del IAB actúan como personas, y no como representantes de compañías, agencias u otros organismos.

La misión del IETF es desarrollar, actualizar y mantener Internet y las tecnologías TCP/IP. Una de las responsabilidades clave del IETF es producir documentos de solicitud de comentarios (RFC), que son un memorándum que describe protocolos, procesos y tecnologías para Internet. El IETF consta de grupos de trabajo (WG), el mecanismo principal para desarrollar las pautas y especificaciones del IETF. Los WG son a corto plazo, y después de que se cumplen los objetivos del grupo, se pone fin al WG.

El Internet Engineering Steering Group (IESG) es responsable de la administración técnica del IETF y el proceso de los estándares de Internet.

The Internet Research Task Force (IRTF) se centra en la investigación a largo plazo relacionada con los protocolos, las aplicaciones, la arquitectura y las tecnologías de TCP/IP y de Internet. Mientras que el IETF se centra en problemas más a corto plazo de la creación de estándares, el IRTF consta de grupos de investigación para esfuerzos de desarrollo a largo plazo. Algunos de los grupos de investigación actuales incluyen Anti-Spam Research Group (ASRG), Crypto Forum Research Group (CFRG), Peer-to-Peer Research Group (P2PRG) y Router Research Group (RRG).



Capítulo 3: Protocolos y comunicaciones de red 3.2.3.3 IEEE

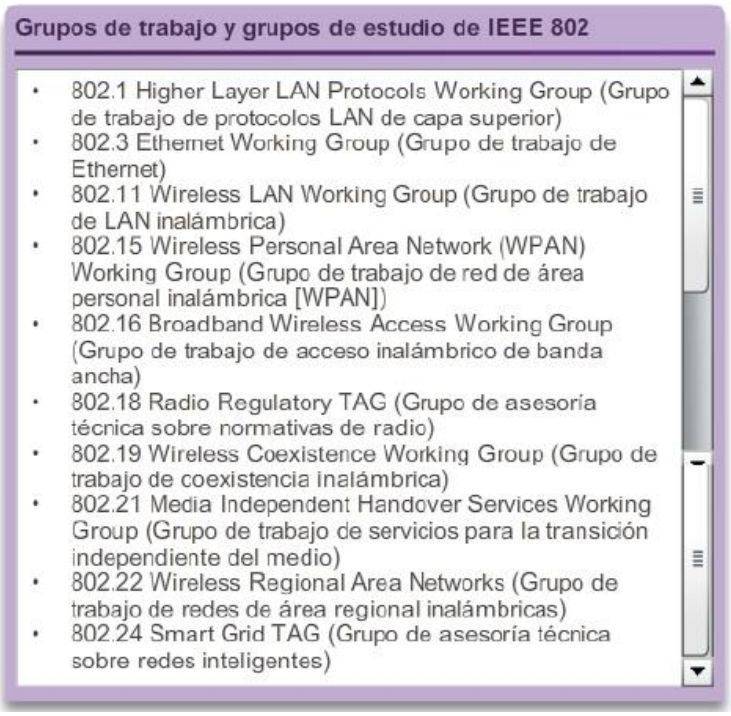
El Instituto de Ingenieros en Electricidad y Electrónica (IEEE, que se pronuncia “I, triple E”) es un organismo profesional para aquellos que trabajan en los campos de la electrónica y de la ingeniería eléctrica y se dedican a promover la innovación tecnológica y crear estándares. A partir de 2012, el IEEE consta de 38 sociedades, publica 130 diarios y patrocina más de 1300 conferencias cada año en todo el mundo. El IEEE tiene más de 1300 estándares y proyectos actualmente en desarrollo.

El IEEE tiene más de 400 000 miembros en más de 160 países. Más de 107 000 de esos miembros son miembros estudiantes. El IEEE proporciona oportunidades de mejora en el ámbito educativo y laboral para promover las habilidades y el conocimiento con el sector de la electrónica.

El IEEE es una de los organismos de estandarización líderes en el mundo. Crea y mantiene estándares que influyen en una amplia variedad de sectores, como energía, salud, telecomunicaciones y redes. La familia de estándares IEEE 802 se ocupa de redes de área local y redes de área metropolitana, incluidas tanto las redes conectadas por cable como las inalámbricas. Como se muestra en la ilustración, cada estándar del IEEE consta de un WG que se encarga de crear y mejorar los estándares.

Los estándares IEEE 802.3 e IEEE 802.11 son estándares IEEE importantes en redes de computadoras. El estándar IEEE 802.3 define el control de acceso al medio (MAC) para Ethernet por cable. Esta tecnología generalmente es para las LAN, pero también tiene aplicaciones para redes de área extensa (WAN). El estándar 802.11 define un conjunto de estándares para implementar redes de área local inalámbricas

(WLAN). Este estándar define el MAC físico y de enlace de datos del modelo de interconexión de sistema abierto (OSI) para las comunicaciones inalámbricas.



Capítulo 3: Protocolos y comunicaciones de red 3.2.3.4 ISO

La ISO, la International Organization for Standardization, es el mayor desarrollador del mundo de estándares internacionales para una amplia variedad de productos y servicios. ISO no es un acrónimo del nombre del organismo; por el contrario, el término proviene de la palabra griega “isos”, que significa “igual”. La International Organization for Standardization eligió el término ISO para afirmar su posición como igualitaria para todos los países.

En redes, la ISO se conoce principalmente por su modelo de referencia de interconexión de sistema abierto (OSI). La ISO publicó el modelo de referencia OSI en 1984 para desarrollar un esquema en capas para los protocolos de red. El objetivo original de este proyecto era no solo crear un modelo de referencia sino también servir como base para una suite de protocolos que se fuera a usar para Internet. Esto se conoció como la “suite de protocolos OSI”. Sin embargo, debido a la creciente popularidad de la suite TCP/IP, desarrollada por Robert Kahn, Vinton Cerf y otros, no se eligió la suite de protocolos OSI como la suite de protocolos para Internet. En cambio, se seleccionó la suite de protocolos TCP/IP. La suite de protocolos OSI se implementó en equipos de telecomunicaciones y aún puede encontrarse en redes de telecomunicaciones antiguas.

Es posible que conozca algunos de los productos que utilizan estándares ISO. La extensión de archivo ISO se utiliza en muchas imágenes de CD para indicar que utiliza el estándar ISO 9660 para el sistema de archivos. La ISO también es responsable de crear estándares para protocolos de enrutamiento.

Capítulo 3: Protocolos y comunicaciones de red 3.2.3.5 Otros organismos de estandarización

Los estándares de redes incluyen otros varios organismos de estandarización. Algunos de los más comunes son los siguientes:

- EIA: la Electronic Industries Alliance (EIA), conocida anteriormente como Electronics Industries Association, es un organismo internacional comercial y de estandarización para organizaciones de la industria electrónica. La EIA es conocida principalmente por sus estándares relacionados con el cableado eléctrico, los conectores y los bastidores de 19 in que se utilizan para montar equipos de red.

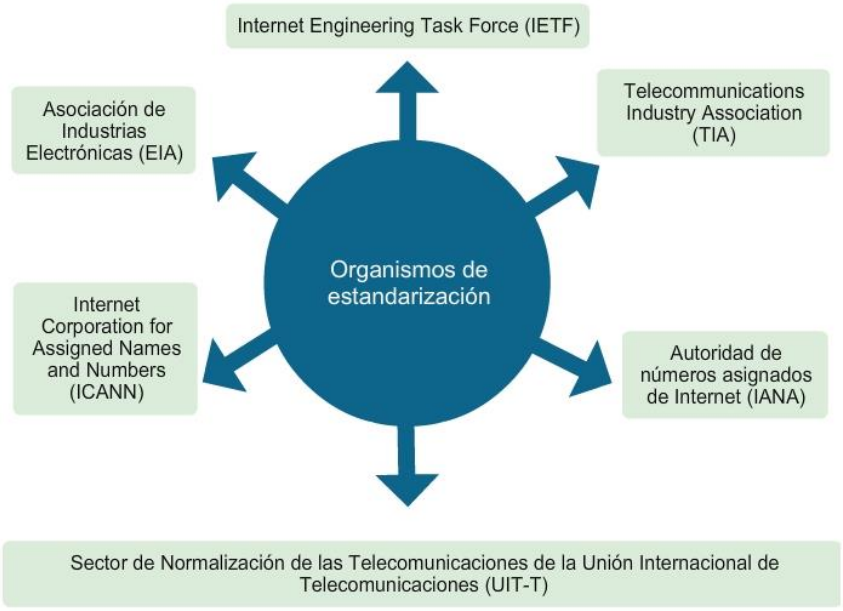
- TIA: la Telecommunications Industry Association (TIA) es responsable de desarrollar estándares de comunicación en diversas áreas, entre las que se incluyen equipos de radio, torres de telefonía móvil, dispositivos de voz sobre IP (VoIP) y comunicaciones satelitales. Muchos de los estándares se crean en colaboración con la EIA.

- UIT-T: el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T) es uno de los organismos de estandarización de comunicación más grandes y más antiguos. El UIT-T define estándares para la compresión de videos, televisión de protocolo de Internet (IPTV) y comunicaciones de banda ancha, como la línea de suscriptor digital (DSL). Por ejemplo, al marcar a otro país, se utilizan los códigos de país de la UIT para realizar la conexión.

- ICANN: la Internet Corporation for Assigned Names and Numbers (ICANN) es un organismo sin fines de lucro con base en los Estados Unidos que coordina la asignación de direcciones IP, la administración de nombres de dominio utilizados por DNS y los identificadores de protocolo o los números de puerto utilizados por los protocolos TCP y UDP. ICANN crea políticas y tiene una responsabilidad general sobre estas asignaciones.

- IANA: la Internet Assigned Numbers Authority (IANA) es un departamento de ICANN responsable de controlar y administrar la asignación de direcciones IP, la administración de nombres de dominio y los identificadores de protocolo para ICANN.

Conocer los organismos que crean estándares que se utilizan en redes lo ayudará a obtener una mayor comprensión de la forma en que estos estándares crean una Internet abierta y neutral en lo que respecta a proveedores, y le permitirá obtener información sobre nuevos estándares a medida que se desarrollan.



Capítulo 3: Protocolos y comunicaciones de red 3.2.4.1 Beneficios del uso de un modelo en capas

Los modelos en capas, como el modelo TCP/IP, con frecuencia se utilizan para ayudar a visualizar la interacción entre diversos protocolos. Un modelo en capas describe el funcionamiento de los protocolos que se produce en cada capa y la interacción de los protocolos con las capas que se encuentran por encima y por debajo de ellas.

Hay beneficios por el uso de un modelo en capas para describir protocolos de red y operaciones. Uso de un modelo en capas:

- Ayuda en el diseño de protocolos, ya que los protocolos que operan en una capa específica tienen información definida según la cual actúan, y una interfaz definida para las capas superiores e inferiores.
- Fomenta la competencia, ya que los productos de distintos proveedores pueden trabajar en conjunto.
- Evita que los cambios en la tecnología o en las capacidades de una capa afecten otras capas superiores e inferiores.
- Proporciona un lenguaje común para describir las funciones y capacidades de redes.

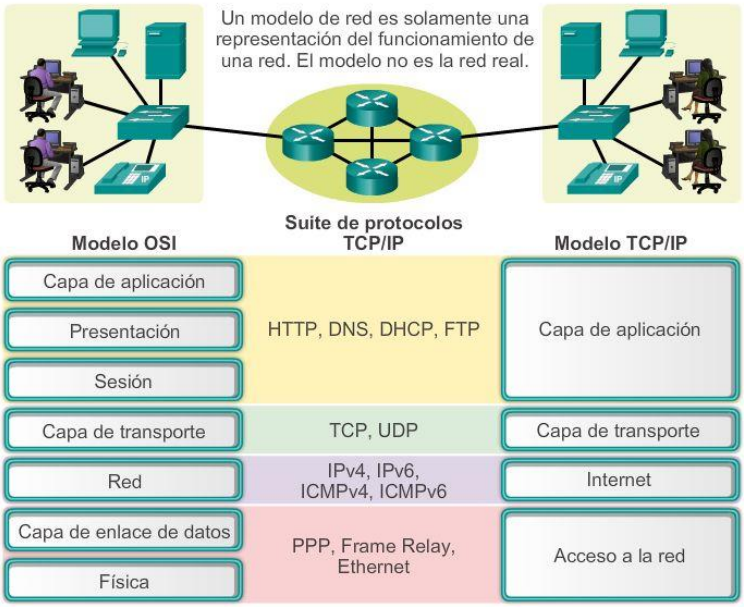
Existen dos tipos básicos de modelos de redes:

- Modelo de protocolo: este modelo coincide con precisión con la estructura de una suite de protocolos determinada. El conjunto jerárquico de protocolos relacionados en una suite representa típicamente toda la funcionalidad requerida para interconectar la red humana con la red de datos. El modelo TCP/IP es un modelo de protocolo, porque describe las funciones que tienen lugar en cada capa de protocolos dentro de una suite TCP/IP.
- Modelo de referencia: este modelo es coherente con todos los tipos de servicios y protocolos de red al describir qué es lo que se debe hacer en una capa determinada, pero sin regir la forma en que se debe lograr. Un modelo de referencia no está pensado para ser una especificación de implementación ni para proporcionar un nivel de detalle suficiente para definir de forma precisa los servicios de la arquitectura de

red. El objetivo principal de un modelo de referencia es ayudar a lograr un mejor entendimiento de las funciones y procesos involucrados.

El modelo OSI es el modelo de referencia de internetwork más conocido. Se usa para diseño de redes de datos, especificaciones de funcionamiento y resolución de problemas.

Como se muestra en la ilustración, los modelos TCP/IP y OSI son los modelos principales que se utilizan al hablar de funcionalidad de red. Los diseñadores de protocolos, servicios o dispositivos de red pueden crear sus propios modelos para representar sus productos. Por último, se solicita a los diseñadores que se comuniquen con la industria asociando sus productos o servicios con el modelo OSI, el modelo TCP/IP o ambos.



Capítulo 3: Protocolos y comunicaciones de red 3.2.4.2 Modelo de referencia OSI

Inicialmente, el modelo OSI fue diseñado por la ISO para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas exclusivos.

En última instancia, la velocidad a la que fue adoptada Internet basada en TCP/IP y la proporción en la que se expandió ocasionaron que el desarrollo y la aceptación de la suite de protocolos OSI quedaran atrás. Aunque pocos de los protocolos que se crearon mediante las especificaciones OSI se utilizan ampliamente en la actualidad, el modelo OSI de siete capas hizo más contribuciones al desarrollo de otros protocolos y productos para todo tipo de redes nuevas.

El modelo OSI proporciona una amplia lista de funciones y servicios que se pueden presentar en cada capa.

También describe la interacción de cada capa con las capas directamente por encima y por debajo de él. Si bien el contenido de este curso está estructurado en torno al modelo de referencia OSI, el análisis se centra en los protocolos identificados en el modelo de protocolo TCP/IP. Haga clic en cada nombre de la capa para ver los detalles.

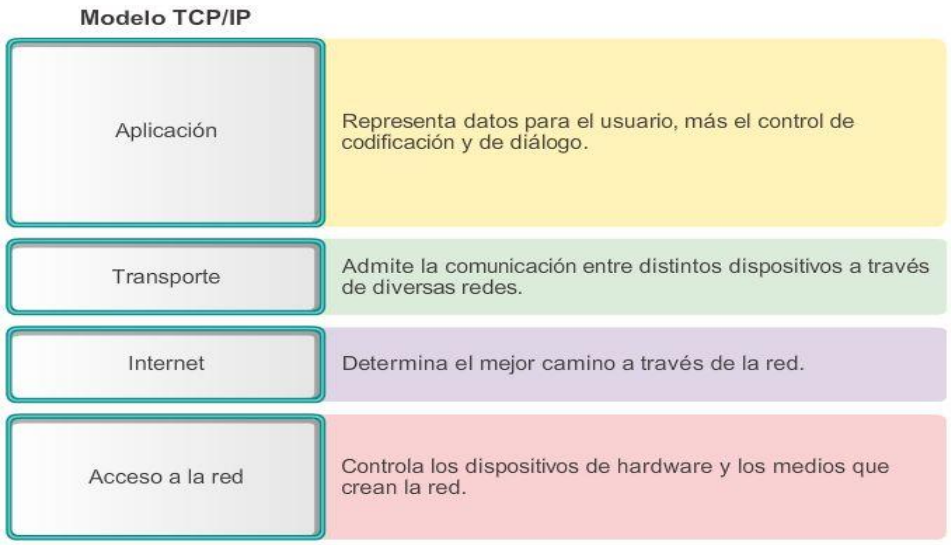
Nota: mientras que a las capas del modelo TCP/IP se hace referencia solo por el nombre, las siete capas del modelo OSI se mencionan con frecuencia por número y no por nombre. Por ejemplo, la capa física se conoce como capa 1 del modelo OSI.

Capítulo 3: Protocolos y comunicaciones de red 3.2.4.3 Modelo de protocolo TCP/IP

El modelo de protocolo TCP/IP para comunicaciones de internetwork se creó a principios de la década de los setenta y se conoce con el nombre de modelo de Internet. Como se muestra en la ilustración, define cuatro categorías de funciones que deben ocurrir para que las comunicaciones se lleven a cabo correctamente. La arquitectura de la suite de protocolos TCP/IP sigue la estructura de este modelo. Por lo tanto, el modelo de Internet es conocido normalmente como modelo TCP/IP.

La mayoría de los modelos de protocolos describen un stack de protocolos específicos del proveedor. Sin embargo, puesto que el modelo TCP/IP es un estándar abierto, una compañía no controla la definición del modelo. Las definiciones del estándar y los protocolos TCP/IP se explican en un foro público y se definen en un conjunto de RFC disponibles al público. Las RFC contienen la especificación formal de los protocolos de comunicación de datos y los recursos que describen el uso de los protocolos.

Las RFC también contienen documentos técnicos y organizacionales sobre Internet, entre los que se incluyen las especificaciones técnicas y los documentos de las políticas elaborados por el IETF.



Capítulo 3: Protocolos y comunicaciones de red 3.2.4.4 Comparación entre el modelo OSI y el modelo TCP/IP

Los protocolos que forman la suite de protocolos TCP/IP pueden describirse en términos del modelo de referencia OSI. En el modelo OSI, la capa de acceso a la red y la capa de aplicación del modelo TCP/IP están subdivididas para describir funciones discretas que deben producirse en estas capas.

En la capa de acceso a la red, la suite de protocolos TCP/IP no especifica qué protocolos se deben utilizar cuando se transmite por un medio físico, sino que solo describe la transferencia desde la capa de Internet hacia los protocolos de red física. Las capas 1 y 2 de OSI tratan los procedimientos necesarios para acceder a los medios y las maneras físicas de enviar datos a través de una red.

Como se muestra en la ilustración, los paralelismos fundamentales entre los dos modelos de red se producen en las capas 3 y 4 de OSI. La capa 3 de OSI, la capa de red, se utiliza casi universalmente para describir el alcance de los procesos que ocurren en todas las redes de datos para dirigir y enrutar mensajes a través de una internetwork. IP es el protocolo de la suite TCP/IP que incluye la funcionalidad descrita en la capa 3 de OSI.

La capa 4, la capa de transporte del modelo OSI, describe los servicios y las funciones generales que proporcionan la entrega ordenada y confiable de datos entre los hosts de origen y de destino. Estas funciones incluyen acuse de recibo, recuperación de errores y secuenciamiento. En esta capa, los protocolos TCP/IP, el protocolo TCP y el protocolo de datagramas del usuario (UDP) proporcionan la funcionalidad necesaria.

La capa de aplicación de TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos que funcionan en redes.

Comparación del modelo OSI con el modelo TCP/IP

Las similitudes clave se encuentran en la capa de transporte y en la capa de red. Sin embargo, los dos modelos se diferencian en el modo en que se relacionan con las capas que están por encima y por debajo de cada capa.

Capítulo 3: Protocolos y comunicaciones de red 3.3.1.1 Comunicación de mensajes

En teoría, una única comunicación, como un video musical o un mensaje de correo electrónico, podría enviarse a través de una red desde un origen hasta un destino como un stream de bits masivo y continuo. Si en realidad los mensajes se transmitieron de esta manera, significará que ningún otro dispositivo podrá enviar

o recibir mensajes en la misma red mientras esta transferencia de datos está en progreso. Estos grandes streams de datos originarán retrasos importantes. Además, si falla un enlace en la infraestructura de la red interconectada durante la transmisión, el mensaje completo se perdería y tendría que retransmitirse completamente.

Un método mejor es dividir los datos en partes más pequeñas y manejables para enviarlas por la red. La división del stream de datos en partes más pequeñas se denomina segmentación. La segmentación de mensajes tiene dos beneficios principales:

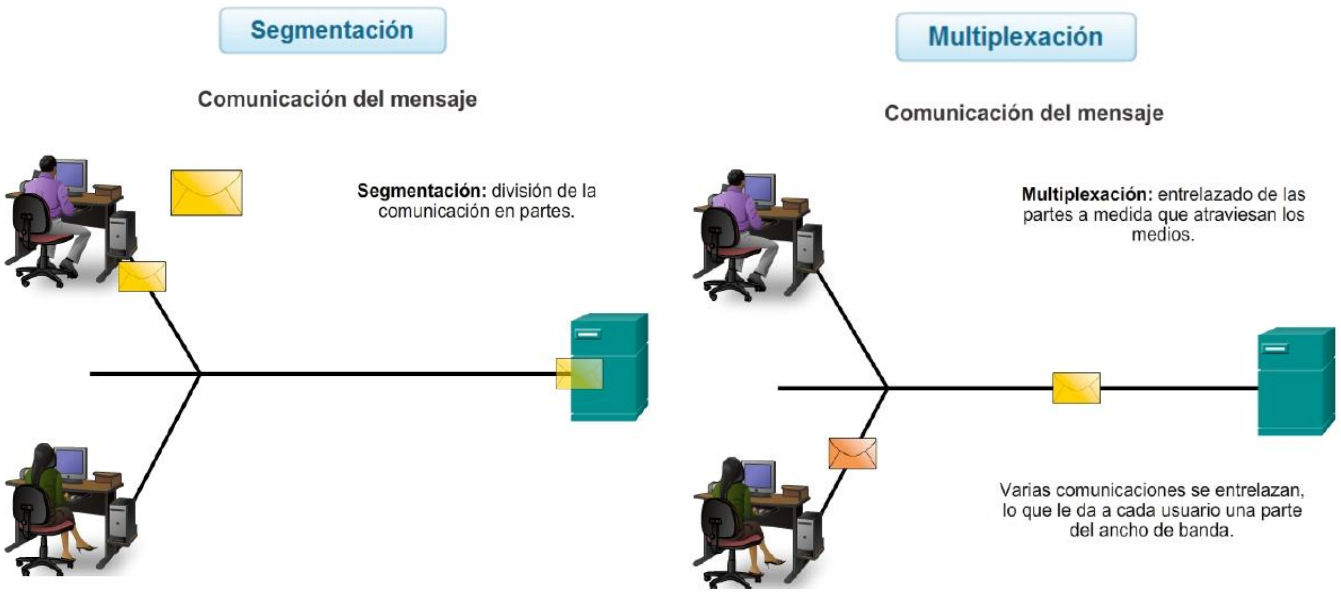
- Al enviar partes individuales más pequeñas del origen al destino, se pueden intercalar muchas conversaciones diversas en la red. El proceso que se utiliza para intercalar las piezas de conversaciones separadas en la red se denomina multiplexación. Haga clic en cada botón de la figura 1 y, a continuación, haga clic en el botón Reproducir para ver las animaciones de segmentación y de multiplexación.

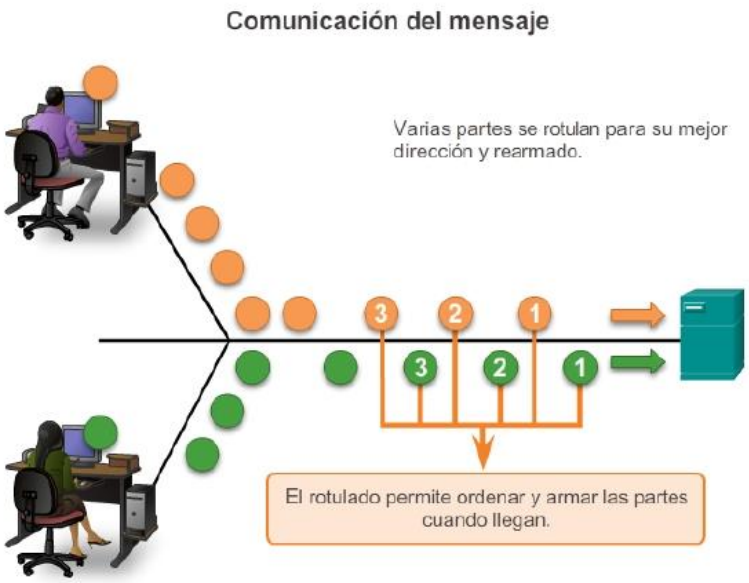
- La segmentación puede aumentar la confiabilidad de las comunicaciones de red. No es necesario que las partes separadas de cada mensaje sigan el mismo recorrido a través de la red desde el origen hasta el destino. Si una ruta en particular se satura con el tráfico de datos, o falla, las partes individuales del mensaje aún pueden direccionarse hacia el destino mediante los recorridos alternativos. Si parte del mensaje no logra llegar al destino, solo se deben retransmitir las partes faltantes.

La desventaja de utilizar segmentación y multiplexación para transmitir mensajes a través de la red es el nivel de complejidad que se agrega al proceso. Supongamos que tuviera que enviar una carta de 100 páginas, pero en cada sobre solo cabe una. El proceso de escribir la dirección, etiquetar, enviar, recibir y abrir los 100 sobres requeriría mucho tiempo tanto para el emisor como para el destinatario.

En las comunicaciones de red, cada segmento del mensaje debe seguir un proceso similar para asegurar que llegue al destino correcto y que pueda volverse a armar en el contenido del mensaje original, como se muestra en la figura 2.

Varios tipos de dispositivos en toda la red participan para asegurar que las partes del mensaje lleguen a los destinos de manera confiable.





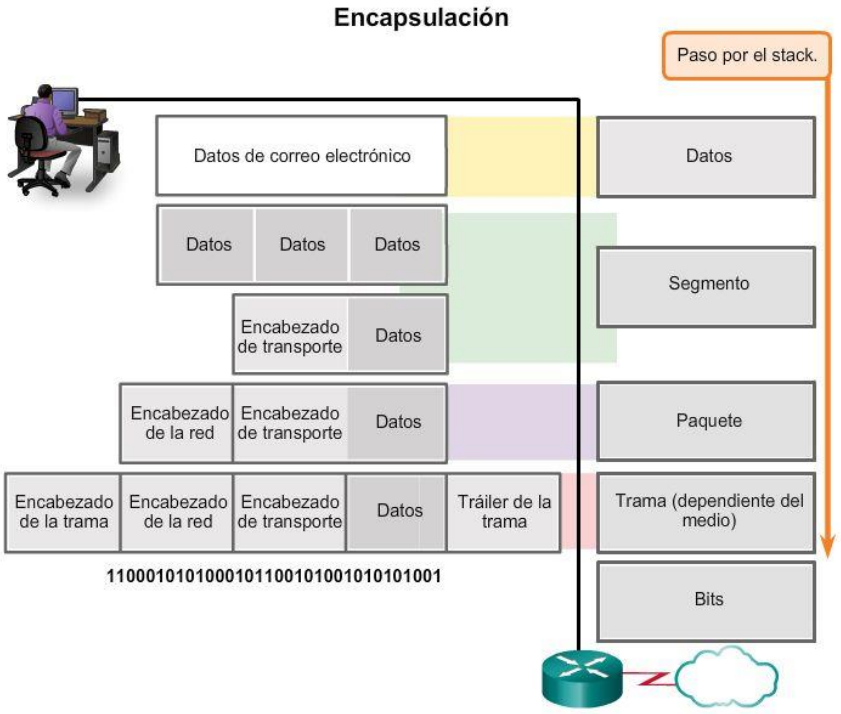
Capítulo 3: Protocolos y comunicaciones de red 3.3.1.2 Unidades de datos del protocolo (PDU)

Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.

La forma que adopta una porción de datos en cualquier capa se denomina “unidad de datos del protocolo (PDU)”. Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza.

En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus nuevas funciones. Aunque no existe una convención universal de nomenclatura para las PDU, en este curso se denominan de acuerdo con los protocolos de la suite TCP/IP, como se muestra en la ilustración:

- Datos: término general para la PDU que se utiliza en la capa de aplicación.
- Segmento: PDU de la capa de transporte.
- Paquete: PDU de la capa de red
- Trama: PDU de la capa de enlace de datos
- Bits: PDU de la capa física que se utiliza cuando se transmiten datos físicamente por el medio



Capítulo 3: Protocolos y comunicaciones de red 3.3.1.3 Encapsulación

La encapsulación de datos es el proceso que agrega la información adicional del encabezado del protocolo a los datos antes de la transmisión. En la mayoría de las formas de comunicaciones de datos, los datos originales se encapsulan o envuelven en varios protocolos antes de transmitirse.

Cuando se envían mensajes en una red, el stack de protocolos de un host opera desde las capas superiores hacia las capas inferiores. En el ejemplo del servidor Web podemos utilizar el modelo TCP/IP para ilustrar el proceso de envío de una página Web HTML a un cliente.

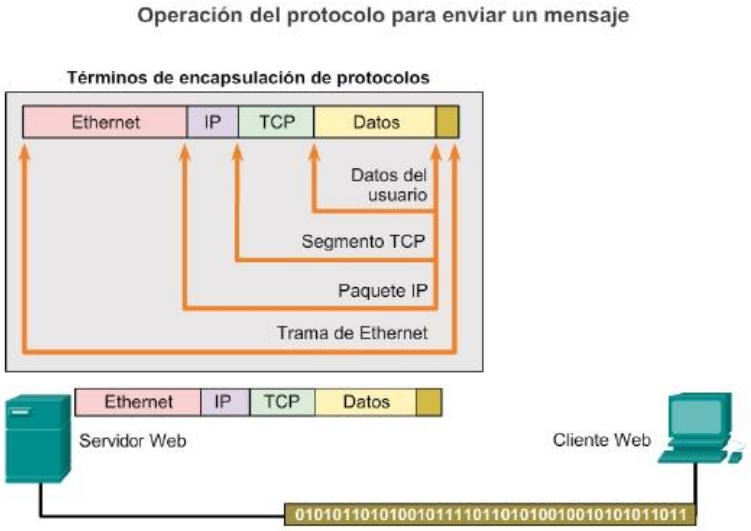
El protocolo de capa de aplicación, HTTP, comienza el proceso entregando los datos de la página Web con formato HTML a la capa de transporte.

Allí, los datos de aplicación se dividen en segmentos de TCP. A cada segmento de TCP se le otorga una etiqueta, denominada encabezado, que contiene información sobre qué procesos que se ejecutan en la computadora de destino deben recibir el mensaje. También contiene la información que permite que el proceso de destino rearme los datos en su formato original.

La capa de transporte encapsula los datos HTML de la página Web dentro del segmento y los envía a la capa de Internet, donde se implementa el protocolo IP. Aquí, el segmento de TCP se encapsula en su totalidad dentro de un paquete IP que agrega otro rótulo denominado encabezado IP. El encabezado IP contiene las direcciones IP de host de origen y de destino, como también la información necesaria para entregar el paquete a su proceso de destino correspondiente.

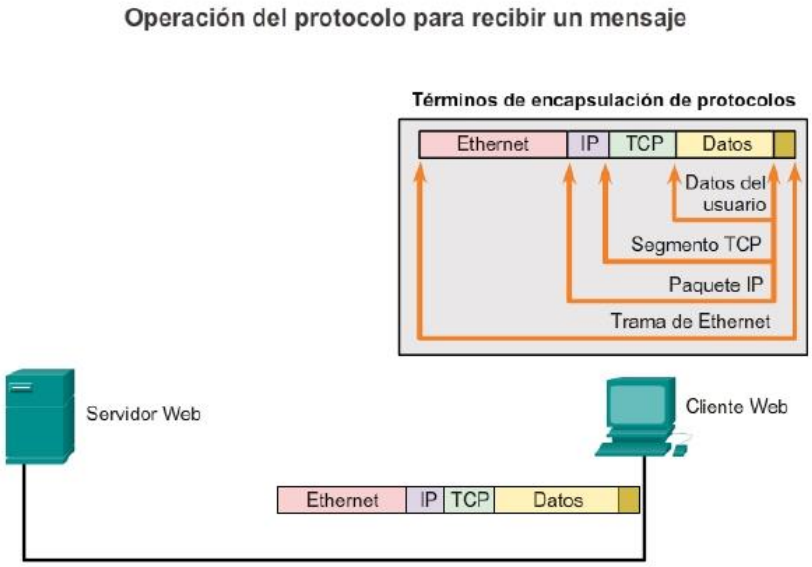
A continuación, el paquete IP se envía a la capa de acceso a la red, donde se encapsula dentro de un encabezado de trama y un tráiler. Cada encabezado de trama contiene una dirección física de origen y de destino. La dirección física identifica de forma exclusiva los dispositivos en la red local. El tráiler contiene información de verificación de errores.

Por último, los bits se codifican en el medio mediante la tarjeta de interfaz de red (NIC) del servidor. Haga clic en el botón Reproducir de la ilustración para ver el proceso de encapsulación.

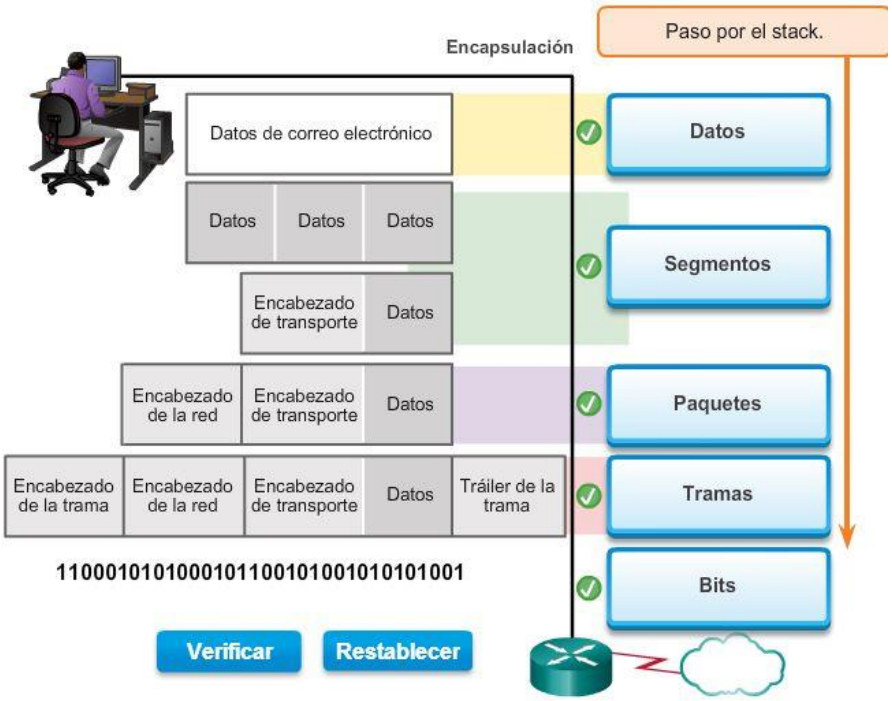


Capítulo 3: Protocolos y comunicaciones de red 3.3.1.4 Desencapsulación

Este proceso se invierte en el host receptor, y se conoce como “desencapsulación”. La desencapsulación es el proceso que utilizan los dispositivos receptores para eliminar uno o más de los encabezados de protocolo. Los datos se desencapsulan mientras suben por el stack hacia la aplicación del usuario final. Haga clic en el botón Reproducir de la ilustración para ver el proceso de desencapsulación.



Capítulo 3: Protocolos y comunicaciones de red 3.3.1.5 Actividad: Identificación de la capa de PDU



Capítulo 3: Protocolos y comunicaciones de red 3.3.2.1 Direcciones de red y direcciones de enlace de datos

El modelo OSI describe los procesos de codificación, asignación de formato, segmentación y encapsulación de datos para la transmisión a través de la red. La capa de red y la capa de enlace de datos son responsables de enviar los datos desde el dispositivo de origen o emisor hasta el dispositivo de destino o receptor. Los protocolos de las dos capas contienen las direcciones de origen y de destino, pero sus direcciones tienen objetivos distintos.

Dirección de red

La dirección lógica de la capa de red, o capa 3, contiene la información necesaria para enviar el paquete IP desde el dispositivo de origen hasta el dispositivo de destino. Una dirección IP de capa 3 tiene dos partes: el prefijo de red y la parte de host.

Los routers utilizan el prefijo de red para reenviar el paquete a la red adecuada. El último router de la ruta utiliza la parte de host para enviar el paquete al dispositivo de destino.

Los paquetes IP contienen dos direcciones IP:

- Dirección IP de origen: la dirección IP del dispositivo emisor.
- Dirección IP de destino: la dirección IP del dispositivo receptor. Los routers utilizan la dirección IP de destino para reenviar un paquete a su destino.

Dirección de enlace de datos

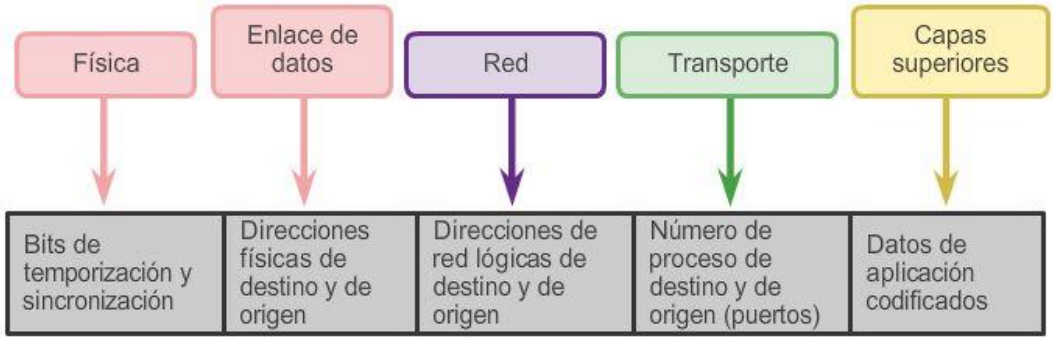
La dirección física de la capa de enlace de datos, o capa 2, tiene una función distinta. Su propósito es enviar la trama de enlace de datos desde una interfaz de red hasta otra interfaz de red en la misma red. Antes de que un paquete IP pueda enviarse a través de una red conectada por cable o inalámbrica, se debe encapsular en una trama de enlace de datos de modo que pueda transmitirse a través del medio físico, la red real.

Las LAN Ethernet y las LAN inalámbricas constituyen dos ejemplos de redes que tienen distintos medios físicos, cada uno con su propio tipo de protocolo de enlace de datos.

El paquete IP se encapsula en una trama de enlace de datos para enviarse a la red de destino. Se agregan las direcciones de enlace de datos de origen y de destino, como se muestra en la ilustración:

- Dirección de enlace de datos de origen: la dirección física del dispositivo que envía el paquete. Inicialmente, es la NIC que es el origen del paquete IP.

- Dirección de enlace de datos de destino: la dirección física de la interfaz de red del router del siguiente salto o de la interfaz de red del dispositivo de destino.



Capítulo 3: Protocolos y comunicaciones de red 3.3.2.2 Comunicación con un dispositivo en la misma red

Para comprender la forma en que la comunicación se lleva a cabo correctamente en la red, es importante entender las funciones de las direcciones de la capa de red y de las direcciones del enlace de datos cuando un dispositivo se comunica con otro dispositivo en la misma red. En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor de archivos, servidor FTP, en la misma red IP.

Direcciones de red

Las direcciones de la capa de red, o direcciones IP, indican la dirección de red y de host del origen y del destino. La porción de red de la dirección será la misma; solamente cambiará la porción de host o de dispositivo de la dirección.

- Dirección IP de origen: la dirección IP del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.

- Dirección IP de destino: la dirección IP del dispositivo receptor, el servidor FTP: 192.168.1.9.

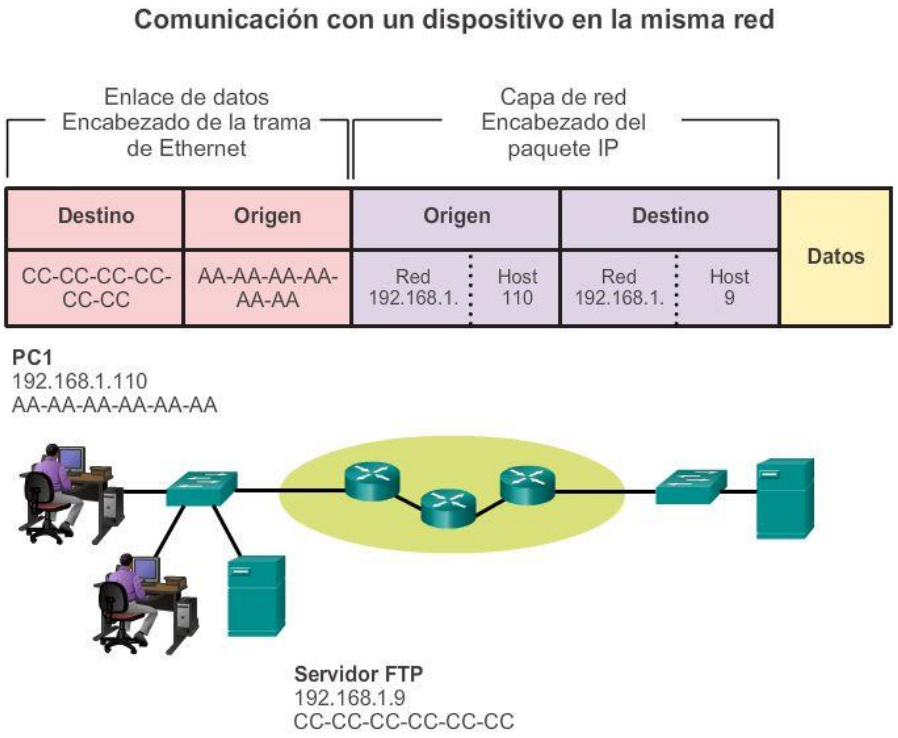
Direcciones de enlaces de datos

Cuando el emisor y el receptor del paquete IP están en la misma red, la trama de enlace de datos se envía directamente al dispositivo receptor. En una red Ethernet, las direcciones de enlace de datos se conocen como direcciones MAC de Ethernet. Las direcciones MAC son direcciones de 48 bits que están integradas físicamente en la NIC Ethernet. Las direcciones MAC también se conocen como direcciones físicas (BIA).

- Dirección MAC de origen: la dirección de enlace de datos, o la dirección MAC de Ethernet, del dispositivo que envía el paquete IP, es decir, PC1. La dirección MAC de la NIC Ethernet de PC1 es AA-AA-AA-AA-AA-AA.

- Dirección MAC de destino: cuando el dispositivo receptor está en la misma red que el dispositivo emisor, la dirección MAC de destino es la dirección de enlace de datos del dispositivo receptor. En este ejemplo, la dirección MAC de destino es la dirección MAC del servidor FTP: CC-CC-CC-CC-CC-CC.

Las direcciones de origen y de destino se agregan a la trama de Ethernet. La trama con el paquete IP encapsulado ahora se puede transmitir desde PC1 directamente hasta el servidor FTP.



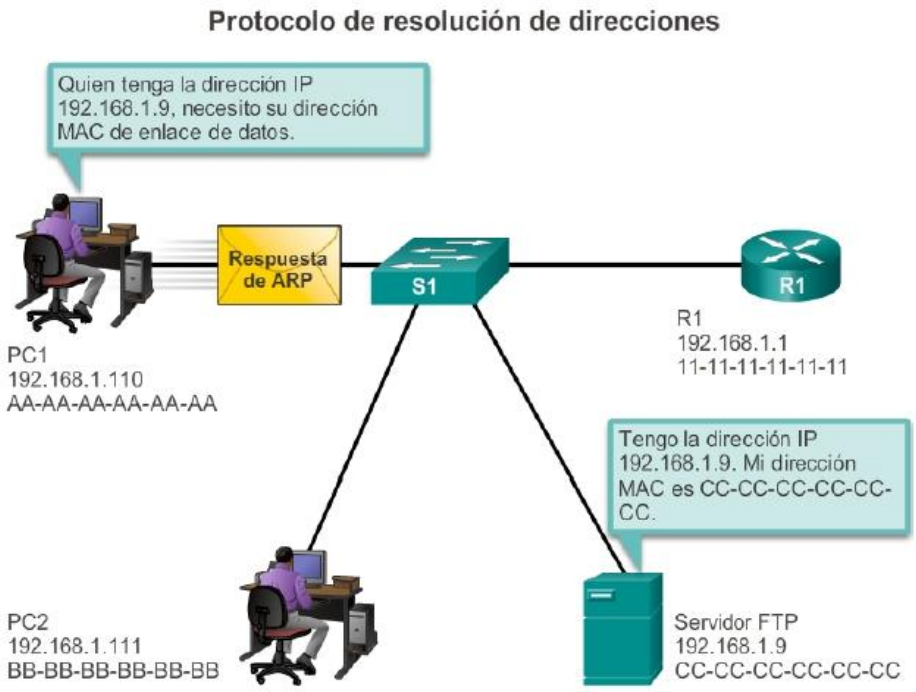
Capítulo 3: Protocolos y comunicaciones de red 3.3.2.3 Direcciones MAC e IP

Ahora debe estar claro que para enviar datos a otro host en la misma LAN, el host de origen debe conocer tanto la dirección física como la dirección lógica del host de destino. Una vez que se conocen estas direcciones, puede crear una trama y enviarla a través de los medios de red. El host de origen puede obtener la dirección IP de destino de diversas maneras. Por ejemplo, puede descubrir la dirección IP mediante el uso del sistema de nombres de dominios (DNS), o puede conocer la dirección IP de destino porque la dirección se introduce en la aplicación en forma manual, como cuando un usuario especifica la dirección IP de un servidor FTP de destino. Sin embargo, ¿cómo determina un host la dirección MAC de Ethernet de otro dispositivo?

La mayoría de las aplicaciones de red dependen de la dirección IP lógica del destino para identificar la ubicación de los hosts entre los que se produce la comunicación. Se requiere la dirección MAC de enlace de datos para enviar el paquete IP encapsulado dentro de la trama de Ethernet a través de la red hasta el destino.

El host emisor utiliza un protocolo denominado “protocolo de resolución de direcciones” (ARP) para descubrir la dirección MAC de cualquiera de los hosts de la misma red local. El host emisor envía un mensaje de solicitud de ARP a toda la LAN. La solicitud de ARP es un mensaje de broadcast. La solicitud de ARP

contiene la dirección IP del dispositivo de destino. Cada dispositivo en la LAN examina la solicitud de ARP para ver si contiene su propia dirección IP. Solamente el dispositivo con la dirección IP contenida en la solicitud de ARP responde con una respuesta de ARP. La respuesta de ARP incluye la dirección MAC asociada con la dirección IP en la solicitud de ARP.



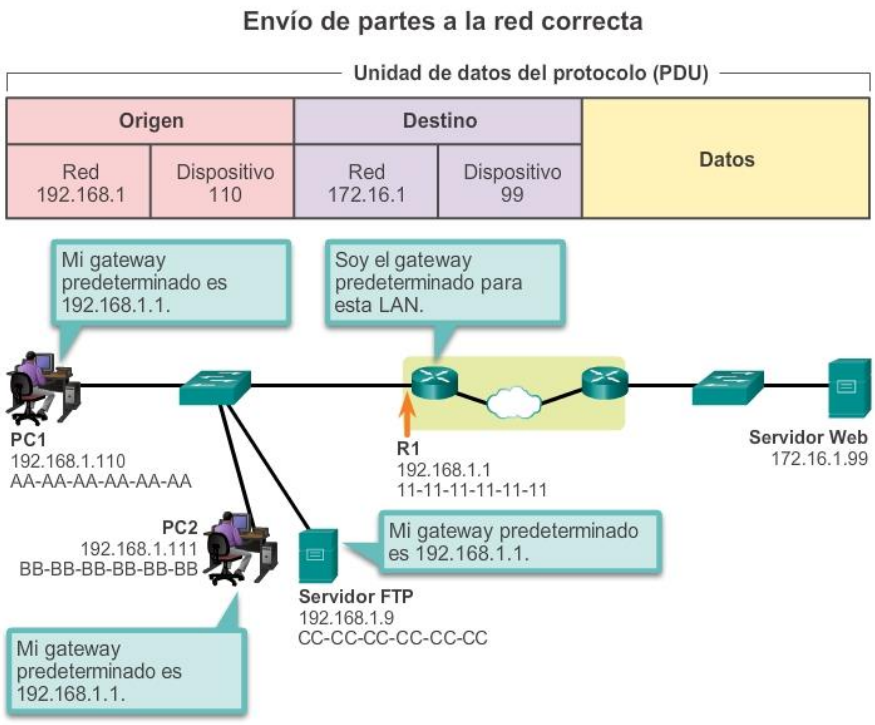
Capítulo 3: Protocolos y comunicaciones de red 3.3.3.1 Gateway predeterminado

El método que utilizan los hosts para enviar mensajes a un destino en una red remota difiere de la manera en la que envían mensajes a un destino en la misma red local. Cuando un host necesita enviar un mensaje a otro host ubicado en la misma red, reenvía el mensaje de manera directa. El host utiliza el ARP para determinar la dirección MAC del host de destino. Incluye la dirección IP de destino dentro del encabezado del paquete y encapsula el paquete en una trama que contiene la dirección MAC del destino y lo reenvía.

Cuando un host necesita enviar un mensaje a una red remota, debe utilizar el router, también conocido como “gateway predeterminado”. El gateway predeterminado es la dirección IP de una interfaz de un router en la misma red que el host emisor.

Es importante que en cada host de la red local se configure la dirección de gateway predeterminado. Si no se define ninguna dirección de gateway predeterminado en la configuración de TCP/IP del host, o si se especifica un gateway predeterminado incorrecto, no se podrán entregar los mensajes dirigidos a hosts de redes remotas.

En la ilustración, los hosts en la LAN utilizan R1 como el gateway predeterminado con la dirección 192.168.1.1 establecida en la configuración de TCP/IP. Si el destino de una PDU se encuentra en una red IP distinta, los hosts envían las PDU al gateway predeterminado en el router para su posterior transmisión.



Capítulo 3: Protocolos y comunicaciones de red 3.3.3.2 Comunicación con un dispositivo en una red remota

Sin embargo, ¿cuáles son las funciones de la dirección de la capa de red y de la dirección de la capa de enlace de datos cuando un dispositivo se comunica con un dispositivo en una red remota? En este ejemplo, tenemos un equipo cliente, PC1, que se comunica con un servidor, en este caso un servidor Web, en una red IP diferente.

Direcciones de red

Las direcciones IP indican las direcciones de red y de los dispositivos de origen y de destino. Cuando el emisor del paquete se encuentra en una red distinta de la del receptor, las direcciones IP de origen y de destino representan los hosts en redes diferentes. Esto lo indica la porción de red de la dirección IP del host de destino.

- Dirección IP de origen: la dirección IP del dispositivo emisor, es decir, el equipo cliente PC1: 192.168.1.110.
- Dirección IP de destino: la dirección IP del dispositivo receptor, es decir, el servidor Web: 172.16.1.99.

Direcciones de enlaces de datos

Cuando el emisor y el receptor del paquete IP se encuentran en redes diferentes, la trama de enlace de datos de Ethernet no se puede enviar directamente al host de destino, debido a que en la red del emisor no se puede tener acceso directamente al host. La trama de Ethernet se debe enviar a otro dispositivo conocido como “router” o “gateway predeterminado”. En nuestro ejemplo, el gateway predeterminado es R1. R1 tiene una interfaz y una dirección IP que se encuentra en la misma red que PC1. Esto permite que PC1 alcance el router directamente.

- Dirección MAC de origen: la dirección MAC de Ethernet del dispositivo emisor, PC1. La dirección MAC de la interfaz Ethernet de PC1 es AA-AA-AA-AA-AA-AA.

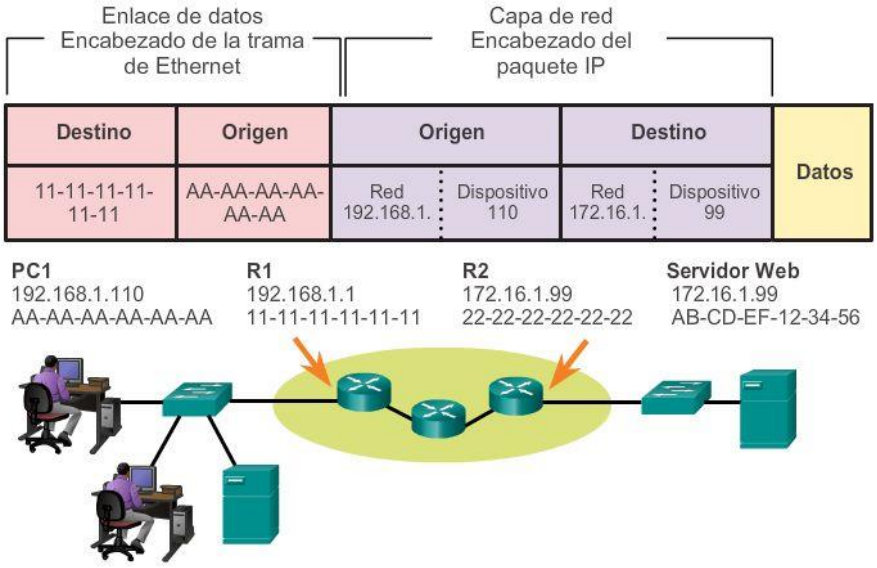
Dirección MAC de destino: cuando el dispositivo receptor está en una red distinta de la del dispositivo emisor, la dirección MAC de destino es la dirección MAC de Ethernet del gateway predeterminado o el router. En este ejemplo, la dirección MAC de destino es la dirección MAC de la interfaz Ethernet de R1 que está conectada a la red de PC1, que es 11-11-11-11-11-11.

La trama de Ethernet con el paquete IP encapsulado ahora se puede transmitir a R1. R1 reenvía el paquete al destino, el servidor Web. Esto puede significar que R1 reenvía el paquete a otro router o directamente al servidor Web si el destino se encuentra en una red conectada a R1.

¿Cómo hace el dispositivo emisor para determinar la dirección MAC del router?

Cada dispositivo conoce la dirección IP del router a través de la dirección de gateway predeterminado definida en la configuración de TCP/IP. La dirección de gateway predeterminado es la dirección de la interfaz del router conectado a la misma red local que el dispositivo de origen. Todos los dispositivos de la red local utilizan la dirección de gateway predeterminado para enviar mensajes al router. Una vez que el host conoce la dirección IP del gateway predeterminado, puede utilizar ARP para determinar la dirección MAC de ese gateway predeterminado. La dirección MAC del gateway predeterminado entonces se coloca en la trama.

Comunicación con un dispositivo en una red remota



Capítulo 3: Protocolos y comunicaciones de red 3.4.1.2 Resumen

Las redes de datos son sistemas de dispositivos finales, dispositivos intermediarios y medios que conectan los dispositivos. Para que se produzca la comunicación, estos dispositivos deben saber cómo comunicarse.

Estos dispositivos deben cumplir con reglas y protocolos de comunicación. TCP/IP es un ejemplo de una suite de protocolos. La mayoría de los protocolos son creados por organismos de estandarización, como el IETF o el IEEE. El Instituto de Ingenieros en Electricidad y Electrónica es un organismo profesional para las personas que trabajan en los campos de la electrónica y de la ingeniería eléctrica. La ISO, la International Organization for Standardization, es el mayor desarrollador del mundo de estándares internacionales para una amplia variedad de productos y servicios.

Los modelos de redes que más se utilizan son OSI y TCP/IP. Asociar los protocolos que establecen las reglas de las comunicaciones de datos con las distintas capas de estos modelos es de gran utilidad para determinar qué dispositivos y servicios se aplican en puntos específicos mientras los datos pasan a través de las LAN y WAN.

Los datos que pasan por el stack del modelo OSI se segmentan en trozos y se encapsulan con direcciones y otras etiquetas. El proceso se revierte a medida que esos trozos se desencapsulan y pasan por el stack de protocolos de destino. El modelo OSI describe los procesos de codificación, formateo, segmentación y encapsulación de datos para transmitir por la red.

La suite de protocolos TCP/IP es un protocolo de estándar abierto que recibió el aval de la industria de redes y fue ratificado, o aprobado, por un organismo de estandarización. La suite de protocolos de Internet es una suite de protocolos necesaria para transmitir y recibir información mediante Internet.

Las unidades de datos del protocolo (PDU) se denominan según los protocolos de la suite TCP/IP: datos, segmento, paquete, trama y bits.

La aplicación de los modelos permite a diversas personas, compañías y asociaciones comerciales analizar las redes actuales y planificar las redes del futuro.

Capítulo 4: Acceso a la red 4.0.1.1 Introducción

Al finalizar este capítulo, podrá hacer lo siguiente:

- Identificar las opciones de conectividad de los dispositivos.
- Describir el propósito y las funciones de la capa física en la red.
- Describir los principios fundamentales de los estándares de la capa física.
- Identificar las características básicas del cableado de cobre.
- Armar un cable UTP para redes Ethernet.
- Describir el cableado de fibra óptica y sus ventajas principales sobre otros medios.
- Describir los medios inalámbricos.
- Seleccionar los medios adecuados para un requisito determinado y conectar los dispositivos.
- Describir el objetivo y la función de la capa de enlace de datos en la preparación de comunicaciones para su transmisión por medios específicos.
- Describir la estructura de trama de la Capa 2 e identificar campos genéricos.
- Identificar varias fuentes de los protocolos y estándares utilizados por la capa de enlace de datos.
- Comparar las funciones de las topologías lógicas y las topologías físicas.
- Describir las características básicas de los métodos de control de acceso al medio en las topologías de WAN.
- Describir las características básicas de los métodos de control de acceso al medio en las topologías de LAN.
- Describir las características y las funciones de la trama de enlace de datos.

Para sostener nuestras comunicaciones, el modelo OSI divide las funciones de una red de datos en capas. Cada capa trabaja con las capas superior e inferior para transmitir datos. Dos capas dentro del modelo OSI están tan relacionadas que, según el modelo TCP/IP, son básicamente una sola. Esas dos capas son la capa de enlace de datos y la capa física.

En el dispositivo emisor, la función de la capa de enlace de datos es preparar los datos para la transmisión y controlar la forma en que estos acceden a los medios físicos. Sin embargo, la capa física controla cómo se transmiten los datos a los medios físicos mediante la codificación en señales de los dígitos binarios que representan los datos.

En el extremo receptor, la capa física recibe señales a través de los medios de conexión. Después de decodificar la señal y convertirla nuevamente en datos, la capa física transmite los datos a la capa de enlace de datos para su aceptación y procesamiento.

En este capítulo, se comienza con las funciones generales de la capa física y los estándares y protocolos que administran la transmisión de datos a través de los medios locales. También se presentan las funciones de la capa de enlace de datos y los protocolos asociados a esta.

Capítulo 4: Acceso a la red 4.0.1.2 Actividad: Administración del medio

Administración del medio

Usted y un colega asisten a una conferencia de redes. Durante el evento, se llevan a cabo muchas charlas y presentaciones. Debido a que estas se superponen, cada uno puede elegir solo un conjunto limitado de sesiones a las cuales asistir.

Por lo tanto, deciden separarse. Cada uno asistirá a un conjunto distinto de presentaciones y, una vez que el evento finalice, compartirán las diapositivas y los conocimientos obtenidos por cada uno.

Intente responder las siguientes preguntas:

- ¿Cómo organizaría personalmente una conferencia donde se llevarán a cabo a varias sesiones al mismo tiempo? ¿Los ubicaría a todos en una misma sala de conferencias o utilizaría varias salas? ¿Por qué?

- Suponga que la sala de conferencias cuenta con equipo audiovisual adecuado para mostrar videos de gran tamaño y amplificar la voz. Si una persona deseara asistir a una determinada sesión, ¿la disposición de los asientos hace alguna diferencia, o es suficiente visitar la sala de conferencias apropiada?

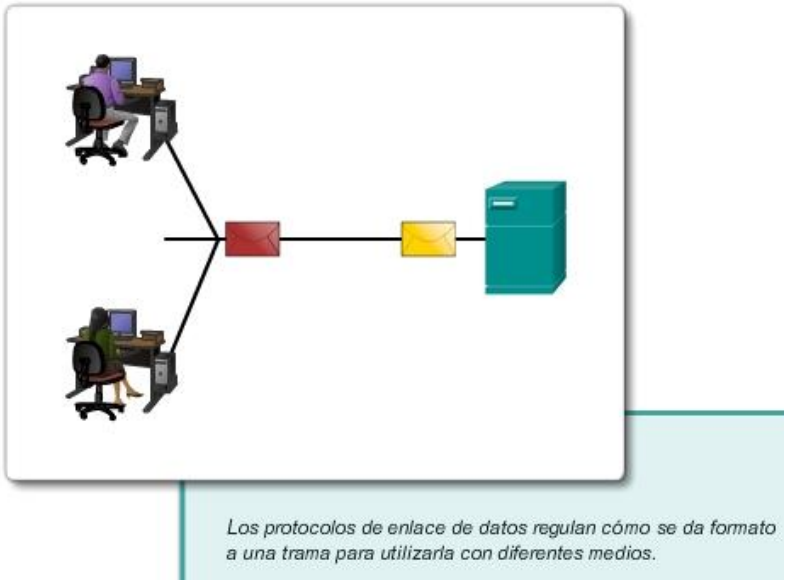
- ¿Se consideraría beneficioso o perjudicial que el discurso pronunciado en una sala de conferencias se filtrara de alguna manera a otra sala?

- Si surgen preguntas durante una presentación, ¿los asistentes deberían simplemente hacer sus preguntas en voz alta o debería existir algún proceso para ordenar las preguntas, como ponerlas por escrito y entregarlas a un coordinador? ¿Qué sucedería sin este proceso?

- Si un tema interesante genera un debate más amplio en el cual muchos asistentes tienen preguntas o comentarios, ¿es posible que se termine el tiempo de la sesión sin que se haya expuesto todo el contenido previsto? ¿Por qué?

- Imagine que la sesión se lleva a cabo en un formato de panel; es decir, un debate más libre entre los asistentes y los panelistas y, quizá, entre los asistentes entre sí. Si una persona desea dirigirse a otra persona dentro de la misma sala, ¿puede hacerlo directamente? ¿Qué se debería hacer si un panelista quisiera invitar a otra persona que no se encuentra actualmente en la sala a que se una al debate?

- ¿Qué se logra mediante el aislamiento de varias sesiones en salas de conferencias independientes si, después del evento, las personas pueden reunirse y compartir información?



Los protocolos de enlace de datos regulan cómo se da formato a una trama para utilizarla con diferentes medios.

Capítulo 4: Acceso a la red 4.1.1.1 Conexión a la red

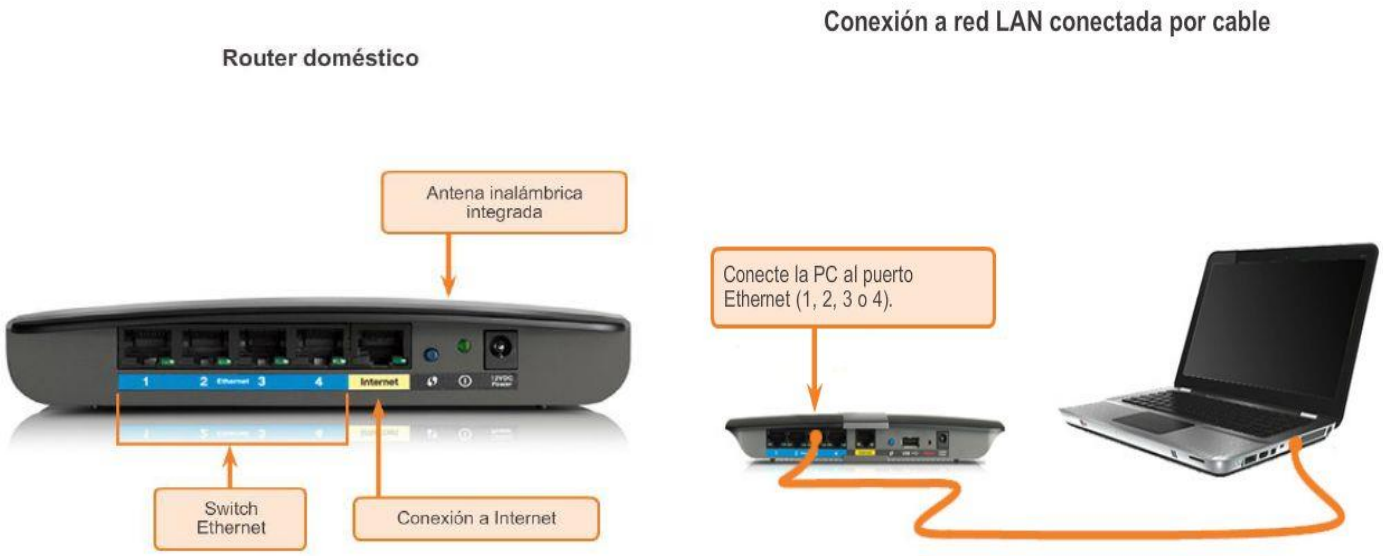
Ya sea una conexión a una impresora local en el hogar o a un sitio Web en otro país, para que se pueda producir cualquier comunicación de red se debe establecer antes una conexión a una red local. Una conexión física puede ser una conexión por cable o una conexión inalámbrica mediante ondas de radio.

El tipo de conexión física utilizada depende por completo de la configuración de la red. Por ejemplo, en muchas oficinas corporativas, los empleados tienen computadoras de escritorio o portátiles que se conectan físicamente, mediante cables, a un switch compartido. Este tipo de configuración es una red conectada por cable en la que los datos se transmiten a través de un cable físico.

Además de las conexiones por cable, algunas empresas también pueden ofrecer conexiones inalámbricas para computadoras portátiles, tablet PC y smartphones. En el caso de los dispositivos inalámbricos, los datos se transmiten mediante ondas de radio. A medida que las personas y las empresas descubren las ventajas de ofrecer servicios inalámbricos, el uso de la conectividad inalámbrica se vuelve cada vez más frecuente.

Para ofrecer capacidad de conexión inalámbrica, las redes deben incorporar un punto de acceso inalámbrico (WAP) al cual se puedan conectar los dispositivos.

Los dispositivos de switch y los puntos de acceso inalámbrico suelen ser dos dispositivos independientes y dedicados dentro de una implementación de red. Sin embargo, también hay dispositivos que ofrecen tanto conectividad por cable como inalámbrica. En muchos hogares, por ejemplo, las personas implementan routers de servicio integrado (ISR) domésticos, como se muestra en la figura 1. Los ISR proporcionan un componente de conmutación con varios puertos, lo que permite conectar varios dispositivos a la red de área local (LAN) con cables, como se muestra en la figura 2. Además, muchos ISR incluyen un WAP, que permite que también se conecten dispositivos inalámbricos.



Capítulo 4: Acceso a la red 4.1.1.2 Tarjetas de interfaz de red

Las tarjetas de interfaz de red (NIC) conectan un dispositivo a la red. Las NIC Ethernet se utilizan para las conexiones por cable, mientras que las NIC de red de área local inalámbrica (WLAN) se utilizan para las conexiones inalámbricas. Los dispositivos para usuarios finales pueden incluir un tipo de NIC o ambos. Una impresora de red, por ejemplo, puede contar solo con una NIC Ethernet y, por lo tanto, se debe conectar a la red mediante un cable Ethernet. Otros dispositivos, como las tablet PC y los smartphones, pueden contener solo una NIC WLAN y deben utilizar una conexión inalámbrica.

En términos de rendimiento, no todas las conexiones físicas son iguales a la hora de conectarse a una red.

Por ejemplo, un dispositivo inalámbrico experimentará una merma en el rendimiento según la distancia a la que se encuentre del punto de acceso inalámbrico. Cuanto más alejado del punto de acceso esté el dispositivo, más débil será la señal inalámbrica que reciba. Esto puede significar menor ancho de banda o la ausencia absoluta de una conexión inalámbrica.

En la ilustración, se muestra que se puede utilizar un extensor de alcance inalámbrico para regenerar la señal inalámbrica en partes de la casa que estén demasiado alejadas del punto de acceso inalámbrico. Por otra parte, las conexiones por cable no sufren una merma del rendimiento; sin embargo, limitan extremadamente el movimiento y, en general, requieren una posición estática.

Todos los dispositivos inalámbricos deben compartir el acceso a las ondas aéreas que se conectan al punto de acceso inalámbrico. Esto significa que el rendimiento de la red puede ser más lento a medida que más dispositivos inalámbricos acceden a la red simultáneamente.

Los dispositivos conectados por cable no necesitan compartir el acceso a la red con otros dispositivos. Cada dispositivo conectado por cable tiene un canal de comunicación independiente a través de su propio cable Ethernet. Esto es importante cuando se tienen en cuenta algunas aplicaciones, como juegos en línea, streaming video y conferencias de video, que requieren más ancho de banda dedicado que otras aplicaciones.

Al analizar los siguientes temas, aprenderá más sobre las conexiones de capa física que se producen y la forma en que esas conexiones afectan el transporte de datos.

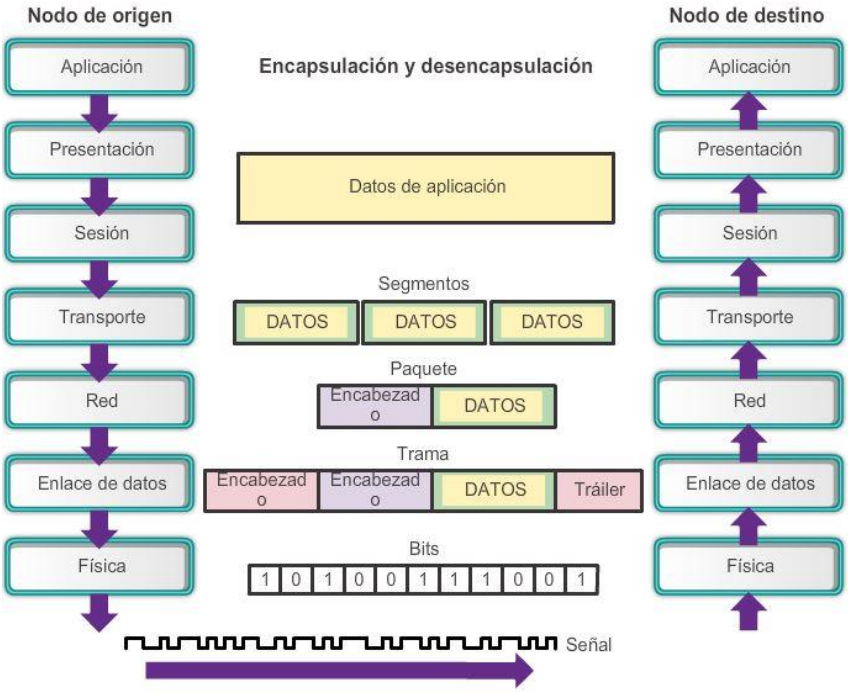
Conexión a una LAN inalámbrica con un extensor de alcance

Capítulo 4: Acceso a la red 4.1.2.1 Capa física

La capa física de OSI proporciona los medios de transporte de los bits que conforman una trama de la capa de enlace de datos a través de los medios de red. Esta capa acepta una trama completa de la capa de enlace de datos y la codifica como una serie de señales que se transmiten a los medios locales. Un dispositivo final o un dispositivo intermediario recibe los bits codificados que componen una trama.

El proceso por el que pasan los datos desde un nodo de origen hasta un nodo de destino es el siguiente:

- La capa de transporte segmenta los datos de usuario, la capa de red los coloca en paquetes, y la capa de enlace de datos los encapsula en forma de trama.
- La capa física codifica las tramas y crea las señales eléctricas, ópticas o de ondas de radio que representan los bits en cada trama.
- Luego, estas señales se envían por los medios una a la vez.
- La capa física del nodo de destino recupera estas señales individuales de los medios, las restaura a sus representaciones en bits y pasa los bits a la capa de enlace de datos en forma de trama completa.



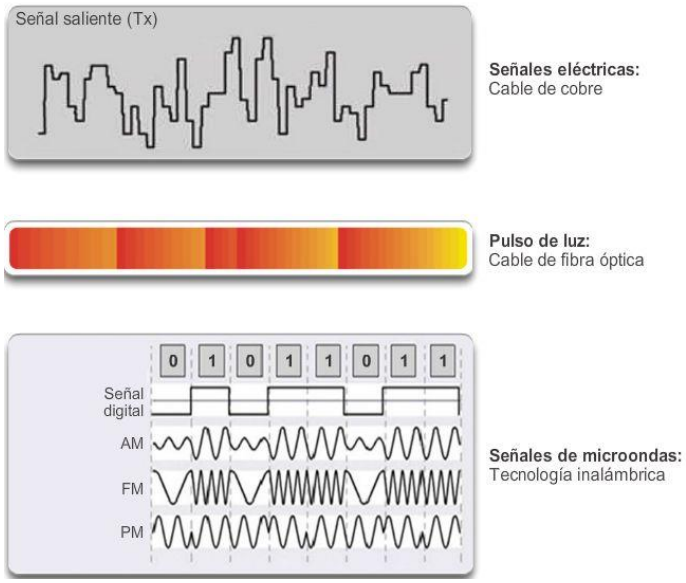
Capítulo 4: Acceso a la red 4.1.2.2 Medios de la capa física

Existen tres formatos básicos de medios de red. La capa física produce la representación y las agrupaciones de bits para cada tipo de medio de la siguiente manera:

- Cable de cobre: las señales son patrones de pulsos eléctricos.
- Cable de fibra óptica: las señales son patrones de luz.
- Conexión inalámbrica: las señales son patrones de transmisiones de microondas.

En la ilustración, se muestran ejemplos de señalización para medios inalámbricos, de cobre y de fibra óptica.

Para habilitar la interoperabilidad de la capa física, los organismos de estandarización rigen todos los aspectos de estas funciones.



Capítulo 4: Acceso a la red 4.1.2.3 Estándares de capa física

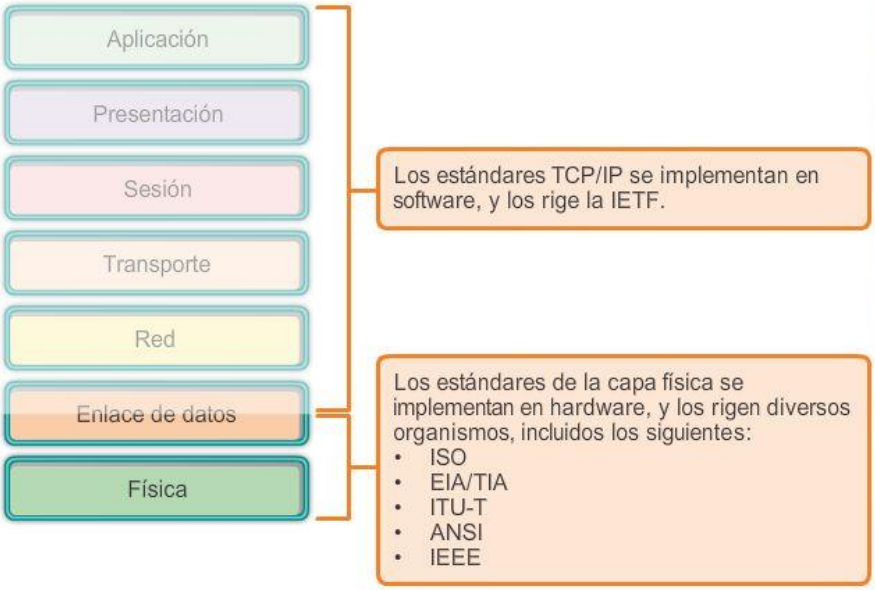
Los protocolos y las operaciones de las capas OSI superiores se llevan a cabo en softwares diseñado por ingenieros en software e informáticos. Por ejemplo, Internet Engineering Task Force (IETF) define los servicios y protocolos de la suite TCP/IP en las RFC, como se muestra en la figura 1.

La capa física consta de circuitos electrónicos, medios y conectores desarrollados por ingenieros. Por lo tanto, es necesario que las principales organizaciones especializadas en ingeniería eléctrica y en comunicaciones definan los estándares que rigen este hardware.

Existen muchos organismos internacionales y nacionales, organismos de regulación gubernamentales y compañías privadas que intervienen en el establecimiento y el mantenimiento de los estándares de la capa física. Por ejemplo, los siguientes organismos definen y rigen los estándares de hardware, medios, codificación y señalización de la capa física:

- Organización Internacional para la Estandarización (ISO)
- Telecommunications Industry Association/Electronic Industries Association (TIA/EIA)
- Unión Internacional de Telecomunicaciones (UIT)
- American National Standards Institute (ANSI)
- Instituto de Ingenieros en Electricidad y Electrónica (IEEE)
- Autoridades nacionales reguladoras de las telecomunicaciones, incluida la Federal Communication Commission (FCC) de los EE. UU. y el European Telecommunications Standards Institute (ETSI)

Además de estos, a menudo existen grupos regionales de estandarización de cableado, como la Canadian Standards Association (CSA), el European Committee for Electrotechnical Standardization (CENELEC) y la Japanese Standards Association (JSA/JIS), los cuales desarrollan las especificaciones locales.



Organismo de estandarización	Estándares de red
ISO	• ISO 8877: adoptó oficialmente los conectores RJ (p. ej., RJ-11, RJ-45). • ISO 11801: Estándar de cableado de red similar a EIA/TIA 568.
EIA/TIA	• TIA-568-C: estándares de cableado de telecomunicaciones, utilizados en casi todas las redes de datos, voz y video. • TIA-569-B: estándares de construcción comercial para rutas y espacios de telecomunicaciones. • TIA-598-C: código de colores para fibra óptica. • TIA-942: estándar de infraestructura de telecomunicaciones para centros de datos.
ANSI	568-C: Diagrama de pines RJ-45. Desarrollado conjuntamente con EIA/TIA.
ITU-T	G.992: ADSL
IEEE	• 802.3: Ethernet • 802.11: LAN inalámbrica (WLAN) y malla (certificación Wi-Fi) • 802.15: Bluetooth

Capítulo 4: Acceso a la red 4.1.3.1 Principios fundamentales de la capa física

Los estándares de la capa física abarcan tres áreas funcionales:

Componentes físicos

Los componentes físicos son los dispositivos electrónicos de hardware, los medios y otros conectores que transmiten y transportan las señales para representar los bits. Todos los componentes de hardware, como los adaptadores de red (NIC), las interfaces y los conectores, así como los materiales y el diseño de los cables, se especifican en los estándares asociados con la capa física. Los diversos puertos e interfaces de un router Cisco 1941 también son ejemplos de componentes físicos con conectores y diagramas de pines específicos derivados de los estándares.

Codificación

La codificación, o codificación de línea, es un método que se utiliza para convertir un stream de bits de datos en un “código” predefinido. Los códigos son grupos de bits utilizados para ofrecer un patrón predecible que pueda reconocer tanto el emisor como el receptor. En el caso de las redes, la codificación es un patrón de voltaje o corriente utilizado para representar los bits; los 0 y los 1.

Además de crear códigos para los datos, los métodos de codificación en la capa física también pueden proporcionar códigos de control, como la identificación del comienzo y el final de una trama.

Entre los métodos de codificación de redes de uso frecuente, se incluyen los siguientes:

- Codificación Manchester: los 0 se representan mediante una transición de voltaje de alto a bajo, y los 1 se representan como una transición de voltaje de bajo a alto. Este tipo de codificación se utiliza en las versiones más antiguas de Ethernet, RFID y la transmisión de datos en proximidad.

- Sin retorno a cero (NRZ): se trata de una forma frecuente de codificación de datos que tiene dos estados denominados “cero” y “uno”, sin posición neutral o de descanso. En los medios, los 0 pueden estar representados por un nivel de voltaje, y los 1, por un voltaje diferente.

Nota: las velocidades de datos más elevadas requieren una codificación más compleja, como 4B/5B; sin embargo, la explicación de estos métodos excede el ámbito de este curso.

Señalización

La capa física debe generar las señales inalámbricas, ópticas o eléctricas que representan los “1” y los “0” en los medios. El método de representación de bits se denomina método de señalización. Los estándares de la capa física deben definir qué tipo de señal representa un “1” y qué tipo de señal representa un “0”. Esto puede ser tan simple como un cambio en el nivel de una señal eléctrica o de un pulso óptico. Por ejemplo, un pulso largo puede representar un 1, mientras que un pulso corto representa un 0.

Esto es similar a la forma en que se utiliza el código morse para la comunicación. El código morse es otro método de señalización que utiliza la presencia o ausencia de una serie de tonos, luces o clics para enviar texto a través de cables telefónicos o entre barcos en el mar.

Las señales se pueden transmitir de dos maneras:

- Asíncrona: las señales de datos se transmiten sin una señal de reloj asociada. El espacio de tiempo entre los caracteres o los bloques de datos puede tener una duración arbitraria, lo que significa que dicho espacio no está estandarizado. Por lo tanto, las tramas requieren indicadores de comienzo y de detención.

- Síncrona: las señales de datos se envían junto con una señal de reloj que se produce en duraciones de tiempo espaciadas de manera uniforme denominadas “tiempo de bit”.

Existen muchas formas de transmitir señales. Un método habitual para enviar datos consiste en utilizar técnicas de modulación. La modulación es el proceso por el cual la característica de una onda (la señal) modifica a otra onda (la portadora). Las siguientes técnicas de modulación se utilizan ampliamente para transmitir datos en un medio:

- Modulación de frecuencia (FM): método de transmisión en el que la frecuencia de la portadora varía de acuerdo con la señal.

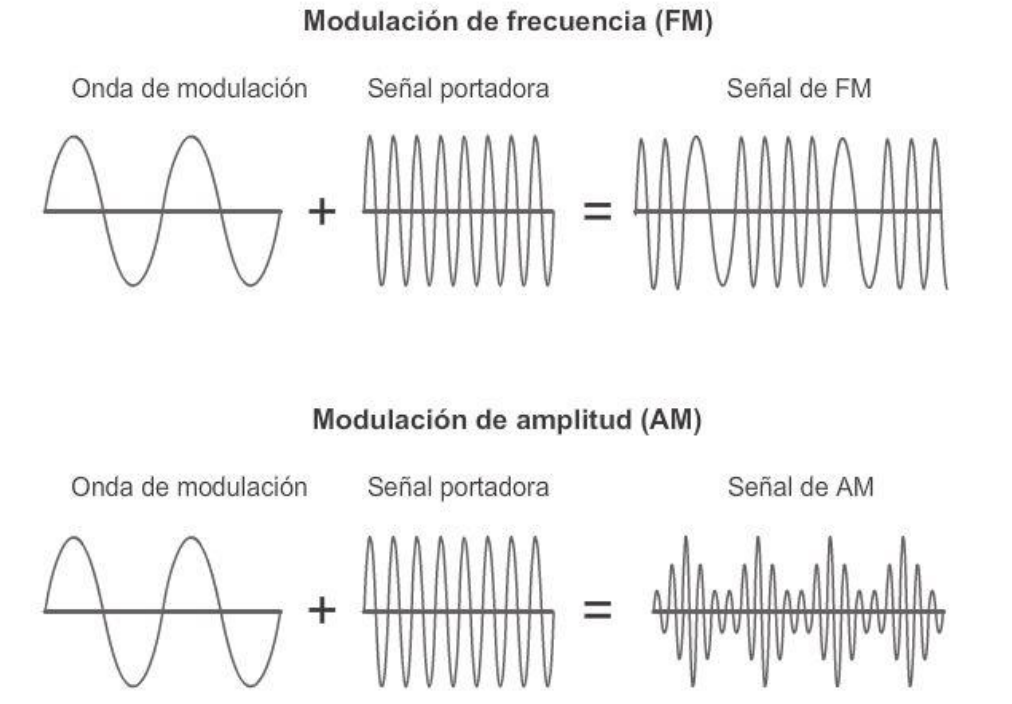
- Modulación de amplitud (AM): técnica de transmisión en la que la amplitud de la portadora varía de acuerdo con la señal.

- Modulación por códigos de pulsos (PCM): técnica en la que una señal analógica, como la voz, se convierte en una señal digital mediante el muestreo de la amplitud de la señal y la expresión de amplitudes diferentes como un número binario. La velocidad de muestreo debe ser, por lo menos, el doble de la frecuencia más alta en la señal.

La naturaleza de las señales reales que representan los bits en los medios dependerá del método de señalización que se utilice. Algunos métodos pueden utilizar un atributo de señal para representar un único 0 y utilizar otro atributo de señal para representar un único 1.

En la figura 2, se muestra cómo se utilizan las técnicas de AM y FM para enviar una señal.

Medios	Componentes físicos	Técnica de codificación de la trama	Método de señalización
Cable de cobre	• UTP • Coaxial • Conectores • NIC • Puertos • Interfaces	• Codificación Manchester • Técnicas sin retorno a cero (NRZ) • Los códigos 4B/5B se utilizan con la señalización de nivel 3 de la transición de múltiples niveles (MLT-3). • 8B/10B • PAM5	• Cambios en el campo electromagnético • Intensidad del campo electromagnético • Fase de la onda electromagnética



Capítulo 4: Acceso a la red 4.1.3.2 Ancho de banda

Los diferentes medios físicos admiten la transferencia de bits a distintas velocidades. Por lo general, la transferencia de datos se analiza en términos de ancho de banda y rendimiento.

El ancho de banda es la capacidad de un medio para transportar datos. El ancho de banda digital mide la cantidad de datos que pueden fluir desde un lugar hasta otro en un período determinado. El ancho de banda generalmente se mide en kilobits por segundo (kb/s) o megabits por segundo (Mb/s).

El ancho de banda práctico de una red se determina mediante una combinación de factores:

- Las propiedades de los medios físicos
- Las tecnologías seleccionadas para la señalización y la detección de señales de red

Las propiedades de los medios físicos, las tecnologías actuales y las leyes de la física desempeñan una función al momento de determinar el ancho de banda disponible.

En la tabla, se muestran las unidades de medida comúnmente utilizadas para el ancho de banda.

Unidad de ancho de banda	Abreviatura	Equivalencia
Bits por segundo	bps	1bps=unidad fundamental de ancho de banda
Kilobits por segundo	kbps	1kbps=1000bps = 10^3bps
Megabits per second, megabits por segundo	Mbps	1Mbps =1000000bps=10^6bps
Gigabits per second, gigabits por segundo	Gbps	1Gbps=1000000000bps=10^9bps
Terabits per second, terabits por segundo	Tbps	1Tbps=1000000000000bps=10^12bps

Capítulo 4: Acceso a la red 4.1.3.3 Rendimiento

El rendimiento es la medida de transferencia de bits a través de los medios durante un período de tiempo determinado.

Debido a diferentes factores, el rendimiento no suele coincidir con el ancho de banda especificado en las implementaciones de capa física. Muchos factores influyen en el rendimiento, incluidos los siguientes:

- La cantidad de tráfico
- El tipo de tráfico
- La latencia creada por la cantidad de dispositivos de red encontrados entre origen y destino

La latencia se refiere a la cantidad de tiempo, incluidas las demoras, que les toma a los datos transferirse desde un punto determinado hasta otro.

En una internetwork o una red con múltiples segmentos, el rendimiento no puede ser más rápido que el enlace más lento de la ruta de origen a destino. Incluso si todos los segmentos o gran parte de ellos tienen un ancho de banda elevado, sólo se necesita un segmento en la ruta con un rendimiento inferior para crear un cuello de botella en el rendimiento de toda la red.

Existen muchas pruebas de velocidad en línea que pueden revelar el rendimiento de una conexión a Internet. En la ilustración, se proporcionan resultados de ejemplo de una prueba de velocidad.

Nota: existe una tercera medición relacionada con la transferencia de datos utilizables, que se conoce como “capacidad de transferencia útil”. La capacidad de transferencia útil es la medida de datos utilizables transferidos durante un período determinado. Esta capacidad representa el rendimiento sin la sobrecarga de tráfico para establecer sesiones, acuses de recibo y encapsulaciones.

Capítulo 4: Acceso a la red 4.1.3.4 Tipos de medios físicos

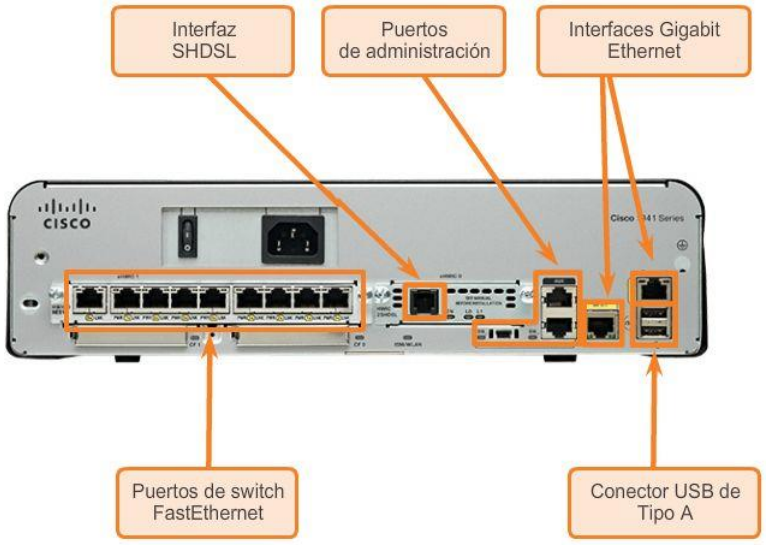
La capa física produce la representación y las agrupaciones de bits en forma de voltajes, frecuencias de radio o pulsos de luz. Muchas organizaciones que establecen estándares han contribuido con la definición de las propiedades mecánicas, eléctricas y físicas de los medios disponibles para diferentes comunicaciones de datos.

Estas especificaciones garantizan que los cables y los conectores funcionen según lo previsto mediante diferentes implementaciones de capa de enlace de datos.

Por ejemplo, los estándares para los medios de cobre se definen según lo siguiente:

- Tipo de cableado de cobre utilizado
- Ancho de banda de la comunicación
- Tipo de conectores utilizados
- Diagrama de pines y códigos de colores de las conexiones a los medios
- Distancia máxima de los medios

En la ilustración, se muestran distintos tipos de interfaces y puertos disponibles en un router 1941.



Capítulo 4: Acceso a la red 4.2.1.1 Características de los medios de cobre

Las redes utilizan medios de cobre porque son económicos y fáciles de instalar, y tienen baja resistencia a la corriente eléctrica. Sin embargo, los medios de cobre se ven limitados por la distancia y la interferencia de señales.

Los datos se transmiten en cables de cobre como impulsos eléctricos. Un detector en la interfaz de red de un dispositivo de destino debe recibir una señal que pueda decodificarse exitosamente para que coincida con la

señal enviada. No obstante, cuanto mayor sea la distancia que recorre la señal, más se deteriora. Este fenómeno que se denomina “atenuación de la señal”. Por este motivo, todos los medios de cobre deben seguir limitaciones de distancia estrictas según lo especifican los estándares que los rigen.

Los valores de temporización y voltaje de los pulsos eléctricos también son vulnerables a las interferencias de dos fuentes:

- Interferencia electromagnética (EMI) o interferencia de radiofrecuencia (RFI): las señales de EMI y RFI pueden distorsionar y dañar las señales de datos que transportan los medios de cobre. Las posibles fuentes de EMI y RFI incluyen las ondas de radio y dispositivos electromagnéticos como las luces fluorescentes o los motores eléctricos, como se muestra en la ilustración.

- Crosstalk: se trata de una perturbación causada por los campos eléctricos o magnéticos de una señal de un hilo a la señal de un hilo adyacente. En los circuitos telefónicos, el crosstalk puede provocar que se escuche parte de otra conversación de voz de un circuito adyacente. Específicamente, cuando la corriente eléctrica fluye por un hilo, crea un pequeño campo magnético circular alrededor de dicho hilo, que puede captar un hilo adyacente.

Reproduzca la animación de la ilustración para ver la forma en que la transmisión de datos puede verse afectada por interferencias.

Para contrarrestar los efectos negativos de la EMI y la RFI, algunos tipos de cables de cobre se empaquetan con un blindaje metálico y requieren una conexión a tierra adecuada.

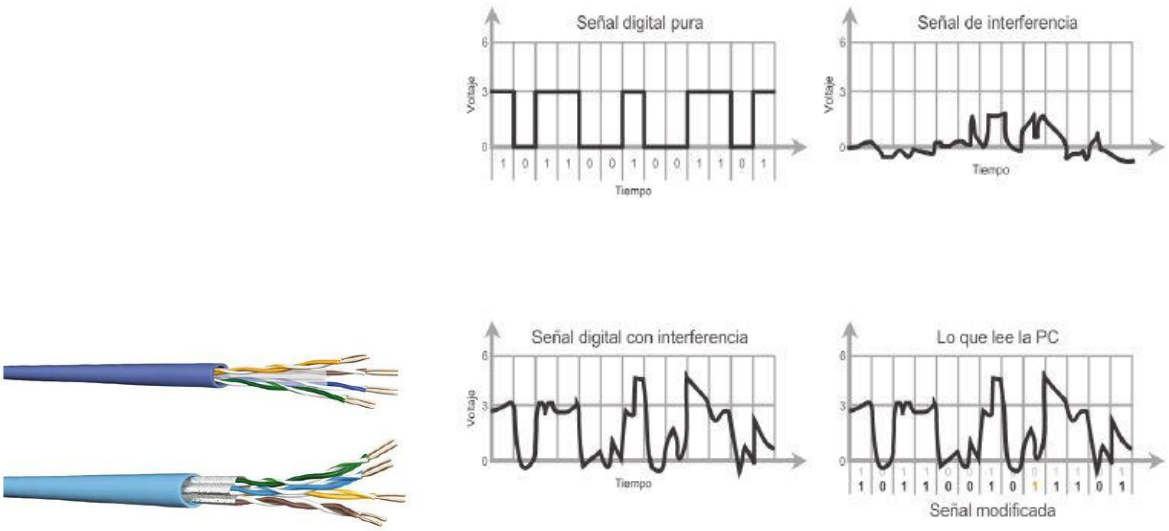
Para contrarrestar los efectos negativos del crosstalk, algunos tipos de cables de cobre tienen pares de hilos de circuitos opuestos trenzados que cancelan dicho tipo de interferencia en forma eficaz.

La susceptibilidad de los cables de cobre al ruido electrónico también puede estar limitada por:

- La elección del tipo o la categoría de cable más adecuados a un entorno de red determinado.

- El diseño de una infraestructura de cables para evitar las fuentes de interferencia posibles y conocidas en la estructura del edificio.

- El uso de técnicas de cableado que incluyen el manejo y la terminación apropiados de los cables.



Capítulo 4: Acceso a la red 4.2.1.2 Medios de cobre

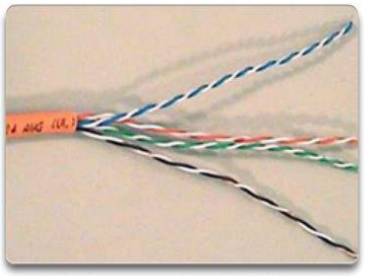
Existen tres tipos principales de medios de cobre que se utilizan en las redes:

- Par trenzado no blindado (UTP)
- Par trenzado blindado (STP)
- Coaxial

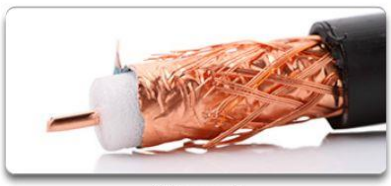
Estos cables se utilizan para interconectar los nodos en una LAN y los dispositivos de infraestructura, como switches, routers y puntos de acceso inalámbrico. Cada tipo de conexión y sus dispositivos complementarios tienen requisitos de cableado estipulados por los estándares de la capa física.

Los diferentes estándares de la capa física especifican el uso de distintos conectores. Estos estándares especifican las dimensiones mecánicas de los conectores y las propiedades eléctricas aceptables de cada tipo. Los medios de red utilizan conectores modulares para facilitar la conexión y la desconexión. Además, puede utilizarse un único tipo de conector físico para diferentes tipos de conexiones.

Por ejemplo, el conector RJ-45 se utiliza ampliamente en las LAN con un tipo de medio y en algunas WAN con otro tipo de medio.


Cable de par trenzado no blindado (UTP)


Cable de par trenzado blindado (STP)

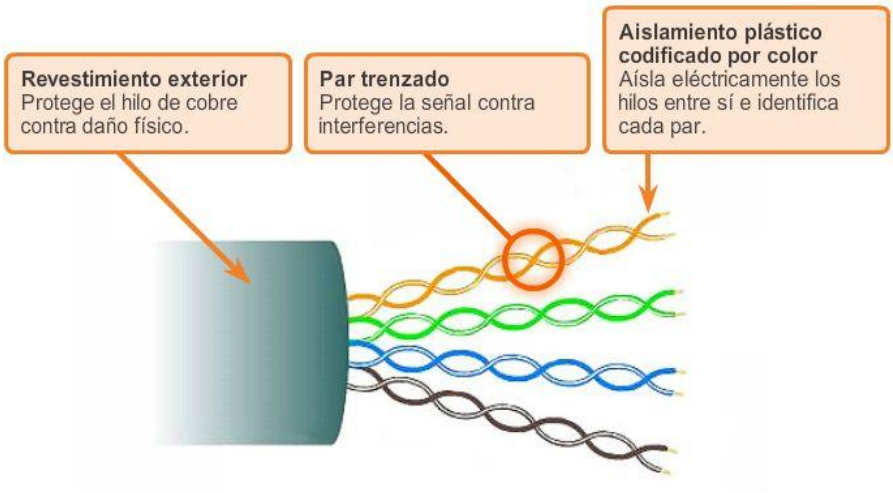

Cable coaxial

Capítulo 4: Acceso a la red 4.2.1.3 Cable de par trenzado no blindado

El cableado de par trenzado no blindado (UTP) es el medio de red más común. El cableado UTP, que se termina con conectores RJ-45, se utiliza para interconectar hosts de red con dispositivos intermediarios de red, como switches y routers.

En las redes LAN, el cable UTP consta de cuatro pares de hilos codificados por color que están trenzados entre sí y recubiertos con un revestimiento de plástico flexible que los protege contra daños físicos menores. El trenzado de los hilos ayuda a proteger contra las interferencias de señales de otros hilos.

Como se muestra en la ilustración, los códigos de color identifican los pares individuales con sus hilos y sirven de ayuda para la terminación de cables.



Capítulo 4: Acceso a la red 4.2.1.4 Cable de par trenzado blindado (STP)

El par trenzado blindado (STP) proporciona una mejor protección contra ruido que el cableado UTP. Sin embargo, en comparación con el cable UTP, el cable STP es mucho más costoso y difícil de instalar. Al igual que el cable UTP, el STP utiliza un conector RJ-45.

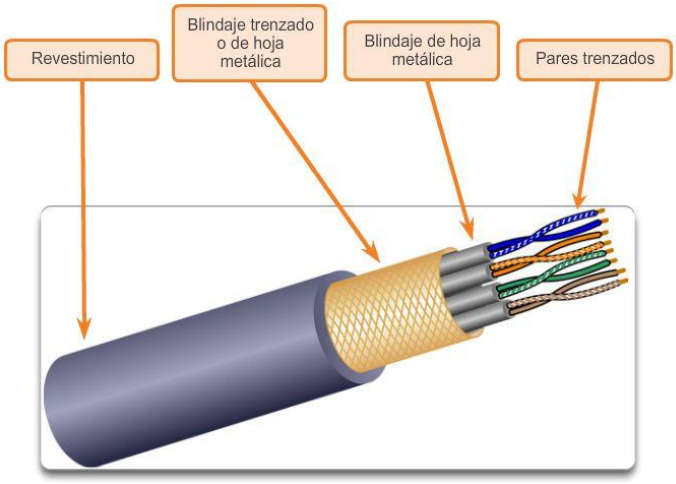
El cable STP combina las técnicas de blindaje para contrarrestar la EMI y la RFI, y el trenzado de hilos para contrarrestar el crosstalk. Para obtener los máximos beneficios del blindaje, los cables STP se terminan con conectores de datos STP blindados especiales. Si el cable no se conecta a tierra correctamente, el blindaje puede actuar como antena y captar señales no deseadas.

Existen distintos tipos de cables STP con diferentes características. Sin embargo, hay dos variantes comunes de STP:

- El cable STP blinda la totalidad del haz de hilos con una hoja metálica que elimina prácticamente toda la interferencia (más común).
- El cable STP blinda todo el haz de hilos, así como cada par de hilos, con una hoja metálica que elimina todas las interferencias.

El cable STP que se muestra utiliza cuatro pares de hilos. Cada uno de estos pares está empaquetado primero con un blindaje de hoja metálica y, luego, el conjunto se empaqueta con una malla tejida o una hoja metálica.

Durante muchos años, STP fue la estructura de cableado de uso específico en instalaciones de red Token Ring. Con la disminución en el uso de Token Ring, también se redujo la demanda de cableado de par trenzado blindado. Sin embargo, el nuevo estándar de 10 GB para Ethernet incluye una disposición para el uso de cableado STP que genera un renovado interés en el cableado de par trenzado blindado.



Capítulo 4: Acceso a la red 4.2.1.5 Cable coaxial

El cable coaxial obtiene su nombre del hecho de que hay dos conductores que comparten el mismo eje. Como se muestra en la ilustración, el cable coaxial consta de lo siguiente:

- Un conductor de cobre utilizado para transmitir las señales electrónicas.
- El conductor de cobre está rodeado por una capa de aislamiento plástico flexible.
- Sobre este material aislante, hay una malla de cobre tejida o una hoja metálica que actúa como segundo hilo en el circuito y como blindaje para el conductor interno. La segunda capa o blindaje reduce la cantidad de interferencia electromagnética externa.
- La totalidad del cable está cubierta por un revestimiento para protegerlo contra daños físicos menores.

Nota: se utilizan diferentes tipos de conectores con cable coaxial.

Tradicionalmente, el cable coaxial, capaz de transmitir en una dirección, se utilizó para la televisión por cable. También se utilizó mucho en las primeras instalaciones de Ethernet.

Si bien el cable UTP esencialmente reemplazó al cable coaxial en las instalaciones de Ethernet modernas, el diseño del cable coaxial se adaptó para los siguientes usos:

- Instalaciones inalámbricas: los cables coaxiales conectan antenas a los dispositivos inalámbricos. También transportan energía de radiofrecuencia (RF) entre las antenas y el equipo de radio.
- Instalaciones de Internet por cable: actualmente, los proveedores de servicio de cable están convirtiendo los sistemas unidireccionales en sistemas bidireccionales para proporcionar a sus clientes conectividad a Internet. Para proporcionar estos servicios, las partes de cable coaxial y los elementos de amplificación compatibles se reemplazan con cables de fibra óptica. Sin embargo, la conexión final hacia la ubicación del cliente y el cableado dentro de sus instalaciones aún sigue siendo de cable coaxial. Este uso combinado de fibra y coaxial se denomina fibra coaxial híbrida (HFC).

Capítulo 4: Acceso a la red 4.2.1.6 Seguridad de los medios de cobre

Los tres tipos de medios de cobre son vulnerables a peligros eléctricos y de incendio.

Los peligros de incendio se deben a que el revestimiento y el aislamiento de los cables pueden ser inflamables o producir emanaciones tóxicas cuando se calientan o se queman. Las organizaciones o autoridades edilicias pueden estipular estándares de seguridad relacionados para las instalaciones de hardware y cableado.

Los peligros eléctricos son un problema potencial, dado que los hilos de cobre podrían conducir electricidad en formas no deseadas.

Esto puede exponer al personal y el equipo a una variedad de peligros eléctricos. Por ejemplo, un dispositivo de red defectuoso podría conducir corriente al bastidor de otros dispositivos de red. Además, el cableado de red podría representar niveles de voltaje no deseados cuando se utiliza para conectar dispositivos que incluyen fuentes de energía con diferentes potenciales de conexión a tierra. Estos casos son posibles cuando el cableado de cobre se utiliza para conectar redes en diferentes edificios o pisos que utilizan distintas instalaciones de energía. Finalmente, el cableado de cobre puede conducir los voltajes provocados por descargas eléctricas a los dispositivos de red.

Como consecuencia, las corrientes y los voltajes no deseados pueden generar un daño a los dispositivos de red y a las computadoras conectadas o bien provocar lesiones al personal. Para prevenir situaciones potencialmente peligrosas y perjudiciales, es importante instalar correctamente el cableado de cobre según las especificaciones relevantes y los códigos de edificación.

En la ilustración, se muestran prácticas de cableado adecuadas para evitar posibles peligros eléctricos y de incendio.

La separación del cableado de datos y el de energía eléctrica debe cumplir con los códigos de seguridad.

Los cables deben estar conectados correctamente.

Se deben inspeccionar las instalaciones para detectar daños.

El equipo debe estar correctamente conectado a tierra.

Capítulo 4: Acceso a la red 4.2.2.1 Propiedades del cableado UTP

Cuando se utiliza como medio de red, el cableado de par trenzado no blindado (UTP) consta de cuatro pares de hilos codificados por color que están trenzados entre sí y recubiertos con un revestimiento de plástico flexible. Los cables de red UTP tienen cuatro pares de hilos de cobre de calibre 22 o 24. Los cables UTP tienen un diámetro externo de aproximadamente 0,43 cm (0,17 in), y su tamaño reducido puede ser una ventaja durante la instalación.

Los cables UTP no utilizan blindaje para contrarrestar los efectos de la EMI y la RFI. En cambio, los diseñadores de cables descubrieron que pueden limitar el efecto negativo del crosstalk por medio de los métodos siguiente:

- Anulación los diseñadores ahora emparejan los hilos en un circuito. Cuando dos hilos en un circuito eléctrico están cerca, los campos magnéticos son exactamente opuestos entre sí. Por lo tanto, los dos campos magnéticos se anulan y también anulan cualquier señal de EMI y RFI externa.

- Cambio del número de vueltas por par de hilos: para mejorar aún más el efecto de anulación de los pares de hilos del circuito, los diseñadores cambian el número de vueltas de cada par de hilos en un cable.

  Los cables UTP deben seguir especificaciones precisas que rigen cuántas vueltas o trenzas se permiten por metro (3,28 ft) de cable. Observe en la ilustración que el par naranja y naranja/blanco está menos trenzado que el par azul y azul/blanco. Cada par coloreado se trenza una cantidad de veces distinta.

Los cables UTP dependen exclusivamente del efecto de anulación producido por los pares de hilos trenzados para limitar la degradación de la señal y proporcionar un autoblindaje eficaz de los pares de hilos en los medios de red.

Capítulo 4: Acceso a la red 4.2.2.2 Estándares de cableado UTP

El cableado UTP cumple con los estándares establecidos en conjunto por la TIA/EIA. Específicamente, TIA/EIA-568A estipula los estándares comerciales de cableado para las instalaciones de LAN y es el estándar más utilizado en los entornos de cableado LAN. Algunos de los elementos definidos son:

- Tipos de cables
- Longitudes del cable
- Conectores
- Terminación de los cables
- Métodos para realizar pruebas de cable

El Instituto de Ingenieros en Electricidad y Electrónica (IEEE) define las características eléctricas del cableado de cobre. IEEE califica el cableado UTP según su rendimiento. Los cables se dividen en categorías según su capacidad para transportar datos de ancho de banda a velocidades mayores. Por ejemplo, el cable de Categoría 5 (Cat5) se utiliza comúnmente en las instalaciones de FastEthernet 100BASE-TX. Otras categorías incluyen el cable de categoría 5 mejorada (Cat5e), la categoría 6 (Cat6) y la categoría 6a.

Los cables de categorías superiores se diseñan y fabrican para admitir velocidades superiores de transmisión de datos. A medida que se desarrollan y adoptan nuevas tecnologías Ethernet de velocidades en gigabits, Cat5e es el tipo de cable mínimamente aceptable en la actualidad. Cat6 es el tipo de cable recomendado para nuevas instalaciones edilicias.

En la ilustración, se destacan las distintas categorías de cableado UTP.

Nota: algunos fabricantes producen cables que exceden las especificaciones de la categoría 6a de la TIA/EIA y se refieren a estos como cables de “categoría 7”.

Capítulo 4: Acceso a la red 4.2.2.3 Conectores UTP

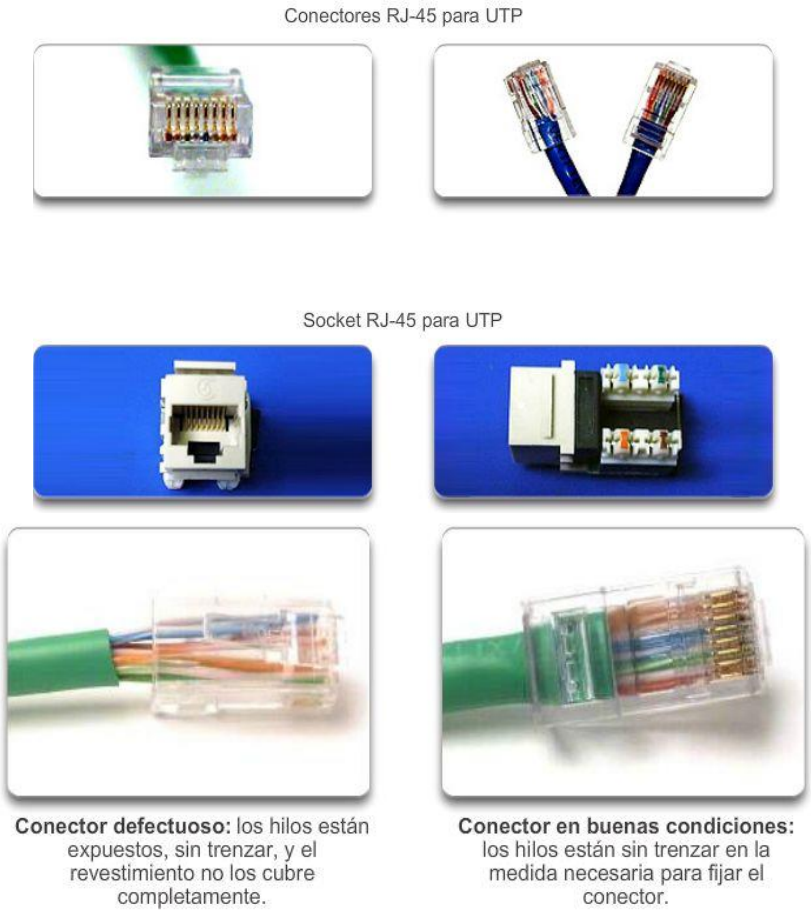
Los cables UTP se terminan generalmente con un conector RJ-45 especificado por el estándar ISO 8877. Este conector se utiliza para una variedad de especificaciones de capa física, una de las cuales es Ethernet. El estándar TIA/EIA 568 describe las asignaciones de los códigos de color de los hilos a los pines (diagrama de pines) de los cables Ethernet.

En el video de la figura 1, se muestra un cable UTP terminado con un conector RJ-45.

Como se muestra en la figura 2, el conector RJ-45 es el componente macho que está engarzado en el extremo del cable. El socket es el componente hembra en un dispositivo de red, una pared, una toma en el tabique divisorio de un cubículo o un panel de conexiones.

Cada vez que se realiza la terminación de un cableado de cobre, existe la posibilidad de que haya pérdida de señal y de que se introduzca ruido en el circuito de comunicación. Cuando las terminaciones se realizan de manera incorrecta, cada cable representa una posible fuente de merma del rendimiento de la capa física. Es fundamental que todas las terminaciones de medios de cobre sean de calidad superior para garantizar un funcionamiento óptimo con tecnologías de redes actuales y futuras.

En la figura 3, se muestra un ejemplo de un cable UTP mal terminado y un cable UTP bien terminado.



La terminación incorrecta de los cables puede afectar el rendimiento de la transmisión.

Capítulo 4: Acceso a la red 4.2.2.4 Tipos de cables UTP

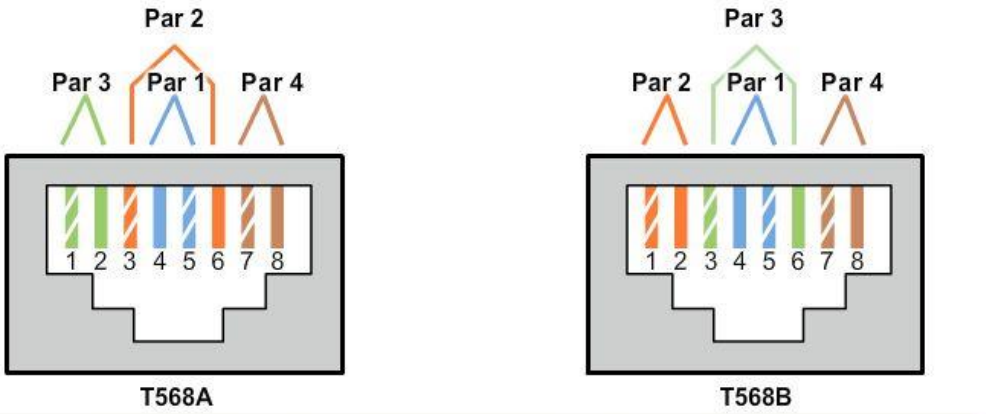
Según las diferentes situaciones, es posible que los cables UTP necesiten armarse según las diferentes convenciones para los cableados. Esto significa que los hilos individuales del cable deben conectarse en diferente orden para distintos grupos de pines en los conectores RJ-45.

A continuación se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado:

- Cable directo de Ethernet: el tipo más común de cable de red. Por lo general, se utiliza para interconectar un host con un switch y un switch con un router.
- Cable cruzado Ethernet: cable poco común utilizado para interconectar dispositivos similares. Por ejemplo, para conectar un switch a un switch, un host a un host o un router a un router.
- Cable de consola: cable exclusivo de Cisco utilizado para conectarse al puerto de consola de un router o de un switch.

Es posible que el uso de un cable de conexión cruzada o de conexión directa en forma incorrecta entre los dispositivos no dañe los dispositivos pero no se producirá la conectividad y la comunicación entre los dispositivos. Éste es un error común de laboratorio. Si no se logra la conectividad, la primera medida para resolver este problema es verificar que las conexiones de los dispositivos sean correctas.

En la ilustración, se muestra el tipo de cable UTP, los estándares relacionados y la aplicación típica de estos cables. También se identifican los pares de hilos individuales para los estándares TIA 568A y TIA 568B.



Tipo de cable	Estándar	Capa de aplicación
Cable directo de Ethernet	Ambos extremos son T568A o T568B.	Conecta un host de red a un dispositivo de red, como un switch o un hub.
Cruzado Ethernet	Un extremo es T568A, el otro extremo es T568B.	• Conecta dos hosts de red. • Conecta dos dispositivos de red intermediarios (un switch a un switch, o un router a un router).
De consola	Propietario de Cisco	Conecta el puerto serie de una estación de trabajo al puerto de consola de un router mediante un adaptador.

Capítulo 4: Acceso a la red 4.2.2.5 Prueba de los cables UTP

Después de la instalación, se debe utilizar un comprobador de cables UTP para probar los siguientes parámetros:

- Mapa de cableado
- Longitud del cable
- Pérdida de señal debido a atenuación
- Crosstalk

Se recomienda revisar minuciosamente que se cumplan todos los requisitos de instalación de UTP.

Capítulo 4: Acceso a la red 4.2.3.1 Propiedades del cableado de fibra óptica

El cable de fibra óptica se volvió muy popular para interconectar dispositivos de red de infraestructura. Permite la transmisión de datos a través de distancias más extensas y a anchos de banda (velocidades de datos) mayores que cualquier otro medio de red.

La fibra óptica es un hilo flexible, extremadamente delgado y transparente de vidrio muy puro (sílice), no mucho más grueso que un cabello humano. En la fibra, los bits se codifican en forma de impulsos de luz. El cable de fibra óptica actúa como una guía de ondas o una “tubería de luz” para transmitir la luz entre los dos extremos con una pérdida mínima de la señal.

A modo de analogía, imagine un rollo de toallas de papel vacío que mide mil metros de largo y tiene el interior recubierto con material reflectante, y un pequeño puntero láser que se utiliza para enviar señales de código morse a la velocidad de la luz. Básicamente, así es cómo funciona un cable de fibra óptica, excepto que tiene un diámetro más pequeño y utiliza tecnologías de emisión y recepción de luz sofisticadas.

A diferencia de los cables de cobre, el cable de fibra óptica puede transmitir señales con menos atenuación y es totalmente inmune a las EMI y RFI.

En la actualidad, el cableado de fibra óptica se utiliza en cuatro tipos de industrias:

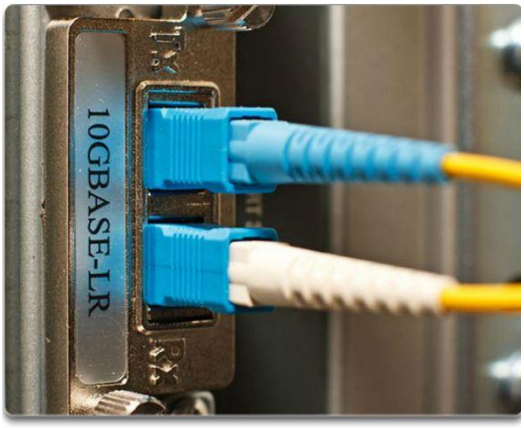
- Redes empresariales: la fibra óptica se utiliza para aplicaciones de cableado backbone y para la interconexión de dispositivos de infraestructura.

- FTTH y redes de acceso: la fibra hasta el hogar (FTTH) se utiliza para proporcionar servicios de banda ancha de conexión permanente a hogares y pequeñas empresas. La tecnología FTTH admite el acceso a Internet de alta velocidad a un precio accesible, así como el trabajo a distancia, la medicina a distancia y el video a petición.

- Redes de largo alcance: los proveedores de servicios utilizan redes de fibra óptica terrestres de largo alcance para conectar países y ciudades. En general, las redes tienen un alcance de algunas decenas a unos miles de kilómetros y utilizan sistemas basados en hasta 10 Gb/s.

- Redes submarinas: se utilizan cables de fibra óptica especiales para proporcionar soluciones confiables de alta velocidad y alta capacidad que puedan subsistir en entornos submarinos adversos por distancias transoceánicas.

Nos centraremos en el uso de la fibra óptica en el nivel de empresa.



Capítulo 4: Acceso a la red 4.2.3.2 Diseño del cable de medios de fibra

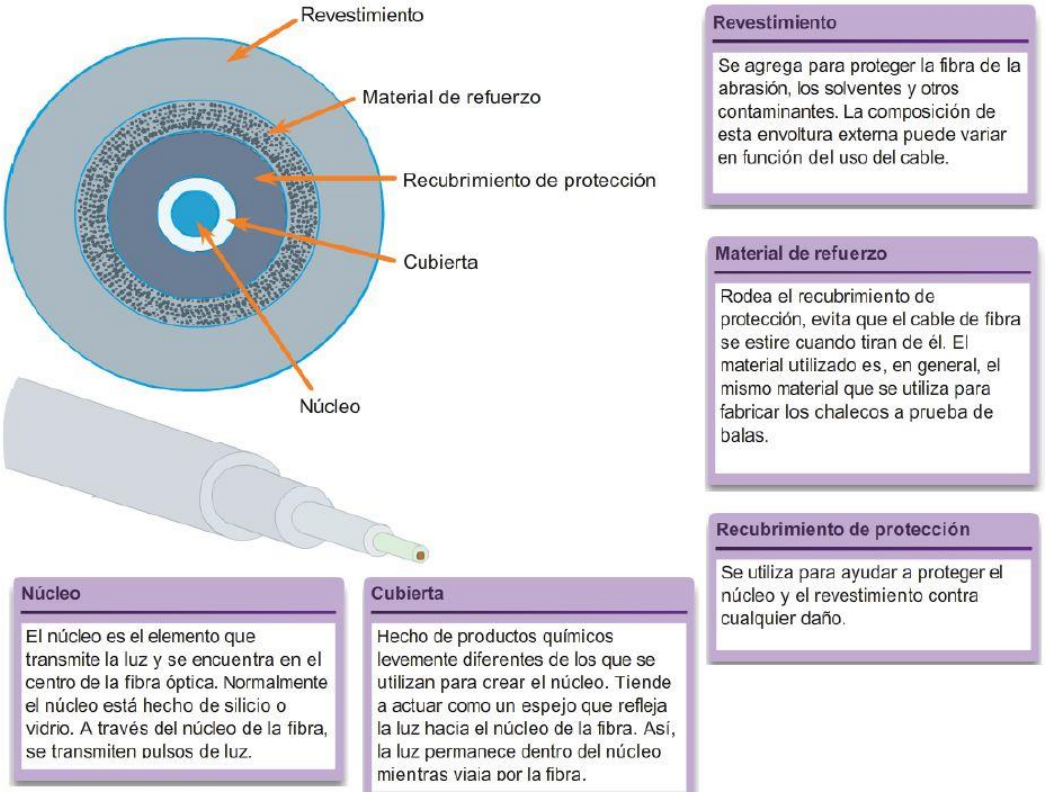
Si bien la fibra óptica es muy delgada, consta de dos tipos de vidrio y de un blindaje externo de protección. Específicamente, estos componentes conforman lo siguiente:

- Núcleo: consta de vidrio puro y es la parte de la fibra por la que se transporta la luz.

- Cubierta: el vidrio que rodea al núcleo y actúa como espejo. Los pulsos de luz se propagan por el núcleo mientras la cubierta los refleja. Esto ayuda a contener los pulsos de luz en el núcleo de la fibra, un fenómeno conocido como “reflexión interna total”.

- Revestimiento: generalmente, es un revestimiento de PVC que protege el núcleo y la cubierta. También puede incluir material de refuerzo y un recubrimiento de protección cuyo objetivo es proteger el vidrio contra rayones y humedad.

Si bien es vulnerable a los dobleces pronunciados, las propiedades del núcleo y la cubierta se modificaron en el nivel molecular para hacerla muy resistente. La fibra óptica se prueba a través de un riguroso proceso de fabricación para que tenga una resistencia mínima de 100 000 lb/pulg2). La fibra óptica es lo suficientemente duradera para soportar el manejo durante la instalación y la implementación en redes en condiciones ambientales adversas en todo el mundo.



Capítulo 4: Acceso a la red 4.2.3.3 Tipos de medios de fibra óptica

Los pulsos de luz que representan los datos transmitidos en forma de bits en los medios son generados por uno de los siguientes:

- Láseres
- Diodos emisores de luz (LED)

Los dispositivos electrónicos semiconductores, denominados fotodiodos, detectan los impulsos de luz y los convierten en voltajes que pueden reconstruirse en tramas de datos.

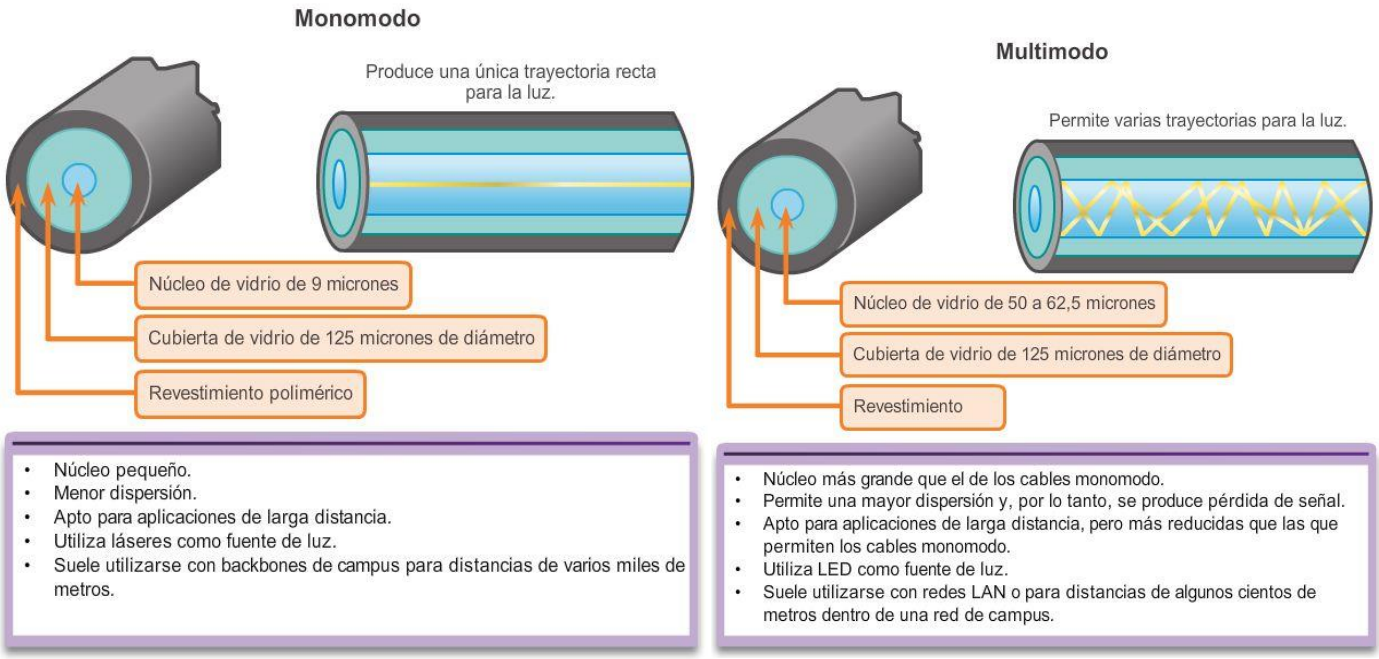
Nota: la luz de láser transmitida a través del cableado de fibra óptica puede dañar el ojo humano. Se debe tener precaución y evitar mirar dentro del extremo de una fibra óptica activa.

En términos generales, los cables de fibra óptica pueden clasificarse en dos tipos:

- Fibra óptica monomodo: la fibra óptica monomodo (SMF) consta de un núcleo muy pequeño y emplea tecnología láser costosa para enviar un único haz de luz. Se usa mucho en situaciones de larga distancia que abarcan cientos de kilómetros, como aplicaciones de TV por cable y telefonía de larga distancia.

- Fibra óptica multimodo: la fibra óptica multimodo (MMF) consta de un núcleo más grande y utiliza emisores LED para enviar pulsos de luz. Específicamente, la luz de un LED ingresa a la fibra multimodo en diferentes ángulos. Se usa mucho en las redes LAN, debido a que se puede alimentar mediante LED de bajo costo. Proporciona un ancho de banda de hasta 10 Gb/s a través de longitudes de enlace de hasta 550 m.

En las figuras 1 y 2, se destacan las características de la fibra óptica multimodo y monomodo. Una de las diferencias destacadas entre la fibra óptica multimodo y monomodo es la cantidad de dispersión. La dispersión se refiere a la extensión de los pulsos de luz con el tiempo. Cuanta más dispersión existe, mayor es la pérdida de intensidad de la señal.



Capítulo 4: Acceso a la red 4.2.3.4 Conectores de red de fibra óptica

El extremo de una fibra óptica se termina con un conector de fibra óptica. Existe una variedad de conectores de fibra óptica. Las diferencias principales entre los tipos de conectores son las dimensiones y los métodos de acoplamiento mecánico. Por lo general, los organismos estandarizan un tipo de conector según el equipo que utilizan comúnmente, o estandarizan por tipo de fibra (uno para MMF, uno para SMF). Si se tienen en cuenta todas las generaciones de conectores, en la actualidad se utilizan alrededor de 70 tipos diferentes.

Como se muestra en la figura 1, los tres conectores de red de fibra óptica más populares son los siguientes:

- Punta recta (ST): conectores antiguos de estilo bayoneta, ampliamente utilizados con la fibra óptica multimodo.

- Conector suscriptor (SC): en ocasiones, se lo denomina “conector cuadrado” o “conector estándar”. Es un conector LAN y WAN ampliamente adoptado que utiliza un mecanismo de inserción/extracción para asegurar la inserción correcta. Este tipo de conector se utiliza con la fibra óptica multimodo y monomodo.

- Conector Lucent (LC): en ocasiones, denominado conector “pequeño” o “local”, cada vez adquiere mayor popularidad debido a su tamaño reducido. Se utiliza con la fibra óptica monomodo y también es compatible con la fibra óptica multimodo.

Nota: otros conectores de fibra óptica, como el conector de férula (FC) y el subminiatura A (SMA) no son de uso extendido en la implementación de redes LAN y WAN. Entre los conectores considerados obsoletos, se incluyen los conectores bicónicos (obsoleto) y los D4. Estos conectores exceden el ámbito de este capítulo.

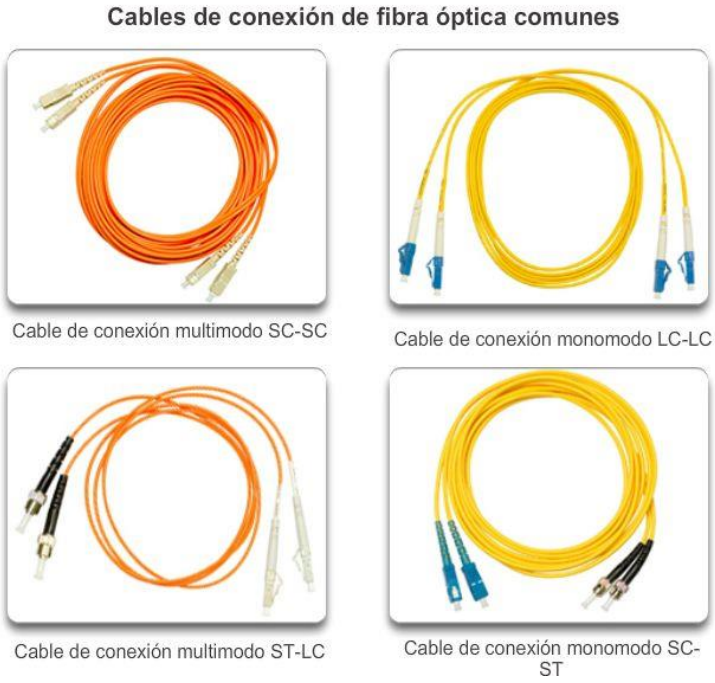
Se requieren dos fibras para realizar una operación full duplex ya que la luz sólo puede viajar en una dirección a través de la fibra óptica. En consecuencia, los cables de conexión de fibra óptica forman un haz de dos cables de fibra óptica, y su terminación incluye un par de conectores de fibra monomodo estándar. Algunos conectores de fibra óptica aceptan las fibras de transmisión y recepción en un único conector, conocido como “conector dúplex”, que también se muestra en la figura 1.

Los cables de conexión de fibra óptica son necesarios para interconectar dispositivos de infraestructura. Por ejemplo, en la figura 2, se muestran diversos cables de conexión comunes:

- Cable de conexión multimodo SC-SC
- Cable de conexión monomodo LC-LC
- Cable de conexión multimodo ST-LC
- Cable de conexión monomodo SC-ST

Los cables de fibra óptica se deben proteger con un pequeño capuchón de plástico cuando no se utilizan.

Observe además el uso de colores para distinguir entre los cables de conexión monomodo y multimodo. Esto se debe al estándar TIA-598, que recomienda el uso de un revestimiento amarillo para los cables de fibra óptica monomodo y uno naranja (o aguamarina) para los cables de fibra óptica multimodo.



Capítulo 4: Acceso a la red 4.2.3.5 Prueba de cables de fibra óptica

La terminación y el empalme del cableado de fibra óptica requiere de equipo y capacitación especiales. La terminación incorrecta de los medios de fibra óptica produce una disminución de las distancias de señalización o una falla total de la transmisión.

Tres tipos comunes de errores de empalme y terminación de fibra óptica son:

- Desalineación: los medios de fibra óptica no se alinean con precisión al unirlos.
- Separación de los extremos: no hay contacto completo de los medios en el empalme o la conexión.
- Acabado de los extremos: los extremos de los medios no se encuentran bien pulidos o puede verse suciedad en la terminación.

Se puede realizar una prueba de campo rápida y sencilla que consiste en iluminar un extremo de la fibra con una linterna potente mientras se observa el otro extremo. Si la luz es visible, entonces la fibra es capaz de transmitir luz. Si bien esta prueba no garantiza el funcionamiento de la fibra, es una forma rápida y económica de detectar una fibra deteriorada.

Se recomienda utilizar un comprobador óptico como el que se muestra en la ilustración para probar los cables de fibra óptica. Se puede utilizar un reflectómetro óptico de dominio de tiempo (OTDR) para probar cada segmento del cable de fibra óptica. Este dispositivo introduce un impulso de luz de prueba en el cable y mide la retrodispersión y el reflejo de la luz detectados en función del tiempo. El OTDR calculará la distancia aproximada en la que se detectan estas fallas en toda la longitud del cable.

Reflectómetro óptico de dominio de tiempo (OTDR)

Capítulo 4: Acceso a la red 4.2.3.6 Comparación entre fibra óptica y cobre

La utilización de cables de fibra óptica ofrece muchas ventajas en comparación con los cables de cobre.

Debido a que las fibras de vidrio que se utilizan en los medios de fibra óptica no son conductores eléctricos, el medio es inmune a la interferencia electromagnética y no conduce corriente eléctrica no deseada cuando existe un problema de conexión a tierra. Las fibras ópticas pueden utilizarse en longitudes mucho mayores que los medios de cobre sin la necesidad de regenerar la señal, ya que son finas y tienen una pérdida de señal relativamente baja. Algunas especificaciones de la capa física de fibra óptica admiten longitudes que pueden alcanzar varios kilómetros.

Algunos de los problemas de implementación de medios de fibra óptica:

- Más costoso (comúnmente) que los medios de cobre para la misma distancia (pero para una capacidad mayor)
- Se necesitan diferentes habilidades y equipos para terminar y empalmar la infraestructura de cables
- Manejo más cuidadoso que los medios de cobre
-

En la actualidad, en la mayor parte de los entornos empresariales se utiliza principalmente la fibra óptica como cableado backbone para conexiones punto a punto con una gran cantidad de tráfico entre los servicios de distribución de datos y para la interconexión de los edificios en el caso de los campus compuestos por varios edificios. Ya que la fibra óptica no conduce electricidad y presenta una pérdida de señal baja, es ideal para estos usos.

En la ilustración, se destacan algunas de estas diferencias.

Cuestiones de implementación	Cableado UTP	Cableado de fibra óptica
Ancho de banda admitido	10 Mb/s – 10 Gb/s	10 Mb/s – 100 Gb/s
Distancia	Relativamente corta (de 1 a 100m)	Relativamente extensa (de 1 a 100000m)
Inmunidad a EMI y RFI	Baja	Alta (totalmente inmune)
Inmunidad a los peligros eléctricos	Baja	Alta (totalmente inmune)
Costos de medios y conectores	Menores	Mayores
Habilidades de instalación requeridas	Menores	Mayores
Precauciones de seguridad	Menores	Mayores

Capítulo 4: Acceso a la red 4.2.4.1 Propiedades de los medios inalámbricos

Los medios inalámbricos transportan señales electromagnéticas que representan los dígitos binarios de las comunicaciones de datos mediante frecuencias de radio y de microondas.

Como medio de redes, el sistema inalámbrico no se limita a conductores o canaletas, como en el caso de los medios de fibra o de cobre. De todos los medios, los inalámbricos proporcionan las mayores opciones de movilidad. Además, la cantidad de dispositivos con tecnología inalámbrica aumenta continuamente. Por estos motivos, la tecnología inalámbrica se convirtió en el medio de preferencia para las redes domésticas. A medida que aumentan las opciones de ancho de banda de red, la tecnología inalámbrica adquiere popularidad rápidamente en las redes empresariales.

En la ilustración, se destacan varios símbolos relacionados con la tecnología inalámbrica.

Sin embargo, existen algunas áreas de importancia para la tecnología inalámbrica, que incluyen las siguientes:

- Área de cobertura: las tecnologías inalámbricas de comunicación de datos funcionan bien en entornos abiertos. Sin embargo, existen determinados materiales de construcción utilizados en edificios y estructuras, además del terreno local, que limitan la cobertura efectiva.

- Interferencia: la tecnología inalámbrica también es vulnerable a la interferencia y puede verse afectada por dispositivos comunes como teléfonos inalámbricos domésticos, algunos tipos de luces fluorescentes, hornos de microondas y otras comunicaciones inalámbricas.

- Seguridad: la cobertura de la comunicación inalámbrica no requiere acceso a un hilo físico de un medio. Por lo tanto, dispositivos y usuarios sin autorización para acceder a la red pueden obtener acceso a la transmisión. En consecuencia, la seguridad de la red es un componente importante de la administración de una red inalámbrica.

Si bien la tecnología inalámbrica es cada vez más popular para la conectividad de escritorio, el cobre y la fibra óptica son los medios de capa física más populares para las implementaciones de redes.

Capítulo 4: Acceso a la red 4.2.4.2 Tipos de medios inalámbricos

Los estándares IEEE y los de la industria de las telecomunicaciones para las comunicaciones inalámbricas de datos abarcan las capas física y de enlace de datos.

Los tres estándares comunes de comunicación de datos que se aplican a los medios inalámbricos son los siguientes:

- Estándar IEEE 802.11: la tecnología de LAN inalámbrica (WLAN), comúnmente denominada “Wi-Fi”, utiliza un sistema por contienda o no determinista con un proceso de acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA) para acceder a los medios.

- Estándar IEEE 802.15: el estándar de red de área personal inalámbrica (WPAN), comúnmente denominado “Bluetooth”, utiliza un proceso de emparejamiento de dispositivos para comunicarse a través de distancias de 1 a 100 m.

- Estándar IEEE 802.16: conocido comúnmente como “interoperabilidad mundial para el acceso por microondas” (WiMAX), utiliza una topología de punto a multipunto para proporcionar acceso a servicios de banda ancha inalámbrica.

En la ilustración, se destacan algunas de las diferencias entre los medios inalámbricos.

Nota: otras tecnologías inalámbricas, como las comunicaciones satelitales y de datos móviles, también pueden proporcionar conectividad a redes de datos. No obstante, estas tecnologías inalámbricas exceden el ámbito de este capítulo.

En cada uno de los ejemplos anteriores, las especificaciones de la capa física se aplican a áreas que incluyen lo siguiente:

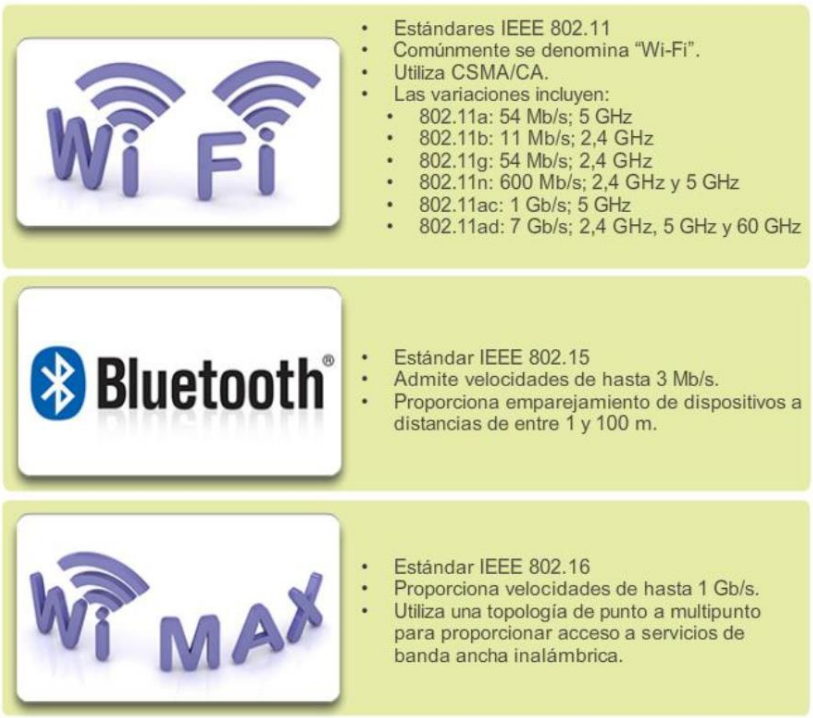
- Codificación de señales de datos a señales de radio

- Frecuencia e intensidad de la transmisión

- Requisitos de recepción y decodificación de señales

- Diseño y construcción de antenas

Nota: Wi-Fi es una marca comercial de Wi-Fi Alliance. La tecnología Wi-Fi se utiliza con productos certificados que pertenecen a los dispositivos WLAN basados en los estándares IEEE 802.11.



Capítulo 4: Acceso a la red 4.2.4.3 LAN inalámbrica

Una implementación común de transmisión inalámbrica de datos permite a los dispositivos conectarse en forma inalámbrica a través de una LAN. En general, una LAN inalámbrica requiere los siguientes dispositivos de red:

- Punto de acceso inalámbrico: el punto de acceso (AP) inalámbrico concentra las señales inalámbricas de los usuarios y se conecta (generalmente a través de un cable de cobre) a la infraestructura de red existente basada en medios de cobre, como Ethernet.

  Los routers inalámbricos domésticos y de pequeñas empresas integran las funciones de un router, un switch y un punto de acceso en un solo dispositivo, como el que se muestra en la ilustración.

- Adaptadores de NIC inalámbricas: proporcionan capacidad de comunicación inalámbrica a cada host de red.

A medida que la tecnología fue evolucionando, surgió una gran cantidad de estándares WLAN basados en Ethernet. Se debe tener precaución al comprar dispositivos inalámbricos para garantizar compatibilidad e interoperabilidad.

Los beneficios de las tecnologías inalámbricas de comunicación de datos son evidentes, especialmente en cuanto al ahorro en el cableado costoso de las instalaciones y en la conveniencia de la movilidad del host. Sin embargo, los administradores de red necesitan desarrollar y aplicar procesos y políticas de seguridad rigurosas para proteger las LAN inalámbricas del daño y el acceso no autorizado.

Router inalámbrico Cisco Linksys EA6500 802.11ac

Capítulo 4: Acceso a la red 4.2.4.4 Estándares de Wi-Fi 802.11

Los distintos estándares 802.11 evolucionaron con los años. Los estándares incluyen:

- IEEE 802.11a: opera en la banda de frecuencia de 5 GHz y proporciona velocidades de hasta 54 Mb/s. Posee un área de cobertura menor y es menos efectivo al penetrar estructuras edilicias ya que opera en frecuencias superiores. Los dispositivos que funcionan conforme a este estándar no son interoperables con los estándares 802.11b y 802.11g que se describen a continuación.

- IEEE 802.11b: opera en la banda de frecuencia de 2,4 GHz y proporciona velocidades de hasta 11 Mb/s. Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejor las estructuras edilicias que los dispositivos basados en 802.11a.

- IEEE 802.11g: opera en la banda de frecuencia de 2,4 GHz y proporciona velocidades de hasta 54 Mbps. Por lo tanto, los dispositivos que implementan este estándar operan en la misma radiofrecuencia y tienen un alcance de hasta 802.11b pero con un ancho de banda de 802.11a.

- IEEE 802.11n: opera en la banda de frecuencia de 2,4 GHz y 5 GHz. Las velocidades de datos típicas esperadas van de 150 Mb/s a 600 Mb/s, con una alcance de hasta 70 m. Es compatible con dispositivos 802.11a, b y g anteriores.

- IEEE 802.11ac: opera en la banda de 5 GHz y proporciona velocidades de datos que van de 450 Mb/s a 1,3 Gb/s (1300 Mb/s); es compatible con dispositivos 802.11a/n.

- IEEE 802.11ad: también conocido como “WiGig”. Utiliza una solución de Wi-Fi de triple banda con 2,4 GHz, 5 GHz y 60 GHz, y ofrece velocidades teóricas de hasta 7 Gb/s.

En la ilustración, se destacan algunas de estas diferencias.

Estándar	Velocidad máxima	Frecuencia	Compatible con modelos anteriores
802.11a	54Mb/s	5 GHz	No
802.11b	11 Mb/s	2,4 GHz	No
802.11g	54Mb/s	2,4 GHz	802.11b
802.11n	600 Mb/s	2,4GHz o 5GHz	802.11a/b/g
802.11ac	1,3 Gb/s (1300 Mb/s)	2,4GHz y 5GHz	802.11a/n
802.11ad	7 Gb/s (7000 Mb/s)	2,4GHz, 5GHz y 60 GHz	802.11a/b/g/n/ac

Capítulo 4: Acceso a la red 4.3.1.1 Capa de enlace de datos

La capa de acceso a la red de TCP/IP equivale a las siguientes capas del modelo OSI:

- Enlace de datos (capa 2)
- Física (capa 1)

Como se muestra en la ilustración, la capa de enlace de datos es responsable del intercambio de tramas entre los nodos a través de un medio de red físico. Permite que las capas superiores accedan a los medios y controla el modo en que los datos se colocan y se reciben en los medios.

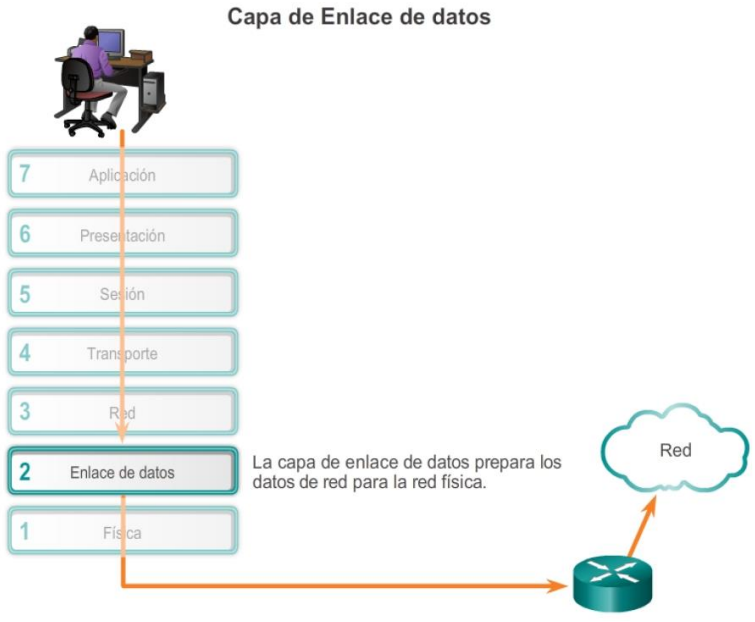
Nota: la notación de la capa 2 para los dispositivos de red conectados a un medio común se denomina “nodo”.

Específicamente, la capa de enlace de datos realiza estos dos servicios básicos:

- Acepta paquetes de la capa 3 y los empaqueta en unidades de datos denominadas “tramas”.
- Controla el acceso al medio y realiza la detección de errores.

La capa de enlace de datos separa de manera eficaz las transiciones de medios que ocurren a medida que el paquete se reenvía desde los procesos de comunicación de las capas superiores. La capa de enlace de datos recibe paquetes de un protocolo de capa superior y los dirige a un protocolo de las mismas características, en este caso, IPv4 o IPv6. Este protocolo de capa superior no necesita saber qué medios utiliza la comunicación.

Nota: en este capítulo, el término “medio” no se refiere a contenido digital y multimedia como audio, animación, televisión y video, sino que se refiere al material que transporta las señales de datos, como los cables de cobre y la fibra óptica.



Capítulo 4: Acceso a la red 4.3.1.2 Subcapas de enlace de datos

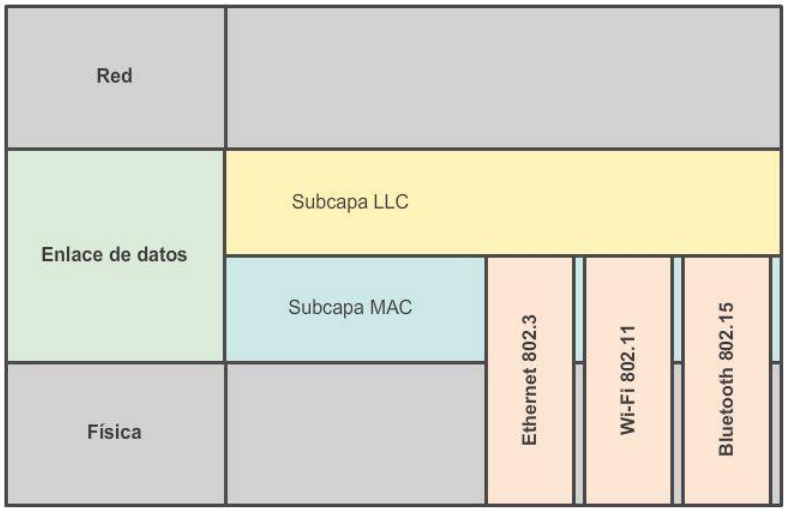
La capa de enlace de datos se divide en dos subcapas:

- Control de enlace lógico (LLC): se trata de la subcapa superior, que define los procesos de software que proporcionan servicios a los protocolos de capa de red. El LLC coloca en la trama información que identifica qué protocolo de capa de red se utiliza para la trama. Esta información permite que varios protocolos de la capa 3, tales como IPv4 e IPv6, utilicen la misma interfaz y los mismos medios de red.

- Control de acceso al medio (MAC): se trata de la subcapa inferior, que define los procesos de acceso al medio que realiza el hardware. Proporciona el direccionamiento de la capa de enlace de datos y la delimitación de los datos de acuerdo con los requisitos de señalización física del medio y con el tipo de protocolo de capa de enlace de datos en uso.

La separación de la capa de enlace de datos en subcapas permite que un tipo de trama definido por la capa superior acceda a distintos tipos de medios definidos por la capa inferior. Tal es el caso en muchas tecnologías LAN, incluida Ethernet.

En la ilustración, se muestra la forma en que la capa de enlace de datos se divide en las subcapas LLC y MAC. El LLC se comunica con la capa de red, mientras que la subcapa MAC admite diversas tecnologías de acceso de red. Por ejemplo, la subcapa MAC se comunica con la tecnología LAN Ethernet para enviar y recibir las tramas a través de cables de cobre o de fibra óptica. La subcapa MAC también se comunica con tecnologías inalámbricas como Wi-Fi y Bluetooth para enviar y recibir tramas en forma inalámbrica.



Capítulo 4: Acceso a la red 4.3.1.3 Control de acceso al medio

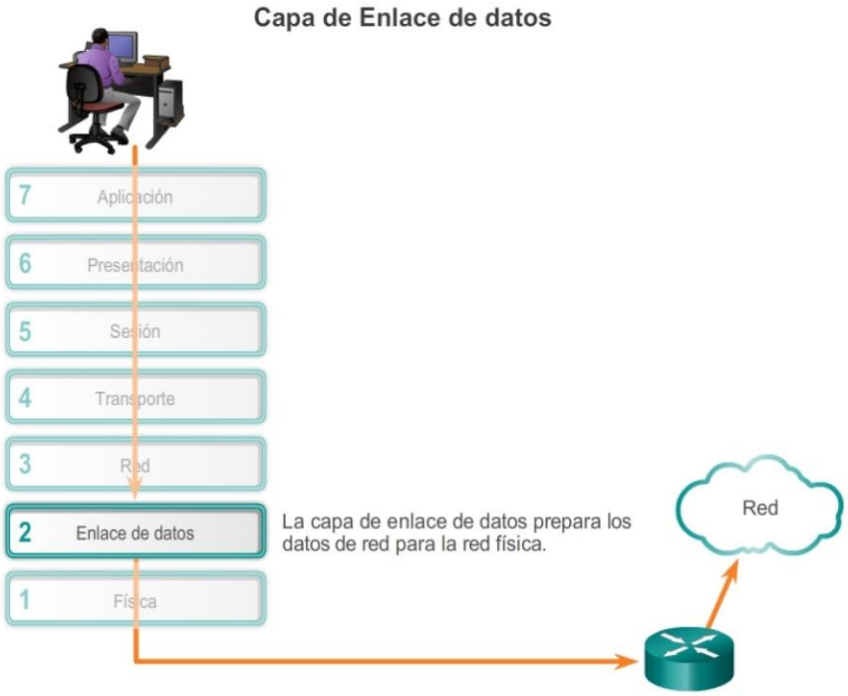
Los protocolos de la Capa 2 especifican la encapsulación de un paquete en una trama y las técnicas para colocar y sacar el paquete encapsulado de cada medio. La técnica utilizada para colocar y sacar la trama de los medios se llama método de control de acceso al medio.

A medida que los paquetes se transfieren del host de origen al host de destino, generalmente deben atravesar diferentes redes físicas. Estas redes físicas pueden constar de diferentes tipos de medios físicos, como cables de cobre, fibra óptica y tecnología inalámbrica compuesta por señales electromagnéticas, frecuencias de radio y microondas, y enlaces satelitales.

Los paquetes no tienen una manera de acceder directamente a los distintos medios. La función de la capa de enlace de datos del modelo OSI es preparar los paquetes de la capa de red para la transmisión y controlar el acceso al medio físico. Los métodos de control de acceso al medio que se describen en los protocolos de capa de enlace de datos definen los procesos mediante los cuales los dispositivos de red pueden acceder a los medios de red y transmitir tramas en distintos entornos de red.

Sin la capa de enlace de datos, los protocolos de capa de red, como el protocolo IP, tendrían que tomar medidas para conectarse a cada tipo de medio que pudiera existir a lo largo de la ruta de entrega. Más aún, IP debería adaptarse cada vez que se desarrolle una nueva tecnología de red o medio. Este proceso dificultaría la innovación y desarrollo de protocolos y medios de red. Éste es un motivo clave para usar un método en capas en interconexión de redes.

En la animación de la ilustración, se proporciona un ejemplo de una PC en París que se conecta a una computadora portátil en Japón. Si bien los dos hosts se comunican exclusivamente mediante el protocolo IP, es probable que se utilicen numerosos protocolos de capa de enlace de datos para transportar los paquetes IP a través de diferentes tipos de redes LAN y WAN. Cada transición en un router puede requerir un protocolo de capa de enlace de datos diferente para el transporte en un medio nuevo.



Capítulo 4: Acceso a la red 4.3.1.4 Provisión de acceso a los medios

Durante una misma comunicación, pueden ser necesarios distintos métodos de control de acceso al medio. Cada entorno de red que los paquetes encuentran cuando viajan desde un host local hasta un host remoto puede tener características diferentes. Por ejemplo, una LAN Ethernet consta de muchos hosts que compiten por acceder al medio de red de forma ad hoc.

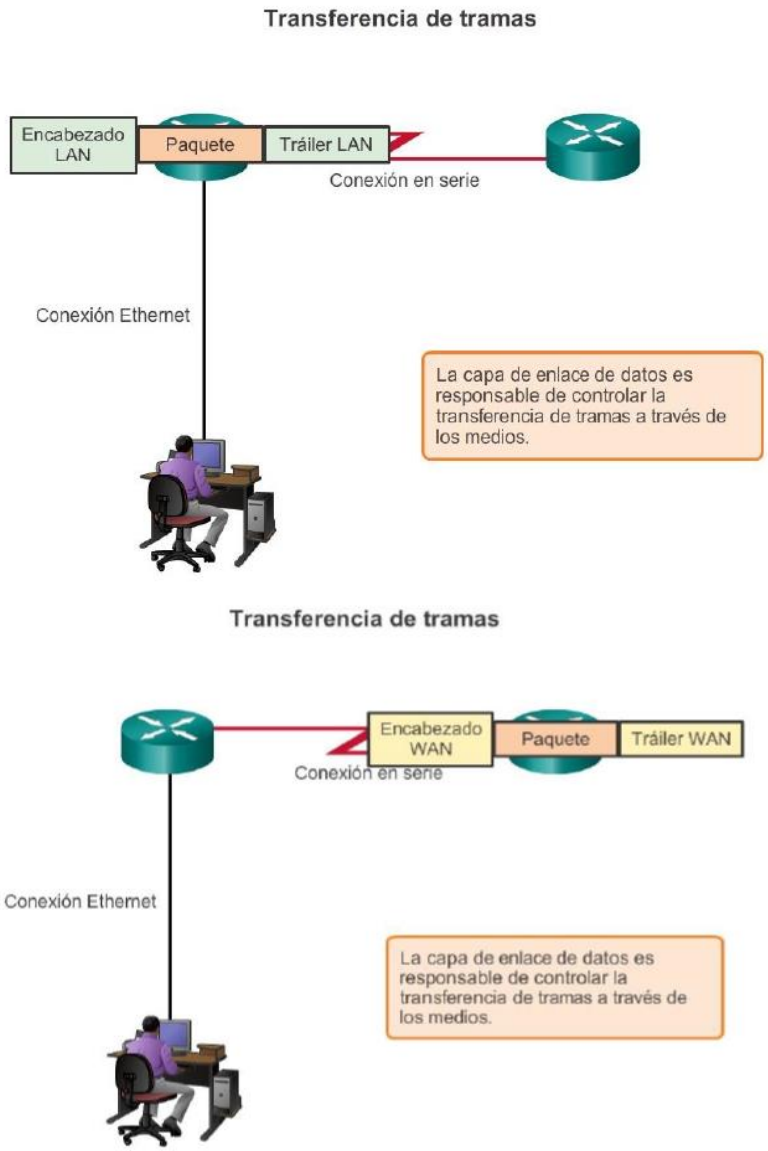
Los enlaces seriales constan de una conexión directa entre dos dispositivos únicamente a través de la cual los datos fluyen en forma de bits de manera secuencial y ordenada.

Las interfaces del router encapsulan el paquete en la trama correspondiente, y se utiliza un método de control de acceso al medio adecuado para acceder a cada enlace. En cualquier intercambio de paquetes de capas de red, puede haber muchas transiciones de medios y de capa de enlace de datos. En cada salto a lo largo de la ruta, los routers realizan lo siguiente:

- Aceptan una trama proveniente de un medio.
- Desencapsulan la trama.

- Vuelven a encapsular el paquete en una trama nueva.
- Reenvían la nueva trama adecuada al medio de ese segmento de la red física.

El router de la figura tiene una interfaz Ethernet para conectarse a la LAN y una interfaz serial para conectarse a la WAN. A medida que el router procesa las tramas, utiliza los servicios de la capa de enlace de datos para recibir la trama de un medio, desencapsularla en la PDU de la capa 3, volver a encapsular la PDU en una trama nueva y colocar la trama en el medio del siguiente enlace de la red.



Capítulo 4: Acceso a la red 4.3.2.1 Formateo de datos para la transmisión

La capa de enlace de datos prepara los paquetes para transportarlos a través de los medios locales mediante su encapsulación con un encabezado y un tráiler para crear una trama. La descripción de una trama es un elemento clave de cada protocolo de capa de enlace de datos.

Los protocolos de capa de enlace de datos requieren información de control para permitir que los protocolos funcionen. Por lo general, la información de control responde las siguientes preguntas:

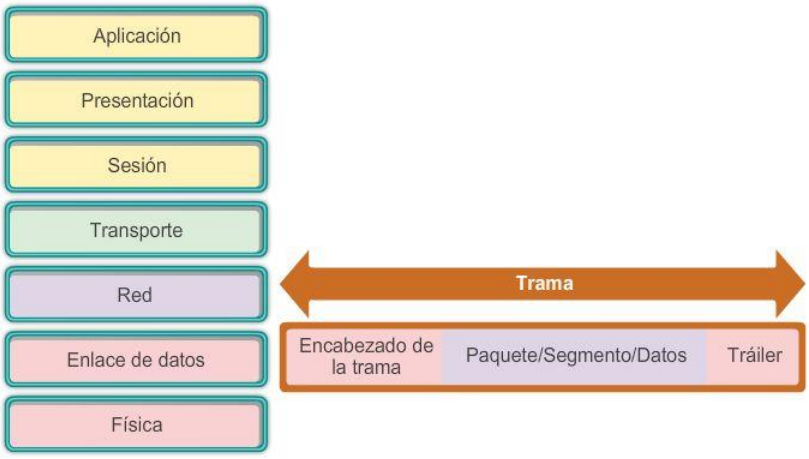
- ¿Qué nodos se comunican entre sí?

- ¿Cuándo comienza la comunicación entre los nodos individuales y cuándo termina?
- ¿Qué errores se produjeron mientras se comunicaron los nodos?
- ¿Qué nodos se comunicarán a continuación?

A diferencia de las otras PDU que se analizaron en este curso, las tramas de la capa de enlace de datos incluyen los siguientes elementos:

- Encabezado: contiene información de control, como direccionamiento, y está ubicado al comienzo de la PDU.
- Datos: contienen el encabezado IP, el encabezado de la capa de transporte y los datos de aplicación.
- Tráiler: contiene la información de control que se agrega al final de la PDU para la detección de errores.

Estos elementos de la trama se muestran en la ilustración y se analizarán con mayor detalle.



Capítulo 4: Acceso a la red 4.3.2.2 Creación de una trama

Cuando los datos viajan por los medios, se convierten en un stream de bits o en números 1 y 0. Si un nodo está recibiendo streams de bits largos ¿cómo determina dónde comienza y termina la trama o qué bits representan una dirección?

El tramado rompe el stream en agrupaciones descifrables, con la información de control insertada en el encabezado y tráiler como valores en campos diferentes. Este formato brinda a las señales físicas una estructura que pueden recibir los nodos y que se puede decodificar en paquetes en el destino.

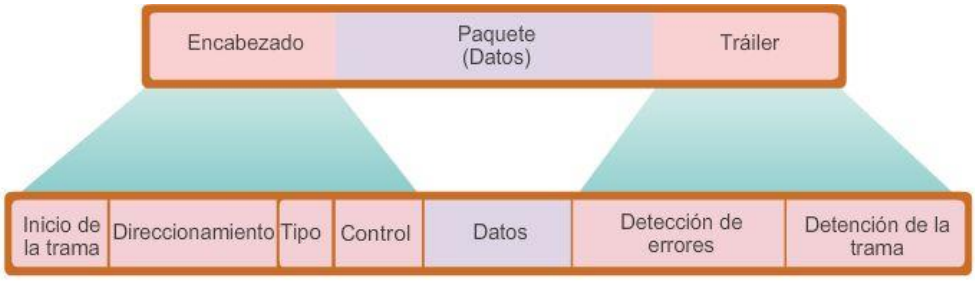
Como se muestra en la ilustración, los tipos de campos de trama genéricos incluyen lo siguiente:

- Indicadores de comienzo y de detención de la trama: la subcapa MAC utiliza estos campos para identificar el inicio y el final de la trama.
- Direccionamiento: la subcapa MAC utiliza este campo para identificar los nodos de origen y destino.
- Tipo: el LLC utiliza este campo para identificar el protocolo de capa 3.

- Control: identifica servicios especiales de control del flujo.
- Datos: incluye el contenido de la trama (es decir, el encabezado del paquete, el encabezado del segmento y los datos).
- Detección de errores: estos campos de trama, que se incluyen después de los datos para formar el tráiler, se utilizan para la detección de errores.

No todos los protocolos incluyen todos estos campos. Los estándares para un protocolo de enlace de datos específico definen el formato real de la trama.

Nota: los ejemplos de formatos de trama se analizarán al final de este capítulo.



Capítulo 4: Acceso a la red 4.3.3.1 Estándares de la capa de enlace de datos

A diferencia de los protocolos de las capas superiores de la suite TCP/IP, los protocolos de capa de enlace de datos no se suelen definir por la solicitud de comentarios (RFC). Si bien el Internet Engineering Task Force (IETF) mantiene los protocolos y servicios funcionales para la suite de protocolos TCP/IP en las capas superiores, no define las funciones ni la operación de la capa de acceso a la red de ese modelo.

Específicamente, los servicios y las especificaciones de la capa de enlace de datos se definen mediante varios estándares basados en diversas tecnologías y medios a los cuales se aplican los protocolos. Algunos de estos estándares integran los servicios de la Capa 2 y la Capa 1.

Los responsables de la definición de los protocolos y servicios funcionales en la capa de enlace de datos son los siguientes:

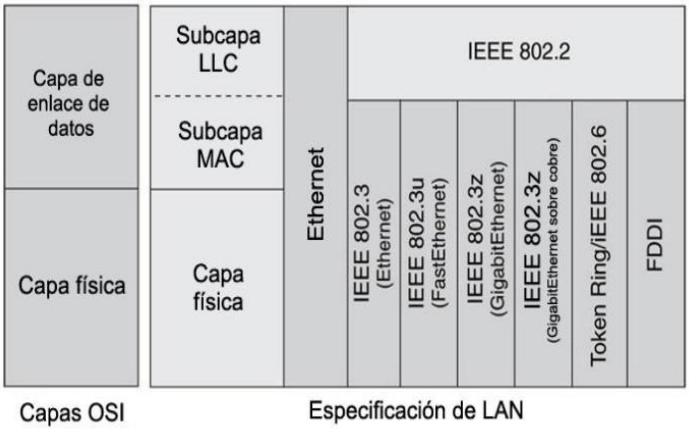
- Organismos de ingeniería que establecen estándares y protocolos públicos y abiertos.
- Compañías de comunicaciones que establecen y utilizan protocolos exclusivos para aprovechar los nuevos avances tecnológicos o las oportunidades del mercado.

Entre los organismos de ingeniería que definen estándares y protocolos abiertos que se aplican a la capa de enlace de datos, se incluyen:

- Instituto de Ingenieros en Electricidad y Electrónica (IEEE)
- Unión Internacional de Telecomunicaciones (UIT)
- Organización Internacional para la Estandarización (ISO)
- American National Standards Institute (ANSI)

En la tabla de la ilustración, se destacan diversos organismos de estandarización y algunos de sus protocolos de capa de enlace de datos más importantes.

Organismo de estandarización	Estándares de red
IEEE	• 802.2: Control de enlace lógico (LLC) • 802.3: Ethernet • 802.4: Token bus • 802.5: Token Ring • 802.11: LAN inalámbrica (WLAN) y malla (certificación Wi-Fi) • 802.15: Bluetooth • 802.16: WiMax
ITU-T	• G.992: ADSL • G.8100 - G.8199: aspectos de MPLS de transporte • Q.921: ISDN • Q.922: Frame Relay
ISO	• Control de enlace de datos de alto nivel (HDLC) • ISO 9314: Control de acceso al medio (MAC) de la FDDI
ANSI	• X3T9.5 y X3T12: Interfaz de datos distribuida por fibra (FDDI)



Capítulo 4: Acceso a la red 4.4.1.1 Control de acceso a los medios

La regulación de la ubicación de las tramas de datos en los medios se encuentra bajo el control de la subcapa de control de acceso al medio.

El control de acceso al medio es el equivalente a las reglas de tránsito que regulan la entrada de vehículos a una autopista. La ausencia de un control de acceso al medio sería el equivalente a vehículos que ignoren el resto del tráfico e ingresen al camino sin tener en cuenta a los demás vehículos. Sin embargo, no todos los caminos y entradas son iguales.

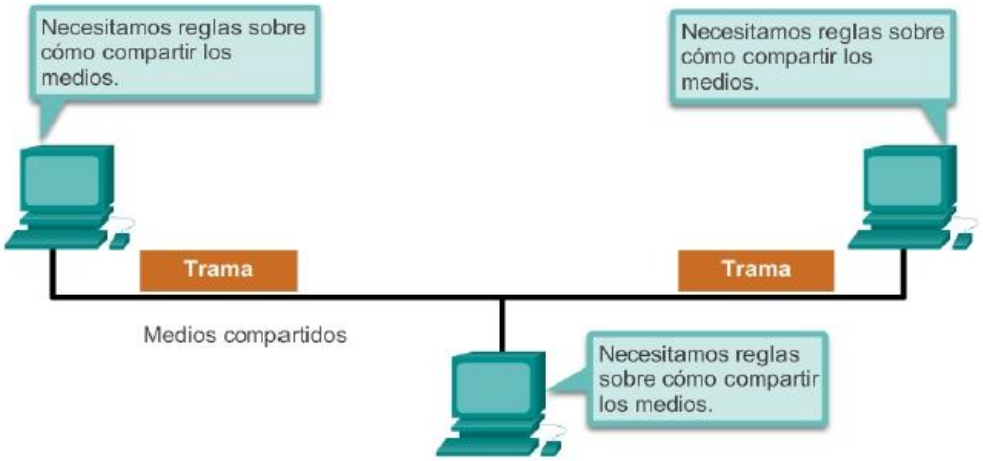
El tráfico puede ingresar a un camino confluyendo, esperando su turno en una señal de parada o respetando el semáforo. Un conductor sigue un conjunto de reglas diferente para cada tipo de entrada.

De la misma manera, existen diferentes formas de regular la colocación de tramas en los medios. Los protocolos de la capa de enlace de datos definen las reglas de acceso a los diferentes medios. Algunos métodos de control de acceso al medio utilizan procesos altamente controlados para asegurar que las tramas se coloquen con seguridad en los medios. Estos métodos se definen mediante protocolos sofisticados que requieren mecanismos que introducen sobrecargas a la red.

Entre las diferentes implementaciones de los protocolos de capa de enlace de datos, existen diferentes métodos para controlar el acceso al medio. Estas técnicas de control de acceso al medio definen si los nodos comparten los medios y de qué manera lo hacen.

El método específico de control de acceso al medio utilizado depende de lo siguiente:

- Topología: cómo aparece la conexión entre los nodos ante la capa de enlace de datos.
- Uso compartido de los medios: la forma en que los nodos comparten los medios. El uso compartido de los medios puede ser punto a punto, como en las conexiones WAN, o compartido, como en las redes LAN.



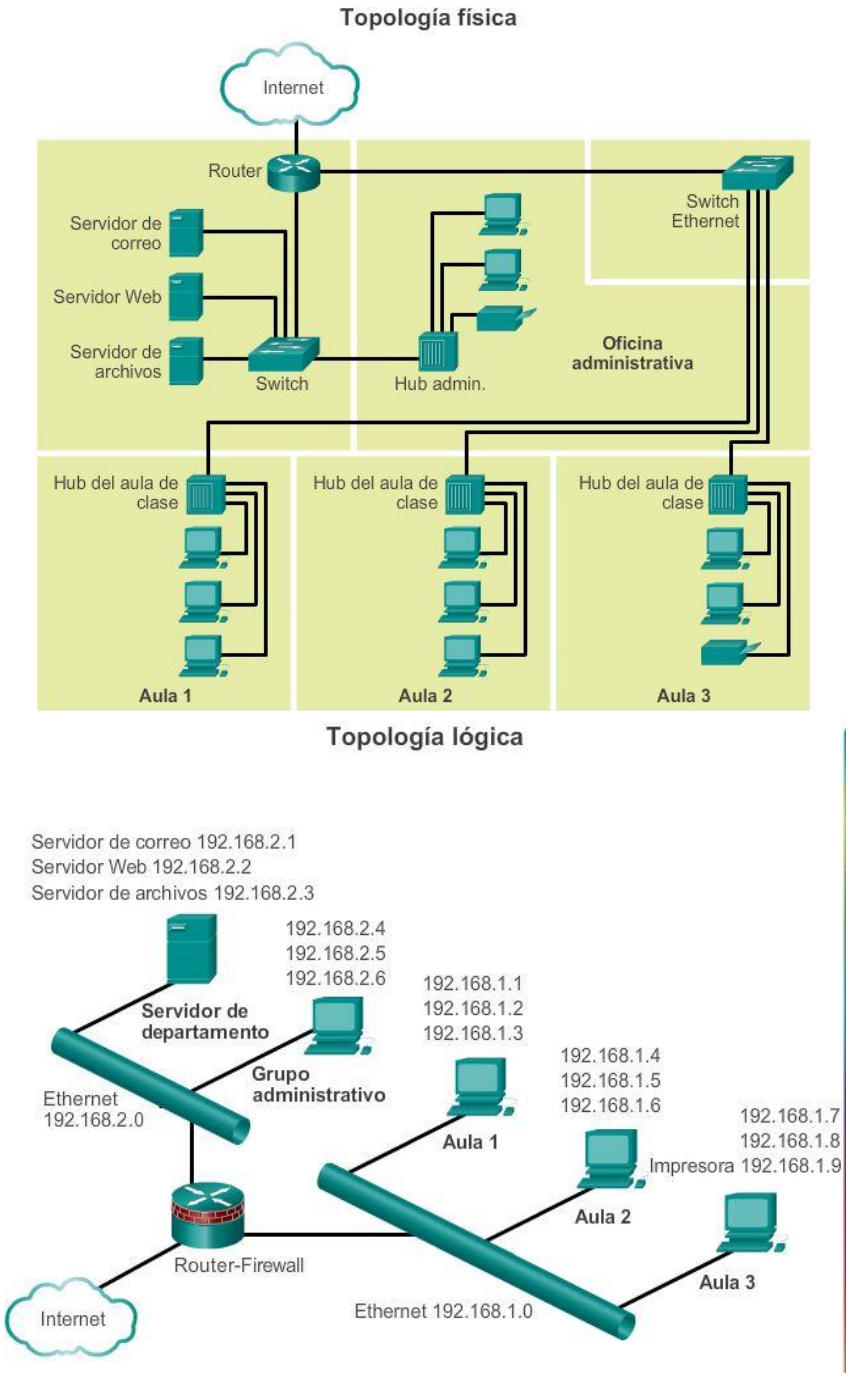
Capítulo 4: Acceso a la red 4.4.1.2 Topologías física y lógica

La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías LAN y WAN se pueden ver de dos maneras:

- Topología física: se refiere a las conexiones físicas e identifica cómo se interconectan los dispositivos finales y de infraestructura, como los routers, los switches y los puntos de acceso inalámbrico. Las topologías físicas generalmente son punto a punto o en estrella. Consulte la Figura 1.
- Topología lógica: se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas.

  La topología lógica de los enlaces punto a punto es relativamente simple, mientras que los medios compartidos ofrecen métodos de control de acceso al medio deterministas y no deterministas. Vea la Figura 2.

La capa de enlace de datos “ve” la topología lógica de una red al controlar el acceso de los datos al medio. La topología lógica influye en el tipo de entramado de red y el control de acceso al medio que se utilizan.



Capítulo 4: Acceso a la red 4.4.2.1 Topologías físicas de WAN comunes

Por lo general, las WAN se interconectan mediante las siguientes topologías físicas:

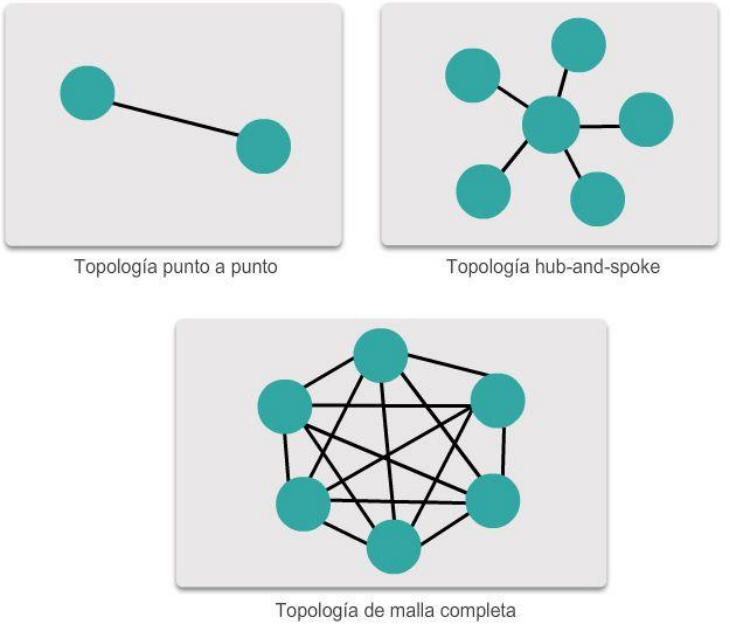
- Punto a punto: esta es la topología más simple, que consta de un enlace permanente entre dos terminales. Por este motivo, es una topología de WAN muy popular.

- Hub-and-spoke: es una versión WAN de la topología en estrella, en la que un sitio central interconecta sitios de sucursal mediante enlaces punto a punto.

- Malla: esta topología proporciona alta disponibilidad, pero requiere que cada sistema final esté interconectado con todos los demás sistemas. Por lo tanto, los costos administrativos y físicos pueden ser importantes. Básicamente, cada enlace es un enlace punto a punto al otro nodo. Las variantes de

esta topología incluyen la topología de malla parcial, en la que se interconectan algunos dispositivos finales, pero no todos.

En la ilustración, se muestran las tres topologías físicas de WAN comunes.



Capítulo 4: Acceso a la red 4.4.2.2 Topología física punto a punto

Las topologías físicas punto a punto conectan dos nodos directamente, como se muestra en la ilustración.

En esta disposición, los dos nodos no tienen que compartir los medios con otros hosts. Además, un nodo no tiene que determinar si una trama entrante está destinada a él o a otro nodo. Por lo tanto, los protocolos de enlace de datos lógicos pueden ser muy simples, dado que todas las tramas en los medios solo pueden transferirse entre los dos nodos. El nodo en un extremo coloca las tramas en los medios y el nodo en el otro extremo las saca de los medios del circuito punto a punto.

Los protocolos de capa de enlace de datos podrían proporcionar procesos más sofisticados de control de acceso al medio para las topologías lógicas punto a punto, pero esto solo agregaría una sobrecarga innecesaria al protocolo.

Capítulo 4: Acceso a la red 4.4.2.3 Topología lógica punto a punto

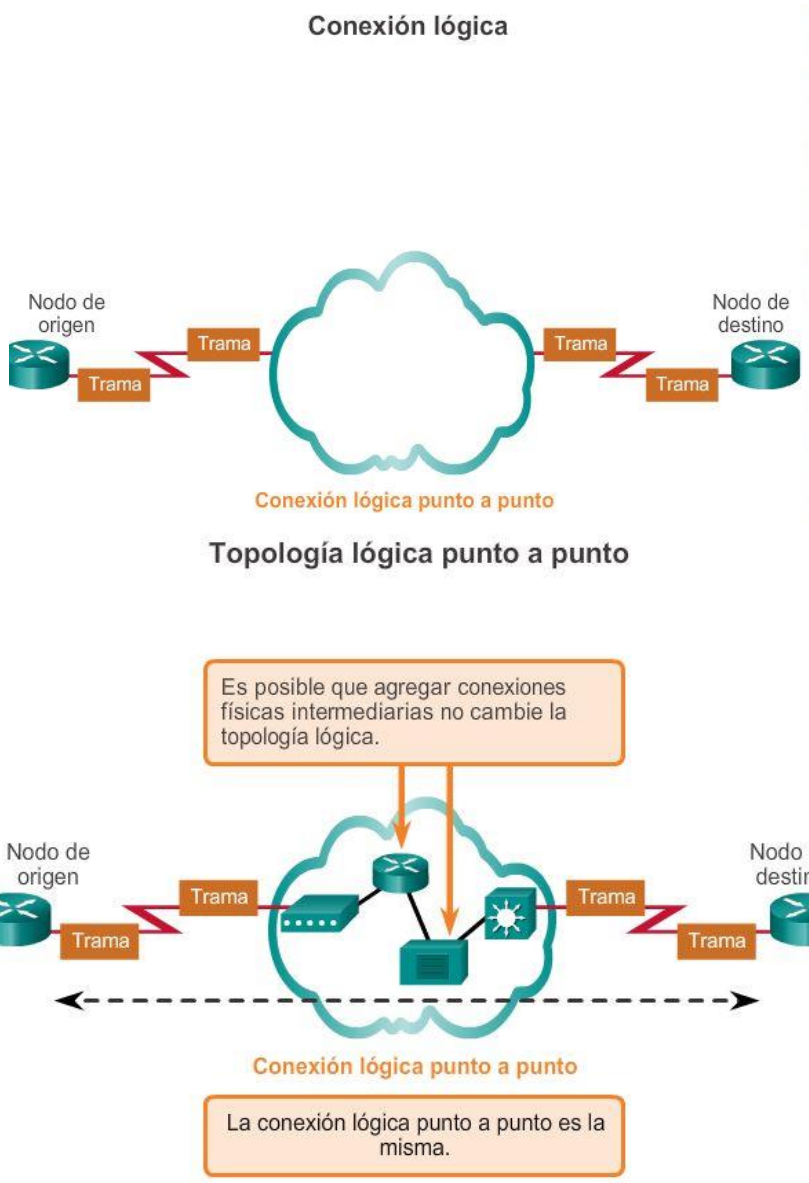
Los nodos de los extremos que se comunican en una red punto a punto pueden estar conectados físicamente a través de una cantidad de dispositivos intermediarios. Sin embargo, el uso de dispositivos físicos en la red no afecta la topología lógica.

Como se muestra en la figura 1, los nodos de origen y destino pueden estar conectados indirectamente entre sí a través de una distancia geográfica. En algunos casos, la conexión lógica entre nodos forma lo que se llama un circuito virtual. Un circuito virtual es una conexión lógica creada dentro de una red entre dos dispositivos de red. Los dos nodos en cada extremo del circuito virtual intercambian las tramas entre sí.

Esto ocurre incluso si las tramas están dirigidas a través de dispositivos intermediarios. Los circuitos virtuales son construcciones de comunicación lógicas utilizadas por algunas tecnologías de la Capa 2.

El método de acceso al medio utilizado por el protocolo de enlace de datos depende de la topología lógica punto a punto, no de la topología física. Esto significa que la conexión lógica de punto a punto entre dos nodos puede no ser necesariamente entre dos nodos físicos en cada extremo de un enlace físico único.

En la figura 2, se muestran los dispositivos físicos entre los dos routers.



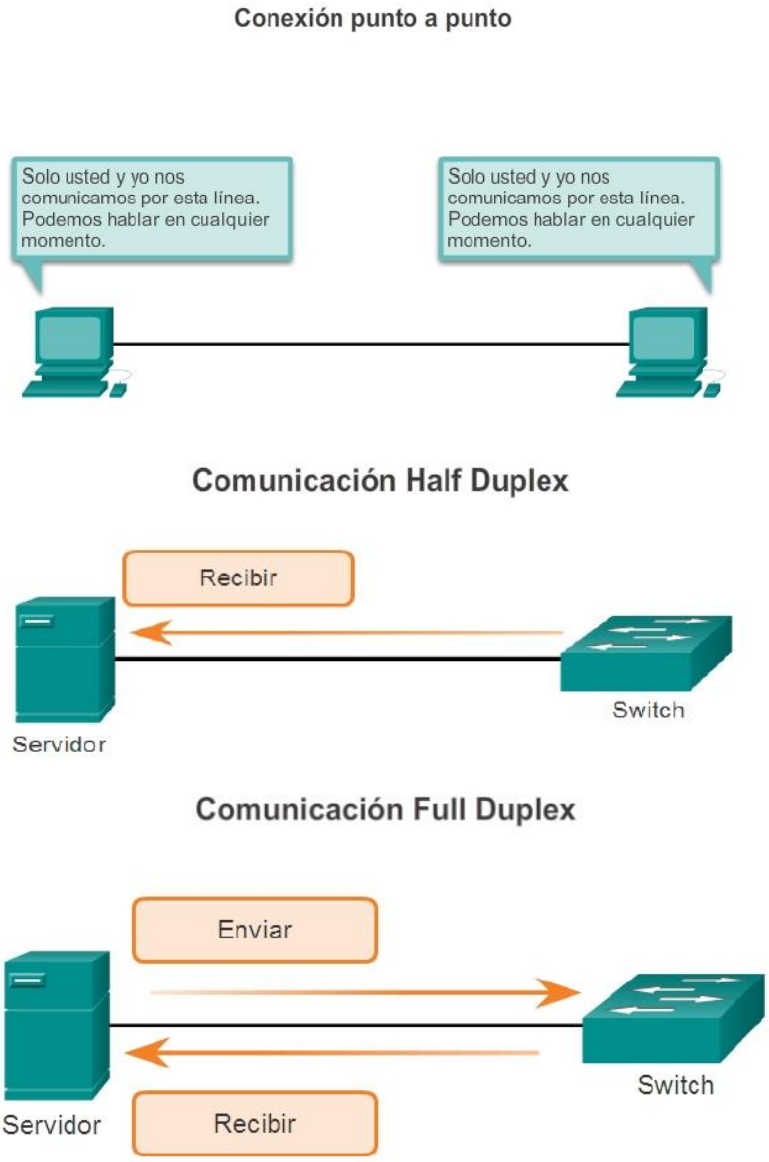
Capítulo 4: Acceso a la red 4.4.2.4 Half duplex y full dúplex

En la figura 1, se muestra una topología punto a punto. En las redes punto a punto, los datos pueden fluir de dos maneras:

- Comunicación half-duplex: ambos dispositivos pueden transmitir y recibir datos en los medios, pero no pueden hacerlo en forma simultánea. Ethernet ha establecido reglas de arbitraje para resolver conflictos que surgen de instancias donde más de una estación intenta transmitir al mismo tiempo. En la figura 2, se muestra la comunicación half-duplex.

- Comunicación full-duplex: ambos dispositivos pueden transmitir y recibir datos en los medios al mismo tiempo. La capa de enlace de datos supone que los medios están disponibles para que ambos nodos

transmitan en cualquier momento. Por lo tanto, no hay necesidad de arbitraje de medios en la capa de enlace de datos. En la figura 3, se muestra la comunicación full-duplex.



Capítulo 4: Acceso a la red 4.4.3.1 Topologías físicas de LAN

La topología física define cómo se interconectan físicamente los sistemas finales. En las redes LAN de medios compartidos, los dispositivos finales se pueden interconectar mediante las siguientes topologías físicas:

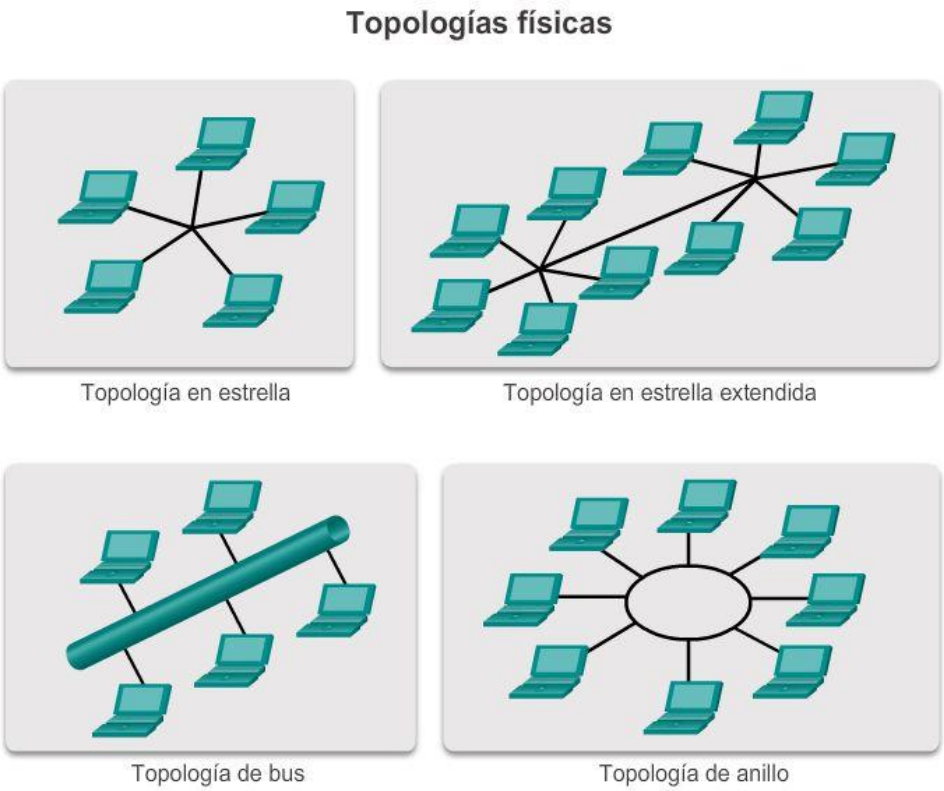
- Estrella: los dispositivos finales se conectan a un dispositivo intermediario central. Las primeras topologías en estrella interconectaban dispositivos finales mediante hubs. Sin embargo, en la actualidad estas topologías utilizan switches. La topología en estrella es la topología física de LAN más común, principalmente porque es fácil de instalar, muy escalable (es fácil agregar y quitar dispositivos finales) y de fácil resolución de problemas.

- Estrella extendida o híbrida: en una topología en estrella extendida, dispositivos intermediarios centrales interconectan otras topologías en estrella. En una topología híbrida, las redes en estrella se pueden interconectar mediante una topología de bus.

- Bus: todos los sistemas finales se encadenan entre sí y terminan de algún modo en cada extremo. No se requieren dispositivos de infraestructura, como switches, para interconectar los dispositivos finales. Las topologías de bus se utilizaban en las antiguas redes Ethernet, porque eran económicas y fáciles de configurar.

- Anillo: los sistemas finales se conectan a su respectivo vecino y forman un anillo. A diferencia de la topología de bus, la de anillo no necesita tener una terminación. Las topologías de anillo se utilizaban en las antiguas redes de interfaz de datos distribuida por fibra (FDDI). Específicamente, las redes FDDI emplean un segundo anillo para la tolerancia a fallas o para mejorar el rendimiento.

En la ilustración, se muestra cómo se interconectan los dispositivos finales en las redes LAN.



Capítulo 4: Acceso a la red 4.4.3.2 Topología lógica para medios compartidos

La topología lógica de una red está estrechamente relacionada con el mecanismo que se utiliza para administrar el acceso a la red. Los métodos de acceso proporcionan los procedimientos para administrar el acceso a la red para que todas las estaciones tengan acceso. Cuando varias entidades comparten los mismos medios, deben estar instalados algunos mecanismos para controlar el acceso. Los métodos de acceso se aplican en las redes para regular dicho acceso al medio.

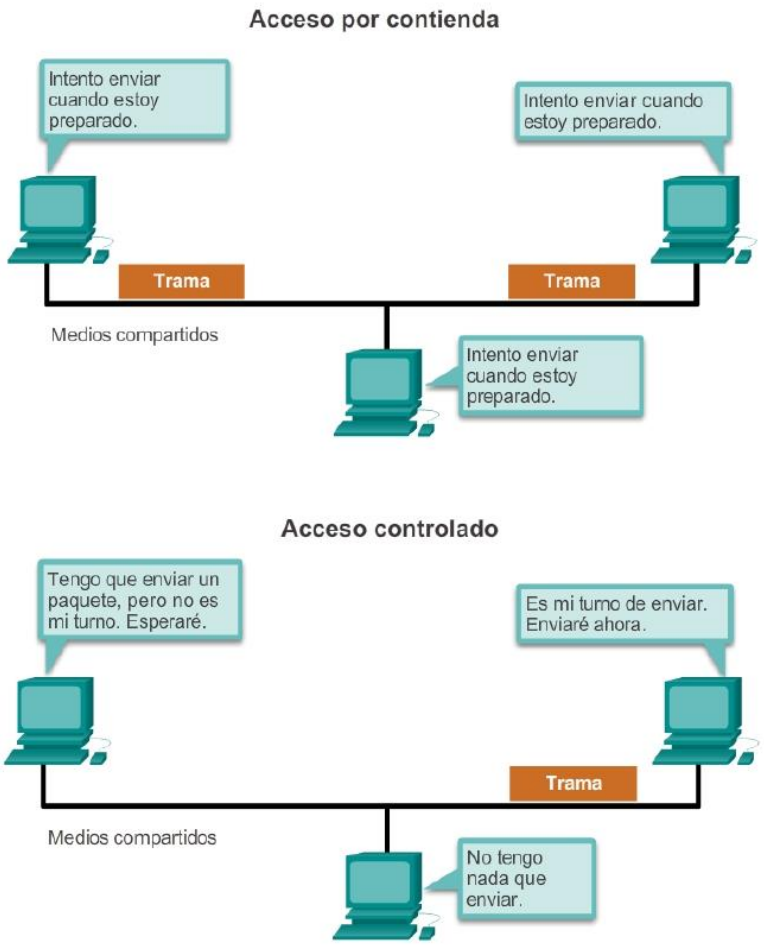
Algunas topologías de red comparten un medio común con varios nodos. En cualquier momento puede haber una cantidad de dispositivos que intentan enviar y recibir datos utilizando los medios de red. Hay reglas que rigen cómo esos dispositivos comparten los medios.

Hay dos métodos básicos de control de acceso al medio para medios compartidos:

- Acceso por contienda: todos los nodos compiten por el uso del medio, pero tienen un plan si se producen colisiones. En la figura 1, se muestra el acceso por contienda.

- Acceso controlado: cada nodo tiene su propio tiempo para utilizar el medio. En la figura 2, se muestra el acceso controlado.

El protocolo de capa de enlace de datos especifica el método de control de acceso al medio que proporciona el equilibrio adecuado entre control de trama, protección de trama y sobrecarga de red.



Capítulo 4: Acceso a la red 4.4.3.3 Acceso por contienda

Al utilizar un método de contienda no determinista, los dispositivos de red pueden intentar acceder al medio cada vez que tengan datos para enviar. Para evitar caos completo en los medios, estos métodos usan un proceso de Acceso múltiple por detección de portadora (CSMA) para detectar primero si los medios están transportando una señal.

Si se detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo está transmitiendo. Cuando un dispositivo está intentando transmitir y nota que el medio está ocupado, esperará e intentará después de un período de tiempo corto. Si no se detecta una señal portadora, el dispositivo transmite sus datos. Las redes Ethernet e inalámbricas utilizan control de acceso al medio por contención.

Es posible que el proceso de CSMA falle y que dos dispositivos transmitan al mismo tiempo y ocasionen una colisión de datos. Si esto ocurre, los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Los métodos de control de acceso al medio por contención no tienen la sobrecarga de los métodos de acceso controlado. No se requiere un mecanismo para analizar quién posee el turno para acceder al medio. Sin embargo, los sistemas por contención no escalan bien bajo un uso intensivo de los medios. A medida que el

uso y el número de nodos aumenta, la probabilidad de acceder a los medios con éxito sin una colisión disminuye. Además, los mecanismos de recuperación que se requieren para corregir errores debidos a esas colisiones disminuyen aún más el rendimiento.

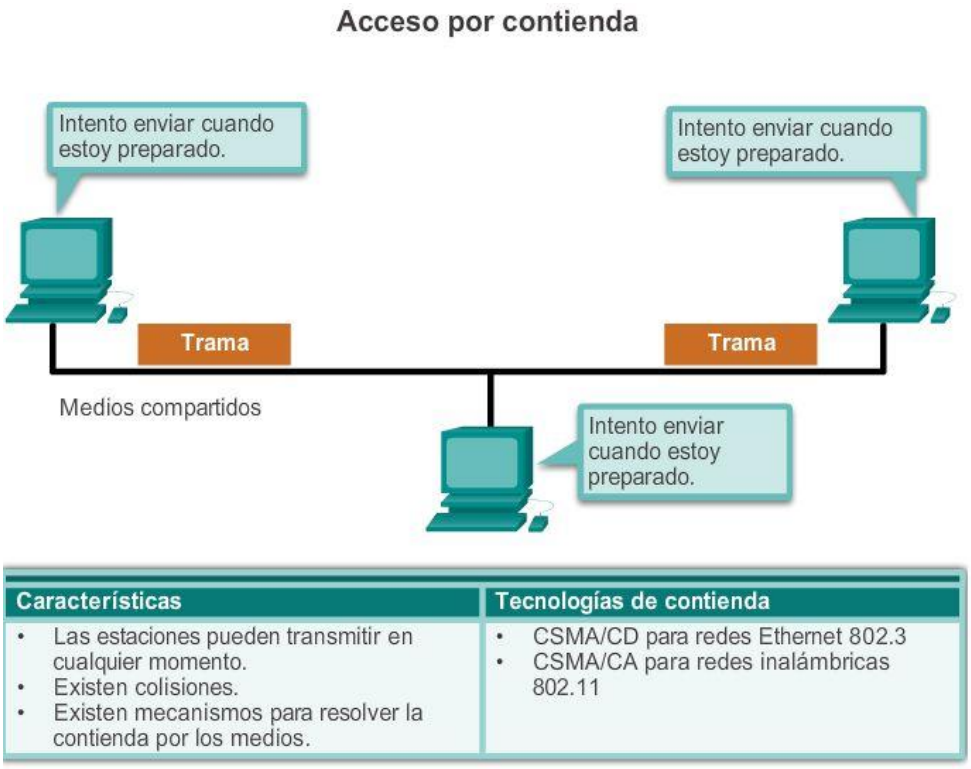
Generalmente se implementa CSMA junto con un método para resolver la contención del medio. Los dos métodos comúnmente utilizados son:

- Acceso múltiple por detección de portadora con detección de colisiones:con el acceso múltiple por detección de portadora y detección de colisiones (CSMA/CD), el dispositivo final supervisa los medios para detectar la presencia de una señal de datos. Si no hay una señal de datos y, en consecuencia, los medios están libres, el dispositivo transmite los datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet utilizan este método.

- Acceso múltiple por detección de portadora y prevención de colisiones:con el acceso múltiple por detección de portadora y prevención de colisiones (CSMA/CA), el dispositivo final examina los medios para detectar la presencia de una señal de datos. Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo. Una vez que recibe autorización para transmitir, el dispositivo envía los datos. Las tecnologías de red inalámbricas 802.11 utilizan este método.

En la ilustración, se muestra lo siguiente:

- Funcionamiento de los métodos de acceso por contienda
- Características de los métodos de acceso por contienda
- Ejemplos de los métodos de acceso por contienda

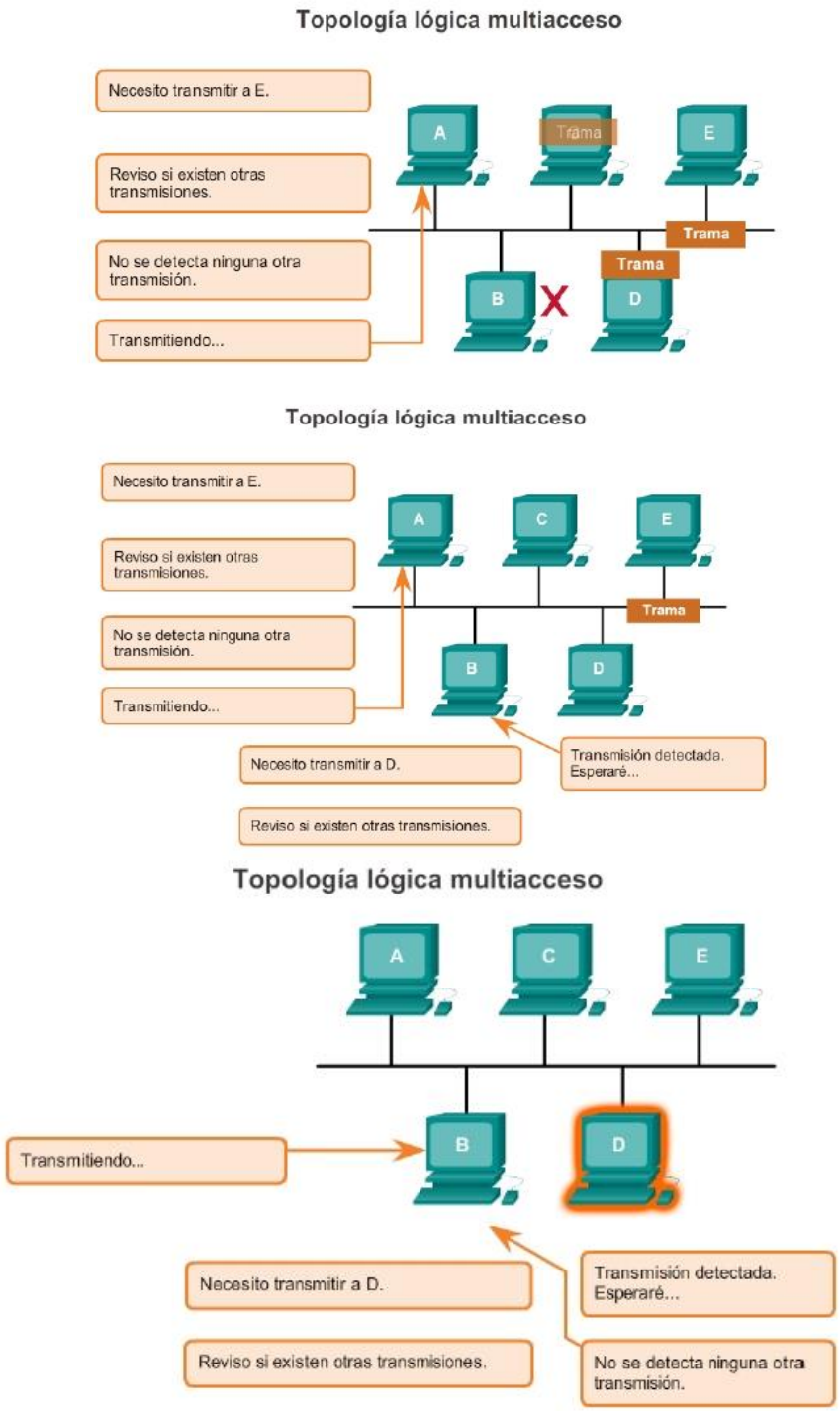


Capítulo 4: Acceso a la red 4.4.3.4 Topología multiacceso

Una topología lógica multiacceso permite a una cantidad de nodos comunicarse utilizando los mismos medios compartidos. Los datos desde un sólo nodo pueden colocarse en el medio en cualquier momento. Cada nodo ve todas las tramas que se encuentran en el medio, pero solamente el nodo al cual se dirige la trama procesa sus contenidos.

Tener muchos nodos que compartan el acceso al medio requiere un método de control de acceso al medio de enlace de datos que regule la transmisión de los datos y, por consiguiente, que reduzca las colisiones entre las distintas señales.

Reproduzca la animación para ver cómo los nodos acceden a los medios en una topología multiacceso.



Capítulo 4: Acceso a la red 4.4.3.5 Acceso controlado

Al utilizar el método de acceso controlado, los dispositivos de red toman turnos en secuencia para acceder al medio. Si un dispositivo final no necesita acceder al medio, el turno pasa al dispositivo final siguiente. Este proceso se facilita por medio de un token. Un dispositivo final adquiere el token y coloca una trama en los medios; ningún otro dispositivo puede hacerlo hasta que la trama se haya recibido y procesado en el destino, y se libere el token.

Nota: este método también se conoce como “acceso programado” o “determinista”.

Aunque el acceso controlado está bien ordenado y provee rendimiento predecible, los métodos determinísticos pueden ser ineficientes porque un dispositivo tiene que esperar su turno antes de poder utilizar el medio.

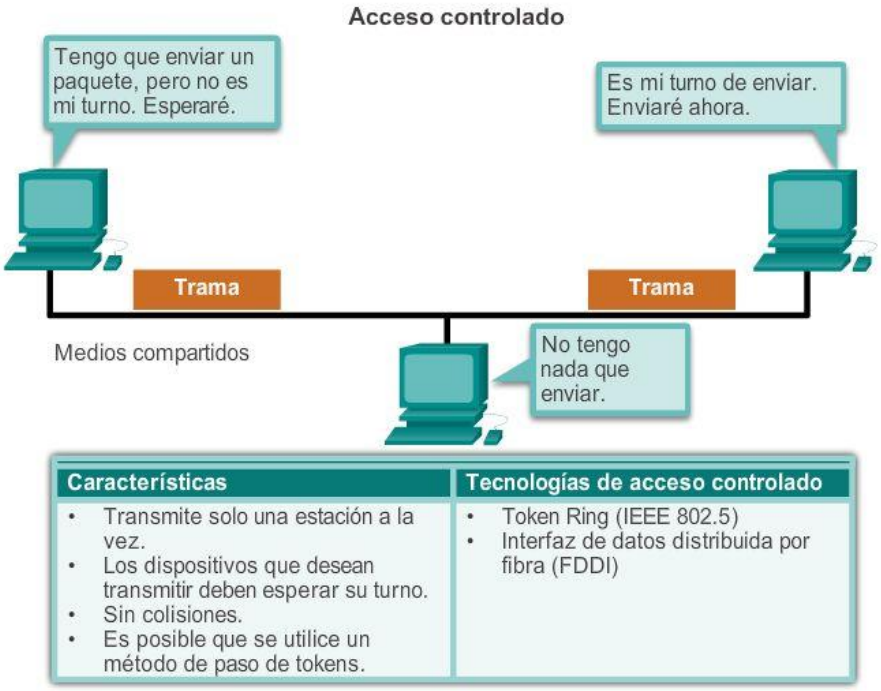
Los ejemplos de acceso controlado incluyen lo siguiente:

- Token Ring (IEEE 802.5)
- Interfaz de datos distribuida por fibra (FDDI), que se basa en el protocolo de token bus IEEE 802.4.

Nota: estos dos métodos de control de acceso al medio se consideran obsoletos.

En la ilustración, se muestra lo siguiente:

- Funcionamiento de los métodos de acceso controlado
- Características de los métodos de acceso controlado
- Ejemplos de métodos de acceso controlado



Capítulo 4: Acceso a la red 4.4.3.6 Topología de anillo

En una topología lógica de anillo, cada nodo recibe una trama por turno. Si la trama no está direccionada al nodo, el nodo pasa la trama al nodo siguiente. Esto permite que un anillo utilice una técnica de control de acceso al medio controlado que se denomina “paso de tokens”.

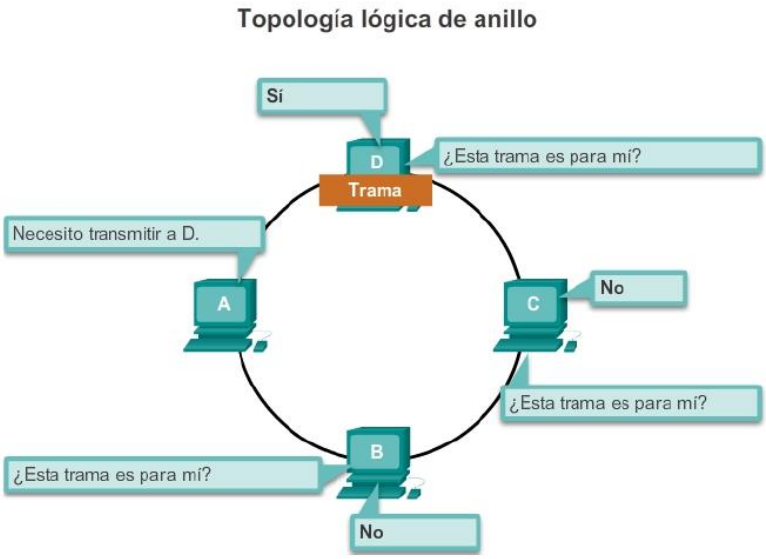
Los nodos en una topología lógica de anillo retiran la trama del anillo, examinan la dirección y la envían si no está dirigida para ese nodo. En un anillo, todos los nodos alrededor del anillo (entre el nodo de origen y el de destino) examinan la trama.

Existen diversas técnicas de control de acceso al medio que pueden usarse con un anillo lógico, según el nivel de control requerido. Por ejemplo: sólo una trama a la vez es generalmente transportada por el medio. Si no

se están transmitiendo datos, se colocará una señal (conocida como token) en el medio y un nodo sólo puede colocar una trama de datos en el medio cuando tiene el token.

Recuerde que la capa de enlace de datos “ve” una topología lógica de anillo. La topología del cableado físico real puede ser otra topología.

Reproduzca la animación para ver cómo acceden los nodos al medio en una topología lógica de anillo.



Capítulo 4: Acceso a la red 4.4.4.1 La trama

Si bien existen muchos protocolos de capa de enlace de datos diferentes que describen las tramas de la capa de enlace de datos, cada tipo de trama tiene tres partes básicas:

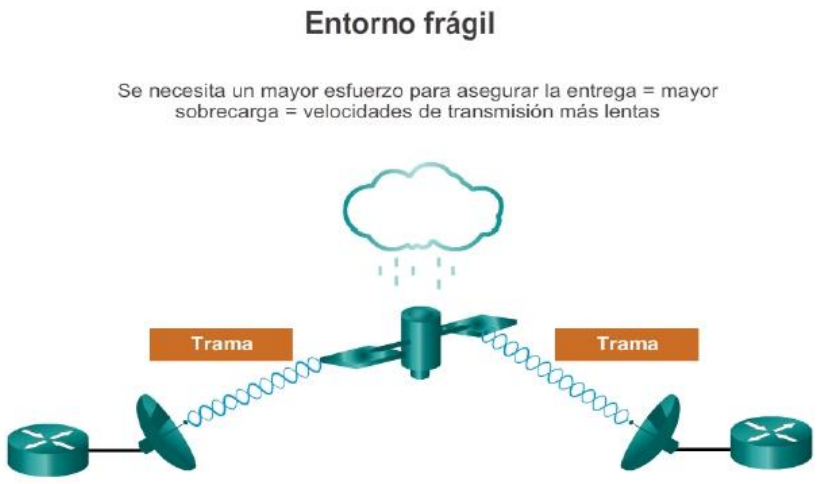
- Encabezado
- Datos
- Tráiler

Todos los protocolos de capa de enlace de datos encapsulan la PDU de la capa 3 dentro del campo de datos de la trama. Sin embargo, la estructura de la trama y los campos contenidos en el encabezado y tráiler varían de acuerdo con el protocolo.

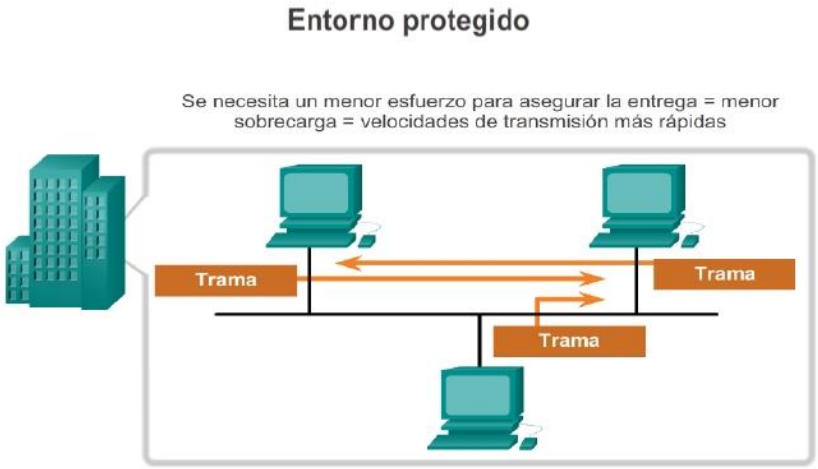
El protocolo de capa de enlace de datos describe las características requeridas para el transporte de paquetes a través de diferentes medios. Estas características del protocolo están integradas en la encapsulación de la trama. Cuando la trama llega a su destino y el protocolo de enlace de datos quita la trama de los medios, la información sobre el entramado se lee y se descarta.

No hay una estructura de trama que cumpla con las necesidades de todos los transportes de datos a través de todos los tipos de medios. Según el entorno, la cantidad de información de control que se necesita en la trama varía para cumplir con los requisitos de control de acceso al medio de la topología lógica y de los medios.

Como se muestra en la figura 1, un entorno frágil requiere más control. Sin embargo, un entorno protegido, como el que se muestra en la figura 2, requiere menos controles.



En un **entorno frágil**, se necesitan más controles para asegurar una entrega. Los campos de encabezado y de tráiler son más grandes, ya que se necesita más información de control.



En un **entorno protegido**, podemos confiar en que la trama llegue a destino. Se necesitan menos controles, lo que tiene como resultado tramas y campos más pequeños.

Capítulo 4: Acceso a la red 4.4.4.2 El encabezado

El encabezado de la trama contiene la información de control que especifica el protocolo de capa de enlace de datos para la topología lógica y los medios específicos utilizados.

La información de control de trama es única para cada tipo de protocolo. Es utilizada por el protocolo de la Capa 2 para proporcionar las características demandadas por el entorno de comunicación.

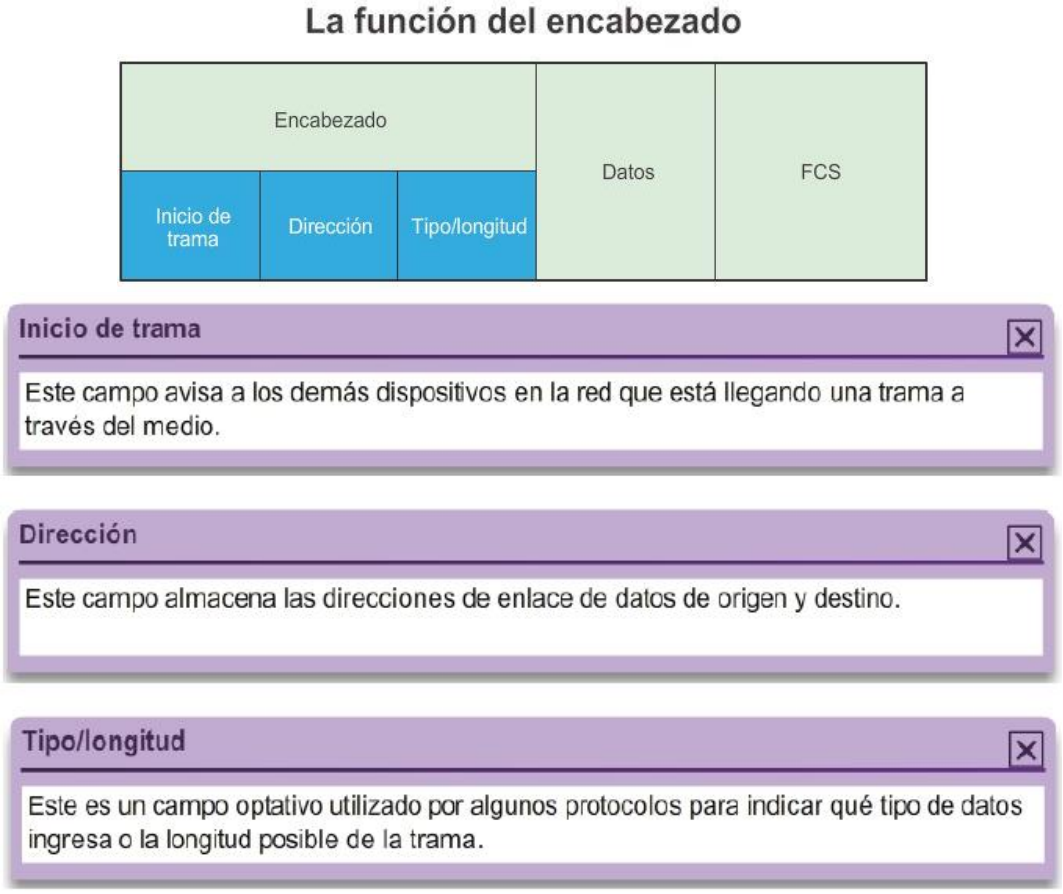
En la ilustración, se muestran los campos de encabezado de la trama de Ethernet:

- Campo Inicio de trama: indica el comienzo de la trama.
- Campos Dirección de origen y Dirección de destino: indican los nodos de origen y destino en los medios.
- Campo Tipo: indica el servicio de capa superior que se incluye en la trama.

Los distintos protocolos de capa de enlace de datos pueden utilizar campos diferentes de los mencionados. Por ejemplo, otros campos de encabezado de trama de protocolo de capa 2 podrían incluir los siguientes:

- Campo Prioridad/Calidad de servicio: indica un tipo específico de servicio de comunicación para el procesamiento.
- Campo Control de conexión lógica: se utiliza para establecer una conexión lógica entre nodos.
- Campo Control de enlace físico: se utiliza para establecer el enlace con los medios.
- Campo Control del flujo: se utiliza para iniciar y detener el tráfico a través de los medios.
- Campo Control de congestión: indica si hay congestión en los medios.

Debido a que los propósitos y las funciones de los protocolos de capa de enlace de datos se relacionan con las topologías y los medios específicos, se debe examinar cada protocolo para comprender en detalle la estructura de la trama. Como los protocolos se analizan en este curso, se explicará más información acerca de la estructura de la trama.



Capítulo 4: Acceso a la red 4.4.4.3 Dirección de capa 2

La capa de enlace de datos proporciona el direccionamiento que se utiliza para transportar una trama a través de los medios locales compartidos. Las direcciones de dispositivo en esta capa se llaman direcciones físicas.

El direccionamiento de la capa de enlace de datos se incluye en el encabezado de la trama y especifica el nodo de destino de la trama en la red local. El encabezado de la trama también puede contener la dirección de origen de la trama.

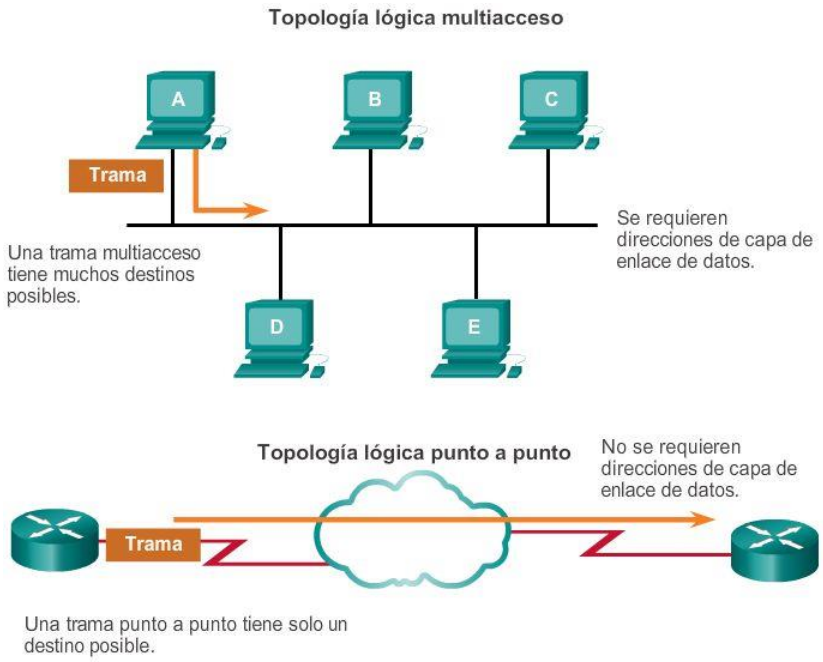
A diferencia de las direcciones lógicas de capa 3, que son jerárquicas, las direcciones físicas no indican en qué red se encuentra el dispositivo.

En cambio, la dirección física es la dirección específica de un dispositivo en particular. Si el dispositivo se traslada a otra red o subred, sigue funcionando con la misma dirección física de la Capa 2.

No se puede utilizar una dirección específica de un dispositivo y no jerárquica para localizar un dispositivo a través de grandes redes o de Internet. Eso sería como intentar localizar una casa específica en todo el mundo, sin más datos que el nombre de la calle y el número de la casa. Sin embargo, la dirección física se puede usar para localizar un dispositivo dentro de un área limitada. Por este motivo, la dirección de la capa de enlace de datos solo se utiliza para entregas locales. Las direcciones en esta capa no tienen significado más allá de la red local. Compare esto con la Capa 3, en donde las direcciones en el encabezado del paquete pasan del host de origen al host de destino sin tener en cuenta la cantidad de saltos de redes a lo largo de la ruta.

Si los datos deben pasar a otro segmento de red, se necesita un dispositivo intermediario, como un router. El router debe aceptar la trama según la dirección física y desencapsularla para examinar la dirección jerárquica, o dirección IP. Con la dirección IP, el router puede determinar la ubicación de red del dispositivo de destino y el mejor camino para llegar a él. Una vez que sabe adónde reenviar el paquete, el router crea una nueva trama para el paquete, y la nueva trama se envía al segmento siguiente hacia el destino final.

En la ilustración, se destacan los requisitos de dirección de capa 2 en las topologías multiacceso y punto a punto.



Capítulo 4: Acceso a la red 4.4.4.4 El tráiler

Los protocolos de capa de enlace de datos agregan un tráiler al final de cada trama. El tráiler se utiliza para determinar si la trama llegó sin errores. Este proceso se denomina “detección de errores” y se logra mediante la colocación en el tráiler de un resumen lógico o matemático de los bits que componen la trama. La detección de errores se agrega a la capa de enlace de datos porque las señales en los medios pueden sufrir interferencias, distorsiones o pérdidas que cambien considerablemente los valores de bits que representan esas señales.

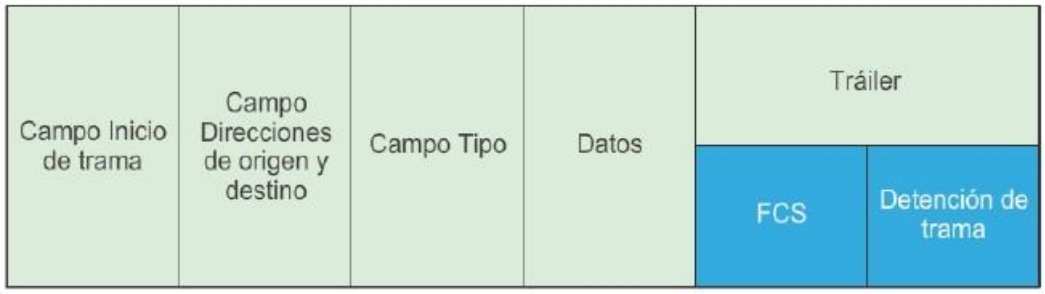
Un nodo transmisor crea un resumen lógico del contenido de la trama. Esto se conoce como valor de comprobación de redundancia cíclica (CRC). Este valor se coloca en el campo Secuencia de verificación de la trama (FCS) para representar el contenido de la trama.

Haga clic en los campos FCS y Detención de trama en la ilustración para obtener más detalles.

Cuando la trama llega al nodo de destino, el nodo receptor calcula su propio resumen lógico, o CRC, de la trama. El nodo receptor compara los dos valores CRC. Si los dos valores son iguales, se considera que la trama llegó como se transmitió. Si el valor CRC en el FCS difiere del CRC calculado en el nodo receptor, la trama se descarta.

Por lo tanto, el campo FCS se utiliza para determinar si se produjeron errores durante la transmisión y la recepción de la trama. El mecanismo de detección de errores proporcionado por el uso del campo FCS descubre la mayoría de los errores provocados en los medios.

Existe siempre la pequeña posibilidad de que una trama con un buen resultado de CRC esté realmente dañada. Los errores en los bits se pueden cancelar entre sí cuando se calcula el CRC. Los protocolos de capa superior entonces deberían detectar y corregir esta pérdida de datos.



Secuencia de verificación de trama

Este campo se utiliza para la verificación de errores. El origen calcula un número en función de los datos de la trama y coloca ese numero en el campo FCS. El destino, entonces, recalcula los datos para determinar si FCS coincide. Si no coinciden, el destino elimina la trama.

Detención de trama

Este campo, también denominado "Tráiler de la trama", es un campo optativo que se utiliza cuando no se especifica la longitud de la trama en el campo Tipo/Longitud. Indica el final de una trama cuando ya se transmitió.

Capítulo 4: Acceso a la red 4.4.4.5 Tramas LAN y WAN

En una red TCP/IP, todos los protocolos de capa 2 del modelo OSI funcionan con la dirección IP en la capa 3. Sin embargo, el protocolo de capa 2 específico que se utilice depende de la topología lógica de la red y la implementación de la capa física. Debido al amplio rango de medios físicos utilizados a través de un rango de topologías en interconexión de redes, hay una gran cantidad correspondiente de protocolos de la Capa 2 en uso.

Cada protocolo lleva a cabo el control de acceso al medio para las topologías lógicas de capa 2 especificadas. Esto significa que una cantidad de dispositivos de red diferentes pueden actuar como nodos que operan en la capa de enlace de datos al implementar esos protocolos. Estos dispositivos incluyen el adaptador de red o tarjetas de interfaz de red (NIC) en computadoras, así como las interfaces en routers y en switches de la Capa 2.

El protocolo de la Capa 2 que se utiliza para una topología de red particular está determinado por la tecnología utilizada para implementar esa topología. La tecnología es, a su vez, determinada por el tamaño de la red, en términos de cantidad de hosts y alcance geográfico y los servicios que se proveerán a través de la red.

En general, las redes LAN utilizan una tecnología de ancho de banda elevado que es capaz de admitir una gran cantidad de hosts. El área geográfica relativamente pequeña de una LAN (un único edificio o un campus de varios edificios) y su alta densidad de usuarios hacen que esta tecnología sea rentable.

Sin embargo, utilizar una tecnología de ancho de banda elevado generalmente no es rentable para las redes WAN que abarcan grandes áreas geográficas (varias ciudades, por ejemplo). El costo de los enlaces físicos de larga distancia y la tecnología utilizada para transportar las señales a través de esas distancias, generalmente, ocasiona una menor capacidad de ancho de banda.

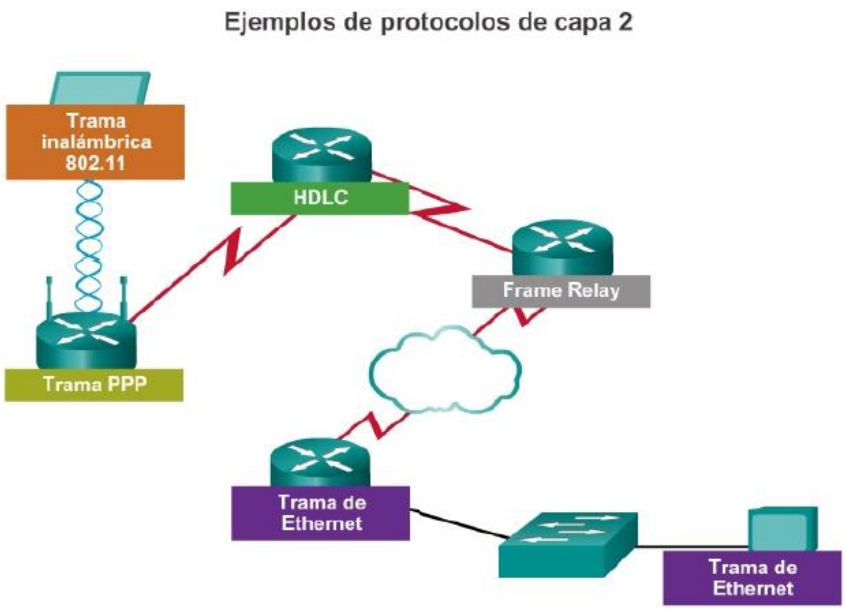
La diferencia de ancho de banda normalmente produce el uso de diferentes protocolos para las LAN y las WAN.

Los protocolos de capa de enlace de datos comunes incluyen los siguientes:

- Ethernet
- Protocolo punto a punto (PPP)
- Inalámbrico 802.11

Otros protocolos que se abordan en el currículo de CCNA son el protocolo de enlace de datos de alto nivel (HDLC) y Frame Relay.

Haga clic en el botón Reproducir para ver ejemplos de protocolos de capa 2.



Capítulo 4: Acceso a la red 4.4.4.6 Trama de Ethernet

Ethernet

Ethernet es la tecnología LAN predominante. Se trata de una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3.

Los estándares de Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. Ethernet es la tecnología LAN más ampliamente utilizada y admite anchos de banda de datos de 10 Mbps, 100 Mbps, 1 Gbps (1000 Mbps) o 10 Gbps (10 000 Mbps).

El formato básico de la trama y las subcapas del IEEE de las Capas OSI 1 y 2 siguen siendo los mismos para todas las formas de Ethernet. Sin embargo, los métodos para detectar y colocar en los medios varían con las diferentes implementaciones.

Ethernet proporciona servicio sin conexión y sin reconocimiento sobre un medio compartido utilizando CSMA/CD como métodos de acceso al medio. Los medios compartidos requieren que el encabezado de la trama de Ethernet utilice una dirección de la capa de enlace de datos para identificar los nodos de origen y destino. Como con la mayoría de los protocolos LAN, esta dirección se llama dirección MAC del nodo. Una dirección MAC de Ethernet es de 48 bits y generalmente se representa en formato hexadecimal.

En la ilustración, se muestran los diversos campos de la trama de Ethernet. En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet. Sin embargo, en la capa física, las diferentes versiones de Ethernet colocan los bits en los medios de forma diferente. Ethernet se analiza más detalladamente en el capítulo siguiente.

Protocolo Ethernet

Un protocolo de capa de enlace de datos común para las redes LAN

	Trama					
Nombre de campo	Preámbulo	Destino	Origen	Tipo	Datos	Secuencia de verificación de trama
Tamaño	8 bytes	6 bytes	6 bytes	2 bytes	46 bytes a 1500 bytes	4 bytes

Preámbulo: se utiliza para la sincronización; también contiene un delimitador para marcar el final de la información de temporización.
Dirección de destino: dirección MAC de 48 bits para el nodo de destino.
Dirección de origen: dirección MAC de 48 bits para el nodo de origen.
Tipo: valor para indicar qué protocolo de capa superior recibirá los datos una vez que finalice el proceso Ethernet.
Datos o contenido: esto es la PDU, normalmente un paquete IPV4, que se debe transportar a través de los medios.
Secuencia de verificación de trama (FCS): un valor utilizado para verificar si hay tramas dañadas.

Capítulo 4: Acceso a la red 4.4.4.7 Trama PPP

Protocolo punto a punto

Otro protocolo de capa de enlace de datos es el protocolo punto a punto (PPP). El protocolo PPP se utiliza para entregar tramas entre dos nodos. A diferencia de muchos protocolos de capa de enlace de datos, definidos por los organismos de ingeniería eléctrica, el estándar PPP se define mediante RFC. PPP fue desarrollado como un protocolo WAN y sigue siendo el protocolo elegido para implementar muchas WAN serie. El protocolo PPP se puede utilizar en diversos medios físicos, incluidos par trenzado, líneas de fibra óptica y transmisiones satelitales, así como para conexiones virtuales.

PPP utiliza una arquitectura en capas. Para incluir a los diferentes tipos de medios, PPP establece conexiones lógicas, llamadas sesiones, entre dos nodos. La sesión PPP oculta el medio físico subyacente del protocolo PPP superior. Estas sesiones también proporcionan a PPP un método para encapsular varios protocolos sobre un enlace punto a punto. Cada protocolo encapsulado en el enlace establece su propia sesión PPP.

PPP también permite que dos nodos negocien opciones dentro de la sesión PPP. Esto incluye la autenticación, compresión y multienlace (el uso de varias conexiones físicas).

Consulte la ilustración para ver los campos básicos de una trama PPP.

Protocolo punto a punto

Un protocolo de enlace de datos común para las redes WAN

	Trama					
Nombre de campo	Señaliza-dor	Dirección	Control	Protocolo	Datos	FCS
Tamaño	1 byte	1 byte	1 byte	2 bytes	variable	2 o 4 bytes

Indicador: un único byte que indica el inicio y el final de una trama. El campo Indicador está formado por la secuencia binaria 01111110.
Dirección: un único byte que contiene la dirección de broadcast PPP estándar. El protocolo PPP no asigna direcciones de estaciones individuales.
Control: un único byte formado por la secuencia binaria 00000011, que requiere la transmisión de datos de usuario en una trama no secuencial.
Protocolo: dos bytes que identifican el protocolo encapsulado en el campo de datos de la trama. Los valores más actualizados del campo Protocolo se especifican en la Solicitud de comentarios (RFC) de números asignados más reciente.
Datos: cero o más bytes que contienen el datagrama para el protocolo especificado en el campo Protocolo.
Secuencia de verificación de trama (FCS): normalmente, tiene 16 bits (2 bytes). Mediante un acuerdo previo, con la aceptación de las implementaciones PPP se puede utilizar una FCS de 32 bits (4 bytes) para una mayor detección de errores.

Capítulo 4: Acceso a la red 4.4.4.8 Trama inalámbrica 802.11

Inalámbrico 802.11

El estándar IEEE 802.11 utiliza el mismo LLC de 802.2 y el mismo esquema de direccionamiento de 48 bits que las demás LAN 802. Sin embargo, existen muchas diferencias en la subcapa MAC y en la capa física. En un entorno inalámbrico, el entorno requiere consideraciones especiales. No hay una conectividad física definible; por lo tanto, factores externos pueden interferir con la transferencia de datos y es difícil controlar el acceso. Para vencer estos desafíos, los estándares inalámbricos tienen controles adicionales.

Comúnmente, el estándar IEEE 802.11 se denomina “Wi-Fi”. Es un sistema de contienda que utiliza un proceso CSMA/CA de acceso al medio. CSMA/CA especifica un procedimiento postergación aleatoria para todos los nodos que están esperando transmitir. La oportunidad más probable para la contención de medio es el momento en que el medio está disponible. Hacer el back off de los nodos para un período aleatorio reduce en gran medida la probabilidad de colisión.

Las redes 802.11 también utilizan acuses de recibo de enlace de datos para confirmar que una trama se recibió correctamente.

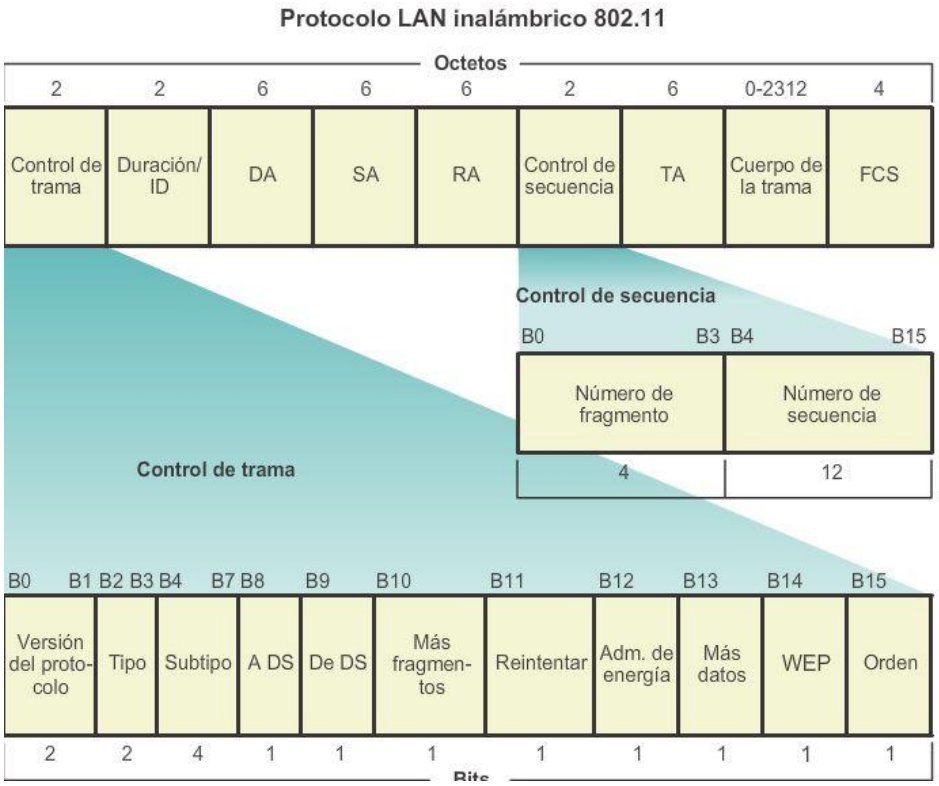
Si la estación transmisora no detecta la trama de reconocimiento, ya sea porque la trama de datos original o el reconocimiento no se recibieron intactos, se retransmite la trama. Este reconocimiento explícito supera la interferencia y otros problemas relacionados con la radio.

Otros servicios admitidos por la 802.11 son la autenticación, asociación (conectividad a un dispositivo inalámbrico) y privacidad (encriptación).

Como se muestra en la ilustración, las tramas 802.11 incluyen los siguientes campos:

- Campo Versión de protocolo: la versión de la trama 802.11 en uso.
- Campos Tipo y Subtipo: identifican una de las tres funciones y subfunciones de la trama (control, datos y administración).
- Campo A DS: se establece en 1 para las tramas de datos destinadas al sistema de distribución (dispositivos en la estructura inalámbrica).
- Campo Desde DS: se establece en 1 para las tramas de datos que salen del sistema de distribución.
- Campo Más fragmentos: se establece en 1 para las tramas que tienen otro fragmento.
- Campo Reintentar: se establece en 1 si la trama es una retransmisión de una trama anterior.
- Campo Administración de energía: se establece en 1 para indicar que un nodo estará en el modo de ahorro de energía.
- Campo Más datos: se establece en 1 para indicarle a un nodo en el modo de ahorro de energía que se almacenan más tramas en búfer para ese nodo.
- Campo Privacidad equivalente por cable (WEP): se establece en 1 si la trama contiene información encriptada mediante WEP para propósitos de seguridad
- Campo Orden: se establece en 1 en una trama de tipo de datos que utiliza la clase de servicio Estrictamente ordenada (no requiere reordenamiento).
- Campo Duración/ID: según el tipo de trama, representa el tiempo que se requiere en microsegundos para transmitir la trama o una identidad de asociación (AID) para la estación que transmitió la trama.
- Campo Dirección de destino (DA): contiene la dirección MAC del nodo de destino final en la red.
- Campo Dirección de origen (SA): contiene la dirección MAC del nodo que inició la trama.

- Campo Dirección del receptor (RA): contiene la dirección MAC que identifica al dispositivo inalámbrico que es el destinatario inmediato de la trama.
- Campo Número de fragmento: indica el número de cada fragmento de la trama.
- Campo Número de secuencia: indica el número de secuencia asignado a la trama. Las tramas retransmitidas se identifican con números de secuencia duplicados.
- Campo Dirección del transmisor (TA): contiene la dirección MAC que identifica al dispositivo inalámbrico que transmitió la trama.
- Campo Cuerpo de la trama: contiene la información que se transporta. En las tramas de datos; generalmente se trata de un paquete IP.
- Campo FCS: contiene una comprobación de redundancia cíclica (CRC) de 32 bits de la trama.



Capítulo 4: Acceso a la red 4.5.1.2 Resumen

La capa de acceso a la red de TCP/IP equivale a la capa de enlace de datos (capa 2) y a la capa física (capa 1) del modelo OSI.

La capa física de OSI proporciona los medios de transporte de los bits que conforman una trama de la capa de enlace de datos a través de los medios de red. Los componentes físicos son los dispositivos electrónicos de hardware, los medios y otros conectores que transmiten y transportan las señales para representar los bits. Todos los componentes de hardware, como los adaptadores de red (NIC), las interfaces y los conectores, así como los materiales y el diseño de los cables, se especifican en los estándares asociados con la capa física. Los estándares de la capa física abordan tres áreas funcionales: los componentes físicos, la técnica de codificación de la trama y el método de señalización.

El uso de los medios adecuados es una parte importante de las comunicaciones de red. Sin la conexión física adecuada, ya sea por cable o inalámbrica, no se produce comunicación entre dispositivos.

La comunicación por cable consta de medios de cobre y cable de fibra óptica.

- Existen tres tipos principales de medios de cobre utilizados en redes: el cable de par trenzado no blindado (UTP), el cable de par trenzado blindado (STP) y el cable coaxial. El cableado UTP es el medio de cobre que más se utiliza en redes.

- El cable de fibra óptica se volvió muy popular para interconectar dispositivos de red de infraestructura. Permite la transmisión de datos a través de distancias más extensas y a anchos de banda (velocidades de datos) mayores que cualquier otro medio de red. A diferencia de los cables de cobre, el cable de fibra óptica puede transmitir señales con menos atenuación y es totalmente inmune a las EMI y RFI.

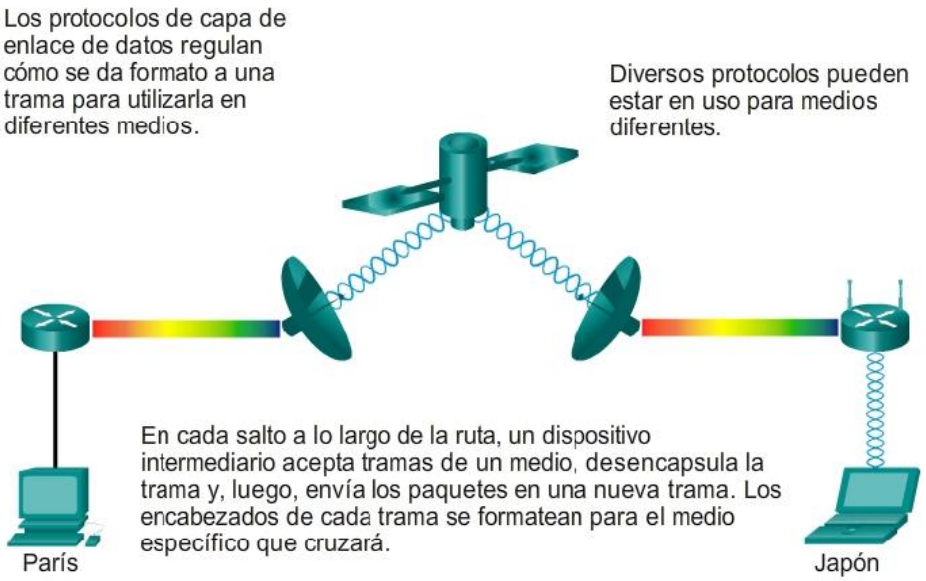
Los medios inalámbricos transportan señales electromagnéticas que representan los dígitos binarios de las comunicaciones de datos mediante frecuencias de radio y de microondas.

La cantidad de dispositivos con tecnología inalámbrica continúa en aumento. Por estos motivos, la tecnología inalámbrica se convirtió en el medio de preferencia para las redes domésticas y cada vez adquiere más popularidad en las redes empresariales.

La capa de enlace de datos es responsable del intercambio de tramas entre nodos a través de los medios de red físicos. Permite que las capas superiores accedan a los medios y controla el modo en que los datos se colocan y se reciben en los medios.

Entre las diferentes implementaciones de los protocolos de capa de enlace de datos, existen diferentes métodos para controlar el acceso al medio. Estas técnicas de control de acceso al medio definen si los nodos comparten los medios y de qué manera lo hacen. El método específico de control de acceso al medio utilizado depende de la topología y los medios compartidos. Las topologías de LAN y de WAN pueden ser físicas o lógicas. La topología lógica influye en el tipo de entramado de red y el control de acceso al medio que se utilizan. En general, las redes WAN se interconectan mediante topologías físicas punto a punto, hub-and-spoke o de malla. En las redes LAN de medios compartidos, los dispositivos finales se pueden interconectar mediante las topologías físicas en estrella, de bus, de anillo o de estrella extendida (híbrida).

Todos los protocolos de capa de enlace de datos encapsulan la PDU de la capa 3 dentro del campo de datos de la trama. Sin embargo, la estructura de la trama y los campos contenidos en el encabezado y tráiler varían de acuerdo con el protocolo.



Capítulo 5: Ethernet 5.0.1.1 Introducción

La capa física de OSI proporciona los medios de transporte de los bits que conforman una trama de la capa de enlace de datos a través de los medios de red.

En la actualidad, Ethernet es la tecnología LAN predominante en el mundo. Ethernet funciona en la capa de enlace de datos y en la capa física. Los estándares del protocolo Ethernet definen muchos aspectos de la comunicación de red, incluidos el formato y el tamaño de la trama, la temporización y la codificación. Cuando se envían mensajes entre hosts a través de una red Ethernet, los hosts asignan un formato a los mensajes según la configuración de trama que especifican los estándares. Las tramas también se conocen como unidades de datos de protocolo (PDU).

Dado que Ethernet se compone de estándares en estas capas inferiores, es probable que sea más sencillo de entender con referencia al modelo OSI. El modelo OSI separa las funcionalidades de direccionamiento, entramado y acceso a los medios de la capa de enlace de datos de los estándares de la capa física de los medios. Los estándares de Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. Si bien las especificaciones de Ethernet admiten diferentes medios, anchos de banda y otras variaciones de Capa 1 y 2, el formato de trama básico y el esquema de direcciones son los mismos para todas las variedades de Ethernet.

Este capítulo analiza las características y el funcionamiento de la Ethernet en términos de su evolución desde una tecnología de medios compartidos de comunicación de datos basada en contenciones hasta convertirse en la actual tecnología full-duplex de gran ancho de banda.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Describir el funcionamiento de las subcapas de Ethernet.
- Identificar los campos principales de la trama de Ethernet.
- Describir el propósito y las características de la dirección MAC de Ethernet.
- Describir el propósito del protocolo ARP.
- Explicar la forma en que las solicitudes ARP afectan el rendimiento de la red y del host.
- Explicar conceptos básicos de conmutación.
- Comparar switches de configuración fija y switches modulares.
- Configurar un switch de capa 3.

Capítulo 5: Ethernet 5.0.1.2 Actividad: Únase a mi círculo social

Únase a mi círculo social

Gran parte de nuestra comunicación de red se realiza mediante mensajería (de texto o instantánea), contacto por video y publicaciones en medios sociales, entre otros.

Para esta actividad, elija una de las redes de comunicación que más utilice:

- Mensajería de texto (o instantánea)
- Conferencias de audio o video
- Envío de mensajes por correo electrónico
- Juegos de azar

Ahora que seleccionó un tipo de comunicación de red, registre sus respuestas a las siguientes preguntas:

- ¿Existe un procedimiento que deba seguir para registrar a otras personas y a usted mismo a fin de formar un grupo de comunicaciones?
- ¿Cómo inicia el contacto con las personas con quienes desea comunicarse?
- ¿Cómo limita las conversaciones para que solo las reciban aquellas personas con quienes desea comunicarse?

Esté preparado para explicar en clase las respuestas registradas.

Capítulo 5: Ethernet 5.1.1.1 Subcapas LLC y MAC

Ethernet es la tecnología LAN más ampliamente utilizada en la actualidad.

Ethernet funciona en la capa de enlace de datos y en la capa física. Se trata de una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3. Ethernet admite los anchos de banda de datos siguientes:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10.000 Mb/s (10 Gb/s)
- 40.000 Mb/s (40 Gb/s)

- 100.000 Mb/s (100 Gb/s)

Como se muestra en la figura 1, los estándares de Ethernet definen tanto los protocolos de capa 2 como las tecnologías de capa 1. En lo que respecta a los protocolos de capa 2, al igual que sucede con todos los estándares IEEE 802, Ethernet depende de las dos subcapas separadas de la capa de enlace de datos para funcionar: la subcapa de control de enlace lógico (LLC) y la subcapa MAC.

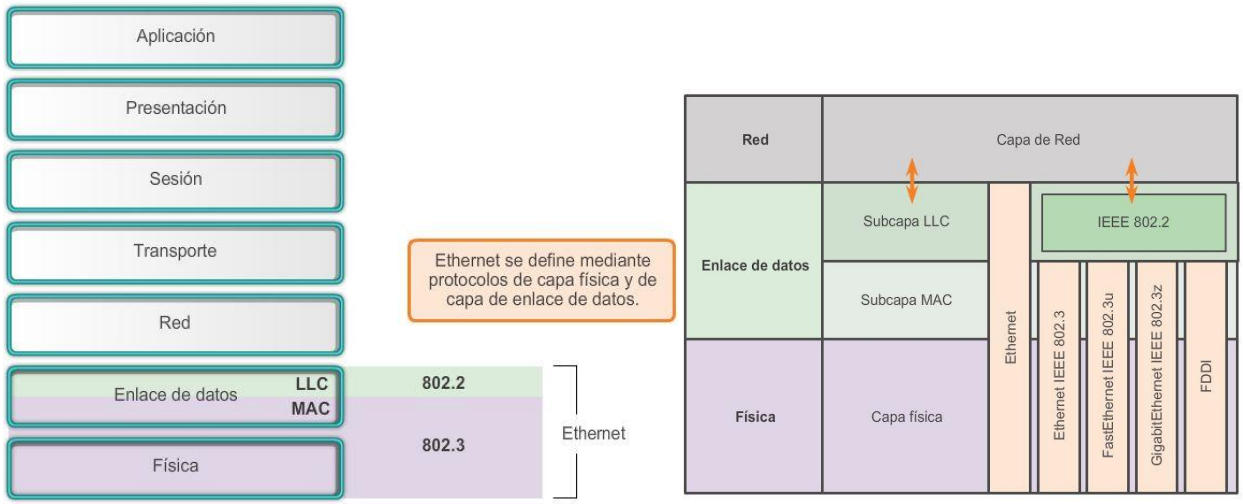
Subcapa LLC

La subcapa LLC de Ethernet se ocupa de la comunicación entre las capas superiores y las capas inferiores. Generalmente, esta comunicación se produce entre el software de red y el hardware del dispositivo. La subcapa LLC toma los datos del protocolo de la red, que generalmente son un paquete IPv4, y agrega información de control para ayudar a entregar el paquete al nodo de destino. El LLC se utiliza para comunicarse con las capas superiores de la aplicación y para la transición del paquete a las capas inferiores para su entrega.

El LLC se implementa en software, y su implementación no depende del hardware. En una PC, el LLC se puede considerar el controlador de la NIC. El controlador de la NIC es un programa que interactúa directamente con el hardware de la NIC para transmitir los datos entre la subcapa MAC y los medios físicos.

Subcapa MAC

La MAC constituye la subcapa inferior de la capa de enlace de datos. La MAC se implementa mediante hardware, por lo general, en la NIC de la PC. Los detalles se especifican en los estándares IEEE 802.3. En la figura 2, se enumeran los estándares IEEE de Ethernet comunes.



Capítulo 5: Ethernet 5.1.1.2 Subcapa MAC

Como se muestra en la ilustración, la subcapa MAC de Ethernet tiene dos responsabilidades principales:

- Encapsulación de datos
- Control de acceso al medio

Encapsulación de datos

El proceso de encapsulación de datos incluye el armado de la trama antes de la transmisión y el desarmado de la trama en el momento en que se la recibe. Cuando se forma la trama, la capa MAC agrega un encabezado y un tráiler a la PDU de la capa de red.

La encapsulación de datos proporciona tres funciones principales:

- Delimitación de tramas: el proceso de entramado proporciona delimitadores importantes que se utilizan para identificar un grupo de bits que componen una trama. Este proceso ofrece una sincronización entre los nodos transmisores y receptores.

- Direccionamiento: el proceso de encapsulación también proporciona direccionamiento de la capa de enlace de datos. Cada encabezado Ethernet agregado a la trama contiene la dirección física (dirección MAC) que permite que la trama se envíe a un nodo de destino.

- Detección de errores: cada trama de Ethernet contiene un tráiler con una comprobación de redundancia cíclica (CRC) del contenido de la trama. Una vez que se recibe una trama, el nodo receptor crea una CRC para compararla con la de la trama. Si estos dos cálculos de CRC coinciden, puede asumirse que la trama se recibió sin errores.

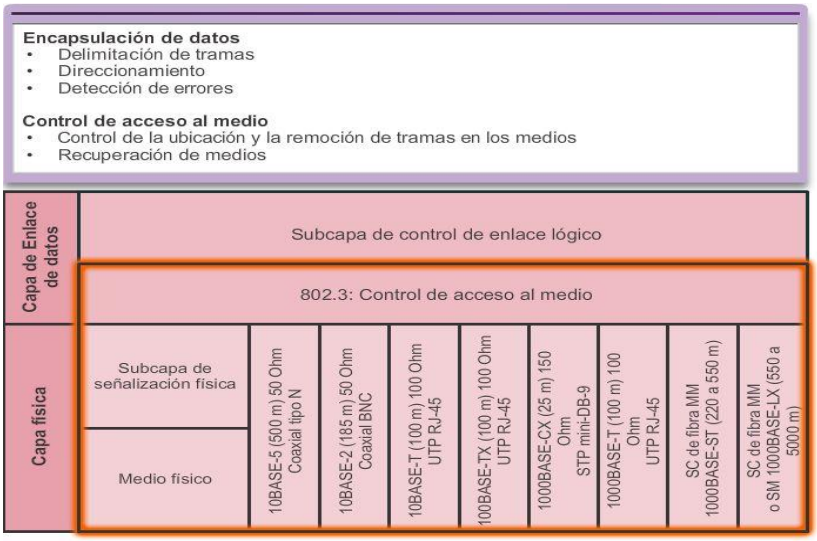
La utilización de tramas facilita la transmisión de bits a medida que se colocan en los medios y la agrupación de bits en el nodo receptor.

Control de acceso al medio

La segunda responsabilidad de la subcapa MAC es el control de acceso al medio. El control de acceso al medio es responsable de la ubicación y la remoción de tramas en los medios.

Como su nombre lo indica, controla el acceso a los medios. Esta subcapa se comunica directamente con la capa física.

La topología lógica subyacente de Ethernet es de bus de multiacceso; por lo tanto, todos los nodos (dispositivos) en un mismo segmento de red comparten el medio. Ethernet es un método de red de contienda. Recuerde que en un método por contienda, o método no determinista, cualquier dispositivo puede intentar transmitir datos a través del medio compartido siempre que tenga datos para enviar. Sin embargo, tal como sucede si dos personas intentan hablar al mismo tiempo, si hay varios dispositivos en un único medio que intentan reenviar datos simultáneamente, los datos colisionan, lo que provoca que estos se dañen y no se puedan utilizar. Por este motivo, Ethernet proporciona un método para controlar la forma en que los nodos comparten el acceso mediante el uso de una tecnología de acceso múltiple por detección de portadora (CSMA).



Capítulo 5: Ethernet 5.1.1.3 Control de acceso al medio

En primera instancia, el proceso de CSMA se utiliza para detectar si los medios transportan una señal. Si se detecta una señal portadora en el medio desde otro nodo, quiere decir que otro dispositivo está transmitiendo. Cuando un dispositivo está intentando transmitir y nota que el medio está ocupado, esperará e intentará después de un período de tiempo corto. Si no se detecta una señal portadora, el dispositivo transmite sus datos. Es posible que el proceso CSMA falle si dos dispositivos transmiten al mismo tiempo. A esto se le denomina colisión de datos. Si esto ocurre, los datos enviados por ambos dispositivos se dañarán y deberán enviarse nuevamente.

Los métodos de control de acceso al medio por contienda no requieren mecanismos para llevar la cuenta de a quién le corresponde acceder al medio; por lo tanto, no tienen la sobrecarga de los métodos de acceso controlado. Sin embargo, los sistemas por contención no escalan bien bajo un uso intensivo de los medios.

A medida que el uso y el número de nodos aumenta, la probabilidad de acceder a los medios con éxito sin una colisión disminuye. Además, los mecanismos de recuperación que se requieren para corregir errores debidos a esas colisiones disminuyen aún más el rendimiento.

Como se muestra en la ilustración, el CSMA se suele implementar junto con un método para resolver la contienda de los medios. Los dos métodos comúnmente utilizados son:

CSMA/Detección de colisión

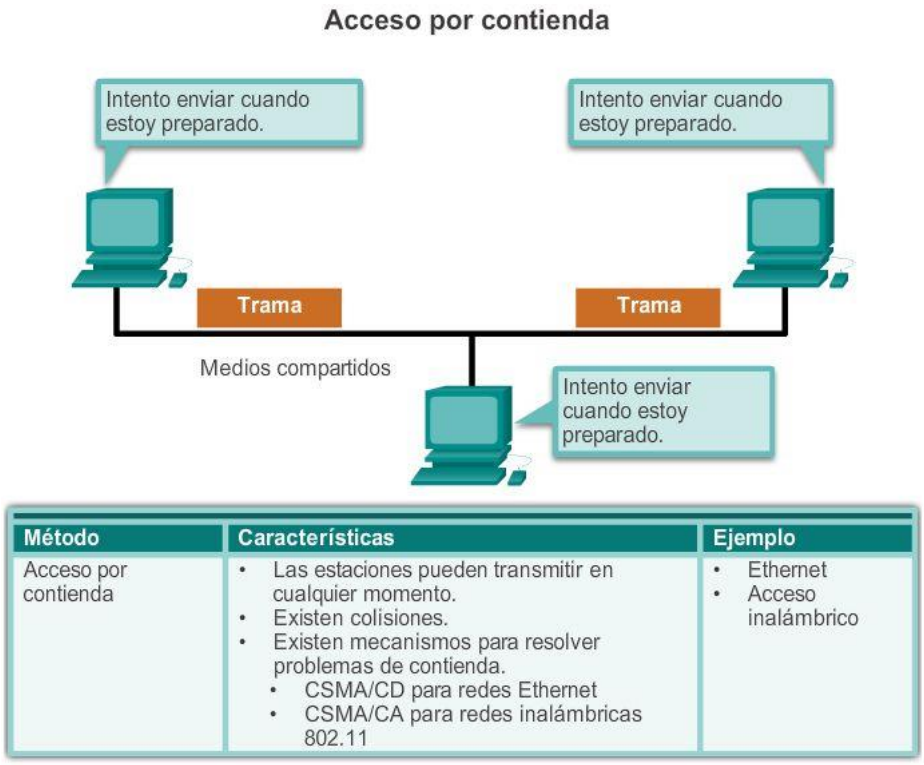
Con el método CSMA/Detección de colisión (CSMA/CD), el dispositivo controla los medios para detectar la presencia de una señal de datos. Si no hay una señal de datos, que indica que el medio está libre, el dispositivo transmite los datos. Si luego se detectan señales que muestran que otro dispositivo estaba transmitiendo al mismo tiempo, todos los dispositivos dejan de enviar e intentan después. Las formas tradicionales de Ethernet se desarrollaron para utilizar este método.

La incorporación a gran escala de tecnologías conmutadas en las redes modernas reemplazó ampliamente la necesidad original de implementación de CSMA/CD en redes de área local. Hoy en día, casi todas las conexiones por cable entre dispositivos en una LAN son conexiones full-duplex, es decir, un mismo dispositivo puede enviar y recibir información simultáneamente. Esto significa que, si bien las redes Ethernet se diseñan con tecnología CSMA/CD, con los dispositivos intermediarios actuales no se producen colisiones y los procesos utilizados por el CSMA/CD son realmente innecesarios.

Sin embargo, todavía se deben tener en cuenta las colisiones en conexiones inalámbricas en entornos LAN. Los dispositivos LAN inalámbricos utilizan el método de acceso al medio CSMA/Prevención de colisiones (CSMA/CA).

CSMA/Prevención de colisiones

Con el método CSMA/CA, el dispositivo analiza los medios para detectar la presencia de una señal de datos. Si el medio está libre, el dispositivo envía una notificación a través del medio, sobre su intención de utilizarlo. El dispositivo luego envía los datos. Las tecnologías de red inalámbricas 802.11 utilizan este método.



Método	Características	Ejemplo

Acceso por contienda	• Las estaciones pueden transmitir en cualquier momento.
	• Existen colisiones.
	• Existen mecanismos para resolver problemas de contienda.
	  • CSMA/CD para redes Ethernet
	  • CSMA/CA para redes inalámbricas 802.11
		• Ethernet
		• Acceso inalámbrico

Capítulo 5: Ethernet 5.1.1.4 Dirección MAC: identidad de Ethernet

Como se indicó anteriormente, la topología lógica subyacente de Ethernet es de bus de multiacceso. Cada dispositivo de red está conectado a los mismos medios compartidos, y todos los nodos reciben todas las tramas que se transmiten.

El problema es que si todos los dispositivos reciben cada trama, ¿cómo puede determinar cada dispositivo si es el receptor previsto sin la sobrecarga de tener que procesar y desencapsular la trama para obtener la dirección IP? Esta cuestión se vuelve aún más problemática en redes con alto volumen de tráfico donde se reenvían muchas tramas.

Para evitar la sobrecarga excesiva relacionada con el procesamiento de cada trama, se creó un identificador único denominado “dirección MAC” que identifica los nodos de origen y de destino reales dentro de una red Ethernet. Sin importar qué variedad de Ethernet se utilice, el direccionamiento MAC proporciona un método para la identificación de dispositivos en el nivel inferior del modelo OSI. Como recordará, el direccionamiento MAC se agrega como parte de una PDU de capa 2. Una dirección MAC de Ethernet es un valor binario de 48 bits expresado como 12 dígitos hexadecimales (4 bits por dígito hexadecimal).

Estructura de la dirección MAC

Las direcciones MAC deben ser únicas en el mundo. El valor de la dirección MAC es el resultado directo de las normas implementadas por el IEEE para proveedores con el objetivo de garantizar direcciones únicas para cada dispositivo Ethernet. Las normas establecidas por el IEEE obligan a los proveedores de dispositivos Ethernet a registrarse en el IEEE. El IEEE le asigna al proveedor un código de 3 bytes (24 bits), denominado “Identificador único de organización” (OUI).

El IEEE requiere que un proveedor siga dos reglas sencillas, como se muestra en la ilustración:

- Todas las direcciones MAC asignadas a una NIC u otro dispositivo Ethernet deben utilizar el OUI que se le asignó a dicho proveedor como los 3 primeros bytes.

Se les debe asignar un valor exclusivo (código del fabricante o número de serie) a todas las direcciones MAC con el mismo OUI (Identificador exclusivo de organización) en los últimos 3 bytes.

Estructura de la dirección MAC de Ethernet

Capítulo 5: Ethernet 5.1.1.5 Procesamiento de tramas

La dirección MAC suele denominarse “dirección física” (BIA) porque, históricamente, se graba en la ROM (memoria de solo lectura) de la NIC. Esto significa que la dirección se codifica en el chip de la ROM de manera permanente (el software no puede cambiarla).

Nota: en los sistemas operativos de PC y en las NIC modernos, es posible cambiar la dirección MAC mediante software. Esto es útil cuando se trata de acceder a una red que filtra sobre la base de la BIA. Esto quiere decir que el filtrado o control del tráfico sobre la base de la dirección MAC ya no es tan seguro como antes.

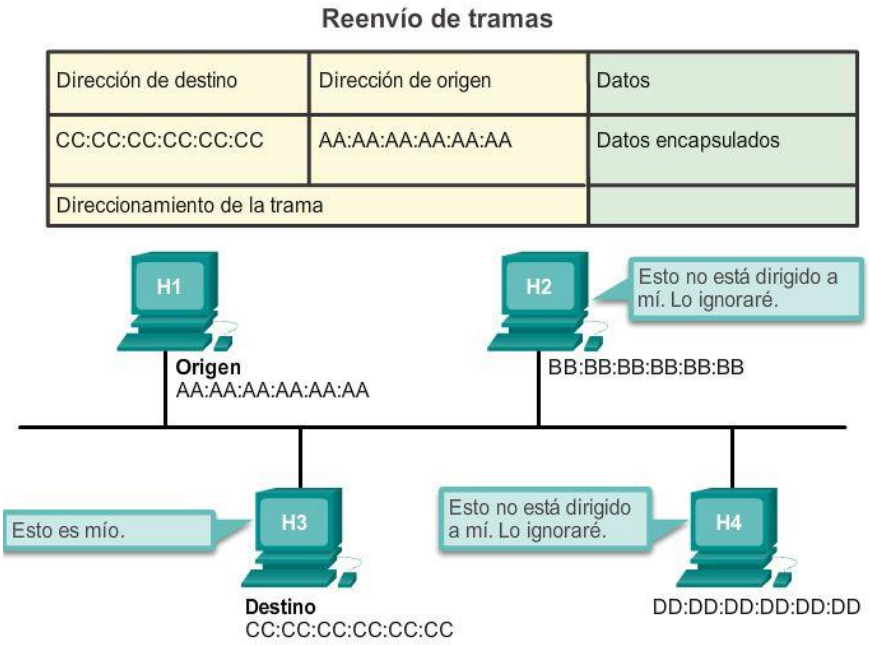
Las direcciones MAC se asignan a estaciones de trabajo, servidores, impresoras, switches y routers, es decir, a cualquier dispositivo que debe originar o recibir datos en una red. Todos los dispositivos conectados a una LAN Ethernet tienen interfaces con direcciones MAC. Diferentes fabricantes de hardware y software pueden representar las direcciones MAC en distintos formatos hexadecimales. Los formatos de las direcciones pueden ser similares a los siguientes:

- 00-05-9A-3C-78-00

- 00:05:9A:3C:78:00
- 0005.9A3C.7800

Cuando se inicia la PC, lo primero que hace la NIC es copiar la dirección MAC del ROM en la RAM. Cuando un dispositivo reenvía un mensaje a una red Ethernet, adjunta al paquete la información del encabezado. La información del encabezado contiene la dirección MAC de origen y destino. El dispositivo de origen envía los datos a través de la red.

Cada NIC en la red revisa la información en la subcapa MAC para ver si la dirección MAC de destino que está en la trama coincide con la dirección MAC física del dispositivo almacenada en la RAM. Si no hay coincidencia, el dispositivo descarta la trama. Cuando la trama llega al destino en que la MAC de la NIC coincide con la MAC de destino de la trama, la NIC pasa la trama a las capas OSI, donde se lleva a cabo el proceso de desencapsulación.



Capítulo 5: Ethernet 5.1.2.1 Encapsulación de Ethernet

Desde la creación de Ethernet en 1973, los estándares han evolucionado para especificar versiones más rápidas y flexibles de la tecnología. Esta capacidad que tiene Ethernet de evolucionar con el paso del tiempo es una de las principales razones por las que se ha popularizado. Las primeras versiones de Ethernet eran relativamente lentas, con una velocidad de 10 Mbps. Las últimas versiones de Ethernet funcionan a 10 Gigabits por segundo e incluso más rápido. En la figura 1, se destacan los cambios en las diferentes versiones de Ethernet.

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet. La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía.

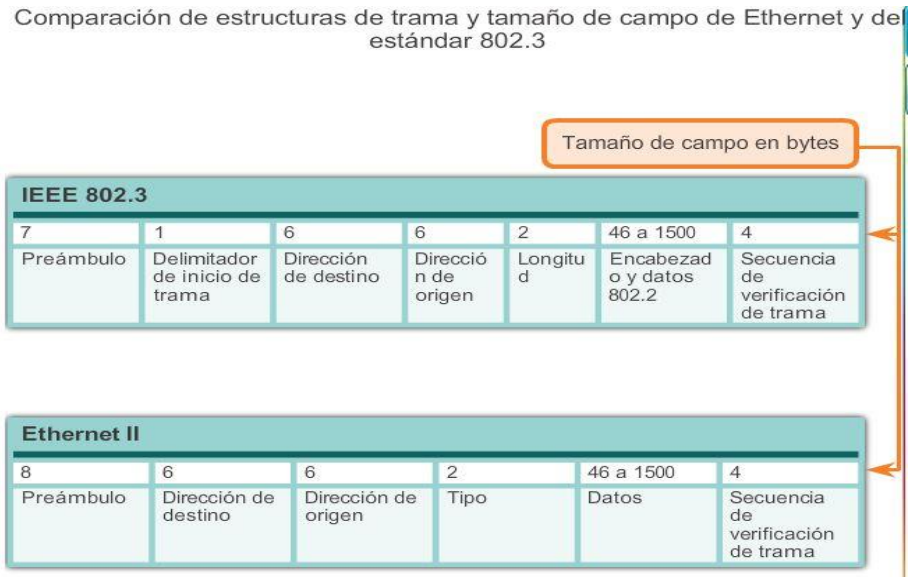
Tanto el tráiler como el encabezado de Ethernet cuentan con varias secciones de información que utiliza el protocolo Ethernet. Cada sección de la trama se denomina campo. Como se muestra en la figura 2, hay dos estilos de entramado de Ethernet:

- El estándar IEEE 802.3 de Ethernet que se actualizó varias veces para incluir nuevas tecnologías.

- El estándar DIX de Ethernet que ahora se denomina “Ethernet II”.

Las diferencias entre los estilos de tramas son mínimas. La diferencia más importante entre los dos estándares es el agregado de un delimitador de inicio de trama (SFD) y el cambio del campo Tipo por el campo Longitud en el estándar 802.3.

Ethernet II es el formato de trama de Ethernet utilizado en las redes TCP/IP.



Capítulo 5: Ethernet 5.1.2.2 Tamaño de la trama de Ethernet

Tanto el estándar Ethernet II como el IEEE 802.3 definen el tamaño mínimo de trama en 64 bytes y el tamaño máximo de trama en 1518 bytes. Esto incluye todos los bytes del campo Dirección MAC de destino a través del campo Secuencia de verificación de trama (FCS). Los campos Preámbulo y Delimitador de inicio de trama no se incluyen en la descripción del tamaño de una trama.

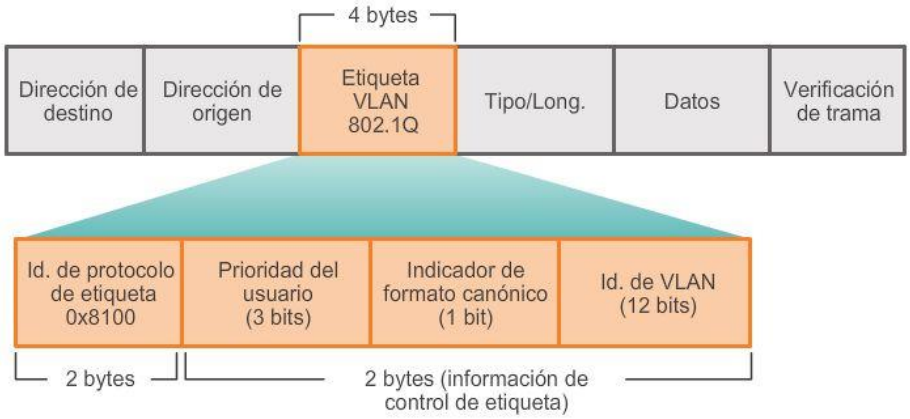
Cualquier trama con menos de 64 bytes de longitud se considera un "fragmento de colisión" o "runt frame" y las estaciones receptoras la descartan automáticamente.

El estándar IEEE 802.3ac, publicado en 1998, amplió el tamaño de trama máximo permitido a 1522 bytes. Se aumentó el tamaño de la trama para que se adapte a una tecnología denominada Red de área local virtual (VLAN). Las VLAN se crean dentro de una red conmutada y se presentarán en otro curso. Además, muchas tecnologías de calidad de servicio (QoS) hacen uso del campo Prioridad del usuario para implementar diversos niveles de servicio, como el servicio de prioridad para el tráfico de voz. En la ilustración, se muestran los campos contenidos en la etiqueta VLAN 802.1Q.

Si el tamaño de una trama transmitida es menor que el mínimo o mayor que el máximo, el dispositivo receptor descarta la trama. Es posible que las tramas descartadas se originen en colisiones u otras señales no deseadas y, por lo tanto, se consideran no válidas.

En la capa de enlace de datos, la estructura de la trama es casi idéntica. En la capa física, las diferentes versiones de Ethernet varían en cuanto al método para detectar y colocar datos en los medios.

Los 4 bytes adicionales permiten tecnologías de QoS y VLAN



Capítulo 5: Ethernet 5.1.2.3 Introducción a la trama de Ethernet

Los campos principales de la trama de Ethernet son los siguientes:

- Campos Preámbulo y Delimitador de inicio de trama: los campos Preámbulo (7 bytes) y Delimitador de inicio de trama (SFD), también conocido como “Inicio de trama” (1 byte), se utilizan para la sincronización entre los dispositivos emisores y receptores. Estos ocho primeros bytes de la trama se utilizan para captar la atención de los nodos receptores. Básicamente, los primeros bytes le indican al receptor que se prepare para recibir una trama nueva.

- Campo Dirección MAC de destino: este campo de 6 bytes es el identificador del destinatario previsto. Como recordará, la Capa 2 utiliza esta dirección para ayudar a los dispositivos a determinar si la trama viene dirigida a ellos. La dirección de la trama se compara con la dirección MAC del dispositivo. Si coinciden, el dispositivo acepta la trama.

- Campo Dirección MAC de origen: este campo de 6 bytes identifica la NIC o la interfaz que origina la trama.

- Campo Longitud: para todos los estándares IEEE 802.3 anteriores a 1997, el campo Longitud define la longitud exacta del campo de datos de la trama. Esto se utiliza posteriormente como parte de la FCS para garantizar que el mensaje se reciba adecuadamente. Por lo demás, el propósito del campo es describir qué protocolo de capa superior está presente. Si el valor de los dos octetos es igual o mayor que 0x0600 hexadecimal o 1536 decimal, el contenido del campo Datos se decodifica según el protocolo EtherType indicado.

  Por otro lado, si el valor es igual o menor que el hexadecimal de 0x05DC o el decimal de 1500, el campo Longitud se está utilizando para indicar el uso del formato de trama de IEEE 802.3. Así se diferencian las tramas de Ethernet II y 802.3.

- Campo Datos: este campo (de 46 a 1500 bytes) contiene los datos encapsulados de una capa superior, que es una PDU de capa 3 genérica o, más comúnmente, un paquete IPv4. Todas las tramas deben tener al menos 64 bytes de longitud. Si se encapsula un paquete pequeño, se utilizan bits adicionales conocidos como “relleno” para incrementar el tamaño de la trama al tamaño mínimo.

- Campo Secuencia de verificación de trama (FCS): este campo de 4 bytes se utiliza para detectar errores en una trama. Utiliza una comprobación de redundancia cíclica (CRC). El dispositivo emisor incluye los resultados de una CRC en el campo FCS de la trama.

  El dispositivo receptor recibe la trama y genera una CRC para buscar errores. Si los cálculos coinciden, significa que no se produjo ningún error. Los cálculos que no coinciden indican que los datos cambiaron y, por consiguiente, se descarta la trama. Un cambio en los datos podría ser resultado de una interrupción de las señales eléctricas que representan los bits.

Campos de la trama de Ethernet
IEEE 802.3

7	1	6	6	2	46 a 1500	4
Preámbulo	Delimitador de inicio de trama	Dirección de destino	Dirección de origen	Longitud	Encabezado y datos de 802.2	Secuencia de verificación de trama

Capítulo 5: Ethernet 5.1.3.1 Direcciones MAC y numeración hexadecimal

El uso de la dirección MAC es uno de los aspectos más importantes de la tecnología LAN Ethernet. Las direcciones MAC utilizan numeración hexadecimal.

“Hexadecimal” es una palabra que se utiliza como sustantivo y como adjetivo. Cuando se utiliza sola (como sustantivo), se refiere al sistema de numeración hexadecimal. El método hexadecimal proporciona una manera conveniente de representar valores binarios.

Así como el decimal es un sistema con una base de diez números y el binario es un sistema con una base de dos números, el hexadecimal es un sistema de base dieciséis.

El sistema de numeración de base 16 utiliza los números del 0 al 9 y las letras entre A y F. En la figura 1, se muestran los valores decimales y hexadecimales equivalentes a los valores binarios del 0000 al 1111. Es más fácil expresar un valor con un único dígito hexadecimal que con cuatro bits binarios.

Dado que 8 bits (un byte) es una agrupación binaria común, los binarios 00000000 hasta 11111111 pueden representarse en valores hexadecimales como el intervalo 00 a FF. Los ceros iniciales se muestran siempre para completar la representación de 8 bits. Por ejemplo, el valor binario 0000 1010 se muestra en valor hexadecimal como 0A.

Nota: en lo que respecta a los caracteres del 0 al 9, es importante distinguir los valores hexadecimales de los decimales, tal como se muestra en la figura 1.

Representación de valores hexadecimales

Por lo general, los valores hexadecimales se representan en forma de texto mediante el valor precedido por 0x (por ejemplo, 0x73) o un subíndice 16. Con menor frecuencia, pueden estar seguidos de una H, por ejemplo, 73H. Sin embargo, y debido a que el texto en subíndice no es reconocido en entornos de línea de comando o de programación, la representación técnica de un valor hexadecimal es precedida de "0x" (cero X). Por lo tanto, los ejemplos anteriores deberían mostrarse como 0x0A y 0x73, respectivamente.

El valor hexadecimal se utiliza para representar las direcciones MAC de Ethernet y las direcciones IP versión 6.

Conversiones hexadecimales

Las conversiones numéricas entre valores decimales y hexadecimales son simples, pero no siempre es conveniente dividir o multiplicar por 16. Si es necesario realizar dichas conversiones, generalmente es más fácil convertir el valor decimal o hexadecimal a un valor binario y después convertir dicho valor binario a un valor decimal o hexadecimal, según corresponda.

Con la práctica, es posible reconocer los patrones de bits binarios que coinciden con los valores decimales y hexadecimales. En la figura 2, se muestran estos patrones para valores seleccionados de 8 bits.

Numeración hexadecimal

Equivalentes decimales y binarios a los valores hexadecimales de 0 a F

Decimal	Binario	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Numeración hexadecimal

Equivalentes decimales, binarios y hexadecimales seleccionados

Decimal	Binario	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

Capítulo 5: Ethernet 5.1.3.2 Representaciones de direcciones MAC

En un host de Windows, el comando ipconfig /all se puede utilizar para identificar la dirección MAC de un adaptador de Ethernet. Observe que, en la figura 1, la pantalla indica que la dirección física (dirección MAC)

de la PC es 00-18-DE-C7-F3-FB. Si el usuario tiene acceso, se sugiere intentar esto en su propia computadora.

Según el dispositivo y el sistema operativo, verá distintas representaciones de las direcciones MAC, como se muestra en la figura 2. Los routers y switches Cisco utilizan la forma XXXX.XXXX.XXXX, donde “X” representa un carácter hexadecimal.

Distintas representaciones de direcciones MAC

Con guiones: 00-60-2F-3A-07-BC

Con dos puntos: 00:60:2F:3A:07:BC

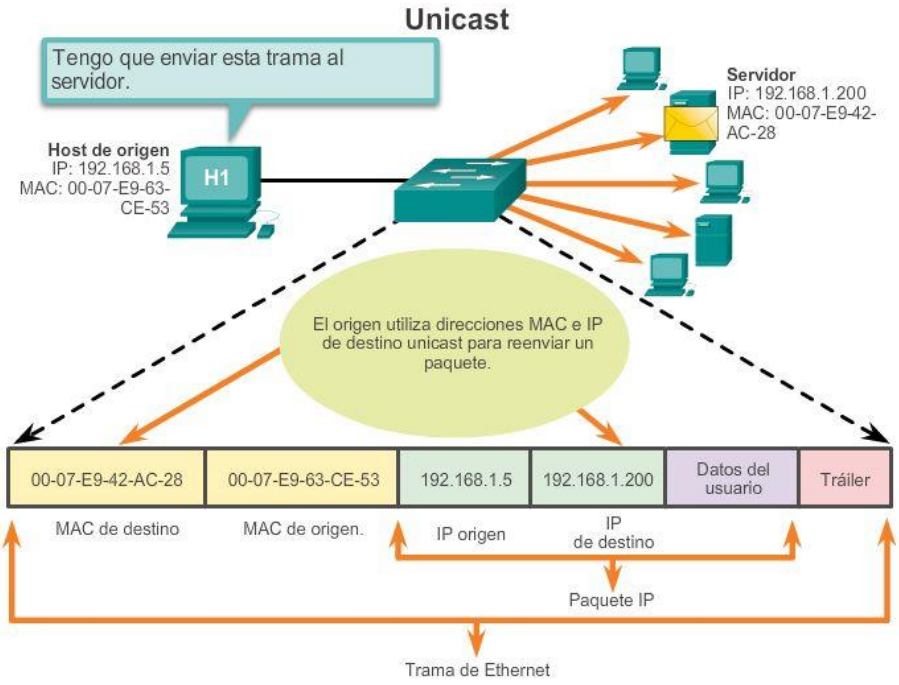
Con puntos: 0060.2F3A.07BC

Capítulo 5: Ethernet 5.1.3.3 Dirección MAC unicast

En Ethernet se utilizan distintas direcciones MAC para las comunicaciones unicast, broadcast y multicast de capa 2.

Una dirección MAC unicast es la dirección exclusiva que se utiliza cuando se envía una trama de un dispositivo de transmisión único a un dispositivo de destino único.

En el ejemplo que se muestra en la figura, un host con una dirección IP 192.168.1.5 (origen) solicita una página web del servidor en la dirección IP 192.168.1.200. Para que un paquete unicast sea enviado y recibido, la dirección IP de destino debe estar incluida en el encabezado del paquete IP. Además, el encabezado de la trama de Ethernet también debe contener una dirección MAC de destino correspondiente. Las direcciones IP y MAC se combinan para la entrega de datos a un host de destino específico.

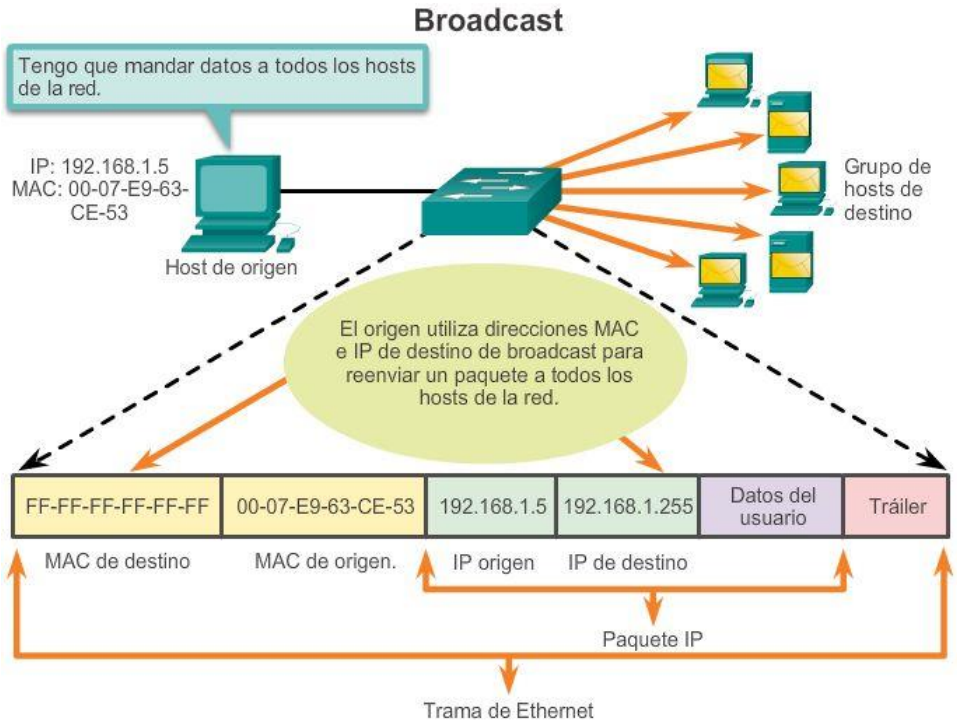


Capítulo 5: Ethernet 5.1.3.4 Dirección MAC de broadcast

Los paquetes de broadcast contienen una dirección IP de destino que contiene solo números uno (1) en la porción de host. Esta numeración en la dirección significa que todos los hosts de esa red local (dominio de broadcast) recibirán y procesarán el paquete. Muchos protocolos de red, como DHCP y el protocolo de resolución de direcciones (ARP), utilizan broadcasts.

Más adelante en este capítulo se analizará cómo el ARP utiliza los broadcasts para asignar direcciones de Capa 2 a direcciones de Capa 3.

Como se muestra en la figura, una dirección IP de broadcast para una red requiere una dirección MAC de broadcast correspondiente en la trama de Ethernet. En las redes Ethernet, la dirección MAC de broadcast está compuesta por 48 unos, que se muestran como el valor hexadecimal FF-FF-FF-FF-FF-FF.



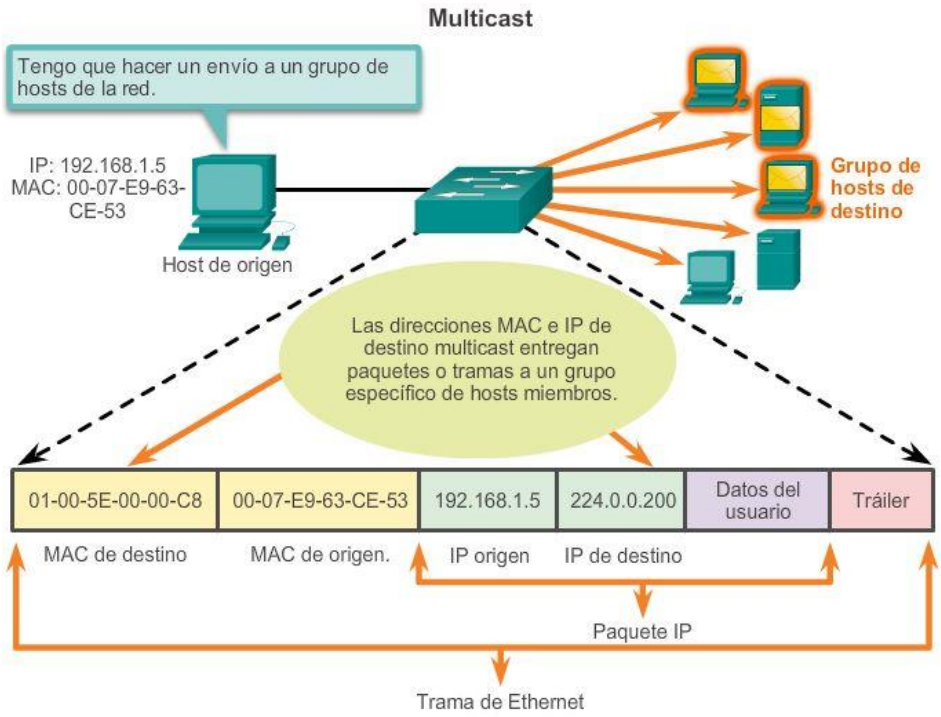
Capítulo 5: Ethernet 5.1.3.5 Dirección MAC Multicast

Las direcciones multicast le permiten a un dispositivo de origen enviar un paquete a un grupo de dispositivos. Una dirección IP de grupo multicast se asigna a los dispositivos que pertenecen a un grupo multicast. El rango de direcciones IPv4 multicast va de 224.0.0.0 a 239.255.255.255. Debido a que las direcciones multicast representan un grupo de direcciones (a veces denominado un grupo de hosts), sólo pueden utilizarse como el destino de un paquete. El origen siempre tendrá una dirección unicast.

Las direcciones multicast se pueden utilizar en juegos remotos, donde muchos jugadores se conectan de forma remota pero juegan al mismo juego. Las direcciones multicast también se pueden utilizar en situaciones de educación a distancia mediante videoconferencias, donde muchos estudiantes se conectan a la misma clase.

Al igual que con las direcciones unicast y de broadcast, la dirección IP multicast requiere una dirección MAC multicast correspondiente para poder enviar tramas en una red local. La dirección MAC multicast es un valor especial que comienza con 01-00-5E en hexadecimal. La porción restante de la dirección MAC multicast se crea mediante la conversión de los 23 bits inferiores de la dirección IP del grupo multicast en 6 caracteres hexadecimales.

Un ejemplo de esto es la dirección hexadecimal multicast 01-00-5E-00-00-C8, que se muestra en la animación.



Capítulo 5: Ethernet 5.1.4.1 MAC e IP

Existen dos direcciones principales asignadas a un dispositivo host:

- Dirección física (dirección MAC)
- Dirección lógica (dirección IP)

Tanto la dirección MAC como la dirección IP operan juntas para identificar un dispositivo en la red. El proceso de utilizar la dirección MAC y la dirección IP para encontrar una PC es similar al proceso de utilizar el nombre y la dirección de una persona para enviarle una carta.

El nombre de una persona generalmente no cambia. Por otro lado, la dirección de una persona indica dónde vive esa persona y puede cambiar.

La dirección MAC en un host, como los nombres de las personas, no cambia; se asigna físicamente a la NIC del host y se conoce como “dirección física”. La dirección física es siempre la misma, independientemente del lugar en donde se encuentre el host.

La dirección IP es similar a la dirección de una persona. Esta dirección está basada en la ubicación real del host. Con esta dirección, la trama puede determinar la ubicación adonde se deben enviar las tramas. La dirección IP, o dirección de red, se conoce como “dirección lógica” porque se asigna de forma lógica. Un administrador de red asigna esta dirección a cada host sobre la base de la red local a la que el host está conectado. En la ilustración, se muestra la naturaleza jerárquica de la localización de una persona sobre la base de una dirección “lógica”. Haga clic en cada grupo para ver cómo se filtra la dirección.

Para que una computadora pueda comunicarse en una red jerárquica, se necesitan tanto la dirección MAC física como la dirección IP lógica, de la misma manera en la que se necesitan el nombre y la dirección de una persona para poder enviarle una carta.

Capítulo 5: Ethernet 5.1.4.2 Conectividad de extremo a extremo, MAC e IP

Un dispositivo de origen envía un paquete sobre la base de una dirección IP. El servicio de nombres de dominios (DNS), en el que una dirección IP se asocia a un nombre de dominio, es una de las formas más comunes en que un dispositivo de origen determina la dirección IP de un dispositivo de destino. Por ejemplo, www.cisco.com equivale a 209.165.200.225. Esta dirección IP envía el paquete a la ubicación de red del dispositivo de destino. Los routers utilizan esta dirección IP para determinar el mejor camino para llegar a destino. Entonces, en resumen, el direccionamiento IP determina el comportamiento de extremo a extremo de un paquete IP.

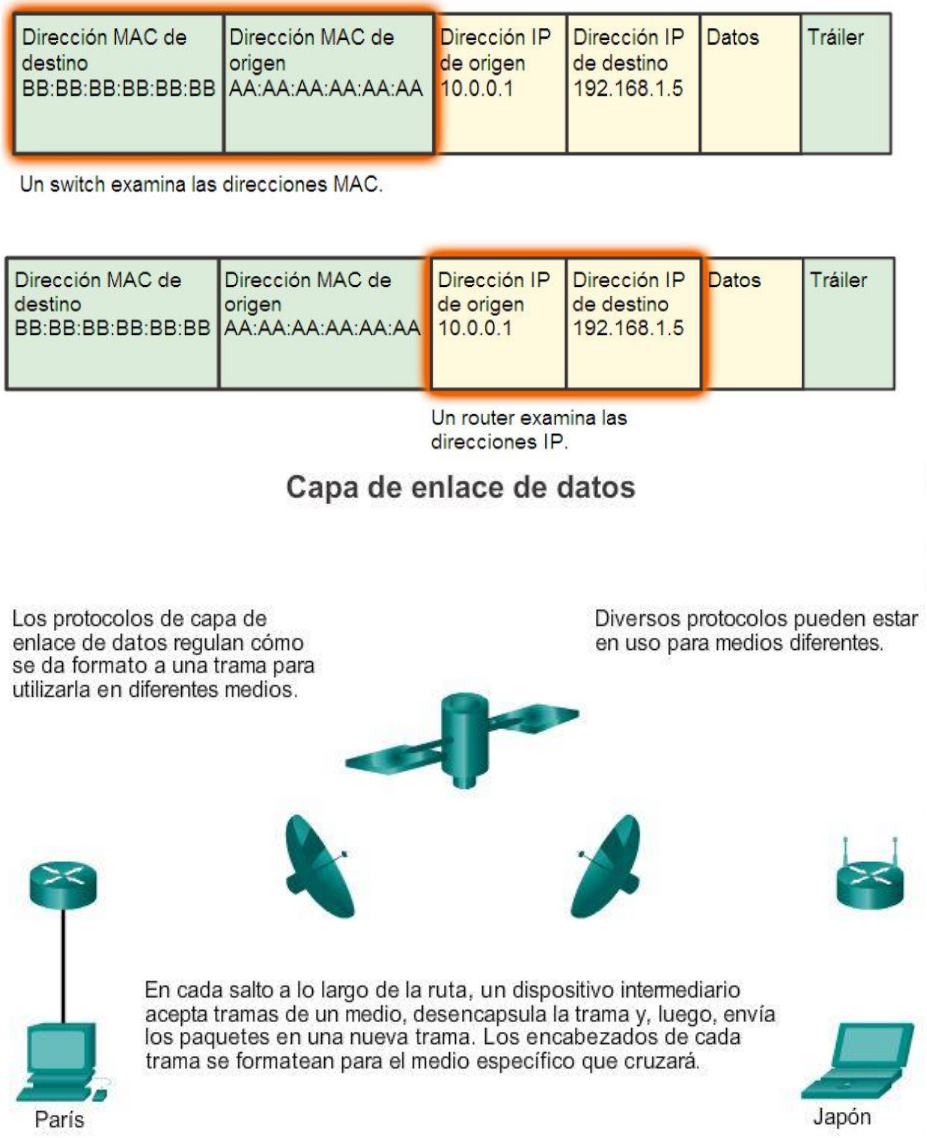
Sin embargo, en cada enlace de la ruta, se encapsula un paquete IP en una trama específica de la tecnología de enlace de datos particular relacionada con ese enlace, como Ethernet. Los dispositivos finales en una red Ethernet no aceptan ni procesan tramas según las direcciones IP. Por el contrario, las tramas se aceptan y procesan según las direcciones MAC.

En las redes Ethernet, las direcciones MAC se utilizan para identificar, en un nivel inferior, los hosts de origen y destino. Cuando un host de una red Ethernet se comunica, envía tramas que contienen su propia dirección MAC como origen y la dirección MAC del destinatario previsto como destino. Todos los hosts que reciben la trama leerán la dirección MAC de destino. El host procesa el mensaje solo si la dirección MAC de destino coincide con la dirección MAC configurada en su NIC.

En la figura 1, se muestra cómo se encapsula un paquete de datos, que contiene información de la dirección IP, con el entramado de la capa de enlace de datos, que contiene información de la dirección MAC.

En la figura 2, se muestra cómo se encapsulan las tramas según la tecnología del enlace real.

¿Cómo se relacionan las direcciones IP de los paquetes IP en un flujo de datos con las direcciones MAC en cada enlace a lo largo de la ruta hacia el destino? Esto se logra mediante un proceso denominado “protocolo de resolución de direcciones” (ARP).



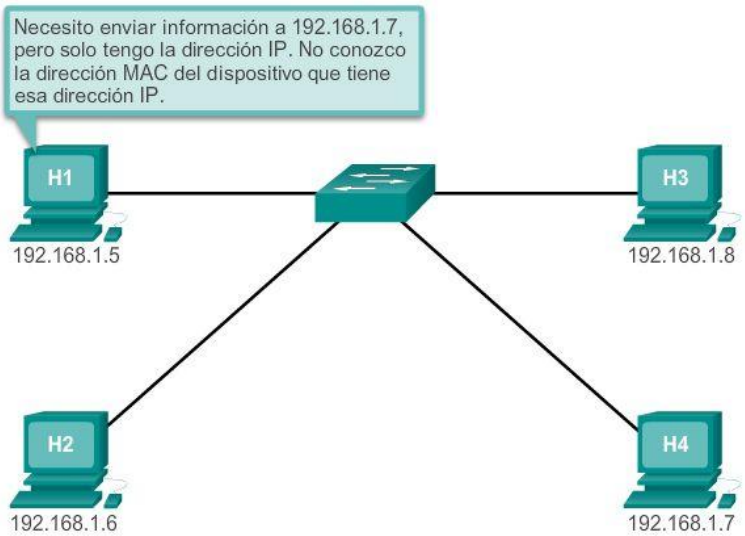
Capítulo 5: Ethernet 5.2.1.1 Introducción a ARP

Recuerde que cada nodo de una red IP tiene tanto una dirección MAC como una dirección IP. Para enviar datos, el nodo debe utilizar ambas direcciones. El nodo debe utilizar sus propias direcciones MAC e IP en los campos de origen y debe proporcionar una dirección MAC y una dirección IP para el destino. Mientras que una capa OSI superior proporciona la dirección IP del destino, pero el nodo de envío necesita encontrar la dirección MAC del destino para un enlace de Ethernet determinado. Ese es el propósito del protocolo ARP.

El protocolo ARP se basa en determinados tipos de mensajes Ethernet de broadcast y unicast, denominados “solicitudes ARP” y “respuestas ARP”.

El protocolo ARP ofrece dos funciones básicas:

- Resolución de direcciones IPv4 a direcciones MAC
- Mantenimiento de una tabla de las asignaciones



Capítulo 5: Ethernet 5.2.1.2 Funciones del protocolo ARP

Resolución de direcciones IPv4 a direcciones MAC

Para que una trama se coloque en los medios de la LAN, debe contar con una dirección MAC de destino. Cuando se envía un paquete a la capa de enlace de datos para que se encapsule en una trama, el nodo consulta una tabla en su memoria para encontrar la dirección de la capa de enlace de datos asignada a la dirección IPv4 de destino. Esta tabla se denomina tabla ARP o caché ARP. La tabla ARP se almacena en la RAM del dispositivo.

Cada entrada o fila de la tabla ARP vincula una dirección IP a una dirección MAC. La relación entre los dos valores se denomina mapa, que simplemente significa que usted puede localizar una dirección IP en la tabla y descubrir la dirección MAC correspondiente. En la tabla ARP, se guardan temporalmente (en caché) las asignaciones de los dispositivos en la LAN local.

Para comenzar el proceso, un nodo transmisor intenta localizar la dirección MAC asignada a un destino IPv4. Si se encuentra este mapa en la tabla, el nodo utiliza la dirección MAC como MAC de destino en la trama que encapsula el paquete IPv4. La trama se codifica entonces en los medios de la red.

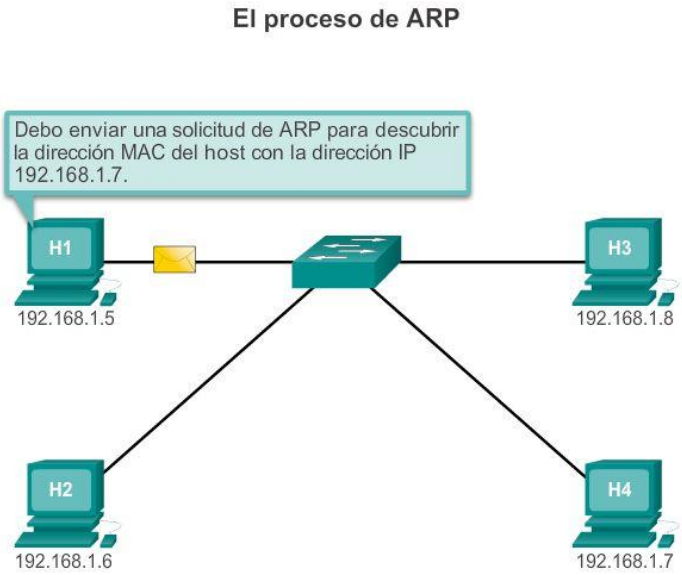
Mantenimiento de la tabla ARP

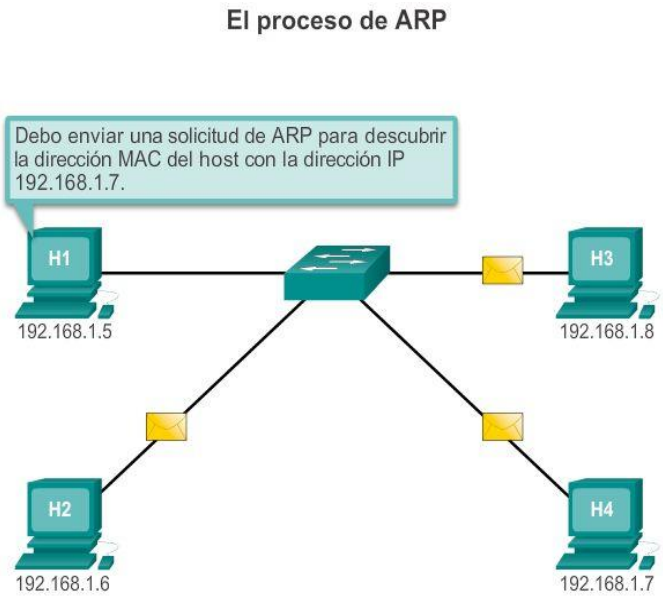
La tabla ARP se mantiene dinámicamente. Existen dos maneras en las que un dispositivo puede reunir direcciones MAC. Una es monitorear el tráfico que se produce en el segmento de la red local. A medida que un nodo recibe tramas de los medios, puede registrar las direcciones IP y MAC de origen como mapeos en la tabla ARP. A medida que las tramas se transmiten en la red, el dispositivo completa la tabla ARP con los pares de direcciones.

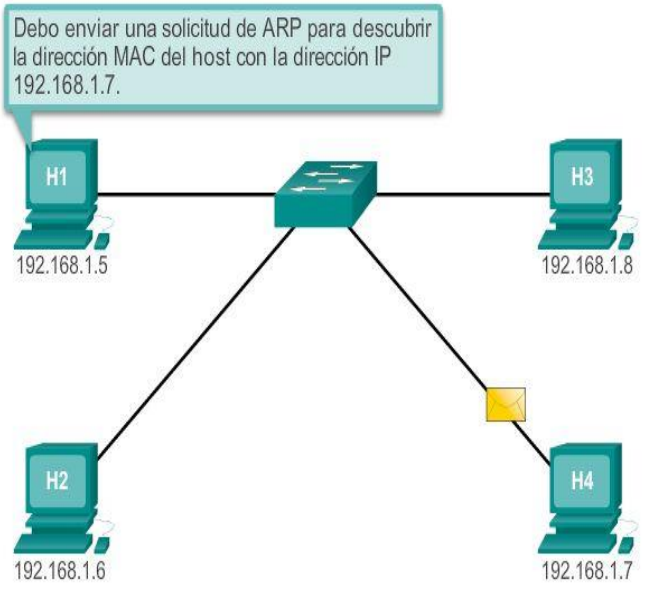
Un dispositivo también puede obtener pares de direcciones mediante el envío de una solicitud de ARP, como se muestra en la ilustración. Una solicitud de ARP es un broadcast de capa 2 que se transmite a todos los dispositivos en la LAN Ethernet. La solicitud de ARP contiene la dirección IP del host de destino y la dirección MAC de broadcast, FFFF.FFFF.FFFF. Dado que se trata de un broadcast, todos los nodos en la LAN Ethernet reciben y examinan el contenido. El nodo cuya dirección IP coincide con la dirección IP en la solicitud de ARP responde. La respuesta es una trama de unicast que incluye la dirección MAC que corresponde a la dirección IP en la solicitud. Esta respuesta se utiliza para crear una entrada nueva en la tabla ARP del nodo de envío.

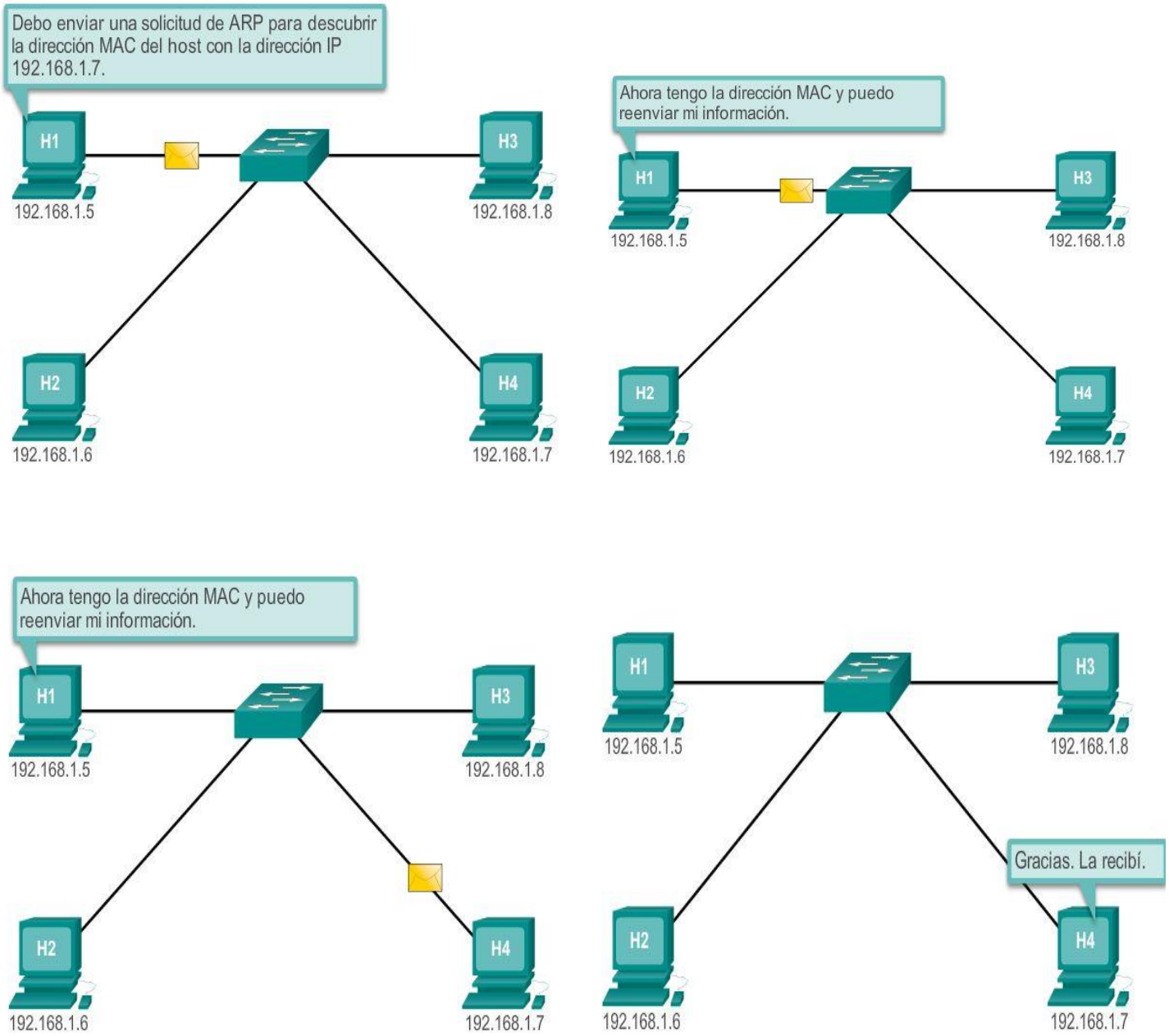
Las entradas en la tabla ARP tienen una marca de hora similar a la de las entradas de la tabla MAC en los switches. Si un dispositivo no recibe una trama de un dispositivo determinado antes de que caduque la marca horaria, la entrada para ese dispositivo se elimina de la tabla ARP.

Además, pueden ingresarse entradas estáticas de asignaciones en una tabla ARP, pero esto no sucede con frecuencia. Las entradas estáticas de la tabla ARP no caducan con el tiempo y deben eliminarse en forma manual.









Capítulo 5: Ethernet 5.2.1.3 Funcionamiento del ARP

Creación de la trama

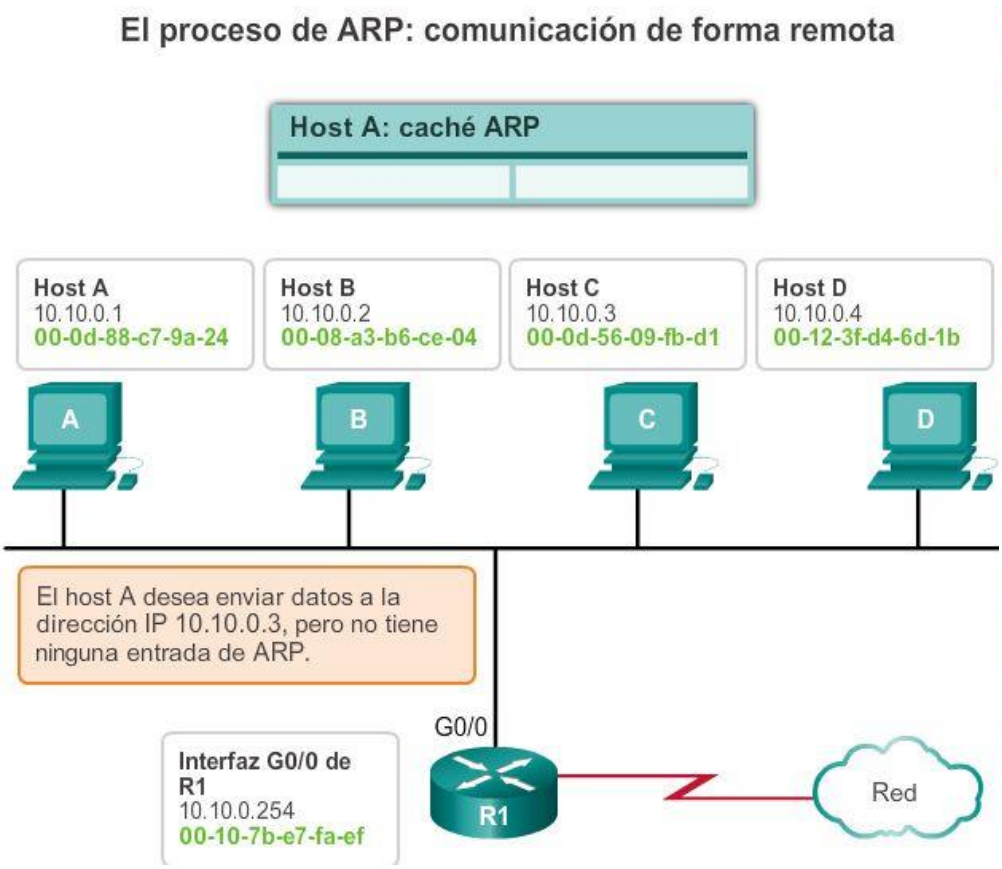
¿Qué hace un nodo cuando debe crear una trama y la caché ARP no contiene una asignación de una dirección IP hacia una dirección MAC de destino? Genera una solicitud de ARP.

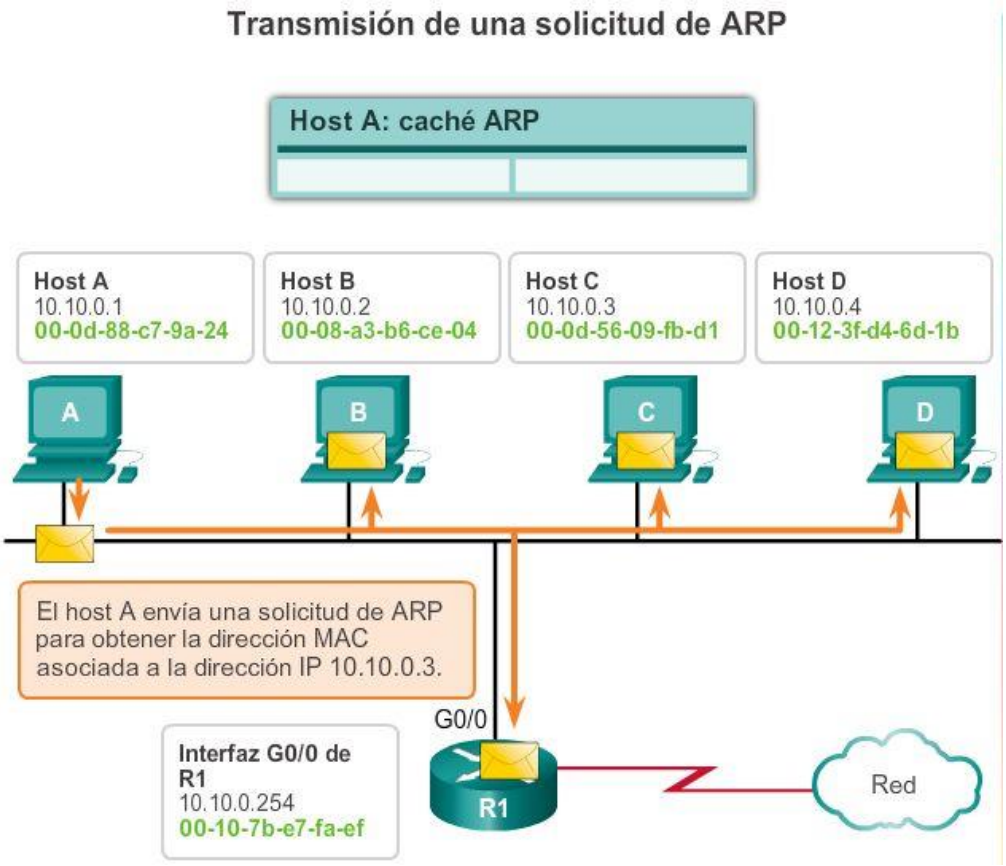
Cuando el ARP recibe una solicitud para mapear una dirección IPv4 a una dirección MAC, busca el mapa almacenado en su tabla ARP. Si no encuentra la entrada, la encapsulación del paquete IPv4 no se realiza y los procesos de Capa 2 notifican al ARP que necesita un mapa. Los procesos ARP envían entonces un paquete de solicitud de ARP para descubrir la dirección MAC del dispositivo de destino de la red local. Si un dispositivo que recibe la solicitud tiene la dirección IP de destino, responde con una respuesta de ARP. Se crea un mapa en la tabla ARP. Los paquetes para esa dirección IPv4 pueden ahora encapsularse en tramas.

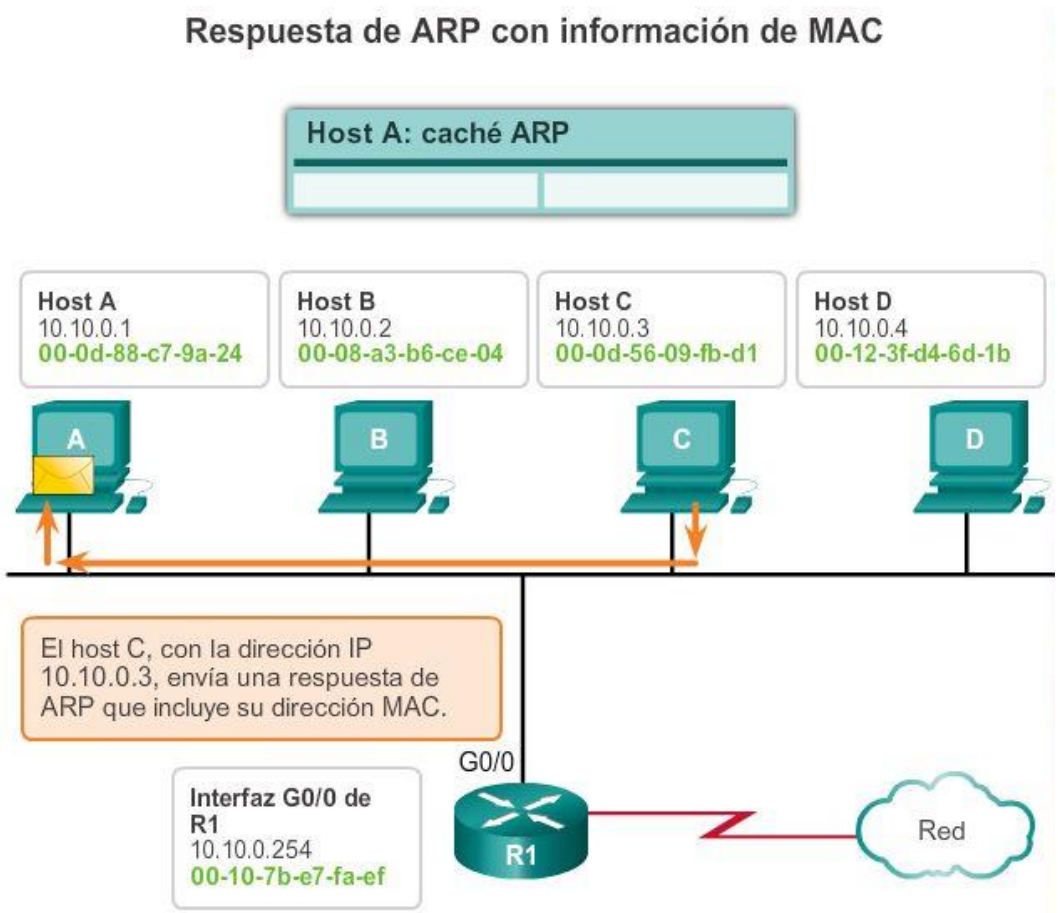
Si ningún dispositivo responde a la solicitud de ARP, el paquete se descarta porque no puede crearse una trama. Esta falla de encapsulación se informa a las capas superiores del dispositivo.

Si el dispositivo es un dispositivo intermediario, como por ejemplo, un router, las capas superiores pueden optar por responder al host de origen con un error en un paquete ICMPv4.

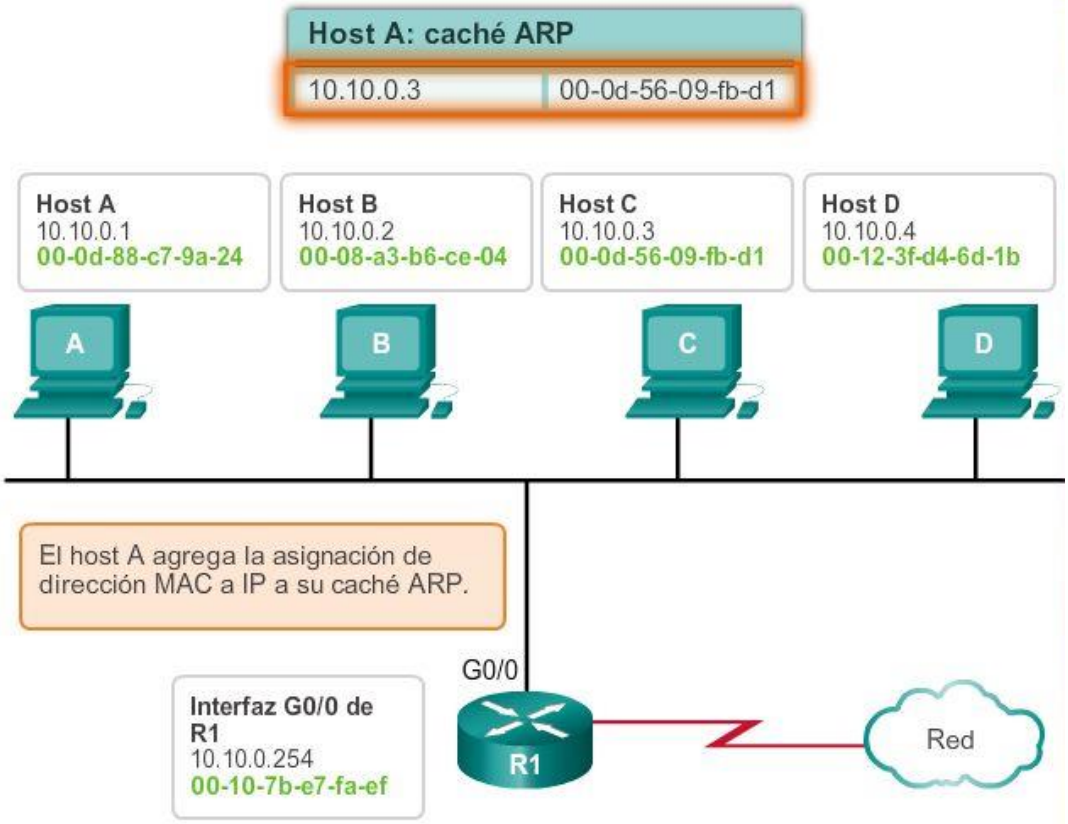
Consulte las figuras 1 a 5 para conocer el proceso utilizado para obtener la dirección MAC del nodo en la red física local.



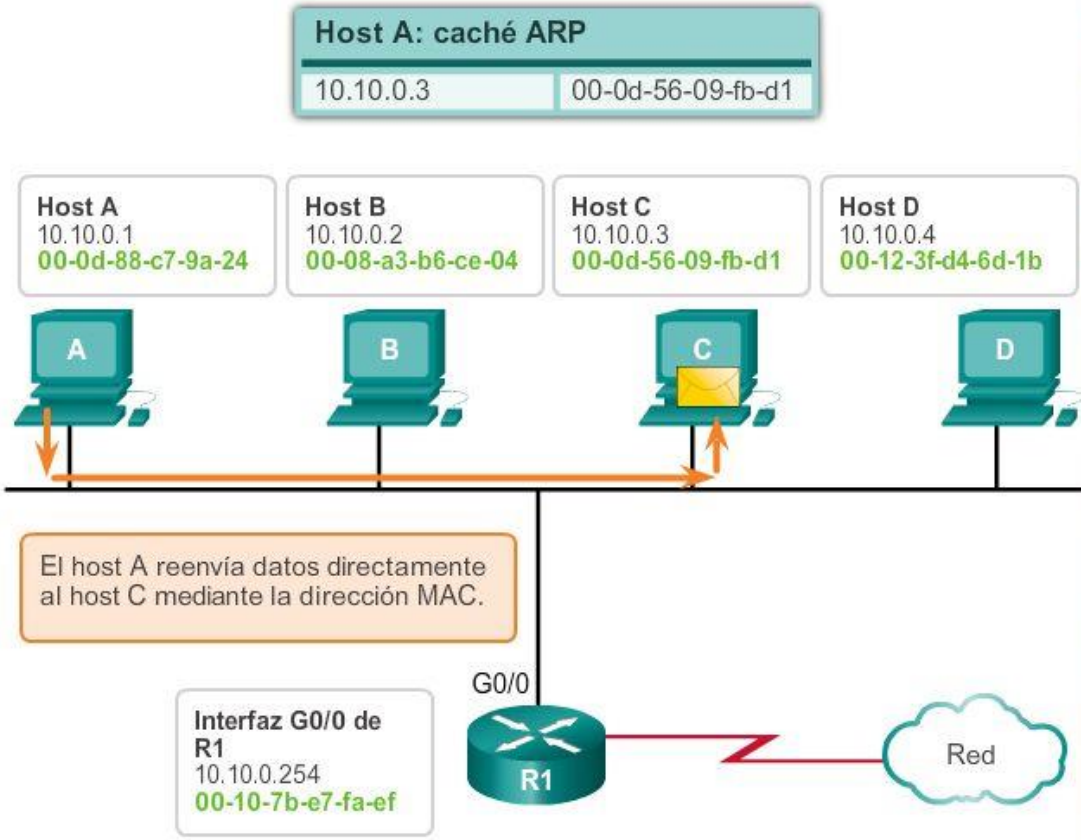

Transmisión de una solicitud de ARP
Host A: caché ARP
Host A
10.10.0.1
00-0d-88-c7-9a-24
Host B
10.10.0.2
00-08-a3-b6-ce-04
Host C
10.10.0.3
00-0d-56-09-fb-d1
Host D
10.10.0.4
00-12-3f-d4-6d-1b
A
B
C
D
El host A envía una solicitud de ARP para obtener la dirección MAC asociada a la dirección IP 10.10.0.3.
G0/0
Interfaz G0/0 de R1
10.10.0.254
00-10-7b-e7-fa-ef
R1
Red


Respuesta de ARP con información de MAC
Host A: caché ARP
Host A
10.10.0.1
00-0d-88-c7-9a-24
Host B
10.10.0.2
00-08-a3-b6-ce-04
Host C
10.10.0.3
00-0d-56-09-fb-d1
Host D
10.10.0.4
00-12-3f-d4-6d-1b
A
B
C
D
El host C, con la dirección IP 10.10.0.3, envía una respuesta de ARP que incluye su dirección MAC.
G0/0
Interfaz G0/0 de R1
10.10.0.254
00-10-7b-e7-fa-ef
R1
Red

Agregado de asignación de MAC a IP en el caché ARP



Reenvío de datos con información de dirección MAC



Capítulo 5: Ethernet 5.2.1.4 Función del protocolo ARP en la comunicación remota

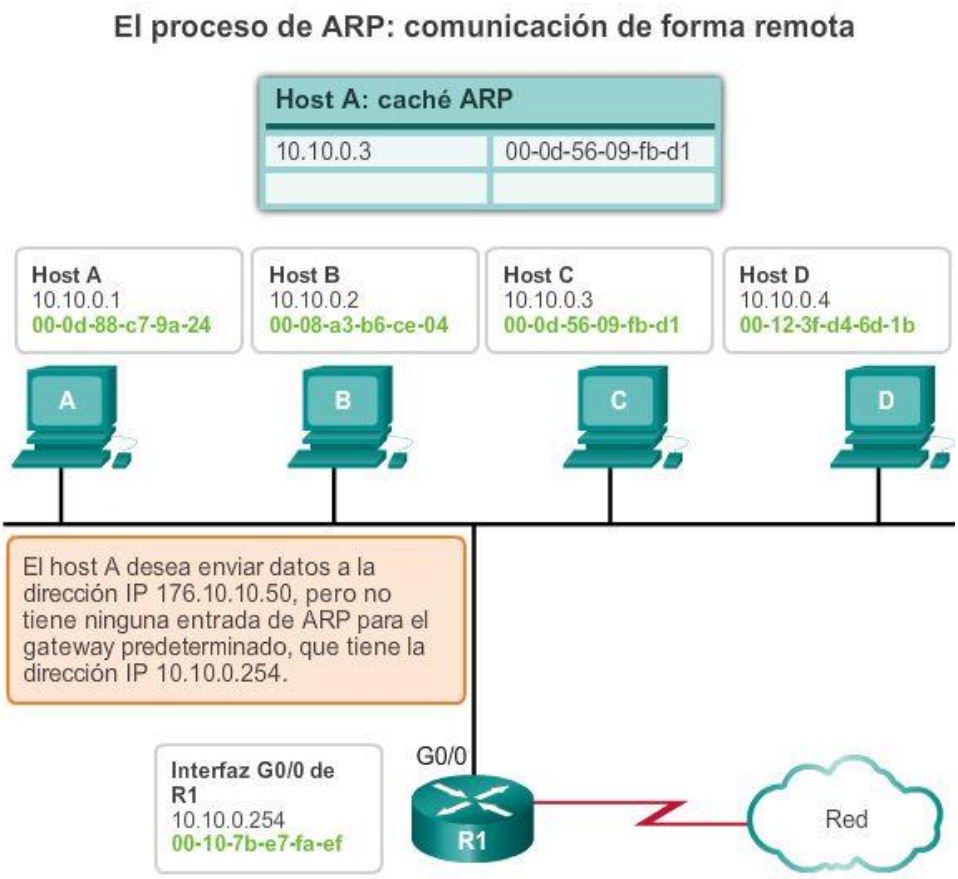
Todas las tramas deben enviarse a un nodo de un segmento de red local. Si el host IPv4 de destino se encuentra en la red local, la trama utilizará la dirección MAC de este dispositivo como la dirección MAC de destino.

Si el host IPv4 de destino no se encuentra en la red local, el nodo de origen necesita enviar la trama a la interfaz del router que es el gateway o el siguiente salto que se utiliza para llegar a dicho destino. El nodo de origen utilizará la dirección MAC del gateway como dirección de destino para las tramas que contengan un paquete IPv4 dirigido a hosts que se encuentren en otras redes.

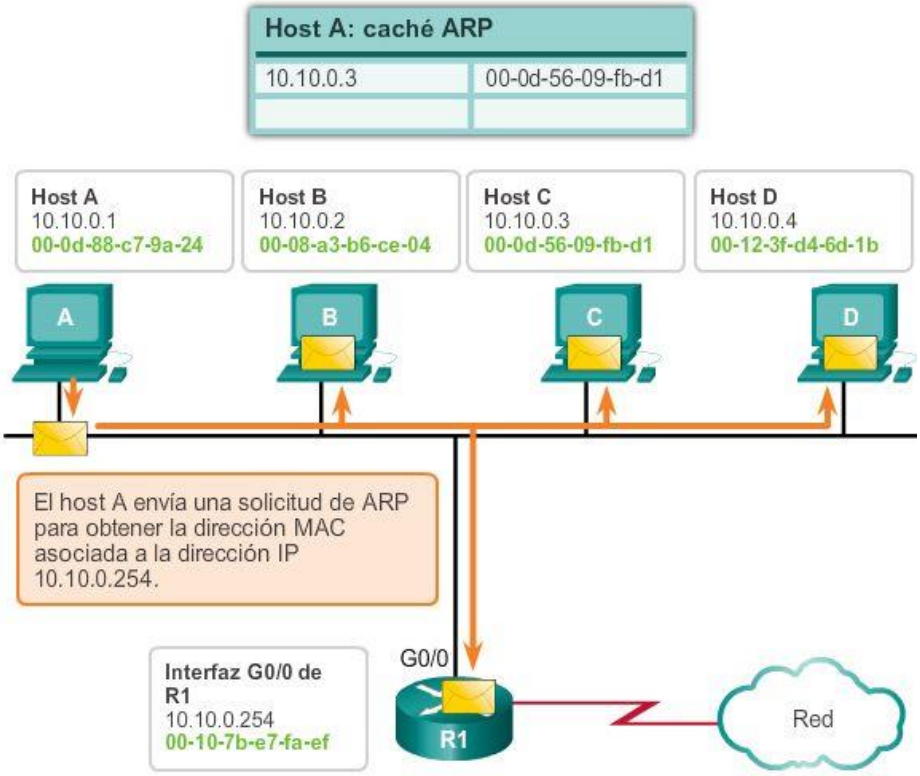
La dirección de gateway de la interfaz del router se almacena en la configuración IPv4 de los hosts. Cuando un host crea un paquete para un destino, compara la dirección IP de destino con su propia dirección IP para determinar si las dos direcciones IP se encuentran en la misma red de Capa 3. Si el host receptor no se encuentra en la misma red, el origen utiliza el proceso de ARP para determinar una dirección MAC para la interfaz del router que sirve de gateway.

En caso de que la entrada de gateway no se encuentre en la tabla, el proceso de ARP normal enviará una solicitud de ARP para recuperar la dirección MAC asociada con la dirección IP de la interfaz del router.

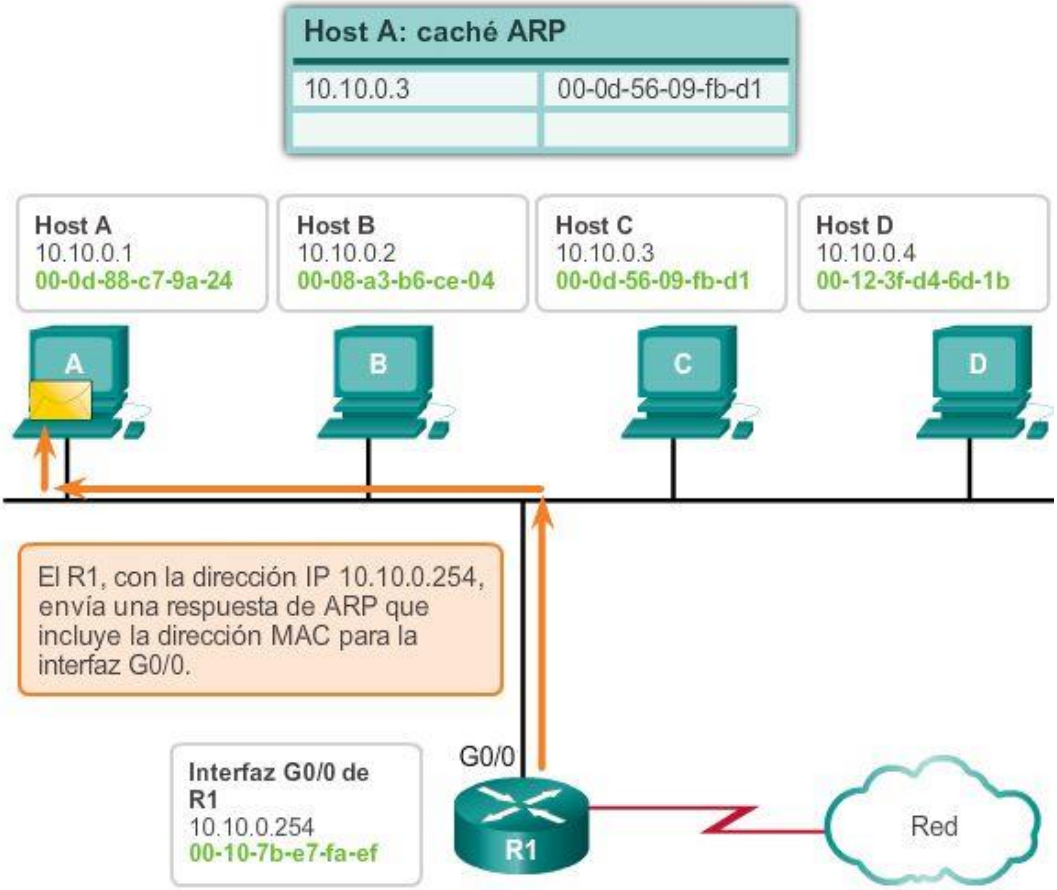
Consulte las figuras 1 a 5 para conocer el proceso utilizado para obtener la dirección MAC del gateway.



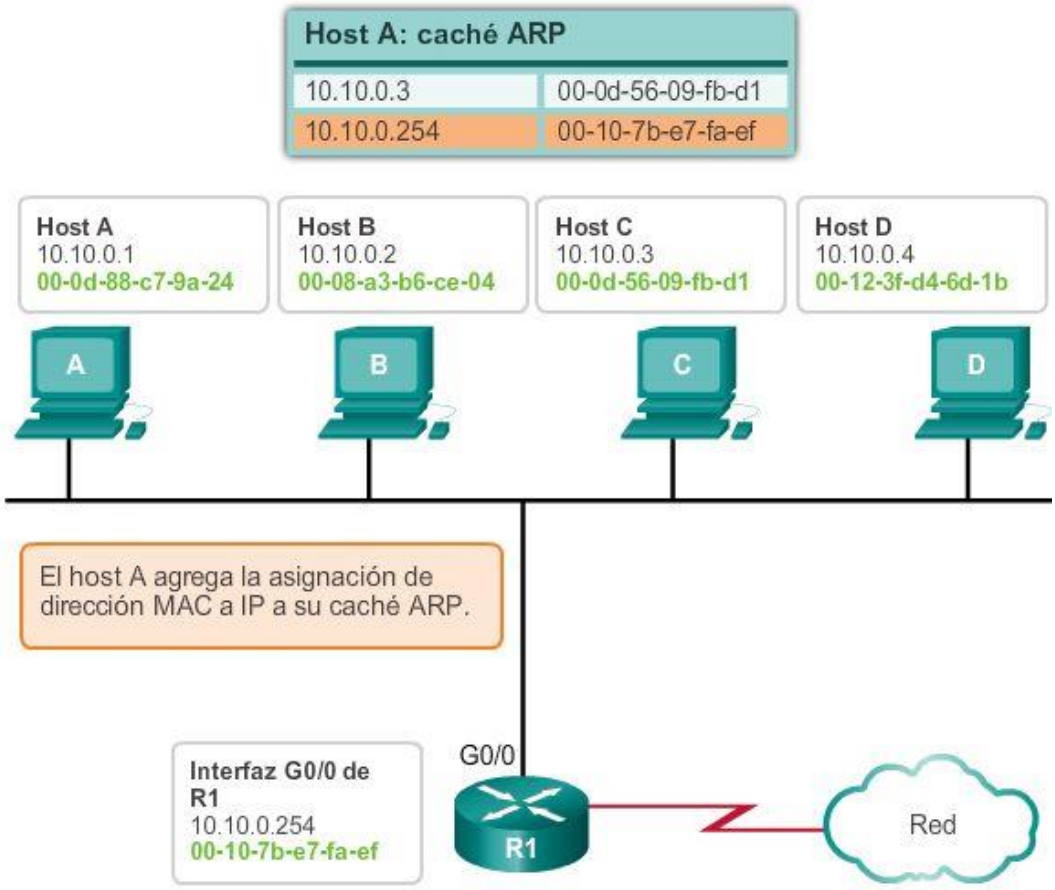
Transmisión de una solicitud de ARP

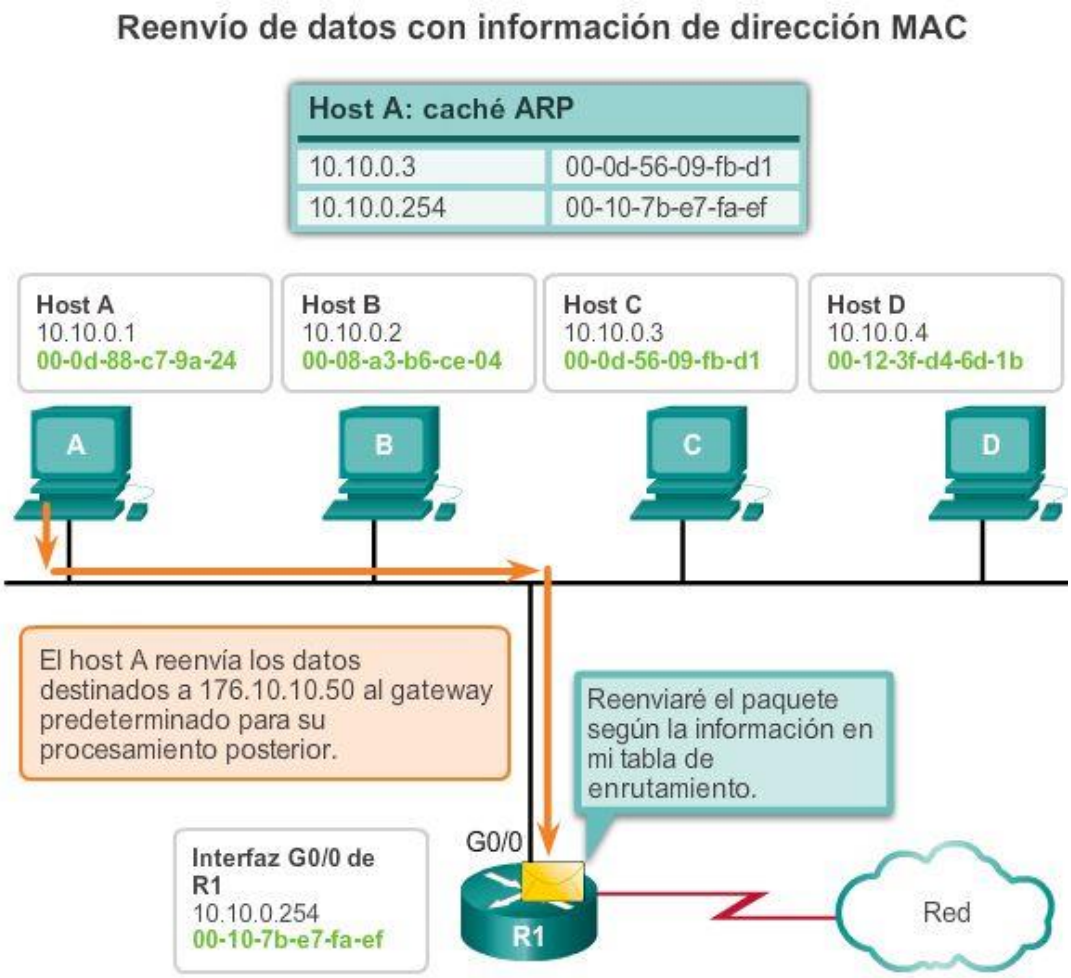


Respuesta de ARP con información de MAC



Agregado de asignación de MAC a IP en el caché ARP





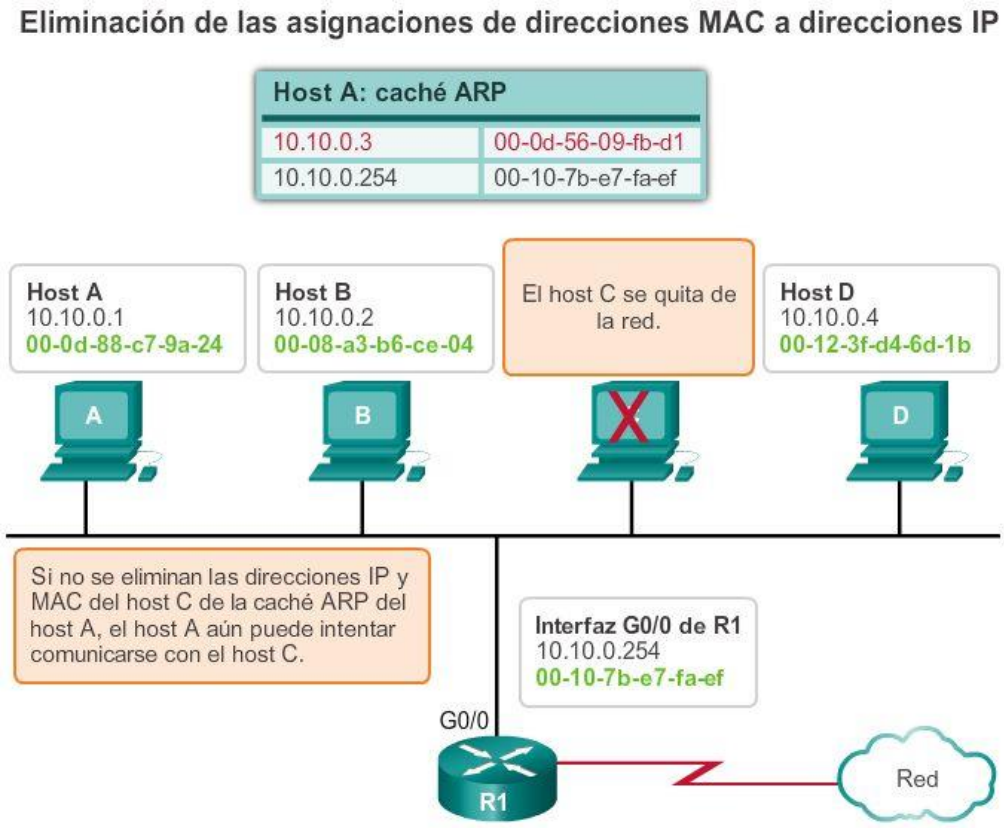
Capítulo 5: Ethernet 5.2.1.5 Eliminación de entradas de una tabla ARP

Para cada dispositivo, un temporizador de caché ARP elimina las entradas ARP que no se hayan utilizado durante un período de tiempo especificado. Los tiempos difieren dependiendo del dispositivo y su sistema operativo. Por ejemplo: algunos sistemas operativos de Windows almacenan las entradas de caché ARP por 2 minutos. Si la entrada se utiliza nuevamente durante ese tiempo, el temporizador ARP para esa entrada se extiende a 10 minutos.

También pueden utilizarse comandos para eliminar manualmente todas o algunas de las entradas de la tabla ARP. Después de eliminar una entrada, el proceso para enviar una solicitud de ARP y recibir una respuesta de ARP debe ocurrir nuevamente para ingresar la asignación en la tabla ARP.

Cada dispositivo tiene un comando específico del sistema operativo para eliminar el contenido de la caché ARP. Estos comandos de ninguna manera invocan la ejecución de ARP, sino que, simplemente, eliminan las entradas de la tabla ARP. El dispositivo integra el servicio ARP dentro del protocolo IPv4 y lo implementa. Su funcionamiento es transparente para aplicaciones y usuarios de capa superior.

Como se muestra en la ilustración, a veces es necesario eliminar una entrada de tabla ARP.



Capítulo 5: Ethernet 5.2.1.6 Tablas ARP en dispositivos de red

En un router Cisco, se utiliza el comando show ip arp para mostrar la tabla ARP, como se muestra en la figura 1.

En una PC con Windows 7, se utiliza el comando arp -a para mostrar la tabla ARP, como se muestra en la figura 2.

Tabla ARP del router

```
Router#show ip arp

                     Age
Protocol  Address          (min)  Hardware Addr   Type   Interface
Internet  172.16.233.229    -    0000.0c59.f892   ARPA   Ethernet0/0
Internet  172.16.233.218    -    0000.0c07.ac00   ARPA   Ethernet0/0
Internet  172.16.168.11     -    0000.0c63.1300   ARPA   Ethernet0/0
Internet  172.16.168.254    9    0000.0c36.6965   ARPA   Ethernet0/0
```

Tabla ARP del host

```
C:\>arp -a

Interface: 192.168.1.67 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.254         64-0f-29-0d-36-91     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.82.253.91 --- 0x10
  Internet Address      Physical Address      Type
  10.82.253.92          64-0f-29-0d-36-91     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Capítulo 5: Ethernet 5.2.2.1 Cómo puede ocasionar problemas el protocolo ARP

En la ilustración, se muestran dos problemas potenciales con el protocolo ARP.

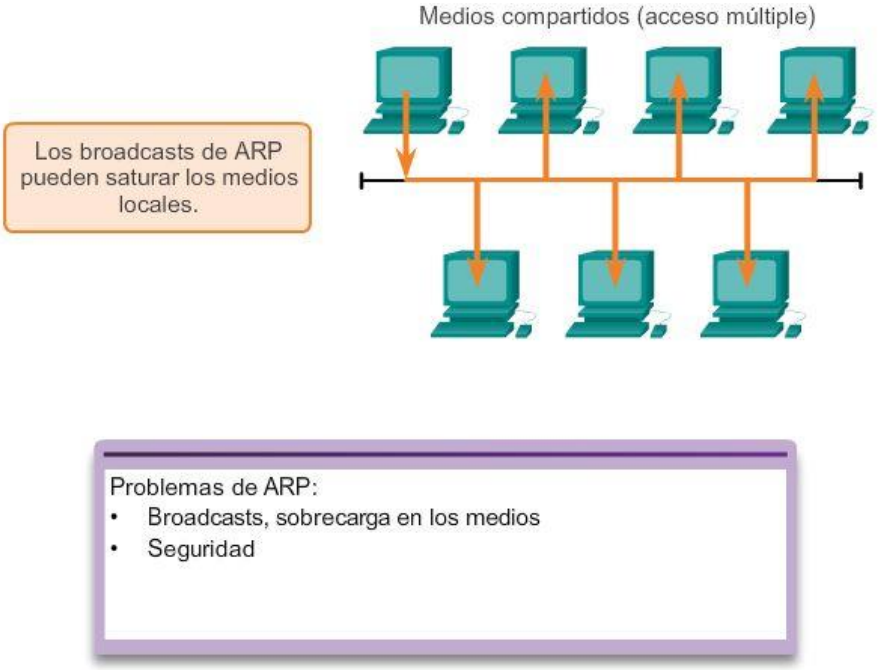
Sobrecarga en los medios

Todos los dispositivos de la red local reciben y procesan una solicitud de ARP debido a que es una trama de broadcast. En una red comercial típica, estos broadcasts tendrían probablemente un impacto mínimo en el rendimiento de la red. Sin embargo, si un gran número de dispositivos se encendiera y todos comenzaran a acceder a los servicios de la red al mismo tiempo, podría haber una disminución del rendimiento durante un período de tiempo breve. Por ejemplo, si todos los estudiantes de una práctica de laboratorio inician sesión en computadoras del aula e intentan acceder a Internet al mismo tiempo, podría haber demoras. Sin embargo, una vez que los dispositivos envían los broadcasts de ARP iniciales y que aprenden las direcciones MAC necesarias, se minimizará todo impacto en la red.

Seguridad

En algunos casos, el uso del ARP puede ocasionar un riesgo potencial de seguridad. La suplantación o el envenenamiento ARP es una técnica que utiliza un atacante para introducir una asociación de direcciones MAC incorrecta en una red emitiendo respuestas ARP falsas. El individuo falsifica la dirección MAC de un dispositivo y de esta manera las tramas pueden enviarse a la dirección equivocada.

Configurar manualmente asociaciones ARP estáticas es una manera de impedir la suplantación de identidad de ARP. Las direcciones MAC autorizadas pueden configurarse en algunos dispositivos de red para que limiten el acceso a la red para sólo los dispositivos indicados.



Los mensajes ARP falsos pueden proporcionar una dirección MAC incorrecta que luego toma control de las tramas que utilizan esa dirección (proceso denominado “suplantación”).

Capítulo 5: Ethernet 5.2.2.2 Mitigación de problemas de ARP

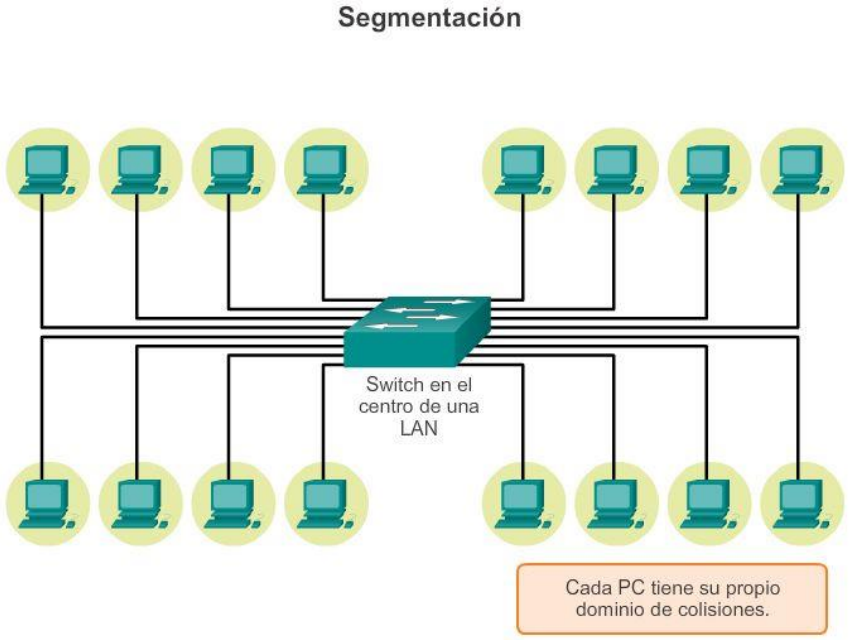
Los switches modernos pueden mitigar los problemas de broadcast y de seguridad relacionados con ARP. Los switches Cisco admiten varias tecnologías de seguridad diseñadas específicamente para mitigar problemas de Ethernet relacionados con los broadcasts, en general, y con ARP, en particular.

Los switches proporcionan la segmentación de LAN, ya que las dividen en dominios de colisiones independientes. Cada puerto de un switch representa un dominio de colisiones distinto y proporciona el ancho de banda de medio completo al nodo o a los nodos conectados a dicho puerto.

Si bien los switches no impiden de manera predeterminada que los broadcasts se propaguen a los dispositivos conectados, aíslan las comunicaciones unicast de Ethernet de modo que solamente las “escuchen” el dispositivo de origen y de destino.

Entonces, si hay una gran cantidad de solicitudes de ARP, cada respuesta de ARP tendrá lugar solamente entre dos dispositivos.

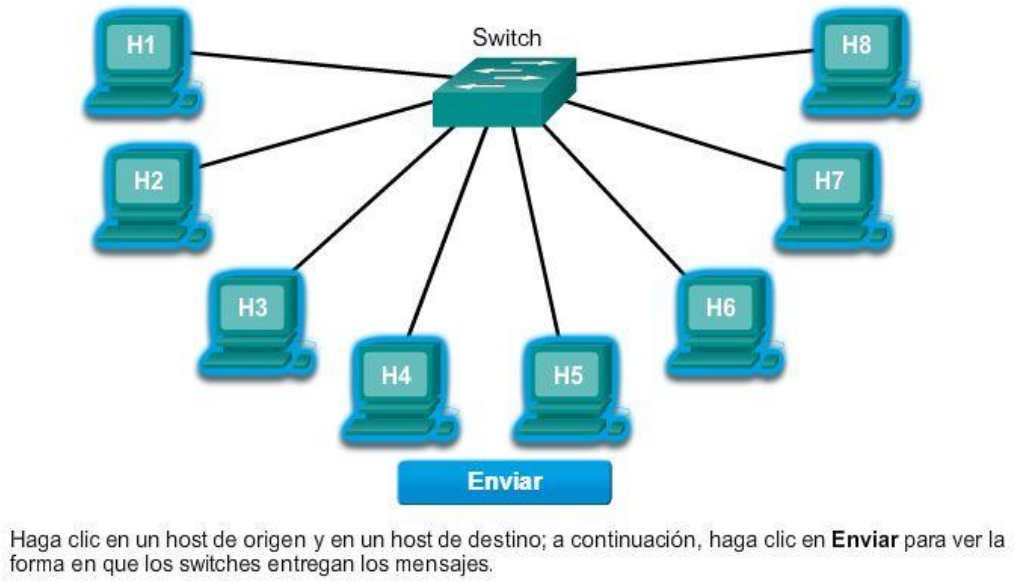
Con respecto a la mitigación de diferentes tipos de ataques de broadcast, a los que las redes Ethernet son propensas, los ingenieros de red implementan tecnologías de seguridad de switches de Cisco, como listas de acceso y seguridad de puertos especializadas.



Capítulo 5: Ethernet 5.3.1.1 Aspectos básicos de los puertos de switch

Recuerde que la topología lógica de una red Ethernet es un bus de multiacceso en el que todos los dispositivos comparten el acceso al mismo medio. Esta topología lógica determina la forma en que los hosts de la red ven y procesan las tramas enviadas y recibidas en la red. Sin embargo, en la actualidad, la topología física de la mayor parte de las redes Ethernet es en estrella y en estrella extendida. Esto significa que, en la mayoría de las redes Ethernet, los dispositivos finales se suelen conectar a un switch LAN de capa 2 de forma punto a punto.

Los switches LAN de capa 2 llevan a cabo los procesos de conmutación y filtrado basándose solamente en la dirección MAC de la capa de enlace de datos (capa 2) del modelo OSI. El switch es completamente transparente para los protocolos de red y las aplicaciones de usuario. Los switches de capa 2 crean una tabla de direcciones MAC que utilizan para tomar decisiones de reenvío. Los switches de capa 2 dependen de los routers para pasar datos entre subredes IP independientes.



Capítulo 5: Ethernet 5.3.1.2 Tabla de direcciones MAC del switch

Los switches emplean direcciones MAC para dirigir las comunicaciones de red a través de su estructura al puerto correspondiente hasta el nodo de destino. La estructura del switch son los circuitos integrados y la programación de máquina adjunta que permite controlar las rutas de datos a través del switch. El switch debe primero saber qué nodos existen en cada uno de sus puertos para poder definir cuál será el puerto que utilizará para transmitir una trama unicast.

El switch determina cómo manejar las tramas de datos entrantes mediante una tabla de direcciones MAC. El switch genera su tabla de direcciones MAC grabando las direcciones MAC de los nodos que se encuentran conectados en cada uno de sus puertos. Una vez que la dirección MAC de un nodo específico en un puerto determinado queda registrada en la tabla de direcciones, el switch ya sabe enviar el tráfico destinado a ese nodo específico desde el puerto asignado a dicho nodo para posteriores transmisiones.

Cuando un switch recibe una trama de datos entrantes y la dirección MAC de destino no figura en la tabla, éste reenvía la trama a todos los puertos excepto al que la recibió en primer lugar. Cuando el nodo de destino responde, el switch registra la dirección MAC de éste en la tabla de direcciones del campo dirección de origen de la trama.

En las redes que cuentan con varios switches interconectados, las tablas de direcciones MAC registran varias direcciones MAC para los puertos que conectan los switches que reflejan los nodos de destino. Generalmente, los puertos de los switches que se utilizan para interconectar dos switches cuentan con varias direcciones MAC registradas en la tabla de direcciones.

Para ver cómo funciona, consulte cada uno de los pasos en las figuras 1 a 6.

A continuación se describe este proceso:

Paso 1. El switch recibe una trama de broadcast de la PC1 en el Puerto 1.

Paso 2. El switch ingresa la dirección MAC de origen y el puerto del switch que recibió la trama en la tabla de direcciones.

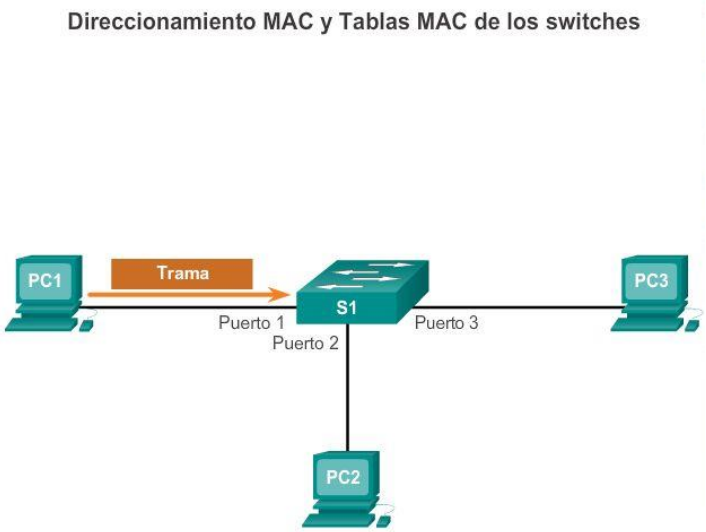
Paso 3. Dado que la dirección de destino es broadcast, el switch satura todos los puertos enviando la trama, excepto el puerto que la recibió.

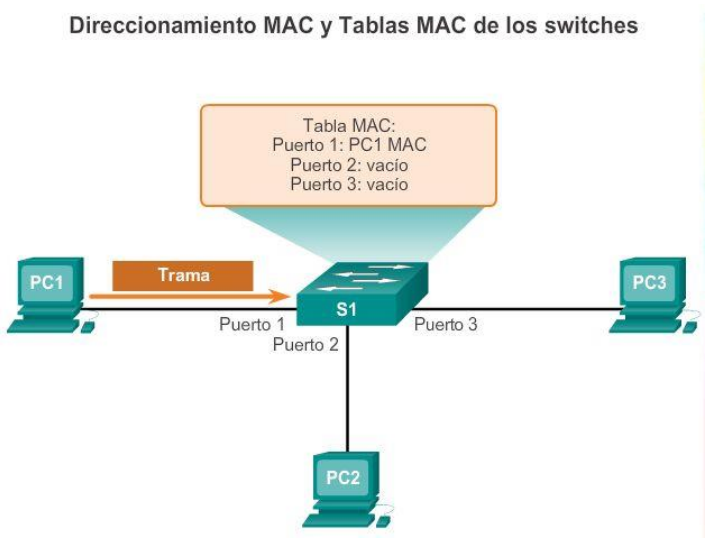
Paso 4. El dispositivo de destino responde al broadcast con una trama de unicast dirigida a la PC1.

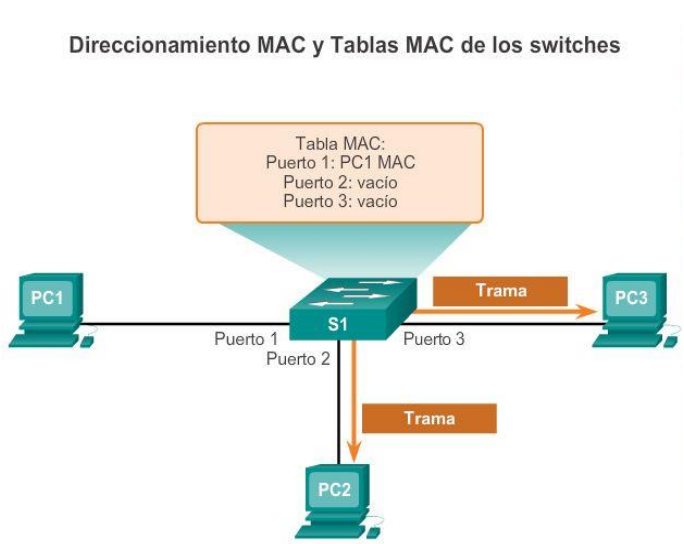
Paso 5. El switch introduce en la tabla de direcciones la dirección MAC de origen de la PC2 y el número del puerto de switch que recibió la trama. En la tabla de direcciones MAC pueden encontrarse la dirección de destino de la trama y su puerto asociado.

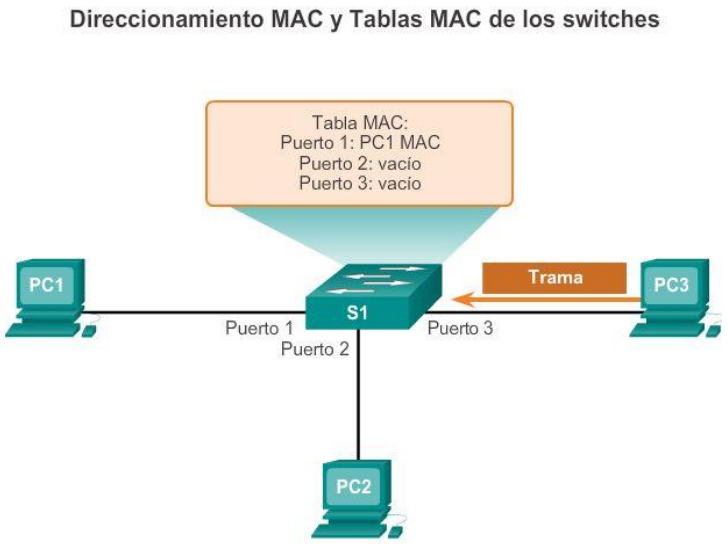
Paso 6. Ahora el switch puede enviar tramas entre los dispositivos de origen y destino sin saturar el tráfico, ya que cuenta con entradas en la tabla de direcciones que identifican a los puertos asociados.

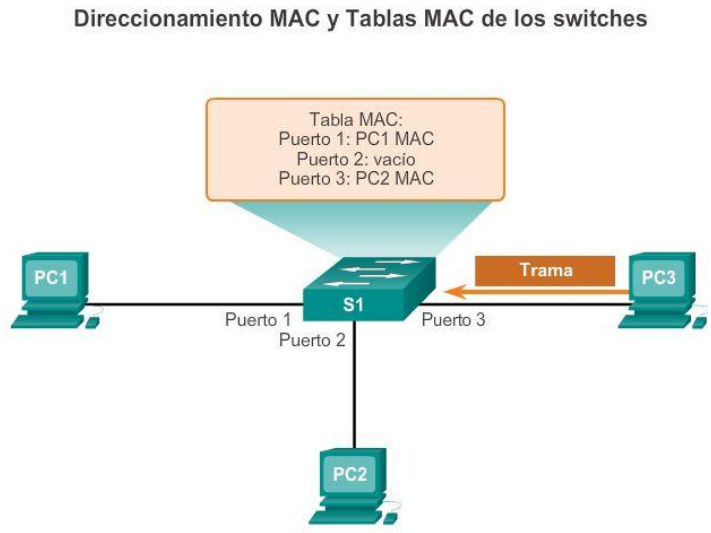
Nota: en ocasiones, la tabla de direcciones MAC se denomina “tabla de memoria de contenido direccionable” (CAM). Si bien el término “tabla CAM” es bastante común, para el propósito de este curso la denominaremos “tabla de direcciones MAC”.

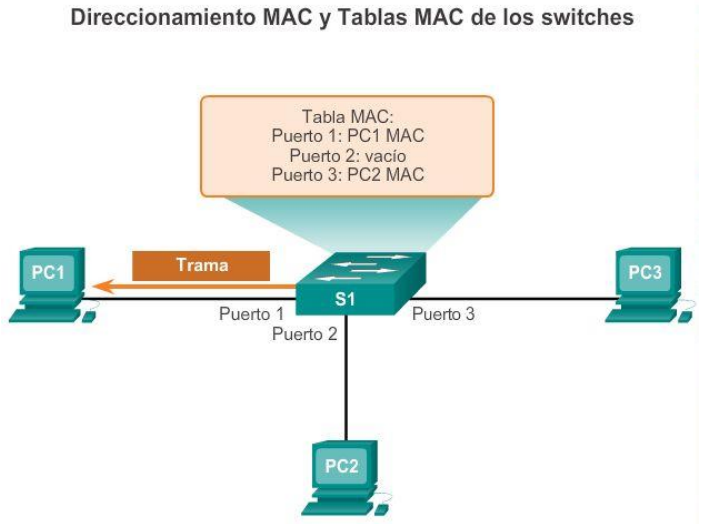












Capítulo 5: Ethernet 5.3.1.3 Configuración de Dúplex

Si bien los switches son transparentes para los protocolos de red y las aplicaciones de usuario, pueden funcionar en modos diferentes que pueden tener tanto efectos positivos como negativos al reenviar tramas de

Ethernet en una red. Una de las configuraciones más básicas de un switch es la configuración de dúplex de cada puerto individual conectado a cada dispositivo host.

Los puertos en los switches debe estar configurados para coincidir con la configuración de dúplex del tipo de medio. Existen dos tipos de configuraciones de dúplex que se utilizan para las comunicaciones en una red Ethernet: half duplex y full duplex.

Half duplex

La comunicación half-duplex se basa en un flujo de datos unidireccional en el que el envío y la recepción de datos no se producen al mismo tiempo. Esto es similar a la función de las radios de dos vías o dos walki-talkies en donde una sola persona puede hablar a la vez. Si una persona habla mientras lo hace la otra, se produce una colisión.

Por ello, la comunicación half-duplex implementa el CSMA/CD con el objeto de reducir las posibilidades de que se produzcan colisiones y detectarlas en caso de que se presenten. Las comunicaciones half-duplex presentan problemas de funcionamiento debido a la constante espera, ya que el flujo de datos sólo se produce en una dirección a la vez. Las conexiones half-duplex suelen verse en los dispositivos de hardware más antiguos, como los hubs.

Los nodos que están conectados a los hubs y que comparten su conexión con un puerto de un switch deben funcionar en el modo half-duplex porque las computadoras finales deben tener la capacidad de detectar las colisiones. Los nodos pueden funcionar en el modo half-duplex si la tarjeta NIC no puede configurarse para hacerlo en full duplex. En este caso, el puerto del switch también adopta el modo half-duplex predeterminado. Debido a estas limitaciones, la comunicación full-duplex ha reemplazado a la half duplex en los elementos de hardware más modernos.

Full duplex

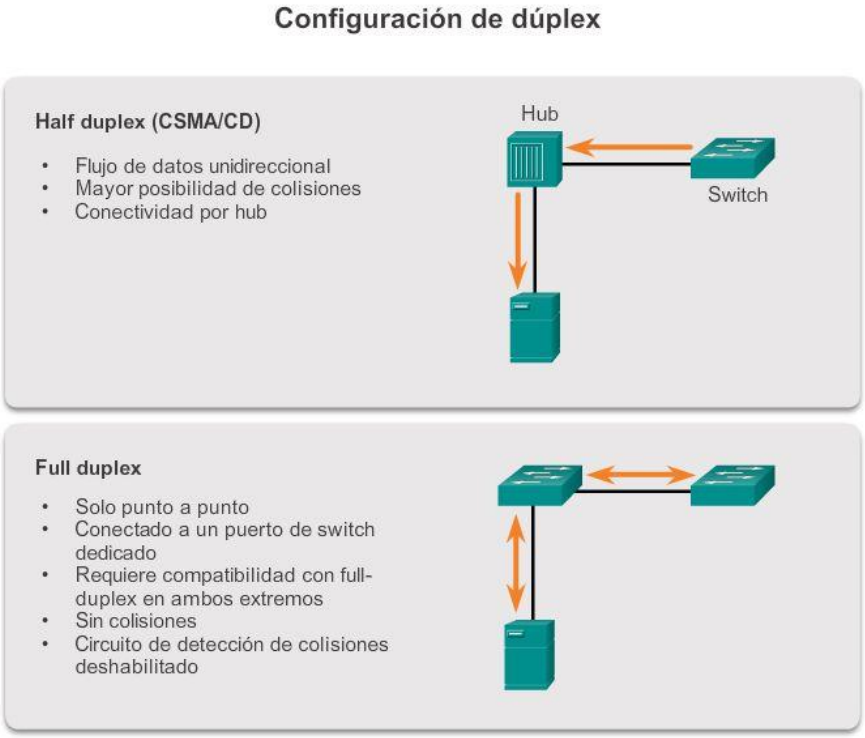
En las comunicaciones full-duplex el flujo de datos es bidireccional, por lo tanto la información puede enviarse y recibirse al mismo tiempo. La capacidad bidireccional mejora el rendimiento, dado que reduce el tiempo de espera entre las transmisiones. Actualmente, la mayoría de las tarjetas NIC Ethernet, Fast Ethernet y Gigabit Ethernet disponibles en el mercado proporciona capacidad full-duplex. En el modo full-duplex, el circuito de detección de colisiones se encuentra desactivado. Las tramas enviadas por los dos nodos finales conectados no pueden colisionar, dado que éstos utilizan dos circuitos independientes en el cable de la red. Cada conexión full-duplex utiliza un solo puerto. Las conexiones full-duplex requieren un switch que admita esta modalidad o bien una conexión directa entre dos nodos compatibles con el modo full duplex. Los nodos que se conecten directamente al puerto de un switch dedicado con tarjetas NIC capaces de admitir full duplex deben conectarse a puertos que estén configurados para funcionar en el modo full-duplex.

La figura muestra los dos parámetros dúplex que están disponibles en los equipos de red modernos.

Los switches Cisco Catalyst admiten tres configuraciones dúplex:

- La opción full establece el modo full-duplex.
- La opción half establece el modo half-duplex.
- La opción auto establece el modo autonegociación de dúplex. Cuando este modo se encuentra habilitado, los dos puertos se comunican para decidir el mejor modo de funcionamiento.

Para los puertos 10/100/1000 y Fast Ethernet la opción predeterminada es auto. Para los puertos 100BASE-FX, la opción predeterminada es full. Los puertos 10/100/1000 funcionan tanto en el modo half-duplex como en el full-duplex cuando se establecen en 10 ó 100 Mb/s, pero sólo funcionan en el modo full-duplex cuando se establecen en 1000 Mb/s.

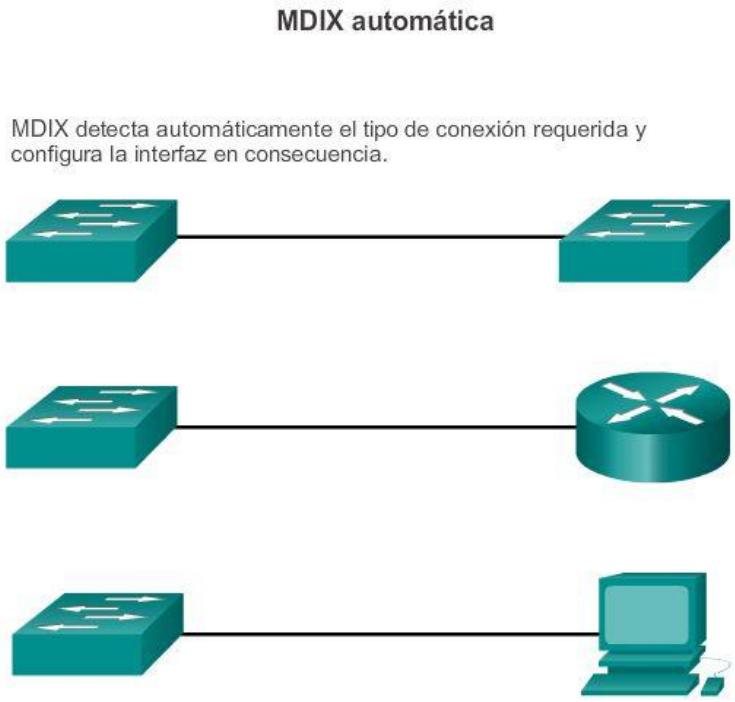


Capítulo 5: Ethernet 5.3.1.4 MDIX automática

Además de tener la configuración de dúplex correcta, también es necesario tener el tipo de cable adecuado definido para cada puerto. Antes, las conexiones entre dispositivos específicos, como las conexiones switch a switch, switch a router, switch a host y router a host, requerían el uso de tipos de cables específicos (de conexión cruzada o de conexión directa). Ahora, en cambio, la mayoría de los dispositivos de switch admiten el comando de configuración de interfazmdix auto en la CLI para habilitar la característica automática de conexión cruzada de interfaz dependiente del medio (MDIX automática o auto-MDIX).

Al habilitar la función auto-MDIX, el switch detecta el tipo de cable que se requiere para las conexiones Ethernet de cobre y, conforme a ello, configura las interfaces. Por lo tanto, se puede utilizar un cable de conexión directa o cruzada para realizar la conexión con un puerto 10/100/1000 de cobre situado en el switch, independientemente del tipo de dispositivo que esté en el otro extremo de la conexión.

La función auto-MDIX se habilita de manera predeterminada en los switches que ejecutan el software Cisco IOS, versión 12.2(18)SE o posterior. En el caso de las versiones existentes entre Cisco IOS, versión 12.1(14)EA1 y 12.2(18)SE, la función auto-MDIX se encuentra deshabilitada de manera predeterminada.



Capítulo 5: Ethernet 5.3.1.5 Métodos de reenvío de tramas en switches Cisco

Anteriormente, los switches solían utilizar uno de los siguientes métodos de reenvío para conmutar datos entre los puertos de la red:

- Conmutación por almacenamiento y envío
- Conmutación por método de corte

En la figura 1, se destacan las diferencias entre estos dos métodos.

En este tipo de conmutación, cuando el switch recibe la trama la almacena en los búferes de datos hasta recibir la trama en su totalidad. Durante el proceso de almacenamiento, el switch analiza la trama para buscar información acerca de su destino. En este proceso, el switch también lleva a cabo una verificación de errores utilizando la porción del tráiler de comprobación de redundancia cíclica (CRC) de la trama de Ethernet.

La CRC utiliza una fórmula matemática, basada en la cantidad de bits (1) de la trama, para determinar si ésta tiene algún error. Después de confirmar la integridad de la trama, ésta se envía desde el puerto correspondiente hasta su destino. Cuando se detecta un error en la trama, el switch la descarta. El proceso de descarte de las tramas con errores reduce la cantidad de ancho de banda consumido por datos dañados. La conmutación por almacenamiento y envío se requiere para el análisis de calidad de servicio (QoS) en las redes convergentes, en donde se necesita una clasificación de la trama para decidir el orden de prioridad del tráfico. Por ejemplo: los flujos de datos de voz sobre IP deben tener prioridad sobre el tráfico de exploración Web.

En la figura 2, reproduzca la animación para ver una demostración del proceso de almacenamiento y envío. El método de almacenamiento y envío es el único método de reenvío que se utiliza en los modelos actuales de los switches Cisco Catalyst.

Métodos de reenvío de paquetes del switch

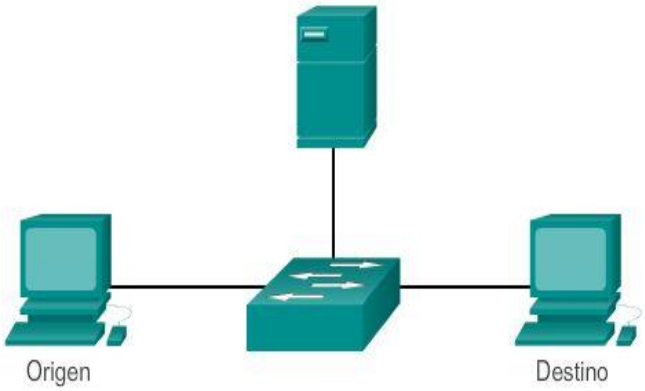
Almacenamiento y envío

Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Método de corte

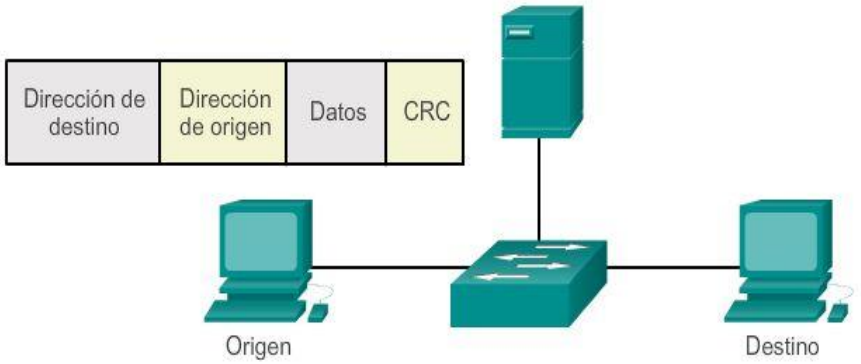
El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.

Conmutación por almacenamiento y envío



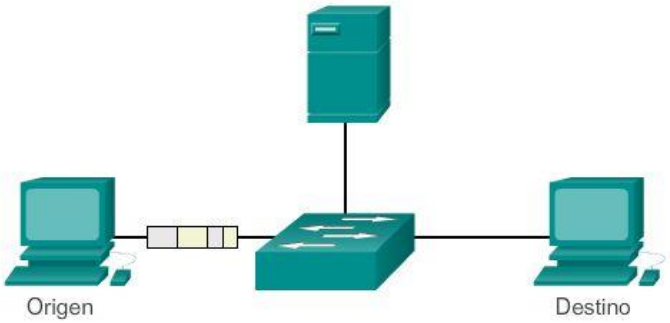
Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío



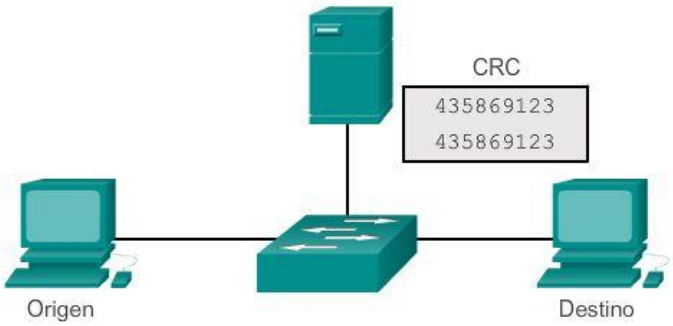
Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío



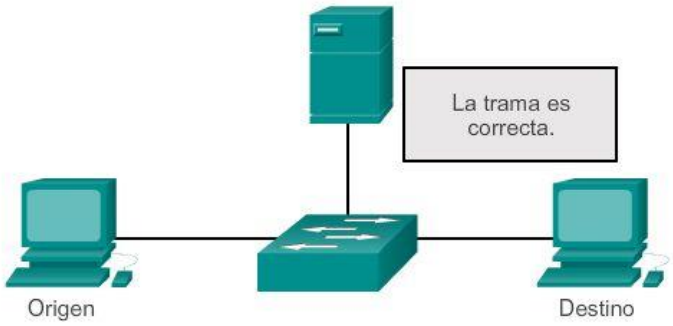
Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío



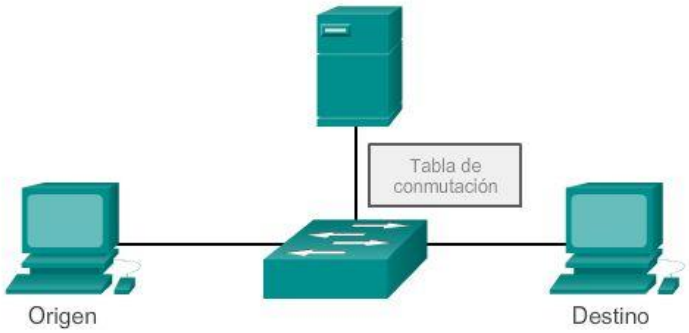
Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío



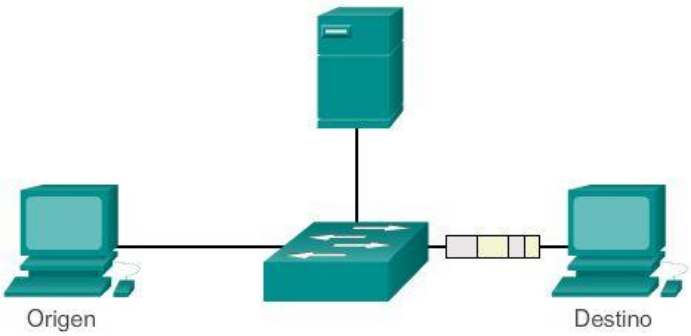
Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío



Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Conmutación por almacenamiento y envío



Un switch de almacenamiento y envío recibe la trama completa y calcula la CRC. Si la CRC es válida, el switch busca la dirección de destino, la cual determina la interfaz de salida. Entonces, se envía la trama por el puerto correcto.

Capítulo 5: Ethernet 5.3.1.6 Conmutación por método de corte

En este tipo de conmutación, el switch actúa sobre los datos apenas los recibe, incluso si la transmisión aún no se ha completado. El switch recopila en el búfer sólo la información suficiente de la trama como para leer la dirección MAC de destino y así determinar a qué puerto debe reenviar los datos. La dirección MAC de destino se encuentra en los primeros 6 bytes de la trama después del preámbulo. El switch busca la dirección MAC de destino en su tabla de conmutación, determina el puerto de la interfaz de salida y reenvía la trama a su destino mediante el puerto de switch designado. El switch no lleva a cabo ninguna verificación de errores en la trama. Dado que el switch no tiene que esperar que la trama se almacene de manera completa en el búfer y que no realiza ninguna verificación de errores, la conmutación por método de corte es más rápida que la de almacenamiento y envío. No obstante, al no llevar a cabo ninguna verificación de errores, el switch reenvía tramas dañadas a través de la red. Las tramas dañadas consumen ancho de banda mientras se reenvían. Al final, la NIC de destino descarta las tramas dañadas.

Reproduzca la animación para ver una demostración del proceso de conmutación por método de corte.

A continuación, se presentan dos variantes de la conmutación por método de corte:

- Conmutación por envío rápido: este tipo de conmutación ofrece el nivel más bajo de latencia. La conmutación por envío rápido reenvía el paquete inmediatamente después de leer la dirección de destino. Como la conmutación por envío rápido comienza a reenviar el paquete antes de haberlo recibido en forma completa, es probable que a veces los paquetes se entreguen con errores. Esto ocurre con poca frecuencia y el adaptador de red de destino descarta los paquetes defectuosos en el momento de su recepción. En el modo de envío rápido, la latencia se mide desde el primer bit recibido hasta el primer bit transmitido. La conmutación por envío rápido es el típico método de corte.

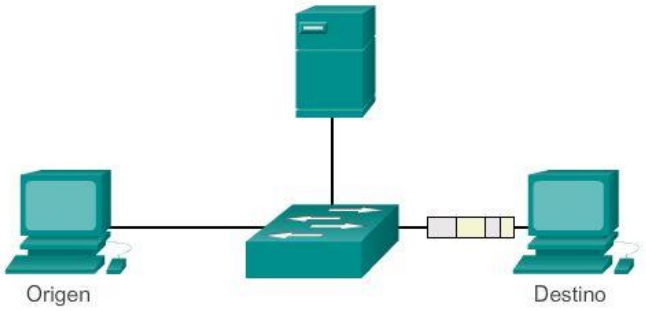
- Conmutación libre de fragmentos: en este método, el switch almacena los primeros 64 bytes de la trama antes de hacer el reenvío. Este tipo de conmutación se puede definir como un punto intermedio entre la conmutación por almacenamiento y envío y la conmutación por método de corte.

  El motivo por el cual la conmutación libre de fragmentos almacena sólo los primeros 64 bytes de la trama es que la mayoría de los errores y las colisiones de la red se producen en esos primeros 64 bytes. El método de conmutación libre de fragmentos intenta mejorar la conmutación por envío rápido mediante una pequeña verificación de errores en los primeros 64 bytes de la trama, a fin de asegurar que no se hayan producido colisiones antes de reenviar la trama. La conmutación libre de fragmentos es un punto intermedio entre el alto nivel de latencia y la gran integridad que ofrece la conmutación por almacenamiento y envío, y el bajo nivel de latencia y la integridad reducida que brinda la conmutación por envío rápido.

En la ilustración, se muestra un ejemplo de conmutación por método de corte.

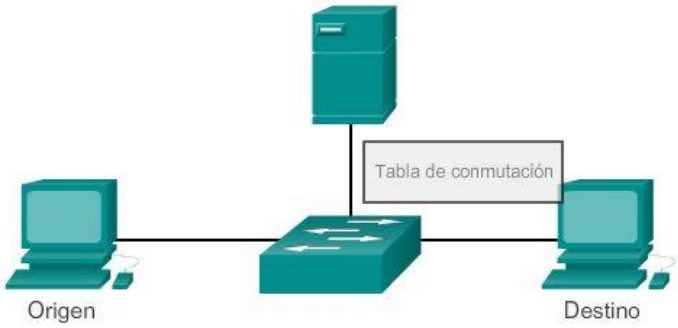
Algunos switches se configuran para realizar una conmutación por método de corte por puerto hasta llegar a un umbral de error definido por el usuario y luego cambian la conmutación al modo de almacenamiento y envío. Si el índice de error está por debajo del umbral, el puerto vuelve automáticamente a la conmutación por método de corte.

Conmutación por método de corte

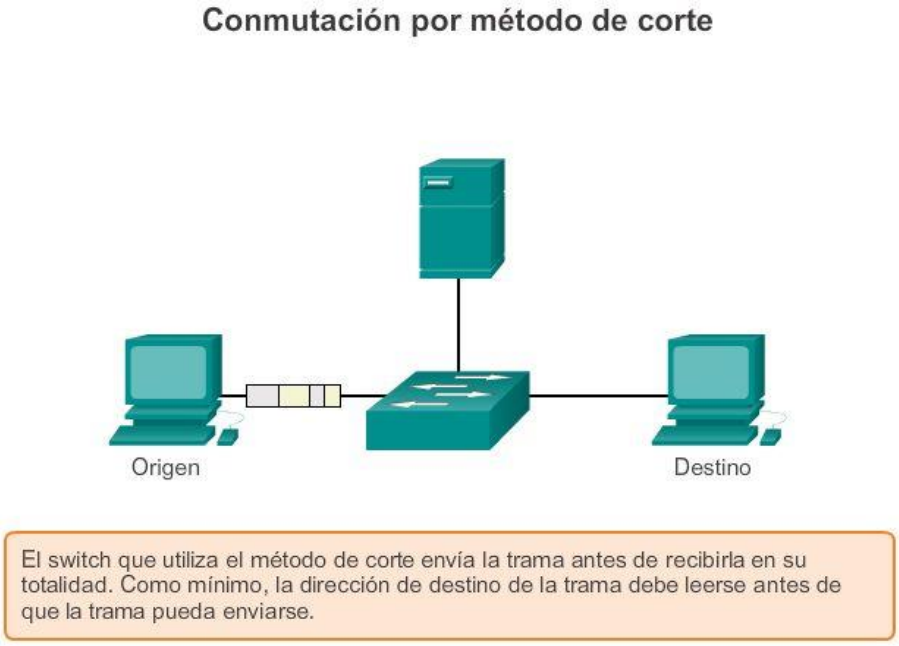


El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.

Conmutación por método de corte



El switch que utiliza el método de corte envía la trama antes de recibirla en su totalidad. Como mínimo, la dirección de destino de la trama debe leerse antes de que la trama pueda enviarse.



Capítulo 5: Ethernet 5.3.1.8 Almacenamiento en búfer de memoria en switches

Según lo analizado, un switch examina parte de un paquete, o su totalidad, antes de reenviarlo al host de destino. Un switch Ethernet puede usar una técnica de bufferes para almacenar tramas antes de enviarlas. El almacenamiento en buffers también puede utilizarse cuando el puerto de destino está ocupado debido a una congestión. El switch almacena la trama hasta el momento en que pueda transmitirse.

Como se muestra en la ilustración, existen dos métodos de almacenamiento en búfer de memoria: el método basado en puerto y el de memoria compartida.

Búfer de memoria basada en puerto

En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada y de salida específicos. Una trama se transmite al puerto de salida una vez que todas las tramas que están delante de ella en la cola se hayan transmitido con éxito. Es posible que una sola trama retarde la transmisión de todas las tramas almacenadas en la memoria debido al tráfico del puerto de destino. Este retraso se produce aunque las demás tramas puedan transmitirse a puertos de destino abiertos.

Almacenamiento en búfer de memoria compartida

El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch. La cantidad de memoria de búfer que requiere un puerto se asigna de forma dinámica. Las tramas en el búfer se vinculan de forma dinámica al puerto de destino. Esto permite que se pueda recibir el paquete por un puerto y se pueda transmitir por otro puerto, sin tener que colocarlo en otra cola.

El switch conserva un mapa de enlaces de trama a puerto que indica dónde debe transmitirse el paquete. El enlace del mapa se elimina una vez que la trama se ha transmitido con éxito. La cantidad de tramas almacenadas en el búfer se encuentra limitada por el tamaño del búfer de memoria en su totalidad y no se limita a un solo búfer de puerto. Esto permite la transmisión de tramas más amplias y que se descarte una menor cantidad de ellas. Esto es muy importante para la conmutación asimétrica.

La conmutación asimétrica permite diferentes velocidades de datos en diferentes puertos. Esto permite que se dedique más ancho de banda a ciertos puertos, como un puerto conectado a un servidor.

Búfer de memoria basado en puerto y búfer de memoria compartida

Memoria basada en puerto	En el búfer de memoria basado en puerto, las tramas se almacenan en colas conectadas a puertos de entrada y de salida específicos.
Memoria compartida	El búfer de memoria compartida deposita todas las tramas en un búfer de memoria común que comparten todos los puertos del switch.

Capítulo 5: Ethernet 5.3.2.1 Comparación de configuración fija y configuración modular

Al seleccionar un switch, es importante comprender las características clave de las opciones de switches disponibles. Esto significa que es necesario tomar decisiones sobre las características, por ejemplo, si es necesario que tenga alimentación por Ethernet (PoE) o cuál es la “velocidad de reenvío” preferida.

Como se muestra en la figura 1, PoE permite que un switch suministre alimentación a un dispositivo, como teléfonos IP y algunos puntos de acceso inalámbrico, a través de los cables de Ethernet existentes. Esto proporciona mayor flexibilidad de instalación.

Las tasas de reenvío definen las capacidades de procesamiento de un switch mediante la estimación de la cantidad de datos que este puede procesar por segundo. Las líneas de productos con switch se clasifican según las velocidades de reenvío.

Los switches de la capa de entrada presentan velocidades inferiores que los switches de la capa empresarial. Otras consideraciones incluyen si el dispositivo es apilable o no apilable, así como el grosor del switch (expresado en cantidad de unidades en bastidor) y la densidad de puertos, o la cantidad de puertos disponibles en un único switch. La densidad de puertos de un dispositivo puede variar, lo que depende de si el dispositivo es de configuración fija o un dispositivo modular.

Con frecuencia estas opciones se denominan factores de forma del switch.

Switches de configuración fija

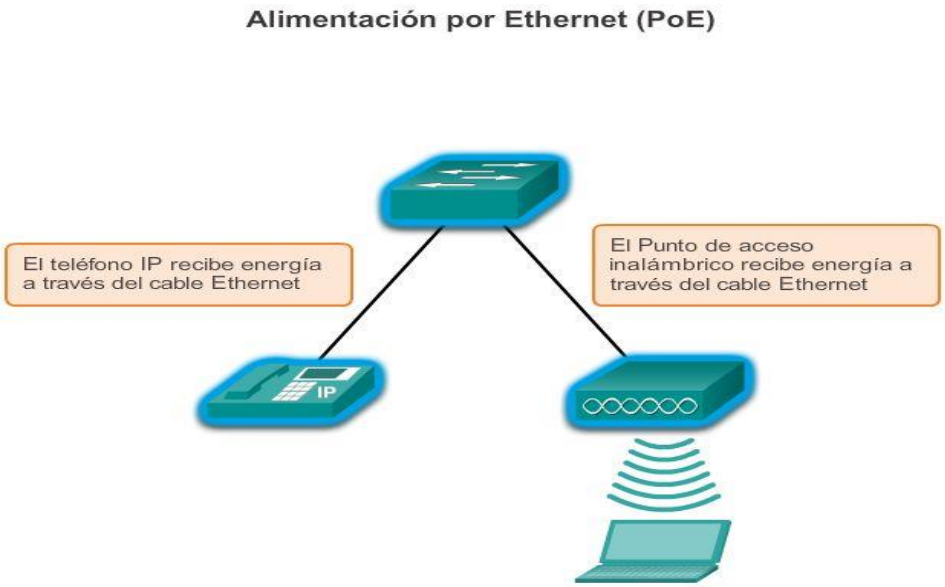
Los switches de configuración fija son sólo lo que podría esperarse: fijos en su configuración. Esto significa que no se pueden agregar características u opciones al switch más allá de las que originalmente vienen con él. El modelo en particular que se compra determina las características y opciones disponibles. Por ejemplo, si se adquiere un switch fijo gigabit de 24 puertos, no se pueden agregar puertos cuando se les necesite. Habitualmente, existen diferentes opciones de configuración que varían en cuanto al número y al tipo de puertos incluidos.

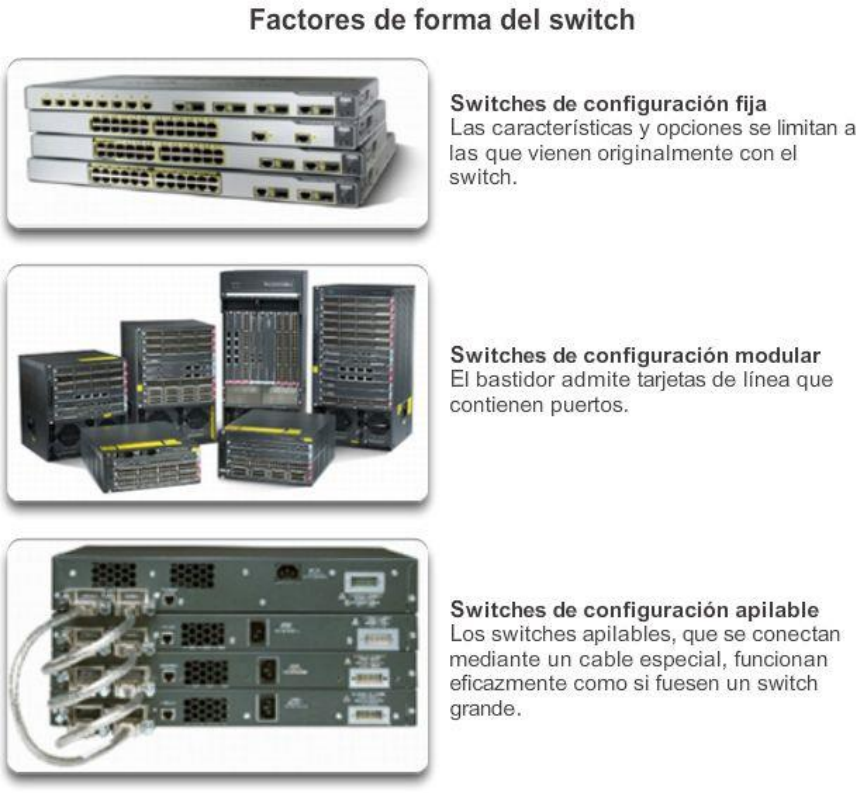
Switches modulares

Los switches modulares ofrecen más flexibilidad en su configuración. Habitualmente, los switches modulares vienen con chasis de diferentes tamaños que permiten la instalación de diferentes números de tarjetas de

líneas modulares. Las tarjetas de línea son las que contienen los puertos. La tarjeta de línea se ajusta al chasis del switch de igual manera que las tarjetas de expansión se ajustan en la PC. Cuanto más grande es el chasis, más módulos puede admitir. Como se observa en la figura, es posible elegir entre muchos tamaños de chasis diferentes. Si se compró un switch modular con una tarjeta de línea de 24 puertos, con facilidad se podría agregar una tarjeta de línea de 24 puertos para hacer que el número de puertos ascienda a 48.

En la figura 2, se muestran ejemplos de switches de configuración fija, modular y apilable.





Capítulo 5: Ethernet 5.3.2.2 Opciones de módulos para ranuras de switches Cisco

Las líneas de productos de switches Cisco se utilizan a gran escala en todo el mundo, en gran parte debido a la flexibilidad que proporcionan para opciones complementarias. Cisco IOS no solo tiene el conjunto más

completo de características disponibles en relación con cualquier otro sistema operativo de red, sino que además el IOS está diseñado a la medida de cada dispositivo de red de Cisco, en especial, los switches.

Para ilustrar las opciones disponibles, que son realmente demasiadas para enumerarlas aquí, nos enfocamos en los switches Catalyst 3560. Los switches Catalyst 3560 tienen puertos de factor de forma conectable pequeño (SFP) que admiten una cantidad de módulos de transceptor SFP. Aquí se presenta una lista de los módulos SFP admitidos en uno o más tipos de switches 3560:

Módulos SFP Fast Ethernet:

- 100BASE-FX (fibra óptica multimodo [MMF]) para 2 km
- 100BASE-LX10 (fibra óptica monomodo [SMF]) para 2 km
- 100BASE-BX10 (SMF) para 10 km
- 100BASE-EX (SMF) para 40 km
- 100BASE-ZX (SMF) para 80 km

Módulos SFP Gigabit Ethernet:

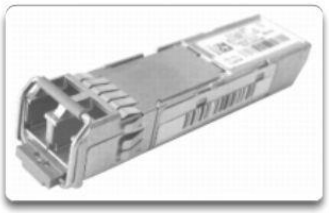
- 1000BASE-SX de 50/62,5 µm (MMF), hasta 550/220 m
- 1000BASE-LX/LH (SMF/MMF), hasta 10 km/0,550 km, respectivamente
- 1000BASE-ZX (SMF), hasta 70 km
- 1000BASE-BX10-D y 1000BASE-BX10-U (SMF), hasta 10 km
- 1000BASE-T (transceptor de hilos de cobre)

Módulos SFP de 10 Gigabit Ethernet:

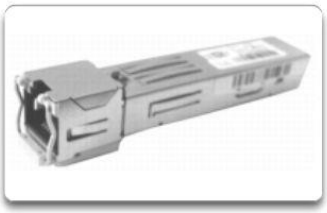
- 10G-SR (MMF), hasta 400 m
- 10G-SR-X (MMF), hasta 400 m (admiten un intervalo de temperatura extendido)
- 10G-LRM (MMF), hasta 220 m
- FET-10G (MMF), hasta 100 m (para uplinks de estructura Nexus)
- 10G-LR (SMF), hasta 10 km
- 10G-LR-X (SMF), hasta 10 km (admiten un intervalo de temperatura extendido)
- 10G-ER (SMF), hasta 40 km
- 10G-ZR (SMF), hasta 80 km
- Cable de conductores axiales retorcidos (transceptor de hilos de cobre), hasta 10 m
- Fibra óptica activa, hasta 10 m (para conexiones entre bastidores e intrabastidor)

Los módulos 40 Gigabit Ethernet y 100 Gigabit Ethernet son compatibles con los dispositivos Cisco de alta gama, como Catalyst 6500, el router CRS, el router de la serie ASR 9000 y el switch de la serie Nexus 7000.

Módulos de Routers de servicios integrados (SFP)



Cisco Optical Gigabit Ethernet SFP



Cisco 1000BASE-T Copper SFP

Cisco 2-channel 1000BASE-BX Optical SFP

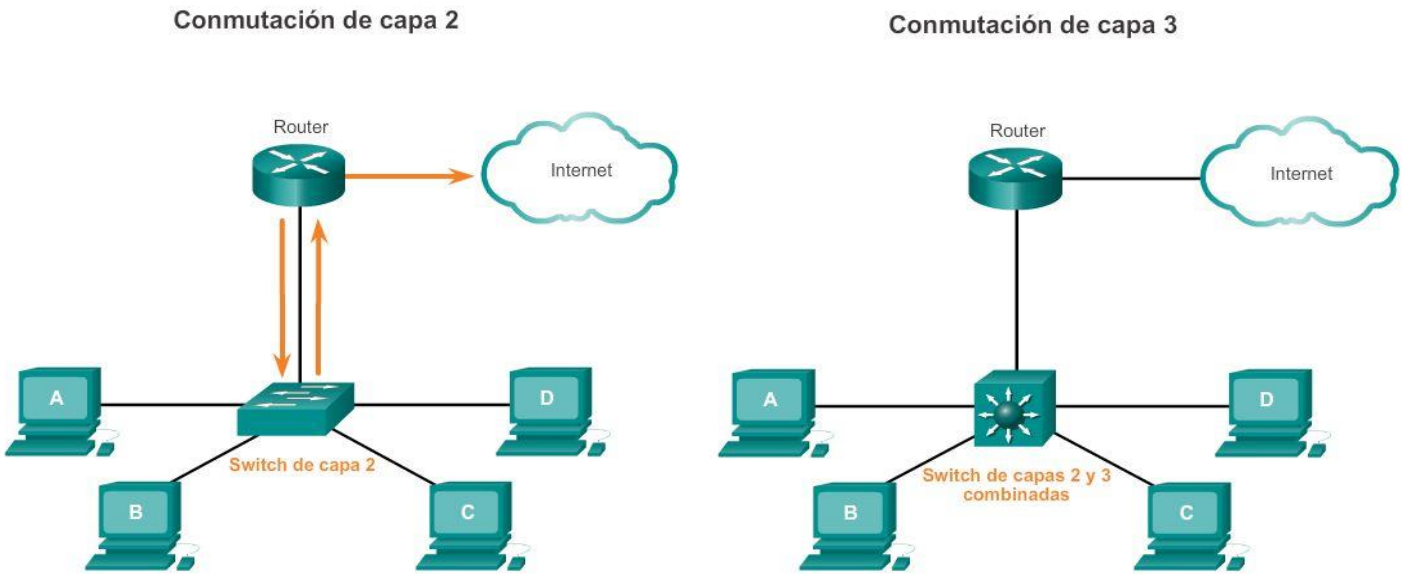
Capítulo 5: Ethernet 5.3.3.1 Comparación de conmutación de capa 2 y conmutación de capa 3

Además de determinar los diversos factores de forma de switch, es posible que también sea necesario elegir entre un switch LAN de capa 2 y un switch de capa 3.

Recuerde que los switches LAN de capa 2 llevan a cabo los procesos de conmutación y filtrado solo según la dirección MAC de la capa de enlace de datos (capa 2) del modelo OSI y dependen de los routers para pasar datos entre subredes IP independientes (consulte la figura 1).

Como se muestra en la figura 2, un switch de capa 3, como el Catalyst 3560, funciona de manera similar a un switch de capa 2, como el Catalyst 2960, pero en lugar de utilizar solo la información de la dirección MAC de la capa 2 para las decisiones de reenvío, los switches de capa 3 también pueden utilizar la información de la dirección IP. En lugar de aprender qué direcciones MAC están vinculadas con cada uno de sus puertos, el switch de Capa 3 puede también conocer qué direcciones IP están relacionadas con sus interfaces. Esto permite que el switch de capa 3 también dirija el tráfico a través de la red sobre la base de la información de la dirección IP.

Los switches de Capa 3 son también capaces de llevar a cabo funciones de enrutamiento de Capa 3, con lo cual se reduce la necesidad de colocar routers dedicados en una LAN. Dado que los switches de Capa 3 cuentan con un hardware de conmutación especializado, pueden normalmente enviar datos con la misma rapidez con la que pueden conmutar.



Capítulo 5: Ethernet 5.3.3.2 Cisco Express Forwarding

Los dispositivos Cisco que admiten conmutación de capa 3 utilizan Cisco Express Forwarding (CEF). Este método de reenvío es muy complejo, pero afortunadamente, como sucede con todas las buenas tecnologías, gran parte de lo que sucede se produce “detrás de escena”. Por lo general, CEF requiere muy poca configuración en los dispositivos Cisco.

Básicamente, CEF desacopla la interdependencia estricta habitual entre la toma de decisiones de capa 2 y de capa 3. Lo que lentifica el reenvío de paquetes IP es la referencia constante en ambos sentidos entre las construcciones de capa 2 y capa 3 dentro de un dispositivo de red. Entonces, en la medida en que se puedan desacoplar las estructuras de datos de capa 2 y la capa 3, se acelera el reenvío.

Los dos componentes principales de la operación de CEF son los siguientes:

- Base de información de reenvío (FIB)
- Tablas de adyacencia

La FIB es conceptualmente similar a una tabla de enrutamiento. Un router utiliza la tabla de enrutamiento para determinar el mejor camino hacia una red de destino sobre la base de la porción de red de la dirección IP de destino. Con CEF, la información que antes se almacenaba en la caché de la ruta se almacena ahora en varias estructuras de datos para la conmutación CEF. Las estructuras de datos proporcionan búsquedas optimizadas para un reenvío de paquetes eficaz. Los dispositivos de red utilizan la tabla de búsqueda de FIB para tomar decisiones de conmutación basadas en el destino sin tener que acceder a la caché de la ruta.

La FIB se actualiza cuando se producen cambios en la red y contiene todas las rutas conocidas hasta ese momento.

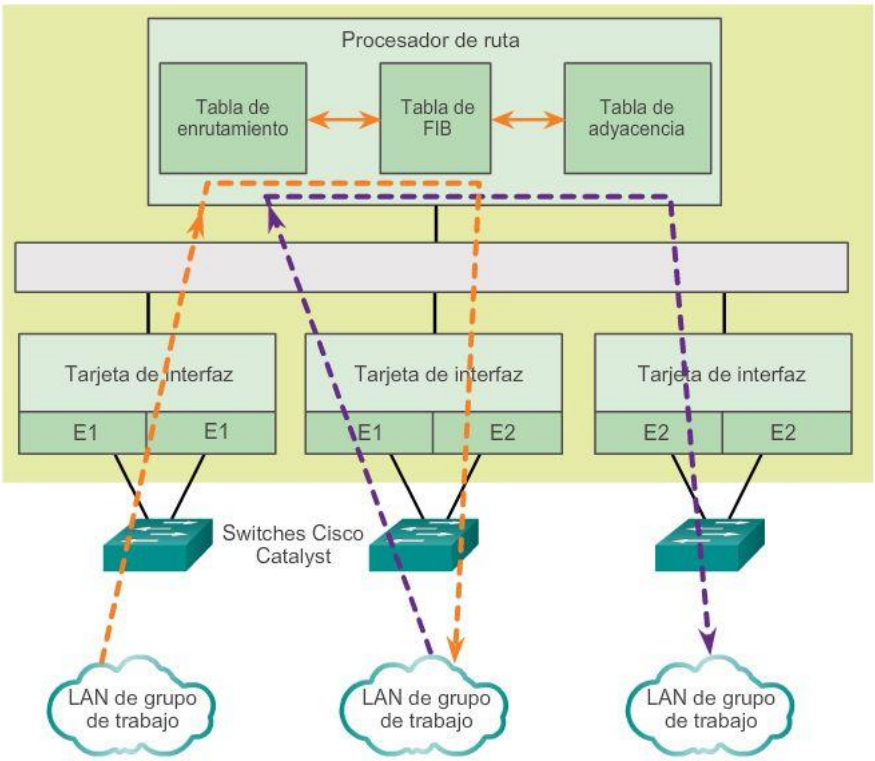
La tabla de adyacencia mantiene las direcciones de siguiente salto de la capa 2 para todas las entradas de FIB.

La separación de la información de posibilidad de conexión (en la tabla FIB) y de la información de reenvío (en la tabla de adyacencia), ofrece varias ventajas:

- La tabla de adyacencia se puede crear independientemente de la tabla FIB, lo que permite que ambas se creen sin que haya paquetes en proceso de conmutación.

- La reescritura del encabezado MAC utilizada para reenviar paquetes no se almacena en las entradas de caché, por lo tanto, los cambios en una cadena de reescritura de encabezado MAC no requiere la invalidación de las entradas de caché.

CEF está habilitado de manera predeterminada en la mayoría de los dispositivos Cisco que realizan conmutación de capa 3.



Capítulo 5: Ethernet 5.3.3.3 Tipos de interfaces de capa 3

Los dispositivos de red Cisco admiten varios tipos de interfaces de capa 3 diferentes. Las interfaces de capa 3 son aquellas que admiten el reenvío de paquetes IP a un destino final sobre la base de la dirección IP.

Los principales tipos de interfaces de capa 3 son los siguientes:

- Interfaz virtual de switch (SVI): interfaz lógica en un switch asociado a una red de área local virtual (VLAN).

- Puerto enrutado: puerto físico en un switch de capa 3 configurado para funcionar como puerto de router.

- EtherChannel de capa 3: interfaz lógica en dispositivos Cisco asociada a un conjunto de puertos enrutados.

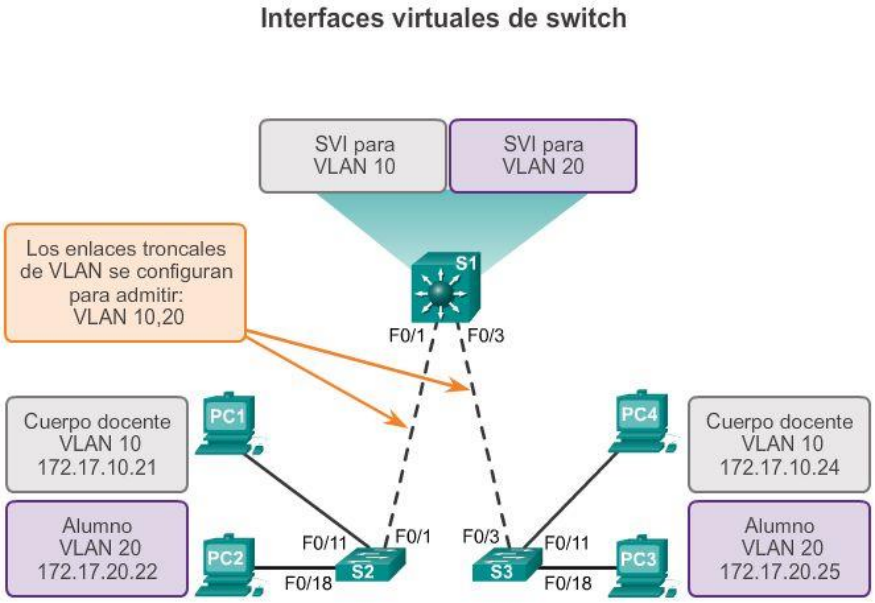
Como se mostró anteriormente, se debe habilitar una SVI para la VLAN predeterminada (VLAN1) a fin de proporcionar conectividad de host IP al switch y permitir la administración remota del switch. También se deben configurar SVI para permitir el enrutamiento entre redes VLAN. Como ya se mencionó, las SVI son

interfaces lógicas configuradas para VLAN específicas; para crear una ruta entre dos o más redes VLAN, cada VLAN debe tener habilitada una SVI independiente.

Los puertos enrutados permiten que los switches Cisco (de capa 3) funcionen como routers de manera eficaz. Cada puerto de un switch tal se puede configurar como puerto en una red IP independiente.

Los EtherChannels de capa 3 se utilizan para agrupar enlaces de Ethernet de capa 3 entre dispositivos Cisco para agregar ancho de banda, por lo general en uplinks.

Nota: además de las SVI y los EtherChannels de capa 3, existen otras interfaces lógicas en los dispositivos Cisco, que incluyen interfaces loopback e interfaces de túnel.



Capítulo 5: Ethernet 5.3.3.4 Configuración de un puerto enrutado en un switch de capa 3

Un puerto de switch se puede configurar para que funcione como puerto enrutado de capa 3 y se comporte como una interfaz de router normal. Las características específicas de un puerto enrutado son las siguientes:

- No está relacionado con una VLAN determinada.
- Se puede configurar con un protocolo de enrutamiento de capa 3.
- Es una interfaz de capa 3 únicamente, y no admite el protocolo de capa 2.

Configure los puertos enrutados colocando la interfaz en modo de capa 3 con el comando de configuración de interfaz no switchport. A continuación, asigne una dirección IP al puerto. Eso es todo.

Aprenderá más sobre las funciones del enrutamiento en el capítulo siguiente.

Configuración de un puerto enrutado

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar  1 00:15:40.115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief
Interface        IP-Address    OK? Method Status                Protocol
Vlan1            unassigned    YES unset  administratively down down
FastEthernet0/1  unassigned    YES unset  down                  down
FastEthernet0/2  unassigned    YES unset  down                  down
FastEthernet0/3  unassigned    YES unset  down                  down
FastEthernet0/4  unassigned    YES unset  down                  down
FastEthernet0/5  unassigned    YES unset  down                  down
FastEthernet0/6  192.168.200.1 YES manual up                    up
FastEthernet0/7  unassigned    YES unset  up                    up
FastEthernet0/8  unassigned    YES unset  up                    up
<Resultado omitido>
```

Capítulo 5: Ethernet 5.4.1.1 Actividad: MAC y Ethernet

MAC y Ethernet

Nota: esta actividad se puede completar en forma individual, en grupos pequeños o en un entorno de aprendizaje con todos los estudiantes del aula.

Vea el video ubicado en el siguiente enlace:

http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet

Los temas que se tratan no incluyen solamente los comienzos del desarrollo de Ethernet, sino también adónde vamos en términos de la tecnología Ethernet (un enfoque futurista).

Después de ver el video y de comparar su contenido con el capítulo 5, vaya a la Web y busque información sobre Ethernet. Utilice un enfoque constructivista:

- ¿Qué características tenía Ethernet en sus orígenes?
- ¿Qué aspectos de Ethernet se mantuvieron durante los últimos 25 años y qué cambios se están implementando para hacerla más útil y aplicable para los métodos actuales de transmisión de datos?

Busque tres imágenes de medios físicos y dispositivos antiguos, actuales y futuros de Ethernet (enfóquese en los switches). Comparta las imágenes en clase y comente sobre los siguientes temas:

- ¿En qué aspectos cambiaron los medios físicos de Ethernet y los dispositivos intermediarios?
- ¿En qué aspectos permanecieron sin alteraciones los medios físicos de Ethernet y los dispositivos intermediarios?
- ¿Qué que cambiará de Ethernet en el futuro?

Capítulo 5: Ethernet 5.4.1.2 Resumen

Ethernet es la tecnología LAN más ampliamente utilizada en la actualidad. Se trata de una familia de tecnologías de red que se definen en los estándares IEEE 802.2 y 802.3. Los estándares de Ethernet definen los protocolos de Capa 2 y las tecnologías de Capa 1. En lo que respecta a los protocolos de capa 2, al igual que sucede con todos los estándares IEEE 802, Ethernet depende de las dos subcapas separadas de la capa de enlace de datos para funcionar: la subcapa de control de enlace lógico (LLC) y la subcapa MAC.

En la capa de enlace de datos, la estructura de la trama es casi idéntica para todas las velocidades de Ethernet. La estructura de la trama de Ethernet agrega encabezados y tráilers a la PDU de Capa 3 para encapsular el mensaje que se envía.

Existen dos estilos de entramado de Ethernet: el estándar IEEE 802.3 de Ethernet y el estándar DIX de Ethernet, al que hoy en día se lo conoce como Ethernet II. La diferencia más importante entre los dos estándares es el agregado de un delimitador de inicio de trama (SFD) y el cambio del campo Tipo por el campo Longitud en el estándar 802.3. Ethernet II es el formato de trama de Ethernet utilizado en las redes TCP/IP. Como implementación de los estándares IEEE 802.2/3, la trama de Ethernet proporciona direccionamiento MAC y comprobación de errores.

El direccionamiento de Capa 2 proporcionado por Ethernet admite comunicaciones unicast, multicast y broadcast. Ethernet utiliza el protocolo de resolución de direcciones para determinar las direcciones MAC de los destinos y asignarlas con direcciones de capa de red conocidas.

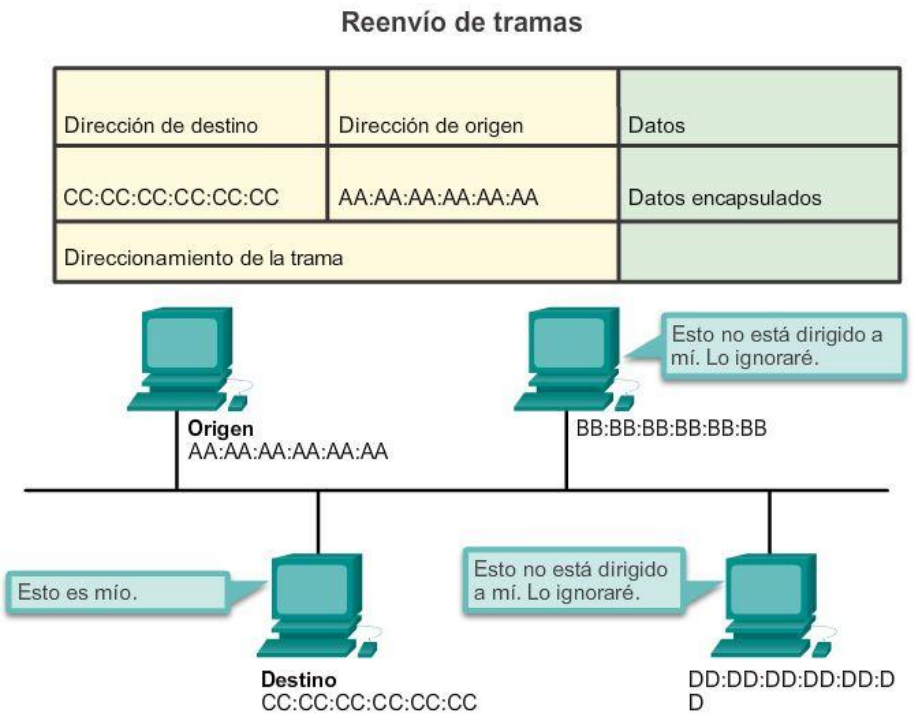
Cada nodo de una red IP tiene una dirección MAC y una dirección IP. El nodo debe utilizar sus propias direcciones MAC e IP en los campos de origen y debe proporcionar una dirección MAC y una dirección IP para el destino. Mientras que una capa OSI superior proporciona la dirección IP del destino, el nodo de envío debe encontrar la dirección MAC del destino para un enlace de Ethernet determinado. Ese es el propósito del protocolo ARP.

El protocolo ARP se basa en determinados tipos de mensajes Ethernet de broadcast y unicast, denominados “solicitudes ARP” y “respuestas ARP”. El protocolo ARP resuelve direcciones IPv4 en direcciones MAC y mantiene una tabla de asignaciones.

En la mayoría de las redes Ethernet, los dispositivos finales se suelen conectar a un switch LAN de capa 2 de forma punto a punto. Los switches LAN de capa 2 llevan a cabo los procesos de conmutación y filtrado basándose solamente en la dirección MAC de la capa de enlace de datos (capa 2) del modelo OSI. Los switches de capa 2 crean una tabla de direcciones MAC que utilizan para tomar decisiones de reenvío. Los switches de capa 2 dependen de los routers para pasar datos entre subredes IP independientes.

Los switches de Capa 3 son también capaces de llevar a cabo funciones de enrutamiento de Capa 3, con lo cual se reduce la necesidad de colocar routers dedicados en una LAN. Dado que los switches de Capa 3

cuentan con un hardware de conmutación especializado, pueden normalmente enviar datos con la misma rapidez con la que pueden conmutar.

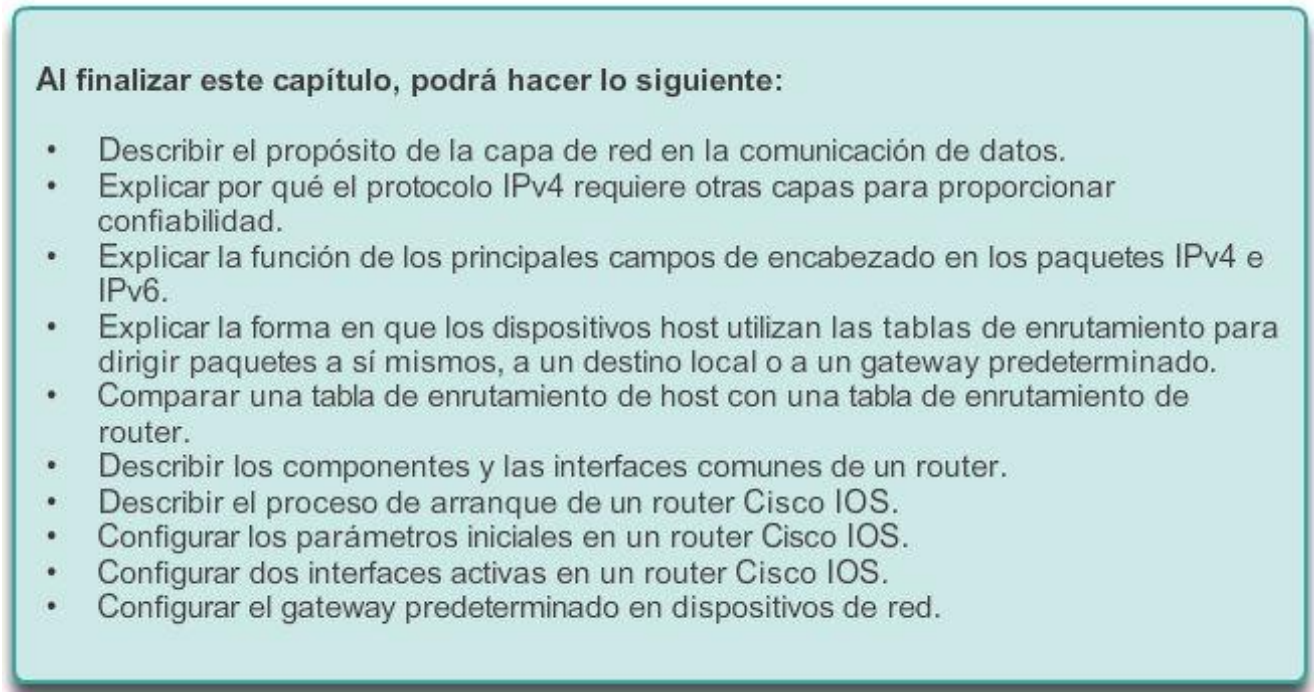


Capítulo 6: Capa de Red 6.0.1.1 Introducción

Las aplicaciones y los servicios de red en un dispositivo final pueden comunicarse con las aplicaciones y los servicios que se ejecutan en otro dispositivo final. ¿Cómo se comunican estos datos a través de la red de manera eficaz?

Los protocolos de la capa de red del modelo OSI especifican el direccionamiento y los procesos que permiten empaquetar y transportar los datos de la capa de transporte. La encapsulación de la capa de red permite transmitir los datos a un destino dentro de la red (o de otra red) con una sobrecarga mínima.

En este capítulo, se analiza la función de la capa de red. Se analiza cómo divide las redes en grupos de hosts para administrar el flujo de paquetes de datos dentro de una red. También se examina la forma en que se facilita la comunicación entre redes. A esta comunicación entre redes se la denomina enrutamiento.



Capítulo 6: Capa de Red 6.0.1.2 Actividad: La ruta menos transitada...

La ruta menos transitada... ¿realmente lo es?

Decidió que el próximo fin de semana irá a visitar a un compañero de curso que está en su casa debido a una enfermedad. Tiene la dirección de su compañero, pero nunca fue a la ciudad donde vive. En lugar de buscar la dirección en el mapa, decide simplificar las cosas y pedir indicaciones a los residentes del lugar después de bajar del tren. Los residentes a los que pide ayuda son muy amables. Sin embargo, todos tienen una costumbre interesante. En lugar de explicar por completo el camino que debe tomar para llegar a destino, todos le dicen: “vaya por esta calle y, en cuanto llegue al cruce más cercano, vuelva a preguntar a alguien allí”.

Confundido por esta situación claramente curiosa, sigue estas instrucciones y finalmente llega a la casa de su compañero pasando cruce por cruce y calle por calle.

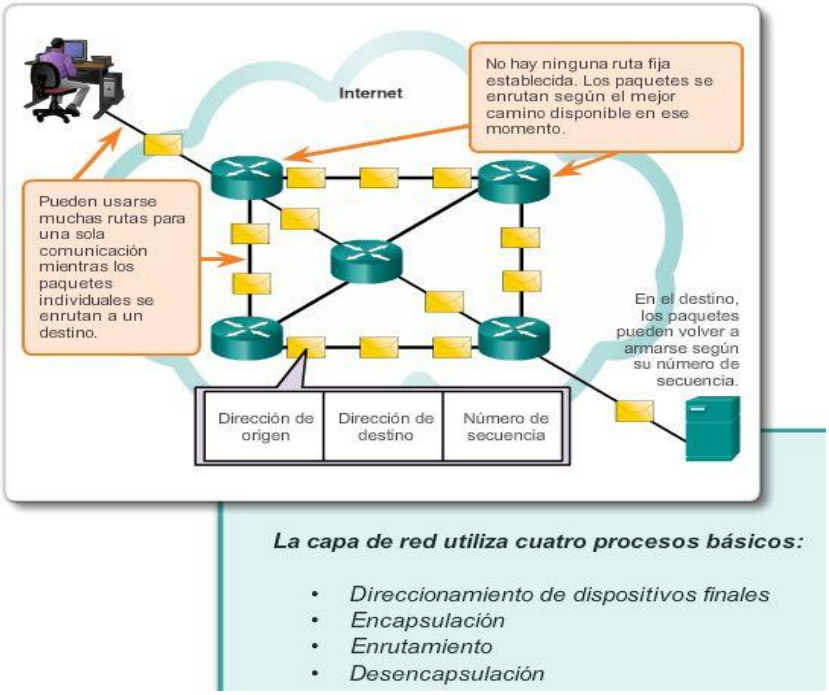
Responda las siguientes preguntas:

- ¿Habría sido muy diferente si, en lugar de que se le indicara que fuera hasta el cruce más cercano, se le hubiera indicado el camino completo o una parte del camino más extensa?

- ¿Habría sido más útil preguntar por la dirección específica o solo por la calle? ¿Qué ocurriría si la persona a la que solicita indicaciones no supiera dónde queda la calle de destino o le indicara un recorrido incorrecto?

- Suponga que en su camino de regreso a casa decide volver a pedirles indicaciones a los residentes. ¿Es seguro que le indicarían seguir el mismo camino que hizo para llegar a la casa de su amigo? Justifique su respuesta.

- ¿Es necesario explicar de dónde parte cuando pide indicaciones para llegar a un destino deseado?



Capítulo 6: Capa de Red 6.1.1.1 La capa de red

La capa de red, o la capa 3 de OSI, proporciona servicios que permiten que los dispositivos finales intercambien datos a través de la red. Para lograr este transporte de extremo a extremo, la capa de red utiliza cuatro procesos básicos:

- Direccionamiento de dispositivos finales: de la misma manera en que un teléfono tiene un número telefónico único, los dispositivos finales deben configurarse con una dirección IP única para su identificación en la red. Un dispositivo final con una dirección IP configurada se denomina “host”.

- Encapsulación: la capa de red recibe una unidad de datos del protocolo (PDU) de la capa de transporte. En un proceso denominado “encapsulación”, la capa de red agrega la información del encabezado IP, como la dirección IP de los hosts de origen (emisor) y de destino (receptor). Una vez que se agrega la información de encabezado a la PDU, esta se denomina “paquete”.

- Enrutamiento: la capa de red proporciona servicios para dirigir los paquetes a un host de destino en otra red. Para que el paquete se transfiera a otras redes, lo debe procesar un router. La función del router es seleccionar las rutas para los paquetes y dirigirlos hacia el host de destino en un proceso conocido como “enrutamiento”.

  Un paquete puede cruzar muchos dispositivos intermediarios antes de llegar al host de destino. Cada ruta que toma el paquete para llegar al host de destino se denomina “salto”.

- Desencapsulación: cuando un paquete llega a la capa de red del host de destino, el host revisa el encabezado IP del paquete. Si la dirección IP de destino en el encabezado coincide con su propia dirección IP, se elimina el encabezado IP del paquete. Este proceso de eliminación de encabezados de las capas inferiores se conoce como “desencapsulación”. Una vez que la capa de red desencapsula el paquete, la PDU de capa 4 que se obtiene como resultado se transfiere al servicio correspondiente en la capa de transporte.

A diferencia de la capa de transporte (capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada host, los protocolos de la capa de red especifican la estructura y el procesamiento de paquete que se utilizan para transportar los datos desde un host hasta otro. Operar sin tener en cuenta los datos transportados en cada paquete permite que la capa de red transporte paquetes para diversos tipos de comunicaciones entre varios hosts.

La animación en la figura muestra el intercambio de datos.

Capítulo 6: Capa de Red 6.1.1.2 Protocolos de la capa de red

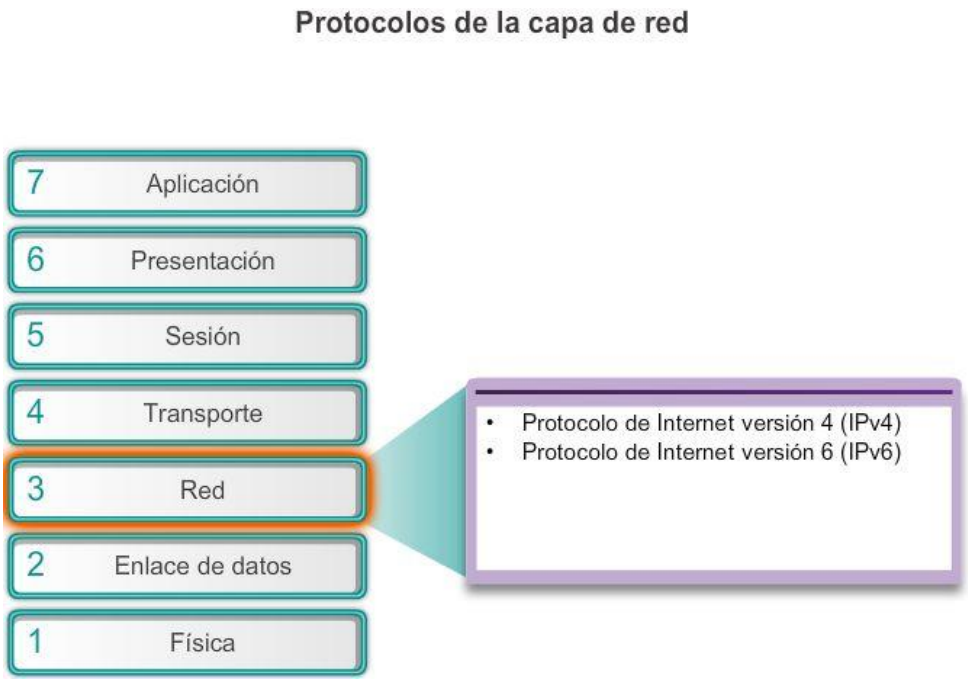
Existen varios protocolos de capa de red; sin embargo, solo los dos que se incluyen a continuación se implementan con frecuencia, como se muestra en la ilustración:

- Protocolo de Internet versión 4 (IPv4)
- Protocolo de Internet versión 6 (IPv6)

Otros protocolos de capa de red antiguos que no tienen un uso muy difundido incluyen los siguientes:

- Intercambio Novell de paquetes de internetwork (IPX)
- AppleTalk
- Servicio de red sin conexión (CLNS/DECNet)

El análisis de estos protocolos antiguos será mínimo.



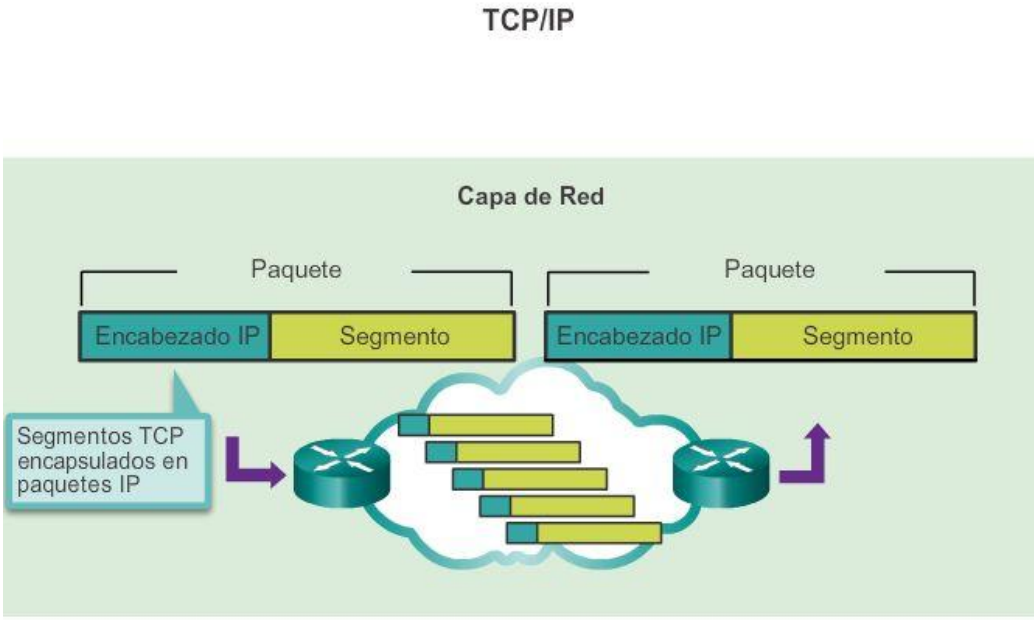
Capítulo 6: Capa de Red 6.1.2.1 Características de IP

El protocolo IP es el servicio de capa de red implementado por la suite de protocolos TCP/IP.

IP se diseñó como protocolo con baja sobrecarga. Provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. De ser necesarias, otros protocolos en otras capas llevan a cabo estas funciones.

Las características básicas del protocolo IP son las siguientes:

- Sin conexión: no se establece ninguna conexión con el destino antes de enviar los paquetes de datos.
- Máximo esfuerzo (no confiable): la entrega de paquetes no está garantizada.
- Independiente de los medios: la operación es independiente del medio que transporta los datos.



Los paquetes IP fluyen a través de la internetwork.

Capítulo 6: Capa de Red 6.1.2.2 IP: sin conexión

La función de la capa de red es transportar paquetes entre los hosts colocando la menor carga posible en la red. La capa de red no se ocupa ni está al tanto del tipo de comunicación contenida dentro de un paquete. IP es un protocolo sin conexión, lo que significa que no se crea ninguna conexión dedicada de extremo a extremo antes de enviar los datos. Conceptualmente, la comunicación sin conexión es similar a enviar una carta a alguien sin notificar al destinatario con anticipación.

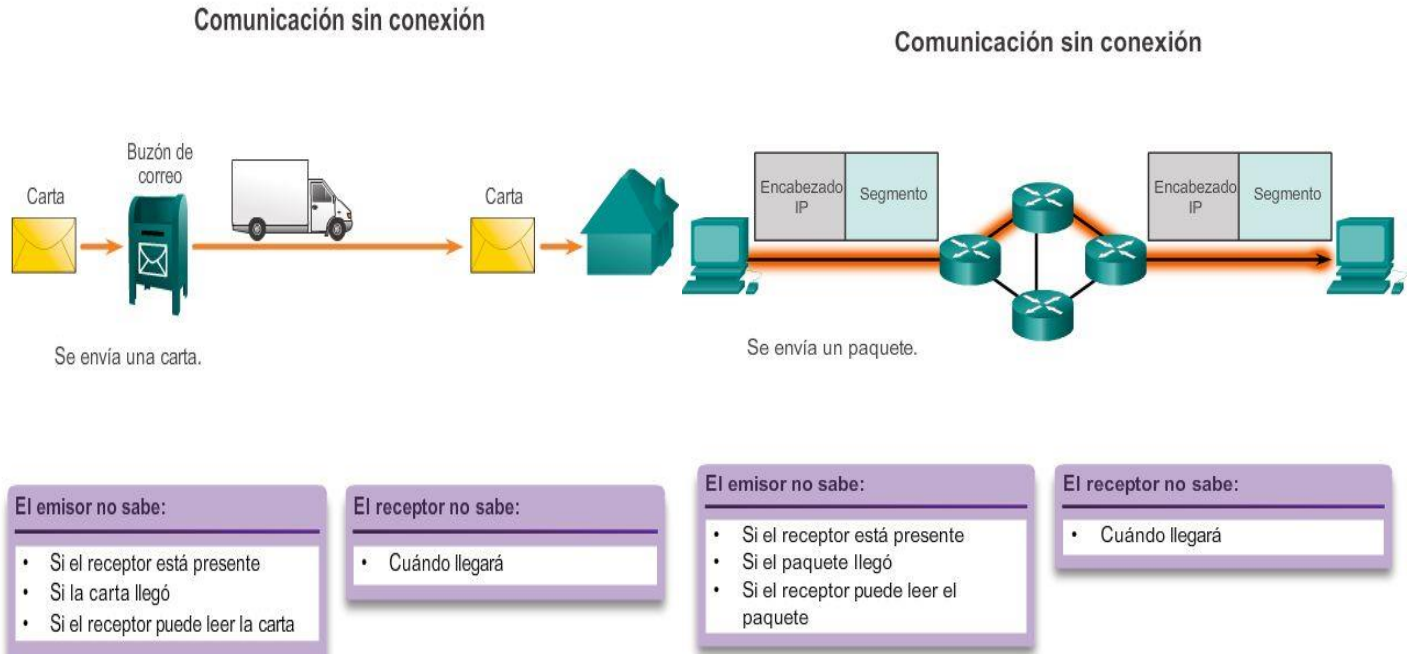
Como se muestra en la figura 1, el servicio postal utiliza la información en una carta para entregarla a un destinatario. La dirección en el sobre no proporciona datos que indiquen si el receptor está presente, si la carta llegará a destino o si el receptor puede leerla. De hecho, el servicio postal no está al tanto de la información contenida dentro del paquete que entrega y, por lo tanto, no puede proporcionar ningún mecanismo de corrección de errores.

Las comunicaciones de datos sin conexión funcionan según el mismo principio.

IP es un protocolo sin conexión y, por lo tanto, no requiere ningún intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de reenviar los paquetes. Además, tampoco requiere campos adicionales en el encabezado de la unidad de datos del protocolo (PDU) para mantener una conexión establecida.

Este proceso reduce en gran medida la sobrecarga del IP. Sin embargo, sin una conexión de extremo a extremo preestablecida, los emisores no saben si los dispositivos de destino están presentes y en condiciones

de funcionamiento cuando envían los paquetes, y tampoco saben si el destino recibe el paquete o si puede acceder al paquete y leerlo. En la figura 2, se muestra un ejemplo de comunicación sin conexión.

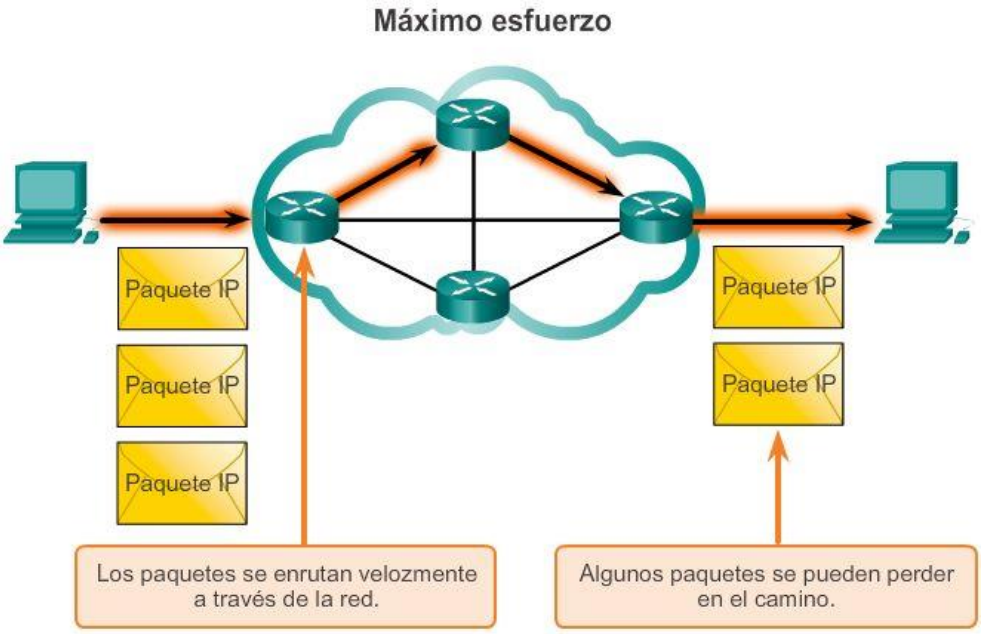


Capítulo 6: Capa de Red 6.1.2.3 IP: máximo esfuerzo de entrega

A menudo, el protocolo IP se describe como un protocolo no confiable o de máximo esfuerzo de entrega. Esto no significa que IP a veces funcione bien y a veces funcione mal, ni que sea un protocolo de comunicación de datos deficiente. “No confiable” significa simplemente que IP no tiene la capacidad de administrar paquetes no entregados o dañados ni de recuperar datos de estos. Esto se debe a que los paquetes IP se envían con información sobre la ubicación de entrega, pero no contienen información que se pueda procesar para informar al emisor si la entrega se realizó correctamente. No se incluyen datos de sincronización en el encabezado del paquete para realizar un seguimiento del orden de entrega de los paquetes. Con el protocolo IP, tampoco hay acuses de recibo de la entrega de los paquetes ni datos de control de errores que permitan realizar un seguimiento de si los paquetes se entregaron sin daños. Los paquetes pueden llegar al destino dañado o fuera de secuencia, o pueden no llegar en absoluto. De acuerdo con la información proporcionada en el encabezado IP, no hay capacidad de retransmisión de paquetes si se producen errores como estos.

Si los paquetes faltantes o que no funcionan generan problemas para la aplicación que usa los datos, los servicios de las capas superiores, como TCP, deben resolver estos problemas. Esto permite que el protocolo IP funcione de forma muy eficaz. Si se incluyera la sobrecarga de confiabilidad en IP, las comunicaciones que no requieren conexión o confiabilidad se cargarían con el consumo de ancho de banda y la demora producidos por esta sobrecarga. En la suite TCP/IP, la capa de transporte puede utilizar el protocolo TCP o UDP, según la necesidad de confiabilidad en la comunicación. Dejar que la capa de transporte decida sobre la confiabilidad hace que el protocolo IP se adapte y se acomode mejor a los distintos tipos de comunicación.

En la ilustración, se muestra un ejemplo de comunicaciones IP. Los protocolos orientados a la conexión, como TCP, requieren el intercambio de datos de control para establecer la conexión. Para mantener la información sobre la conexión, TCP también requiere campos adicionales en el encabezado de la PDU.



Dado que es un protocolo de capa de red no confiable, IP no garantiza que se reciban todos los paquetes enviados. Otros protocolos administran el proceso de seguimiento de paquetes y de aseguramiento de entrega.

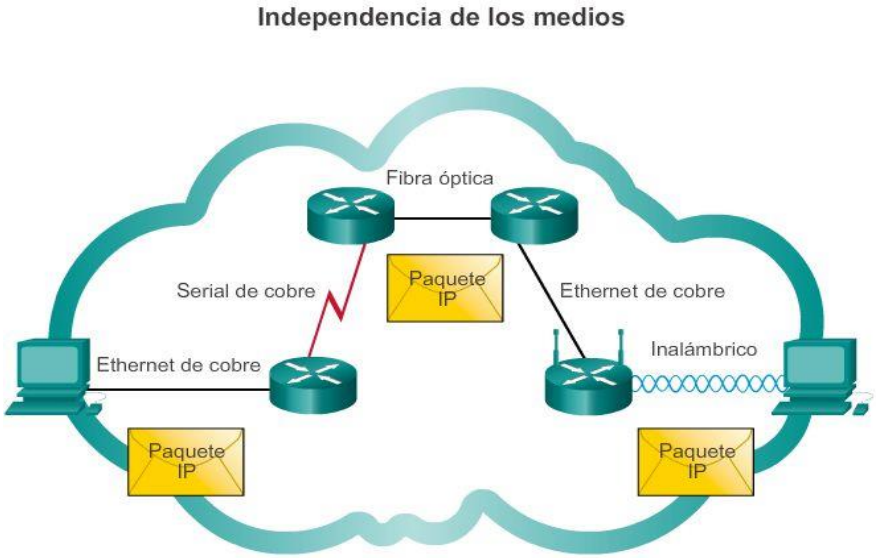
Capítulo 6: Capa de Red 6.1.2.4 IP: independiente de los medios

La capa de red tampoco tiene la carga de las características de los medios por los cuales se transportan los paquetes. IP funciona con independencia de los medios que transportan los datos en las capas inferiores del stack de protocolos. Como se muestra en la figura, cualquier paquete IP individual puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables como señales de radio.

Es responsabilidad de la capa de enlace de datos del modelo OSI tomar un paquete IP y prepararlo para transmitirlo a través del medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

Sin embargo, existe una característica importante de los medios que la capa de red tiene en cuenta: el tamaño máximo de la PDU que cada medio puede transportar. Esta característica se denomina “unidad máxima de transmisión” (MTU). Parte de la comunicación de control entre la capa de enlace de datos y la capa de red consiste en establecer el tamaño máximo para el paquete. La capa de enlace de datos pasa el valor de MTU a la capa de red. A continuación, la capa de red determina cuán grandes pueden ser los paquetes.

En algunos casos, un dispositivo intermediario, generalmente un router, debe dividir un paquete cuando lo reenvía de un medio a otro con una MTU más pequeña. A este proceso se lo llama fragmentación de paquetes o fragmentación.



Los paquetes IP pueden trasladarse a través de diferentes medios.

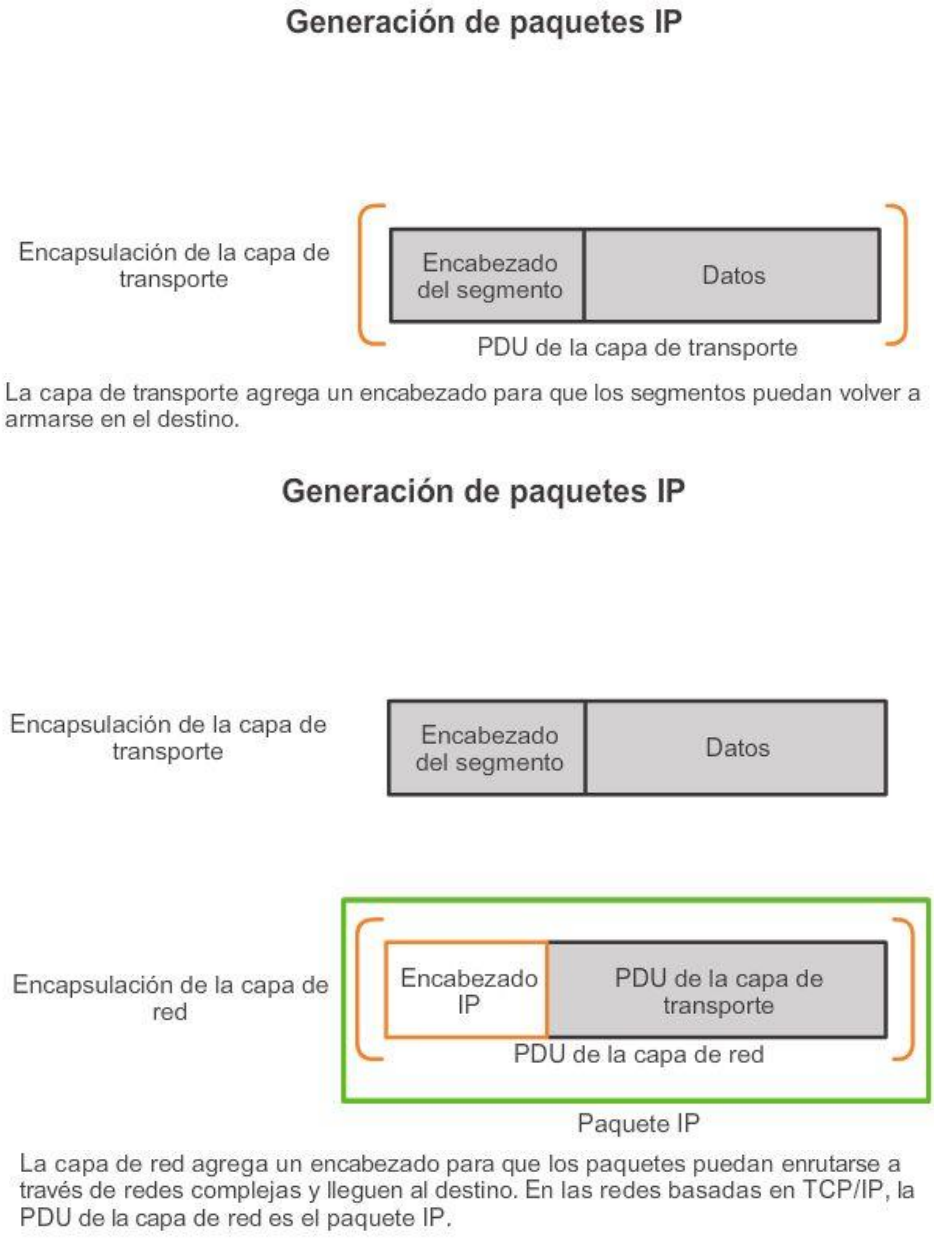
Capítulo 6: Capa de Red 6.1.2.5 Encapsulación de IP

El protocolo IP encapsula o empaqueta el segmento de la capa de transporte agregando un encabezado IP. Este encabezado se utiliza para entregar el paquete al host de destino. El encabezado IP permanece en su lugar desde el momento en que el paquete abandona la capa de red del host de origen hasta que llega a la capa de red del host de destino.

En la figura 1, se muestra el proceso de creación de la PDU de la capa de transporte. En la figura 2, se muestra el proceso subsiguiente de creación de la PDU de la capa de red.

El proceso de encapsulación de datos capa por capa permite el desarrollo y el escalamiento de los servicios de las diferentes capas sin afectar otras capas. Esto significa que el protocolo IPv4 o IPv6, o cualquier protocolo nuevo que se desarrolle en el futuro, pueden empaquetar fácilmente los segmentos de la capa de transporte.

Los routers pueden implementar estos diferentes protocolos de capa de red para operar al mismo tiempo en una red desde y hacia el mismo host o hosts diferentes. El enrutamiento que realizan estos dispositivos intermediarios solo tiene en cuenta el contenido del encabezado del paquete que encapsula el segmento. En todos los casos, la porción de datos del paquete, es decir, la PDU de la capa de transporte encapsulada, no se modifica durante los procesos de la capa de red.



Capítulo 6: Capa de Red 6.1.3.1 Encabezado de paquetes IPv4

IPv4 se utiliza desde 1983, cuando se implementó en la Advanced Research Projects Agency Network (ARPANET, Red de la Agencia de Proyectos de Investigación Avanzada), que fue la precursora de Internet. Internet se basa en gran medida en IPv4, que continua siendo el protocolo de capa de red que más se utiliza.

Los paquetes IPV4 tienen dos partes:

- Encabezado IP: identifica las características del paquete.
- Contenido: contiene la información del segmento de capa 4 y los datos propiamente dichos.

Como se muestra en la ilustración, los encabezados de paquetes IPV4 constan de campos que contienen información importante sobre el paquete. Estos campos contienen números binarios que se examinan en el proceso de capa 3. Los valores binarios de cada campo identifican las distintas configuraciones del paquete IP.

Los campos importantes del encabezado de IPv4 incluyen los siguientes:

- Versión: contiene un valor binario de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv4, este campo siempre se establece en 0100.

- Servicios diferenciados (DS): anteriormente denominado “Tipo de servicio” (ToS), se trata de un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los primeros 6 bits identifican el valor del Punto de código de servicios diferenciados (DSCP), utilizado por un mecanismo de calidad de servicio (QoS). Los últimos 2 bits identifican el valor de Notificación explícita de congestión (ECN), que se puede utilizar para evitar que los paquetes se descarten durante momentos de congestión de la red.

- Tiempo de vida (TTL): contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. Se especifica en segundos, pero comúnmente se denomina “conteo de saltos”.

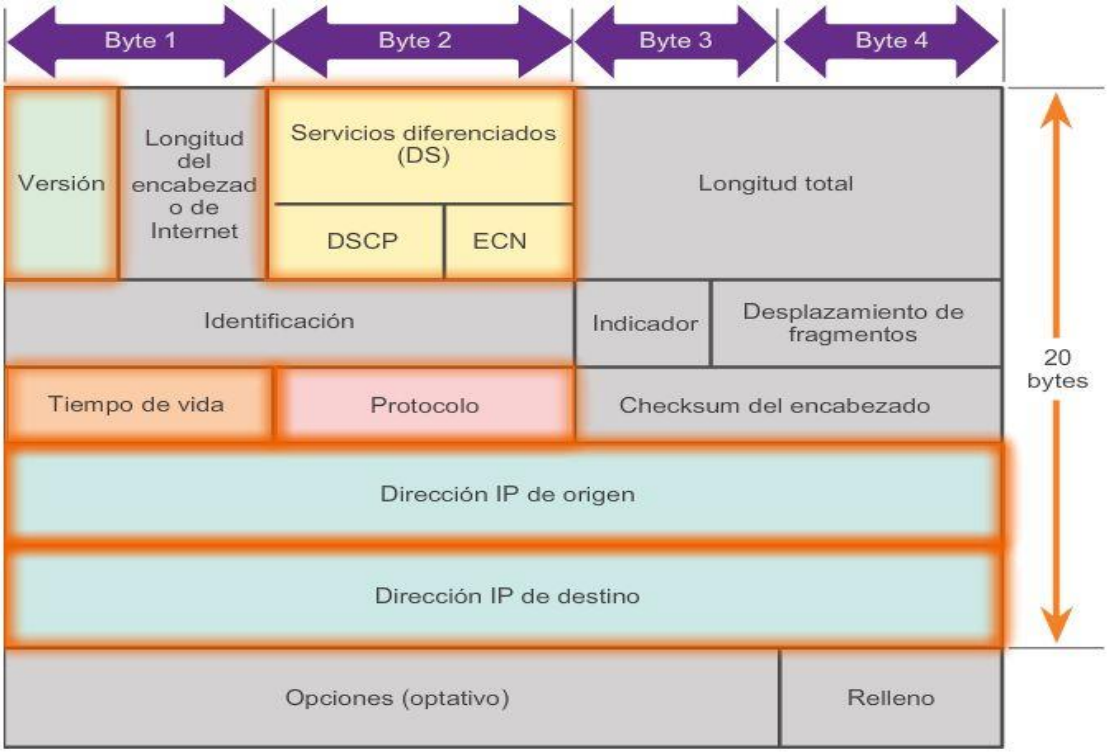
  El emisor del paquete establece el valor inicial de tiempo de vida (TTL), el que disminuye un punto por cada salto, es decir, cada vez que el paquete es procesado por un router. Si el campo TTL disminuye a cero, el router descarta el paquete y envía un mensaje del protocolo de mensajes de control de Internet (ICMP) de Tiempo superado a la dirección IP de origen. El comando tracerouteutiliza este campo para identificar los routers utilizados entre el origen y el destino.

- Protocolo: este valor binario de 8 bits indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Los valores comunes incluyen ICMP (1), TCP (6) y UDP (17).

- Dirección IP de origen: contiene un valor binario de 32 bits que representa la dirección IP de origen del paquete.

- Dirección IP de destino: contiene un valor binario de 32 bits que representa la dirección IP de destino del paquete.

Los dos campos que más comúnmente se toman como referencia son las direcciones IP de origen y de destino. Estos campos identifican de dónde proviene el paquete y adónde va. Por lo general, estas direcciones no se modifican durante la transferencia desde el origen hasta el destino.



Capítulo 6: Capa de Red 6.1.3.2 Campos del encabezado de IPv4

Los campos restantes se utilizan para identificar y validar el paquete, o para volver a ordenar un paquete fragmentado.

Los campos utilizados para identificar y validar el paquete incluyen los siguientes:

- Longitud del encabezado de Internet (IHL): contiene un valor binario de 4 bits que identifica la cantidad de palabras de 32 bits en el encabezado. El valor de IHL varía según los campos Opciones y Relleno. El valor mínimo para este campo es 5 (es decir, 5×32 = 160 bits = 20 bytes), y el valor máximo es 15 (es decir, 15×32 = 480 bits = 60 bytes).

- Longitud total: en ocasiones denominado “Longitud del paquete”, este campo de 16 bits define el tamaño total del paquete (fragmento), incluidos el encabezado y los datos, en bytes. La longitud mínima de paquete es de 20 bytes (encabezado de 20 bytes + datos de 0 bytes), y la máxima es de 65 535 bytes.

- Checksum del encabezado: este campo de 16 bits se utiliza para la verificación de errores del encabezado IP. El checksum del encabezado se vuelve a calcular y se compara con el valor en el campo checksum. Si los valores no coinciden, se descarta el paquete.

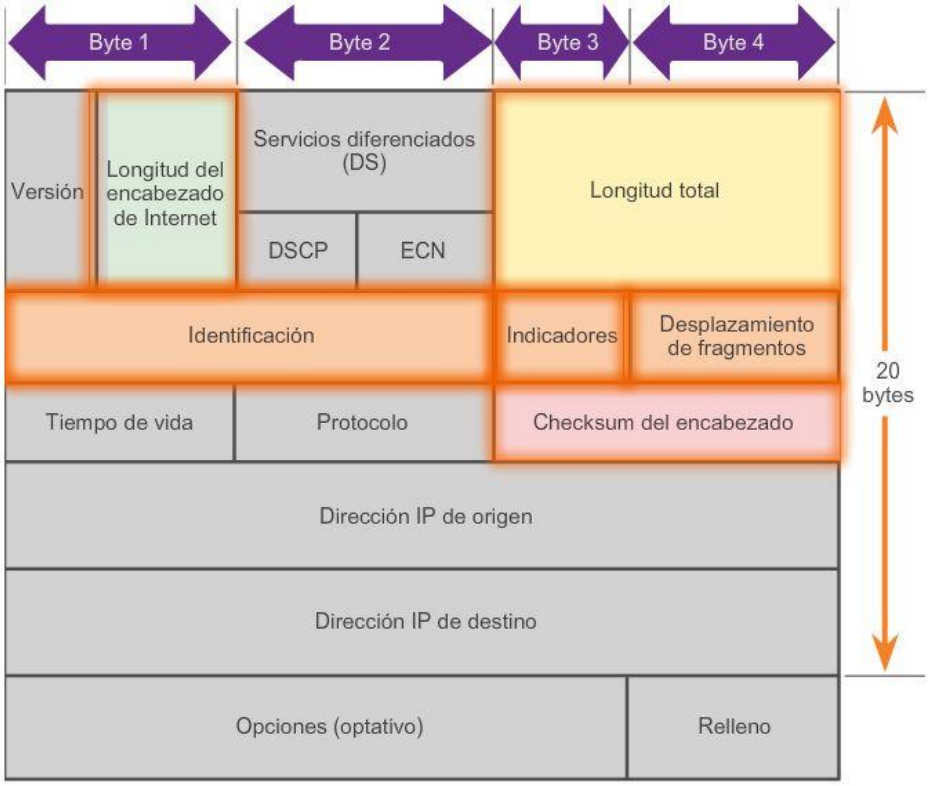
Es posible que un router deba fragmentar un paquete cuando lo reenvía de un medio a otro que tiene una MTU más pequeña. Cuando esto sucede, se produce una fragmentación, y el paquete IPV4 utiliza los siguientes campos para llevar a cabo un seguimiento de los fragmentos:

- Identificación: este campo de 16 bits identifica de forma exclusiva el fragmento de un paquete IP original.

- Indicadores: este campo de 3 bits identifica cómo se fragmenta el paquete. Se utiliza con los campos Desplazamiento de fragmentos e Identificación para ayudar a reconstruir el paquete original con el fragmento.

- Desplazamiento de fragmentos: este campo de 13 bits identifica el orden en que se debe colocar el fragmento del paquete en la reconstrucción del paquete original sin fragmentar.

Nota: los campos Opciones y Relleno se utilizan con poca frecuencia y exceden el ámbito de este capítulo.



Capítulo 6: Capa de Red 6.1.3.3 Encabezados de IPv4 de muestra

Wireshark es una herramienta de control de red útil para cualquier persona que trabaje con redes y se puede utilizar con la mayoría de las prácticas de laboratorio en los cursos de Cisco Certified Network Associate (CCNA) para tareas de análisis de datos y resolución de problemas. Puede utilizarse para ver los valores de muestra contenidos en los campos del encabezado IP.

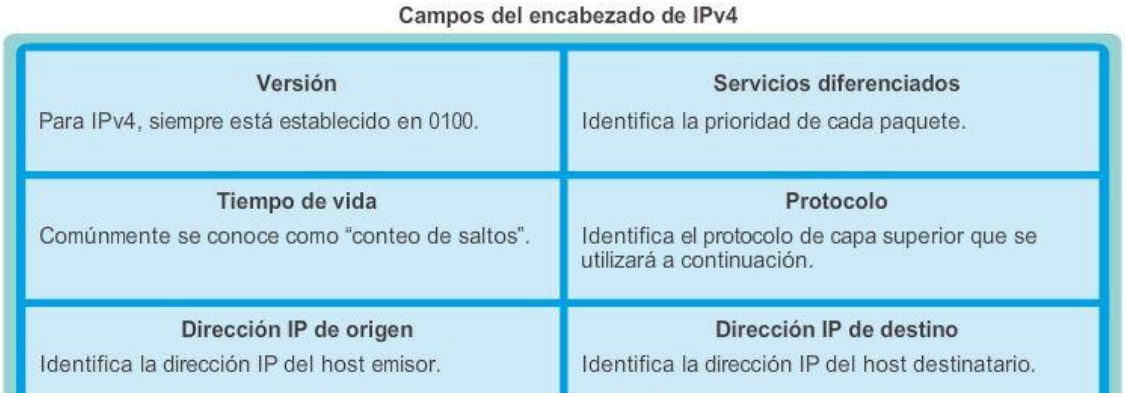
En las tres ilustraciones, se incluyen capturas de muestra de varios paquetes IP:

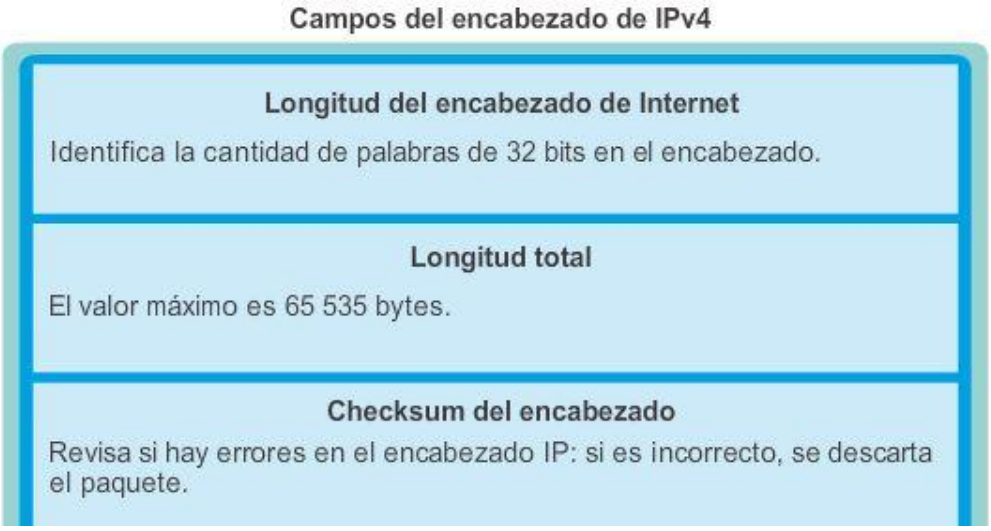
- En la captura de muestra de la figura 1, se muestra el contenido del paquete número 2. Observe que la dirección de origen (Source) figura como 192.168.1.109, y la de destino (Destination) figura como 192.168.1.1. La ventana del centro contiene información sobre el encabezado de IPv4, como la longitud del encabezado (header length), la longitud total (total length) y cualquier indicador (flags) que se establezca.

- En la captura de muestra de la figura 2, se muestra el contenido del paquete número 8. Este es un paquete HTTP. Observe además la presencia de información más allá de la sección TCP.

- Por último, en la captura de muestra de la figura 3, se muestra el contenido del paquete número 16. El paquete de muestra es una petición ping del host 192.168.1.109 al host 192.168.1.1. Observe la ausencia de información de TCP o UDP, debido a que este es un paquete de protocolo de mensajes de control de Internet (ICMP).

Capítulo 6: Capa de Red 6.1.3.4 Actividad: Campos del encabezado de IPv4





Capítulo 6: Capa de Red 6.1.4.1 Limitaciones de IPv4

A través de los años, IPv4 se actualizó para enfrentar nuevos desafíos. Sin embargo, incluso con los cambios, IPv4 continúa teniendo tres problemas importantes:

- Agotamiento de direcciones IP: IPv4 dispone de una cantidad limitada de direcciones IP públicas exclusivas. Si bien existen aproximadamente 4000 millones de direcciones IPv4, la cantidad creciente de dispositivos nuevos con IP habilitado, las conexiones permanentes y el crecimiento potencial de las regiones menos desarrolladas aumentan la necesidad de más direcciones.

- Expansión de la tabla de enrutamiento de Internet: los routers utilizan tablas de enrutamiento para determinar cuál es el mejor camino. A medida que aumenta la cantidad de servidores (nodos) conectados a Internet, también lo hace la cantidad de rutas de la red. Estas rutas IPv4 consumen muchos recursos de memoria y del procesador en los routers de Internet.

- Falta de conectividad de extremo a extremo: la traducción de direcciones de red (NAT) es una tecnología de implementación frecuente en las redes IPv4. La tecnología NAT proporciona una forma de que varios dispositivos compartan una misma dirección IP pública. Sin embargo, dado que comparten la dirección IP pública, la dirección IP de un host de red interno se oculta. Esto puede resultar problemático para las tecnologías que requieren conectividad de extremo a extremo.

Capítulo 6: Capa de Red 6.1.4.2 Presentación de IPv6

A principios de los años noventa, el Internet Engineering Task Force (IETF) comenzó a preocuparse por los problemas de IPv4 y empezó a buscar un reemplazo.

Esta actividad condujo al desarrollo de IP versión 6 (IPv6). IPv6 supera las limitaciones de IPv4 y constituye una mejora eficaz con características que se adaptan mejor a las demandas actuales y previsibles de las redes.

Las mejoras que proporciona IPv6 incluyen lo siguiente:

- Mayor espacio de direcciones: las direcciones IPv6 se basan en un direccionamiento jerárquico de 128 bits, mientras que en IPv4 es de 32 bits. El número de direcciones IP disponibles aumenta drásticamente.

- Mejora del manejo de los paquetes: el encabezado de IPv6 se simplificó con menos campos. Esto mejora el manejo de paquetes por parte de los routers intermediarios y también proporciona compatibilidad para extensiones y opciones para aumentar la escalabilidad y la duración.

- Eliminación de la necesidad de NAT: con tal cantidad de direcciones IPv6 públicas, no se necesita traducción de direcciones de red (NAT). Los sitios de los clientes, ya sean las empresas más grandes o unidades domésticas, pueden obtener una dirección de red IPv6 pública. Esto evita algunos de los problemas de aplicaciones debidos a NAT que afectan a las aplicaciones que requieren conectividad de extremo a extremo.

- Seguridad integrada: IPv6 admite capacidades de autenticación y privacidad de forma nativa. Con IPv4, se debían implementar características adicionales para este fin.

El espacio de direcciones IPv4 de 32 bits proporciona aproximadamente 4 294 967 296 direcciones únicas. De estas, solo 3700 millones de direcciones se pueden asignar, porque el sistema de direccionamiento IPv4 separa las direcciones en clases y reserva direcciones para multicast, pruebas y otros usos específicos.

Como se muestra en la ilustración, el espacio de direcciones IP versión 6 proporciona 340 282 366 920 938 463 463 374 607 431 768 211 456, o 340 sextillones de direcciones, lo que equivale a aproximadamente todos los granos de arena de la Tierra.

Nombre del número	Notación científica	Cantidad de ceros
1millar	10^3	1,000
1millón	10^6	1,000,000
1000 millones	10^9	1,000,000,000
1billón	10^12	1000,000,000,000
1000 billones	10^15	1,000,000,000,000,000
1trillón	10^18	1,000,000,000,000,000,000
1000 trillones	10^21	1,000,000,000,000,000,000,000
1cuatrillón	10^24	1,000,000,000,000,000,000,000,000
1000 cuatrillones	10^27	1,000,000,000000,000,000,000,000,000
1quintillón	10^30	1,000,000,000,000,000,000,000,000,000,000
1000 quintillones	10^33	1,000,000,000,000,000,000,000,000,000,000,000
1sextillón	10^36	1,000,000,000,000,000,000,000,000,000,000,000,000

Leyenda

Hay 4000 millones de direcciones IPv4.

Hay 340 sextillones de direcciones IPv6.

Capítulo 6: Capa de Red 6.1.4.3 Encapsulación de IPv6

Una de las principales mejoras de diseño de IPv6 con respecto a IPv4 es el encabezado de IPv6 simplificado.

El encabezado de IPv4 consta de 20 octetos (hasta 60 bytes si se utiliza el campo Opciones) y 12 campos de encabezado básicos, sin incluir los campos Opciones y Relleno.

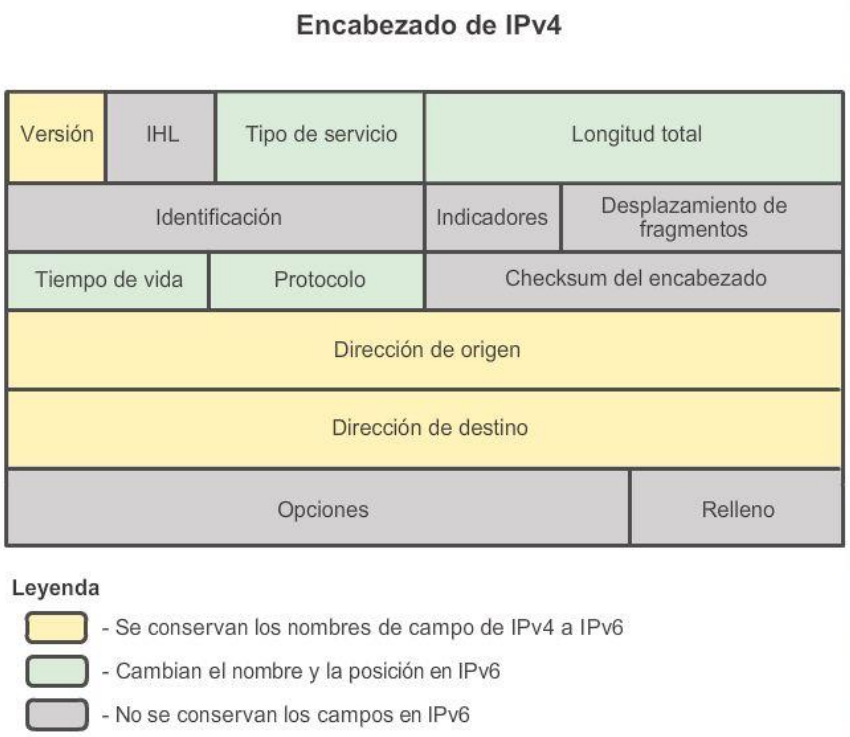
El encabezado de IPv6 consta de 40 octetos (en gran medida, debido a la longitud de las direcciones IPv6 de origen y de destino) y 8 campos de encabezado (3 campos de encabezado IPv4 básicos y 5 campos de encabezado adicionales).

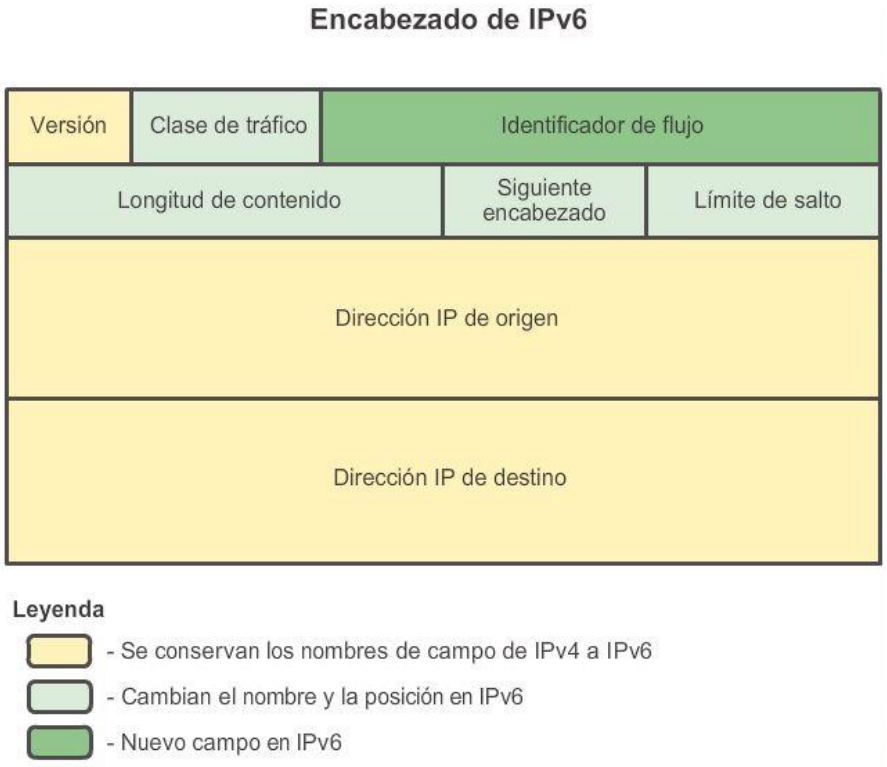
En la figura 1, se muestra la estructura del encabezado de IPv4. Como se muestra en la ilustración, en IPv6 algunos campos permanecen iguales, algunos campos del encabezado de IPv4 no se utilizan, y algunos campos tienen nombres y posiciones diferentes.

Además, se agregó un nuevo campo a IPv6 que no se utiliza en IPv4. El encabezado de IPv6 simplificado se muestra en la figura 2.

El encabezado de IPv6 simplificado ofrece varias ventajas respecto de IPv4:

- Mayor eficacia de enrutamiento para un buen rendimiento y una buena escalabilidad de velocidad de reenvío.
- Sin requisito de procesamiento de checksums.
- Mecanismos de encabezado de extensión simplificados y más eficaces (en comparación con el campo Opciones de IPv4).
- Un campo Identificador de flujo para procesamiento por flujo, sin necesidad de abrir el paquete interno de transporte para identificar los distintos flujos de tráfico.





Capítulo 6: Capa de Red 6.1.4.4 Encabezado de paquete IPv6

Los campos de encabezado de paquetes IPv6 incluyen los siguientes:

- Versión: este campo contiene un valor binario de 4 bits que identifica la versión del paquete IP. Para los paquetes IPv6, este campo siempre se establece en 0110.

- Clase de tráfico: este campo de 8 bits equivale al campo Servicios diferenciados (DS) de IPv4. También contiene un valor de Punto de código de servicios diferenciados (DSCP) de 6 bits utilizado para clasificar

paquetes y un valor de Notificación explícita de congestión (ECN) de 2 bits utilizado para controlar la congestión del tráfico.

- Identificador de flujo: este campo de 20 bits proporciona un servicio especial para aplicaciones en tiempo real. Se puede utilizar para indicar a los routers y switches que deben mantener la misma ruta para el flujo de paquetes, a fin de evitar que estos se reordenen.

- Longitud de contenido: este campo de 16 bits equivale al campo Longitud total del encabezado de IPv4. Define el tamaño total del paquete (fragmento), incluidos el encabezado y las extensiones optativas.

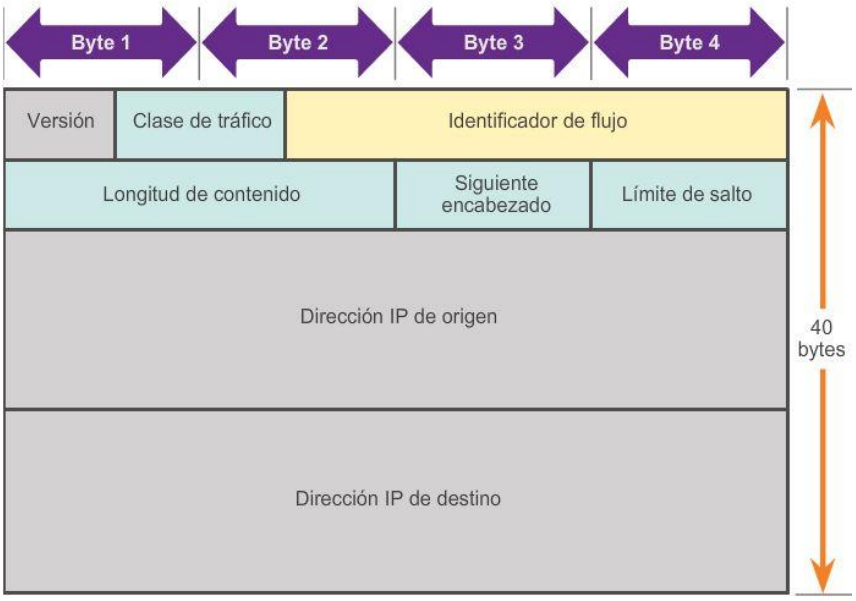
- Siguiente encabezado: este campo de 8 bits equivale al campo Protocolo de IPv4. Indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Este campo también se usa si se agregan encabezados de extensión optativos al paquete IPv6.

- Límite de saltos: este campo de 8 bits reemplaza al campo TTL de IPv4. Cuando cada router reenvía un paquete, este valor disminuye en un punto. Cuando el contador llega a 0, el paquete se descarta y se reenvía un mensaje de ICMPv6 al host emisor en el que se indica que el paquete no llegó a destino.

- Dirección de origen: este campo de 128 bits identifica la dirección IPv6 del host emisor.

- Dirección de destino: este campo de 128 bits identifica la dirección IPv6 del host receptor.

Los paquetes IPv6 también pueden contener encabezados de extensión (EH), que proporcionan información optativa de la capa de red. Los encabezados de extensión son optativos y se colocan entre el encabezado de IPv6 y el contenido. Los EH se utilizan para realizar la fragmentación, aportar seguridad, admitir la movilidad, y más.



Capítulo 6: Capa de Red 6.1.4.5 Encabezados de IPv6 de muestra

Al ver las capturas de IPv6 de Wireshark, observe que el encabezado de IPv6 tiene muchos menos campos que un encabezado de IPv4. Esto hace que el encabezado de IPv6 sea más fácil y más rápido de procesar para el router.

La dirección IPv6 propiamente dicha es muy distinta. Debido al mayor tamaño de las direcciones IPv6, de 128 bits, se utiliza el sistema de numeración hexadecimal para simplificar la representación de las direcciones. En las direcciones IPv6, se utilizan dos puntos para separar las entradas en una serie de bloques hexadecimales de 16 bits.

En la captura de muestra de la figura 1, se muestra el contenido del paquete número 46. El paquete contiene el mensaje inicial del protocolo TCP de enlace de tres vías entre un host IPv6 y un servidor IPv6. Observe los valores en la sección expandida del encabezado de IPv6. Observe, además, que se trata de un paquete TCP y que no contiene más información más allá de la sección TCP.

En la captura de muestra de la figura 2, se muestra el contenido del paquete número 49. El paquete contiene el mensaje GET inicial del protocolo de transferencia de hipertexto (HTTP) para el servidor. Observe que se trata de un paquete HTTP y que ahora contiene información más allá de la sección TCP.

Por último, en la captura de muestra de la figura 3, se muestra el contenido del paquete número 1. El paquete de muestra es un mensaje ICMPv6 de solicitud de vecino. Observe que no hay información de TCP o UDP.

Capítulo 6: Capa de Red 6.2.1.1 Decisión de reenvío de host

Otra función de la capa de red es dirigir los paquetes entre los hosts. Un host puede enviar un paquete:

- A sí mismo: en este caso, se utiliza una dirección IP especial, 127.0.0.1, que se denomina “interfaz loopback”. Esta dirección de loopback se asigna automáticamente a un host cuando se ejecuta TCP/IP. La capacidad de un host de enviarse un paquete a sí mismo mediante la funcionalidad de la red resulta útil para realizar pruebas. Cualquier dirección IP dentro de la red 127.0.0.0/8 se refiere al host local.

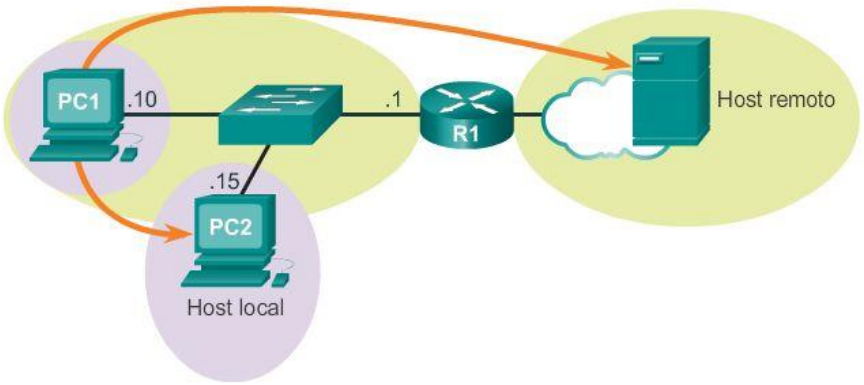
- A un host local: un host en la misma red que el host emisor. Los hosts comparten la misma dirección de red.

- A un host remoto: un host en una red remota. Los hosts no comparten la dirección de red.

Para determinar si un paquete está destinado a un host local o un host remoto, se compara la combinación de la dirección IP y la máscara de subred del dispositivo de origen (o emisor) con la dirección IP y la máscara de subred del dispositivo de destino.

En una red doméstica o comercial, es posible que tenga varios dispositivos conectados por cable o inalámbricos interconectados mediante un dispositivo intermediario, como un switch LAN o un punto de acceso inalámbrico (WAP). Este dispositivo intermediario proporciona interconexiones entre los hosts locales en la red local. Los hosts locales pueden comunicarse y compartir información sin necesidad de ningún dispositivo adicional. Si un host envía un paquete a un dispositivo que está configurado con la misma red IP que el dispositivo host, el paquete tan solo se reenvía por la interfaz del host, a través del dispositivo intermediario, directamente al dispositivo de destino.

Por supuesto, en la mayoría de las situaciones deseamos que los dispositivos puedan conectarse más allá del segmento de red local: a otros hogares, a otras empresas y a Internet. Los dispositivos que están más allá del segmento de red local se conocen como “hosts remotos”. Cuando un dispositivo de origen envía un paquete a un dispositivo de destino remoto, se necesita la ayuda de routers y el enrutamiento. El enrutamiento es el proceso mediante el cual se identifica el mejor camino hacia un destino. El router conectado al segmento de red local se denominagateway predeterminado.



Capítulo 6: Capa de Red 6.2.1.2 Gateway predeterminado

El gateway predeterminado es el dispositivo que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. En un entorno doméstico o de pequeña empresa, el gateway predeterminado se suele utilizar para conectar la red local a Internet.

Si el host envía un paquete a un dispositivo en otra red IP, debe reenviar el paquete al gateway predeterminado a través del dispositivo intermediario. Esto se debe a que los dispositivos host no mantienen la información de enrutamiento más allá de la red local para llegar a destinos remotos; esto lo hace el gateway predeterminado. El gateway predeterminado, que en general es un router, mantiene una tabla de enrutamiento. Una tabla de enrutamiento es un archivo de datos que se encuentra en la RAM y que se utiliza para almacenar información de la ruta sobre la red conectada directamente, así como las entradas de redes remotas descubiertas por el dispositivo. El router utiliza la información en la tabla de enrutamiento para determinar cuál es el mejor camino para llegar a esos destinos.

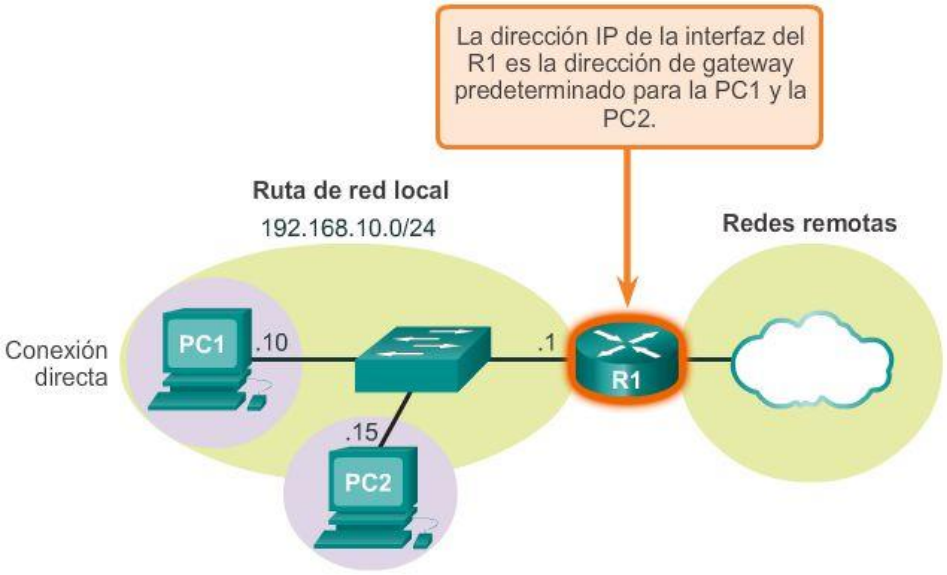
¿Cómo decide un host si debe o no debe reenviar paquetes al gateway predeterminado? Los hosts deben poseer una tabla de enrutamiento local propia para asegurarse de que los paquetes de la capa de red se dirijan a la red de destino correcta. La tabla local del host generalmente contiene lo siguiente:

- Conexión directa: se trata de una ruta a la interfaz loopback (127.0.0.1).
- Ruta de red local: la red a la cual está conectado el host se completa automáticamente en la tabla de enrutamiento del host.
- Ruta predeterminada local: la ruta predeterminada representa la ruta que los paquetes deben seguir para llegar a todas las direcciones de redes remotas. La ruta predeterminada se crea cuando hay una dirección de gateway predeterminado en el host. La dirección de gateway predeterminado es la dirección IP de la interfaz de red del router que está conectada a la red local. La dirección de gateway predeterminado se puede configurar en el host de forma manual o se puede descubrir de manera dinámica.

Es importante observar que la ruta predeterminada y, por lo tanto, el gateway predeterminado, se utilizan solo cuando un host debe reenviar paquetes a una red remota. No se requieren, ni es necesario configurarlos, si solo se envían paquetes a dispositivos en la red local.

Por ejemplo, considere una impresora o un escáner de red. Si la impresora de red tiene una dirección IP y una máscara de subred configuradas, los hosts locales pueden enviar documentos a la impresora para imprimirlos. Además, la impresora puede reenviar los documentos escaneados a cualquier host local. En tanto la impresora se use solo de forma local, no se requiere una dirección de gateway predeterminado.

De hecho, al no configurar una dirección de gateway predeterminado en la impresora, se deniega de manera eficaz el acceso a Internet, lo que puede ser una acertada decisión de seguridad. Sin acceso a Internet, no existe riesgo de seguridad. Si bien algunos dispositivos, como las impresoras, pueden ofrecer la capacidad de realizar actualizaciones automáticas por Internet, por lo general es más fácil y más seguro obtener esas mismas actualizaciones a través de cargarlas en forma local desde un host local protegido, como una PC.



Capítulo 6: Capa de Red 6.2.1.3 Tabla de enrutamiento de host IPv4

En un host de Windows, se pueden utilizar los comandos route print o netstat -r para ver la tabla de enrutamiento del host. Los dos comandos provocan al mismo resultado. Al principio, los resultados pueden parecer abrumadores, pero son bastante fáciles de entender.

Al introducir el comando netstat -r o su equivalente, route print, se ven tres secciones relacionadas con las conexiones de red TCP/IP actuales:

- Lista de interfaces: enumera las direcciones de control de acceso al medio (MAC) y el número de interfaz asignado de cada interfaz con capacidad de red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.

- Tabla de rutas IPv4: enumera todas las rutas IPv4 conocidas, incluidas las conexiones directas, las rutas de red locales y las rutas predeterminadas locales.

- Tabla de rutas IPv6: enumera todas las rutas IPv6 conocidas, incluidas las conexiones directas, las rutas de red locales y las rutas predeterminadas locales.

Nota: los resultados del comando varían según cómo esté configurado el host y los tipos de interfaz que tenga.

En la ilustración, se muestra la sección de la tabla de rutas IPv4 de los resultados. Observe que los resultados se dividen en cinco columnas que identifican lo siguiente:

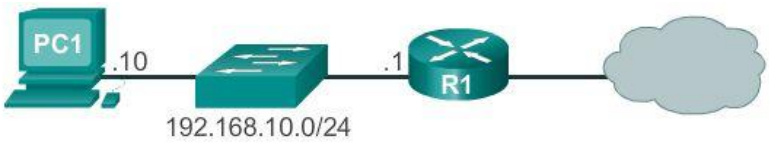
- Destino de red: enumera las redes que se pueden alcanzar.

- Máscara de red: incluye una máscara de subred que le indica al host cómo determinar las porciones de red y de host de la dirección IP.

- Puerta de acceso: indica la dirección que utiliza la PC local para llegar a un destino en una red remota. Si un destino es directamente accesible, se muestra como “En enlace” en esta columna.

- Interfaz: indica la dirección de la interfaz física utilizada para enviar el paquete al gateway que se emplea para llegar al destino de red.

- Métrica: indica el costo de cada ruta y se utiliza para determinar la mejor ruta a un destino.




```
C:\Users\PC1>netstat -r

<Resultado omitido>

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
    192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
   192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
  192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================

<Resultado omitido>
```

Capítulo 6: Capa de Red 6.2.1.4 Entradas de enrutamiento de host IPv4

Para ayudar a simplificar el resultado, las redes de destino se pueden agrupar en cinco secciones, identificadas por las áreas resaltadas en la ilustración:

0.0.0.0

La ruta predeterminada local. Todos los paquetes con destinos que no coincidan con otras direcciones especificadas en la tabla de enrutamiento se reenvían al gateway. Por lo tanto, todas las rutas de destino que no coincidan se envían al gateway con la dirección IP 192.168.10.1 (R1) que sale de la interfaz con la dirección IP 192.168.10.10. Observe que la dirección de destino final especificada en el paquete no cambia; en realidad, el host simplemente sabe que debe reenviar el paquete al gateway para su procesamiento posterior.

127.0.0.0 – 127.255.255.255

Todas estas direcciones de loopback se relacionan con la conexión directa y proporcionan servicios al host local.

192.168.10.0 - 192.168.10.255

Todas estas direcciones se relacionan con el host y la red local. Todos los paquetes con direcciones de destino dentro de esta categoría salen por la interfaz 192.168.10.10.

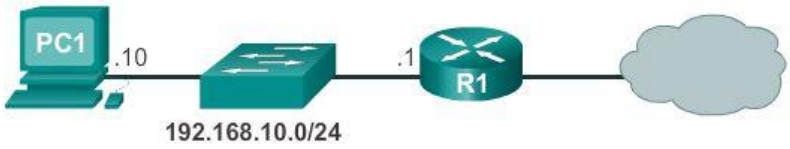
- 192.168.10.0: dirección de la ruta de red local que representa todas las PC en la red 192.168.10.x.
- 192.168.10.10: dirección del host local.
- 192.168.10.255: dirección de broadcast de la red, que envía mensajes a todos los hosts en la ruta de red local.

224.0.0.0

Direcciones multicast de clase D especiales reservadas para usar mediante la interfaz loopback (127.0.0.1) o la dirección IP del host (192.168.10.10).

255.255.255.255

Las últimas dos direcciones representan los valores de direcciones IP de broadcast limitado para usar mediante la interfaz loopback (127.0.0.1) o la dirección IP del host (192.168.10.10). Estas direcciones se pueden utilizar para buscar un servidor de DHCP antes de que se determine la dirección IP local.




```
C:\Users\PC1> netstat -r

<Resultado omitido>

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link       127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link       127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link       127.0.0.1     306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
     192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
    192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link       127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link       127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
===========================================================================

<Resultado omitido>
```

Capítulo 6: Capa de Red 6.2.1.5 Tabla de enrutamiento de host IPv4 de muestra

Por ejemplo, si la PC1 desea enviarle un paquete a 192.168.10.20, debería hacer lo siguiente:

1. Consultar la tabla de rutas IPv4.

2. Encontrar la correspondencia entre la dirección IP de destino y la entrada de destino de red 192.168.10.0 para determinar que el host está en la misma red (En enlace).

3. Luego, la PC1 enviaría el paquete hacia el destino final mediante su interfaz local (192.168.10.10).

En la figura 1, se destaca la ruta en que se encontró coincidencia.

Si la PC1 desea enviar un paquete a un host remoto ubicado en 10.10.10.10, debería hacer lo siguiente:

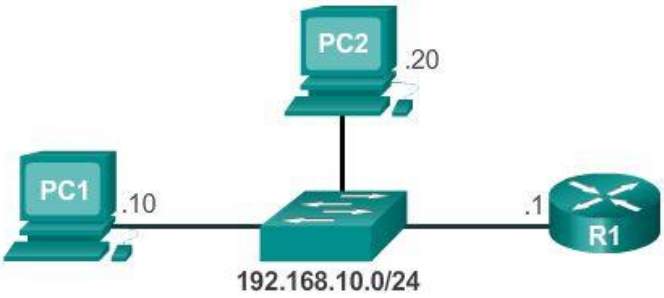
1. Consultar la tabla de rutas IPv4.

2. Determinar que no hay una coincidencia exacta para la dirección IP de destino.

3. Elegir la ruta predeterminada local (0.0.0.0) para descubrir que debe reenviar el paquete a la dirección de gateway 192.168.10.1.

4. Luego, la PC1 reenvía el paquete al gateway para usar su interfaz local (192.168.10.10). A continuación, el dispositivo de gateway determina la siguiente ruta para que el paquete llegue a la dirección de destino final 10.10.10.10.

En la figura 2, se destaca la ruta en que se encontró coincidencia.




```
C:\Users\PC1> netstat -r
<Resultado omitido>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
     192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
    192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================
<Resultado omitido>
```


```
C:\Users\PC1> netstat -r
<Resultado omitido>
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface Metric
          0.0.0.0          0.0.0.0    192.168.10.1    192.168.10.10     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10    281
     192.168.10.10  255.255.255.255         On-link    192.168.10.10    281
    192.168.10.255  255.255.255.255         On-link    192.168.10.10    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10    281
===========================================================================
<Resultado omitido>
```

Capítulo 6: Capa de Red 6.2.1.6 Tabla de enrutamiento de host IPv6 de muestra

El resultado de la tabla de rutas IPv6 difiere en los encabezados de las columnas y el formato, debido a que las direcciones IPv6 son más largas.

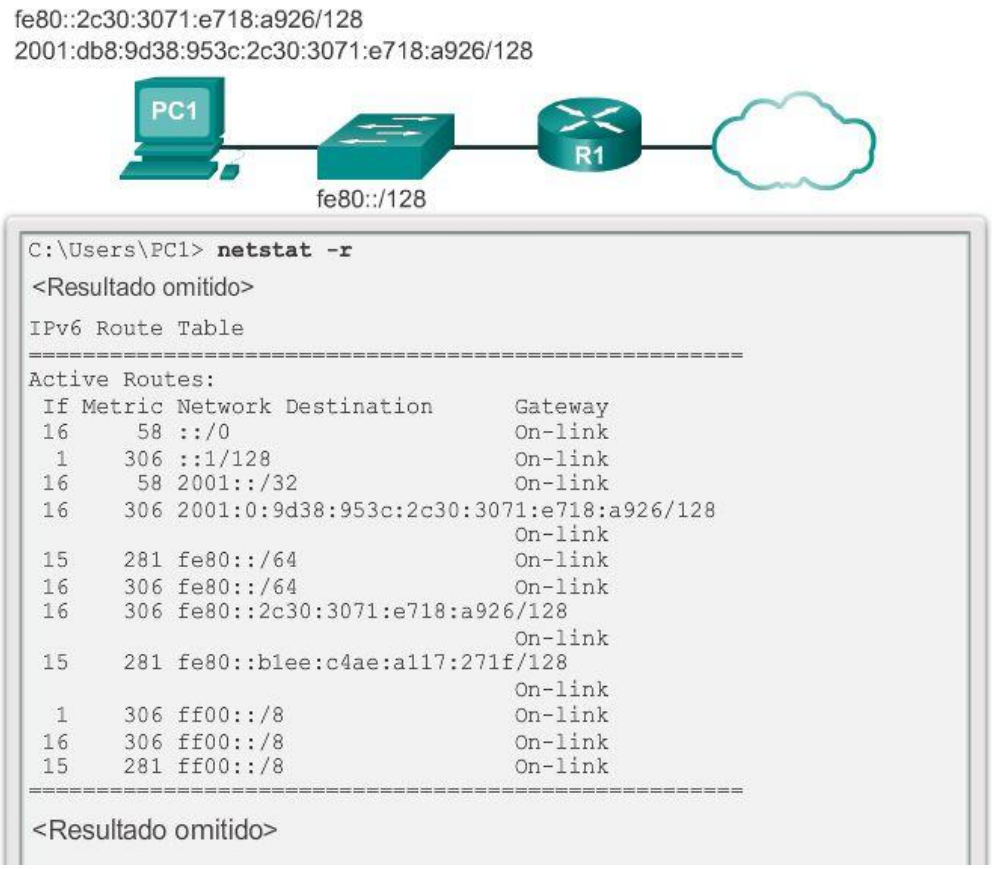
En la sección de la tabla de rutas IPv6, se muestran cuatro columnas que identifican lo siguiente:

- Si: incluye los números de interfaz de la sección Lista de interfaces del comando netstat –r. Los números de interfaz corresponden a las interfaces con capacidad de red en el host, incluidos los adaptadores Ethernet, Wi-Fi y Bluetooth.
- Métrica: indica el costo de cada ruta a un destino. Los números más bajos indican las rutas preferidas.
- Destino de red: enumera las redes que se pueden alcanzar.
- Puerta de acceso: indica la dirección que utiliza el host local para reenviar paquetes a un destino de red remoto. “En enlace” indica que el host actualmente está conectado.

Por ejemplo, en la ilustración, se muestra la sección de rutas IPv6 generada mediante el comando netstat –r para mostrar los siguientes destinos de red:

- ::/0: equivalente en IPv6 a la ruta predeterminada local.
- ::1/128: equivale a la dirección de loopback IPv4 y proporciona servicios al host local.
- 2001::/32: prefijo de red unicast global.
- 2001:0:9d38:953c:2c30:3071:e718:a926/128:dirección IPv6 unicast global de la PC local.
- fe80::/64: dirección de la ruta de red de enlace local, que representa todas las PC en la red IPv6 de enlace local.
- fe80::2c30:3071:e718:a926/128: dirección IPv6 link-local de la PC local.
- ff00::/8: direcciones multicast de clase D especiales y reservadas que equivalen a las direcciones IPv4 224.x.x.x.

Nota: en general, las interfaces en IPv6 tienen dos direcciones IPv6: una dirección link-local y una dirección unicast global. Asimismo, observe que no hay direcciones de broadcast en IPv6. Las direcciones IPv6 se analizan en mayor detalle en el capítulo siguiente.



Capítulo 6: Capa de Red 6.2.2.1 Decisión de reenvío de paquetes del router

Cuando un host envía un paquete a otro host, utiliza la tabla de enrutamiento para determinar adónde enviar el paquete. Si el host de destino está en una red remota, el paquete se reenvía a la dirección de un dispositivo de gateway.

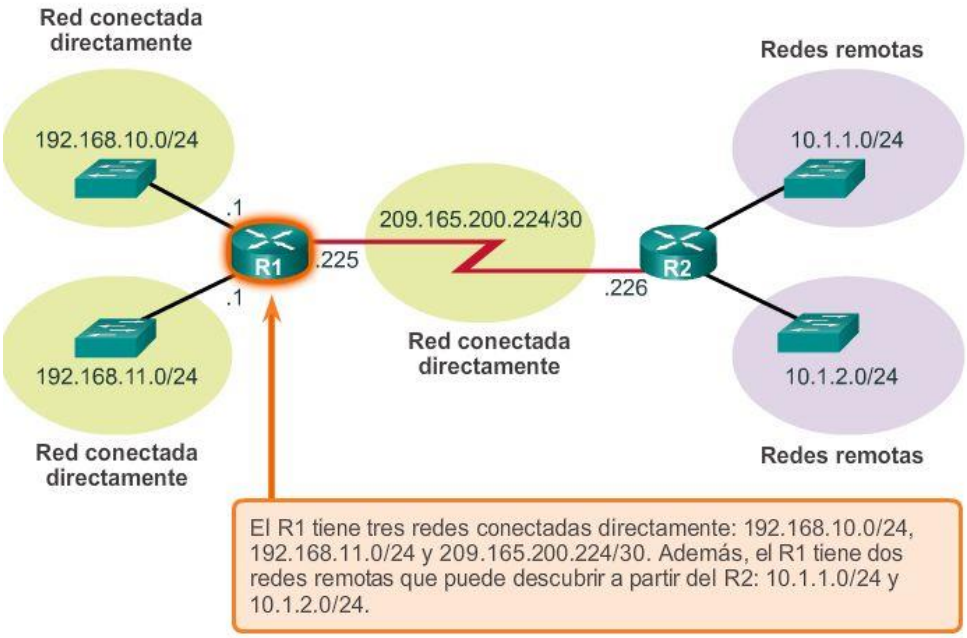
¿Qué sucede cuando un paquete llega a una interfaz del router? El router examina la tabla de enrutamiento para determinar adónde reenviar los paquetes.

La tabla de enrutamiento de un router almacena información sobre lo siguiente:

- Rutas conectadas directamente: estas rutas provienen de las interfaces del router activas. Los routers agregan una ruta conectada directamente cuando se configura una interfaz con una dirección IP y se activa. Cada una de las interfaces del router se conecta a un segmento de red diferente. En la tabla de enrutamiento, los routers mantienen información acerca de los segmentos de red a los que están conectados.

- Rutas remotas: estas rutas provienen de las redes remotas conectadas a otros routers. El administrador de red puede configurar las rutas a estas redes de forma manual en el router local, o estas se pueden configurar de forma dinámica habilitando al router local para que intercambie información de enrutamiento con otros routers mediante protocolos de enrutamiento dinámico.

En la ilustración, se identifican las redes conectadas directamente y las redes remotas del router R1.



Capítulo 6: Capa de Red 6.2.2.2 Tabla de enrutamiento de router IPv4

En una tabla de enrutamiento de host, solo se incluye información sobre las redes conectadas directamente. Un host requiere un gateway predeterminado para enviar paquetes a un destino remoto. La tabla de enrutamiento de un router contiene información similar, pero también puede identificar redes remotas específicas.

La tabla de enrutamiento de un router es similar a la tabla de enrutamiento de un host. Ambas identifican lo siguiente:

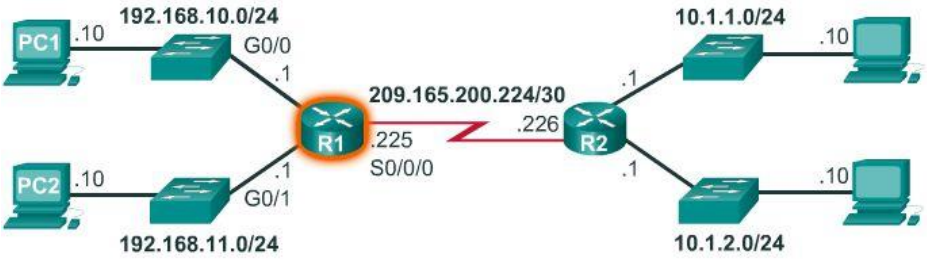
- Red de destino
- Métrica asociada a la red de destino
- Gateway para llegar a la red de destino

En un router Cisco IOS, se puede utilizar el comando show ip route para ver la tabla de enrutamiento. Un router también proporciona información adicional de la ruta, incluida la forma en que se descubrió la ruta, cuándo se actualizó por última vez y qué interfaz específica se debe utilizar para llegar a un destino predefinido.

Cuando un paquete llega a la interfaz del router, este examina el encabezado del paquete para determinar la red de destino. Si la red de destino coincide con una ruta de la tabla de enrutamiento, el router reenvía el paquete utilizando la información especificada en la tabla.

Si hay dos o más rutas posibles hacia el mismo destino, se utiliza la métrica para decidir qué ruta aparece en la tabla de enrutamiento.

En la ilustración, se muestra la tabla de enrutamiento del R1 en una red simple. A diferencia de la tabla de enrutamiento de host, no hay encabezados de columna que identifiquen la información incluida en una entrada de la tabla de enrutamiento. Por lo tanto, es importante conocer el significado de los distintos tipos de información incluidos en cada entrada.




```
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
     10.0.0.0/8 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
R1#
```

Capítulo 6: Capa de Red 6.2.2.3 Entradas de tabla de enrutamiento de red conectada directamente

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 enrutamiento. En la ilustración, se muestran las entradas de la tabla de enrutamiento en el R1 para la red conectada directamente 192.168.10.0. 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

El origen de la ruta se rotula como “A” en la ilustración. Identifica el modo en que se descubrió la ruta. Las interfaces conectadas directamente tienen dos códigos de origen de la ruta.

- C: identifica una red conectada directamente. Las redes conectadas directamente se crean de forma automática cuando se configura una interfaz con una dirección IP y se activa.

- L: identifica que la ruta es link-local. Las redes link-local se crean de forma automática cuando se configura una interfaz con una dirección IP y se activa.

Red de destino

La red de destino se rotula como “B” en la ilustración. Identifica la dirección de la red remota.

Interfaz de salida

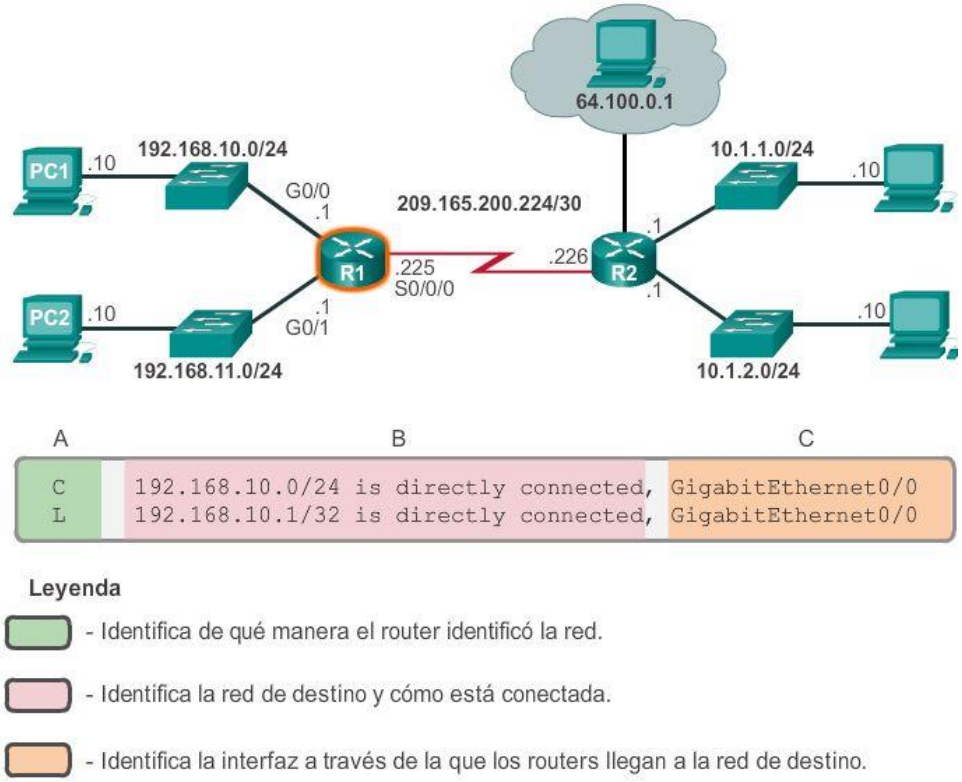
La interfaz de salida se rotula como “C” en la ilustración. Identifica la interfaz de salida que se debe utilizar al reenviar paquetes a la red de destino.

Nota: las entradas de la tabla de enrutamiento de link-local no aparecían en las tablas de enrutamiento antes de la versión 15 de IOS.

En general, los routers tienen varias interfaces configuradas. La tabla de enrutamiento almacena información sobre las rutas conectadas directamente y las remotas. Tal como ocurre con las redes conectadas directamente, el origen de la ruta identifica cómo se descubrió la ruta. Por ejemplo, los códigos comunes para las redes remotas incluyen lo siguiente:

- 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 obtuvo de forma dinámica de otro router mediante el protocolo de enrutamiento de gateway interior mejorado (EIGRP).
- O: indica que la ruta se obtuvo de forma dinámica de otro router mediante el protocolo de enrutamiento Open Shortest Path First (OSPF).

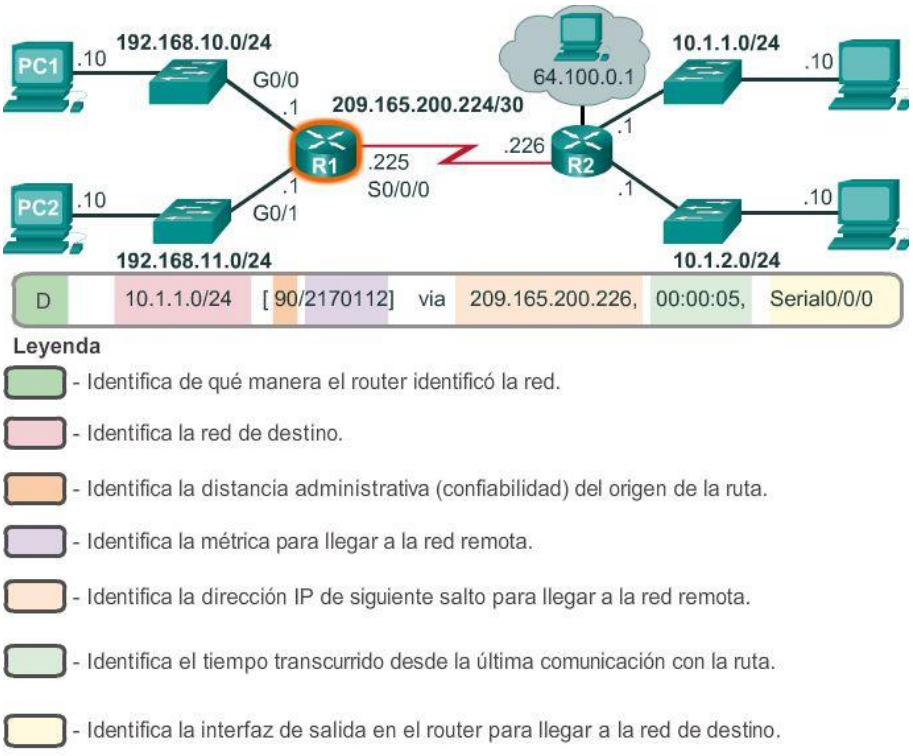
Nota: otros códigos exceden el ámbito de este capítulo.



Capítulo 6: Capa de Red 6.2.2.4 Entradas de tabla de enrutamiento de red remota

En la ilustración, se muestra una entrada de la tabla de enrutamiento 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.
- Métrica: identifica el valor asignado para llegar a la red remota. Los valores más bajos indican las rutas preferidas.
- Siguiente salto: identifica la dirección IP del router siguiente para 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.



Capítulo 6: Capa de Red 6.2.2.5 Dirección Next-Hop

El siguiente salto es la dirección del dispositivo que procesará el paquete a continuación. Para un host en una red, la dirección del gateway predeterminado (interfaz del router) es el siguiente salto para todos los paquetes que se deben enviar a otra red. En la tabla de enrutamiento de un router, cada ruta a una red remota incluye un siguiente salto.

Cuando un paquete destinado a una red remota llega al router, este busca una correspondencia entre la red de destino y una ruta en la tabla de enrutamiento. Si se encuentra una coincidencia, el router reenvía el

paquete a la dirección IP del router de siguiente salto mediante la interfaz que se identificó con la entrada de la ruta.

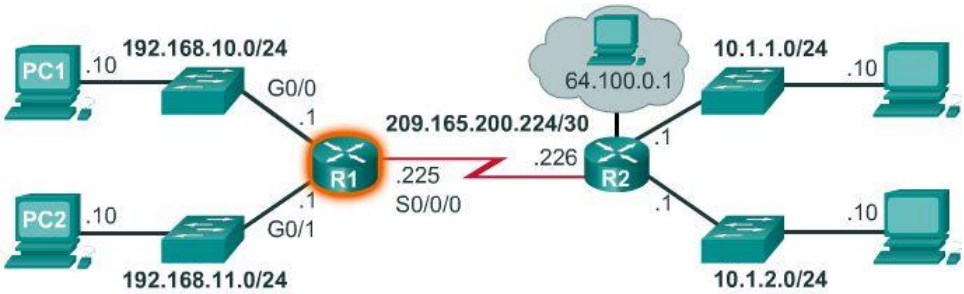
Un router de siguiente salto es el gateway a las redes remotas.

Por ejemplo, en la ilustración, un paquete que llega al R1 destinado a la red 10.1.1.0 o la red 10.1.2.0 se reenvía a la dirección de siguiente salto 209.165.200.226 mediante la interfaz serial 0/0/0.

Las redes conectadas directamente a un router no tienen dirección de siguiente salto, porque los routers pueden reenviar los paquetes en forma directa a los hosts en esas redes mediante la interfaz designada.

El router no puede reenviar los paquetes sin una ruta para la red de destino en la tabla de enrutamiento. Si no hay una ruta que represente la red de destino en la tabla de enrutamiento, el paquete se descarta (es decir, no se reenvía).

Sin embargo, de la misma manera en que un host puede utilizar un gateway predeterminado para reenviar un paquete a un destino desconocido, un router también se puede configurar para que utilice una ruta estática predeterminada para crear un gateway de último recurso. El gateway de último recurso se aborda en mayor detalle en el curso de enrutamiento de CCNA.




```
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
     10.0.0.0/8 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
R1#
```

Capítulo 6: Capa de Red 6.2.2.6 Tabla de enrutamiento de router IPv4 de muestra

Suponga que la PC1 con la dirección IP 192.168.10.10 desea enviar un paquete a otro host en la misma red. La PC1 revisaría la tabla de rutas IPv4 según la dirección IP de destino. Luego, la PC1 descubriría que el host está en la misma red y, simplemente, lo enviaría por su interfaz (En enlace).

Nota: el R1 no participa en la transferencia del paquete. Si la PC1 reenvía un paquete a cualquier red que no sea su red local, debe utilizar los servicios del router R1 y reenviar el paquete a su ruta predeterminada local (192.168.10.1).

Los siguientes ejemplos muestran cómo un host y un router toman decisiones de enrutamiento de paquetes consultando sus respectivas tablas de enrutamiento:

Ejemplo 1: la PC1 desea verificar la conectividad a su gateway predeterminado local en 192.168.10.1 (la interfaz del router).

1. La PC1 consulta la tabla de rutas IPv4 sobre la base de la dirección IP de destino.

2. La PC1 descubre que el host está en la misma red y simplemente envía un paquete ping por la interfaz (En enlace).

3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino.

4. El R1 consulta la tabla de enrutamiento.

5. El R1 busca en esa tabla la entrada que coincide con la dirección IP de destino, la entrada L 192.168.10.1/32, y descubre que esta corresponde a su propia interfaz local, como se muestra en la figura 1.

6. El R1 abre el resto del paquete IP y responde en consecuencia.

Ejemplo 2: la PC1 desea enviar un paquete a la PC2 (192.168.11.10).

1. La PC1 consulta la tabla de rutas IPv4 y descubre que no hay una coincidencia exacta.

2. Por lo tanto, la PC1 utiliza la red de todas las rutas (0.0.0.0) y envía el paquete mediante la ruta predeterminada local (192.168.10.1).

3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino (192.168.11.10).

4. El R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada C 192.168.11.0/24, como se muestra en la figura 2.

5. El R1 reenvía el paquete por la interfaz Gigabit Ethernet 0/1 (G0/1) conectada directamente.

6. La PC2 recibe el paquete y consulta la tabla de enrutamiento IPv4 de host.

7. La PC2 descubre que el paquete está dirigido a ella, abre el resto del paquete y responde en consecuencia.

Ejemplo 3: la PC1 desea enviar un paquete a 209.165.200.226.

1. La PC1 consulta la tabla de rutas IPv4 y descubre que no hay una coincidencia exacta.

2. Por lo tanto, la PC1 utiliza la ruta predeterminada (0.0.0.0/0) y envía el paquete mediante el gateway predeterminado (192.168.10.1).

3. El R1 recibe el paquete en su interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino (209.165.200.226).

4. El R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada C 209.165.200.224/30, como se muestra en la figura 3.

5. La R1 reenvía el paquete por la interfaz serial 0/0/0 (S0/0/0) conectada directamente.

Ejemplo 4: la PC1 desea enviar un paquete al host con la dirección IP 10.1.1.10.

1. La PC1 consulta la tabla de rutas IPv4 y descubre que no hay una coincidencia exacta.

2. Por lo tanto, la PC1 utiliza la red de todas las rutas (0.0.0.0) y envía el paquete a su ruta predeterminada local (192.168.10.1).

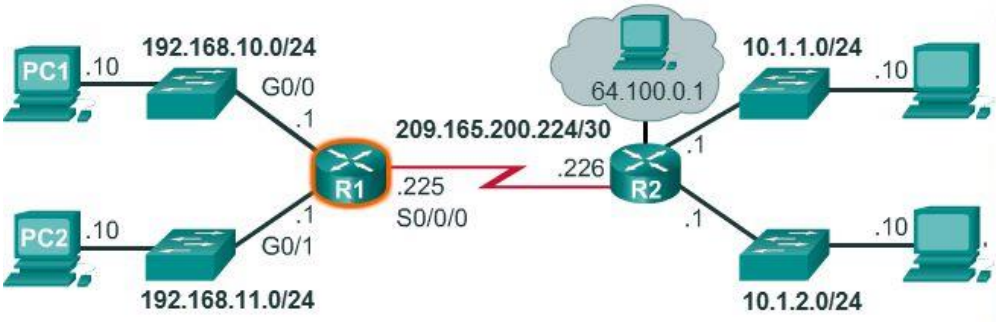
3. El R1 recibe el paquete en la interfaz Gigabit Ethernet 0/0 (G0/0) y examina la dirección IP de destino (10.1.1.10).

4. El R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada D 10.1.1.0/24, como se muestra en la figura 4.

5. El R1 descubre que debe enviar el paquete a la dirección de siguiente salto 209.165.200.226.

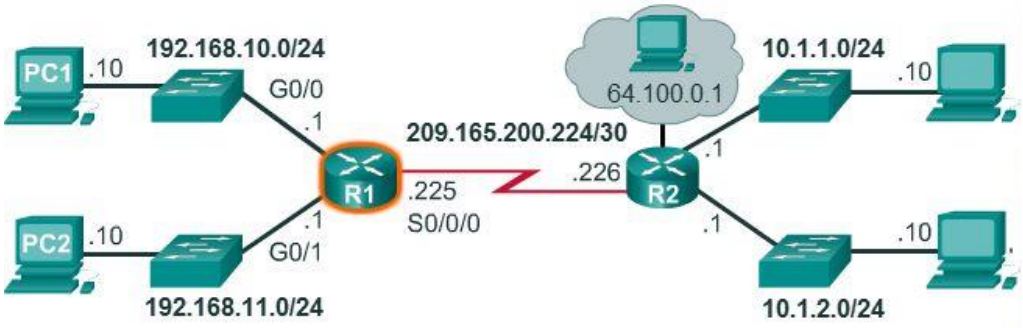
6. Nuevamente, el R1 consulta la tabla de enrutamiento y busca la entrada que coincide con la dirección IP de destino, la entrada C 209.165.200.224/30, como se muestra en la figura 4.

7. La R1 reenvía el paquete por la interfaz serial 0/0/0 (S0/0/0) conectada directamente.



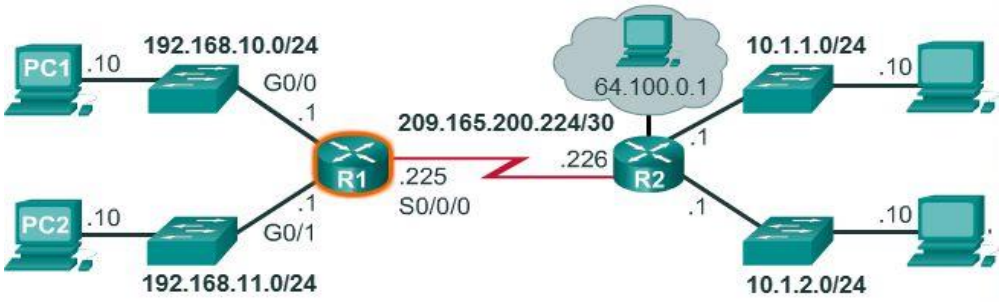

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type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

Gateway of last resort is 209.165.200.226 to network 0.0.0.0
```

```
     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, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        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
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

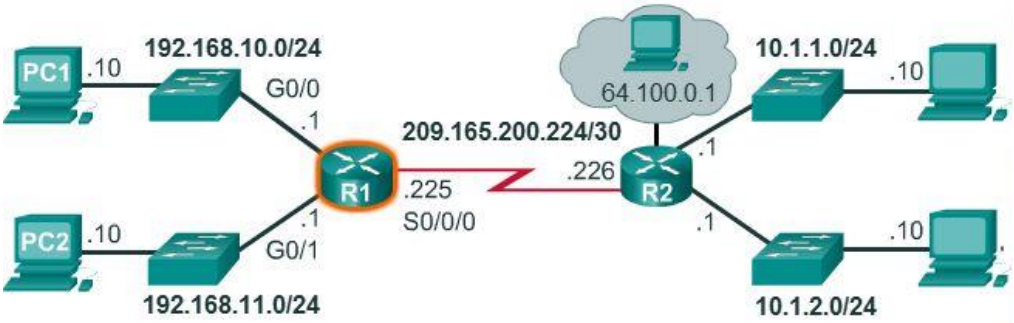



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type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

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     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, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        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
```

```
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
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```




```
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     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, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        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
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```




```
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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
       IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     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, 01:13:55,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 01:13:55,
        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
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

Capítulo 6: Capa de Red 6.3.1.1 Los routers son computadoras

Existen muchos tipos de routers de infraestructura. De hecho, los routers Cisco están diseñados para satisfacer las siguientes necesidades:

- De sucursal: trabajadores a distancia, pequeñas empresas y sucursales medianas. Incluye los routers de servicios integrados (ISR) Cisco 800, 1900, 2900 y 3900 de segunda generación (G2).
- De WAN: grandes empresas y organizaciones. Incluye los switches de la serie Cisco Catalyst 6500 y el router de servicios de agregación (ASR) Cisco 1000.
- De proveedor de servicios: grandes proveedores de servicios. Incluye los routers Cisco ASR 1000, Cisco ASR 9000, Cisco XR 12000, Cisco CRS-3 Carrier Routing System y los de la serie 7600.

La certificación de CCNA se centra en la familia de routers de sucursal. En la ilustración, se muestra la familia de routers ISR G2 Cisco 1900, 2900 y 3900.

Más allá de su función, su tamaño o su complejidad, todos los modelos de routers son, básicamente, computadoras. Al igual que las computadoras, las tablet PC y los dispositivos inteligentes, los routers también requieren lo siguiente:

- Sistemas operativos (OS)
- Unidades centrales de proceso (CPU)
- Memoria de acceso aleatorio (RAM)
- Memoria de solo lectura (ROM)

Los routers también tienen una memoria especial, que incluye memoria flash y memoria de acceso aleatorio no volátil (NVRAM).

Capítulo 6: Capa de Red 6.3.1.2 CPU y OS del router

Al igual que las computadoras, las tablet PC y los dispositivos inteligentes, los dispositivos Cisco requieren una CPU para ejecutar las instrucciones del OS, como la inicialización del sistema y las funciones de enrutamiento y conmutación.

La CPU requiere un OS para ofrecer funciones de enrutamiento y conmutación.

El Sistema operativo Internetwork (IOS, Internetwork Operating System) de Cisco es el software de sistema usado para la mayoría de los dispositivos Cisco, independientemente del tamaño y el tipo de dispositivo. Se usa en routers, switches LAN, pequeños puntos de acceso inalámbrico, grandes routers con decenas de interfaces y muchos otros dispositivos.

El componente destacado en la ilustración es la CPU de un router Cisco 1941 con disipador térmico acoplado.

Capítulo 6: Capa de Red 6.3.1.3 Memoria del router

Los routers tienen acceso a cuatro tipos de memoria: RAM, ROM, NVRAM y flash.

RAM

La RAM se utiliza para almacenar diversas aplicaciones y procesos, incluido lo siguiente:

- Cisco IOS: el IOS se copia en la RAM durante el arranque.
- Archivo de configuración en ejecución: este es el archivo de configuración que almacena los comandos de configuración que el IOS del router utiliza actualmente. También se conoce como “running-config”.
- Tabla de enrutamiento IP: este archivo almacena información sobre las redes conectadas directamente y remotas. Se utiliza para determinar el mejor camino para reenviar paquetes.
- Caché ARP: esta caché contiene la asignación de direcciones IPv4 a direcciones MAC y es similar a la caché de protocolo de resolución de direcciones (ARP) de una PC. La caché ARP se utiliza en routers que tienen interfaces LAN, como interfaces Ethernet.
- Búfer de paquetes: los paquetes se almacenan temporalmente en un búfer cuando se reciben en una interfaz o antes de salir por una.

Al igual que las PC, los routers Cisco utilizan memoria de acceso aleatorio dinámica (DRAM). La DRAM es un tipo muy común de RAM que almacena las instrucciones y los datos necesarios para su ejecución por parte de la CPU. A diferencia de la ROM, la memoria RAM es volátil y requiere alimentación constante para mantener la información. Pierde todo el contenido cuando se apaga o se reinicia el router.

De manera predeterminada, los routers 1941 vienen con 512 MB de DRAM soldada en la placa de sistema principal (incorporada) y una ranura para módulo de memoria en línea doble (DIMM) para realizar actualizaciones de memoria de hasta 2,0 GB adicionales. Los modelos Cisco 2901, 2911 y 2921 vienen con 512 MB de DRAM incorporada. Observe que la primera generación de ISR y los routers Cisco más antiguos no tienen RAM incorporada.

ROM

Los routers Cisco usan la memoria ROM para almacenar lo siguiente:

- Instrucciones de arranque: proporcionan las instrucciones de inicio.
- Software de diagnóstico básico: realiza el autodiagnóstico al encender (POST) de todos los componentes.
- IOS limitado: proporciona una versión limitada de respaldo del OS, en caso de que el router no pueda cargar el IOS con todas las funciones.

La ROM consiste en un firmware incorporado en un circuito integrado en el router y no pierde el contenido cuando el router se reinicia o se apaga.

NVRAM

El Cisco IOS usa la NVRAM como almacenamiento permanente para el archivo de configuración de inicio (startup-config). Al igual que la ROM, la NVRAM no pierde el contenido cuando se apaga el dispositivo.

Memoria Flash

La memoria flash es memoria de PC no volátil que se utiliza como 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.

Los routers Cisco 1941 vienen con dos ranuras externas para memoria Compact Flash. En cada ranura, la densidad de almacenamiento de alta velocidad puede alcanzar los 4 GB.

En la ilustración, se resumen los cuatro tipos de memoria.

Memoria	Volátil/no volátil	Almacena
RAM	Volátil	• IOS en ejecución • Archivo de configuración en ejecución • Enrutamiento de IP y tablas ARP • Buffer de paquetes
ROM	No volátil	• Instrucciones de arranque • Software básico de diagnóstico • IOS limitado
NVRAM	No volátil	• Archivo de configuración de inicio
Flash	No volátil	• IOS (Sistema operativo de internetworking) • Otros archivos de sistema

Capítulo 6: Capa de Red 6.3.1.4 Interior de un router

Aunque existen diferentes tipos y modelos de routers, todos tienen los mismos componentes generales de hardware.

En la ilustración, se muestra el interior de un ISR Cisco 1841 de primera generación. Haga clic en los componentes para ver una breve descripción.

Observe que en la ilustración también se destacan otros componentes que se encuentran en un router, como la fuente de energía, el ventilador de refrigeración, los protectores térmicos y un módulo de integración avanzada (AIM), los cuales exceden el ámbito de este capítulo.

Nota: los profesionales de red deben conocer y comprender la función de los principales componentes internos de un router más que la ubicación exacta de dichos componentes en un router específico. Según el modelo, esos componentes se encuentran en diferentes lugares dentro del router.

Capítulo 6: Capa de Red 6.3.1.5 Backplane del router

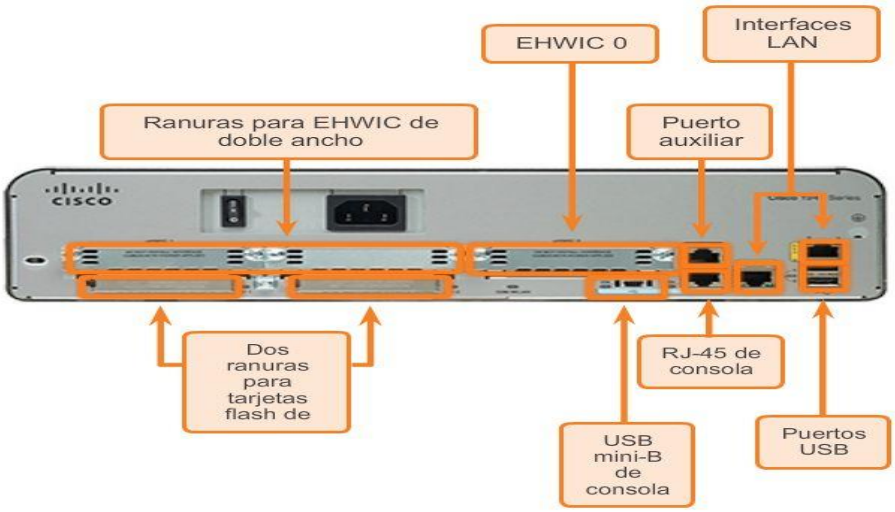
Los routers Cisco 1941 incluyen las siguientes conexiones:

- Puertos de consola: dos puertos de consola para acceder a la administración de la configuración inicial y de la interfaz de línea de comandos (CLI) mediante un puerto RJ-45 común y un nuevo conector USB de tipo B (USB mini-B).
- Puerto auxiliar: un puerto RJ-45 para el acceso a la administración remota; es similar al puerto de consola.
- Dos interfaces LAN: dos interfaces Gigabit Ethernet para obtener acceso a LAN.
- Ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas (EHWIC): dos ranuras que proporcionan modularidad y flexibilidad al permitir que el router admita distintos tipos de módulos de interfaz, incluidos serial, línea de suscriptor digital (DSL), puerto de switch y tecnología inalámbrica.

El ISR Cisco 1941 también tiene ranuras de almacenamiento para admitir capacidades expandidas. Las ranuras para memoria Compact Flash doble admiten tarjetas Compact Flash de 4 GB cada una para aumentar el espacio de almacenamiento. Se incluyen dos puertos de host USB para obtener espacio de almacenamiento adicional y proteger la capacidad de token.

La memoria Compact Flash puede almacenar la imagen del software Cisco IOS, archivos de registro, archivos de configuración de voz, archivos HTML, configuraciones de respaldo o cualquier otro archivo necesario para el sistema. De manera predeterminada, solo la ranura 0 está ocupada con una tarjeta Compact Flash de fábrica y es la ubicación de arranque predeterminada.

En la ilustración, se identifica la ubicación de estas conexiones y ranuras.



Capítulo 6: Capa de Red 6.3.1.6 Conexión al router

Por lo general, los dispositivos, routers y switches Cisco interconectan numerosos dispositivos. Por esta razón, estos dispositivos tienen varios tipos de puertos e interfaces. Estos puertos e interfaces se utilizan para conectar cables al dispositivo.

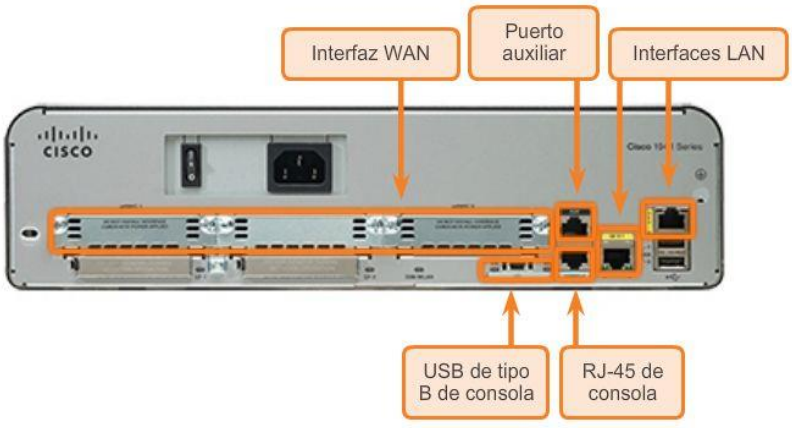
Las conexiones de un router Cisco se pueden agrupar en dos categorías:

- Puertos de administración: estos son los puertos de consola y los puertos auxiliares utilizados para configurar y administrar el router, así como para resolver problemas del dispositivo. A diferencia de las interfaces LAN y WAN, los puertos de administración no se utilizan para el reenvío de paquetes.

- Interfaces del router en banda: estas son las interfaces LAN y WAN configuradas con direccionamiento IP para transportar el tráfico de los usuarios. Las interfaces Ethernet son las conexiones LAN más frecuentes, mientras que las conexiones WAN comunes incluyen las interfaces seriales y DSL.

En la ilustración, se destacan los puertos y las interfaces de un router ISR Cisco 1941 G2.

Al igual que muchos dispositivos de red, los dispositivos Cisco utilizan indicadores de diodos emisores de luz (LED) para proporcionar información de estado. Un LED de interfaz indica la actividad de la interfaz correspondiente. Si un LED está apagado cuando la interfaz está activa y la interfaz está conectada correctamente, puede ser señal de un problema en la interfaz. Si la interfaz está extremadamente ocupada, el LED permanece encendido.



Capítulo 6: Capa de Red 6.3.1.7 Interfaces LAN y WAN

En forma similar a lo que sucede con los switches Cisco, existen varias maneras de acceder al entorno de la CLI de un router Cisco. Los métodos más comunes son los siguientes:

- Consola: utiliza conexiones seriales de baja velocidad o USB para proporcionar acceso de administración fuera de banda con conexión directa a un dispositivo Cisco.
- Telnet o SSH: dos métodos para acceder de forma remota a una sesión de CLI a través de una interfaz de red activa.
- Puerto auxiliar: se utiliza para la administración remota del router mediante una línea telefónica de dial-up y un módem.

El puerto de consola y el auxiliar están ubicados en el router.

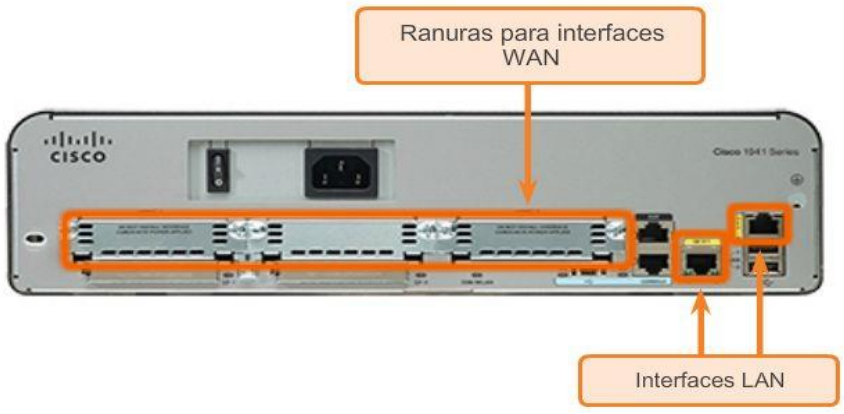
Además de estos puertos, los routers también tienen interfaces de red para recibir y reenviar paquetes IP. Los routers tienen muchas interfaces que se usan para conectarse a múltiples redes. En general, las interfaces se conectan a distintos tipos de redes, lo que significa que se requieren distintos tipos de medios y de conectores.

Cada interfaz en el router es miembro o host de otra red IP. Cada interfaz se debe configurar con una dirección IP y una máscara de subred de una red diferente. Cisco IOS no permite que dos interfaces activas en el mismo router pertenezcan a la misma red.

Las interfaces del router se pueden agrupar en dos categorías:

- Interfaces LAN Ethernet: se utilizan para conectar cables que terminan en dispositivos LAN, como PC y switches. La interfaz también puede utilizarse para conectar routers entre sí. Existen varias convenciones de nomenclatura de uso frecuente para las interfaces Ethernet: Ethernet antigua, FastEthernet y Gigabit Ethernet. El nombre utilizado depende del tipo y el modelo de dispositivo.
- Interfaces WAN seriales: se utilizan para conectar routers a redes externas, generalmente a una distancia geográfica más extensa. Al igual que las interfaces LAN, cada interfaz WAN serial tiene su propia dirección IP y su máscara de subred, que la identifican como miembro de una red específica.

En la ilustración, se muestran las interfaces LAN y seriales del router.



Capítulo 6: Capa de Red 6.3.2.1 Cisco IOS

Los detalles operativos de Cisco IOS varían de acuerdo con los diferentes dispositivos de internetworking, según el propósito y el conjunto de características del dispositivo. No obstante, Cisco IOS para routers proporciona lo siguiente:

- Direccionamiento
- Interfaces
- Enrutamiento
- Seguridad
- QoS
- Administración de recursos

El archivo de IOS propiamente dicho tiene varios megabytes y, al igual que en los switches Cisco IOS, se almacena en la memoria flash. El uso de la memoria flash permite actualizar el IOS a versiones más recientes o agregarle nuevas características. Durante el arranque, el IOS se copia de la memoria flash a la RAM. La DRAM es mucho más rápida que la memoria flash, por lo que copiar el IOS en la RAM aumenta el rendimiento del dispositivo.

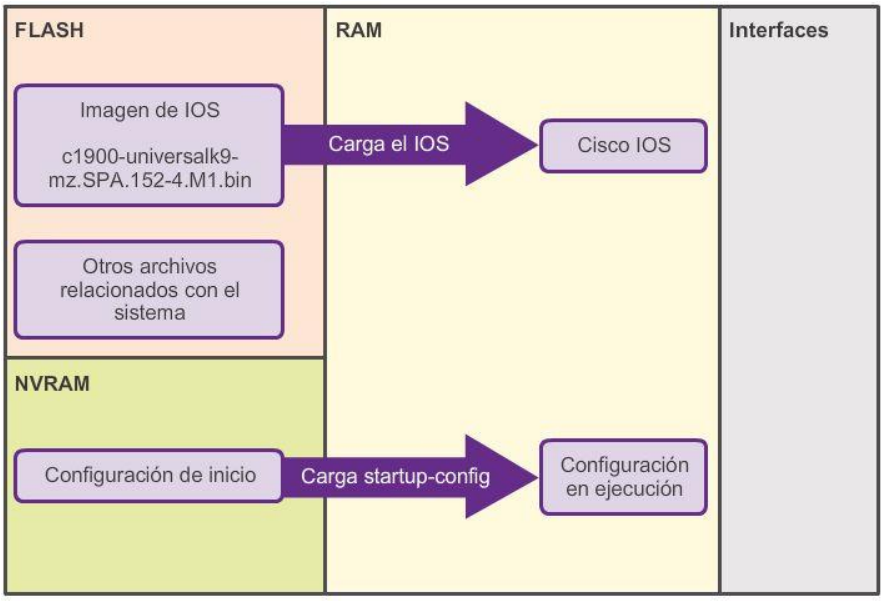
Capítulo 6: Capa de Red 6.3.2.2 Archivos Bootset

Como se muestra en la ilustración, un router carga los siguientes dos archivos en la RAM durante el inicio:

- Archivo de imagen de IOS: el IOS facilita el funcionamiento básico de los componentes de hardware del dispositivo. El archivo de imagen de IOS se almacena en la memoria flash.

- Archivo de configuración de inicio: el archivo de configuración de inicio incluye los comandos que se utilizan para realizar la configuración inicial de un router y crear el archivo de configuración en ejecución almacenado en la RAM. El archivo de configuración de inicio se almacena en NVRAM. Todos los cambios de configuración se almacenan en el archivo de configuración en ejecución, y el IOS los implementa de inmediato.

La configuración en ejecución se modifica cuando el administrador de red realiza la configuración del dispositivo. Cuando se realizan cambios al archivo running-config, este se debe guardar en la NVRAM como archivo de configuración de inicio, en caso de que el router se reinicie o se apague.



Capítulo 6: Capa de Red 6.3.2.3 Proceso de arranque del router

El proceso de arranque que se muestra en la figura 1 consta de tres fases principales:

1. Llevar a cabo el POST y cargar el programa bootstrap.

2. Localizar y cargar el software Cisco IOS.

3. Localizar y cargar el archivo de configuración de inicio o ingresar al modo Setup.

1. Llevar a cabo el POST y cargar el programa bootstrap (figura 2)

La prueba de Autodiagnóstico al encender (POST, Power-On Self Test) es un proceso común que ocurre en casi todas las computadoras durante el arranque. El proceso de POST se utiliza para probar el hardware del router. Cuando se enciende el router, el software en el chip de la ROM ejecuta el POST. Durante este autodiagnóstico, el router ejecuta desde la ROM diagnósticos de varios componentes de hardware, incluidos la CPU, la RAM y la NVRAM. Una vez finalizado el POST, el router ejecuta el programa bootstrap.

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

Nota: en este momento, si existe una conexión de consola al router, comienzan a aparecer resultados en pantalla.

2. Localizar y cargar Cisco IOS (figura 3)

Por lo general, el IOS se almacena en la memoria flash y se copia en la RAM para que lo ejecute la CPU. Durante la autodescompresión del archivo de imagen de IOS, se muestra una cadena de símbolos de almohadilla (#).

Si la imagen de IOS no se encuentra en la memoria flash, el router puede buscarla con un servidor TFTP. Si no se puede localizar una imagen de IOS completa, se copia una versión reducida del IOS de la ROM a la

RAM. Esta versión del IOS se usa para ayudar a diagnosticar cualquier problema y puede usarse para cargar una versión completa del IOS en la RAM.

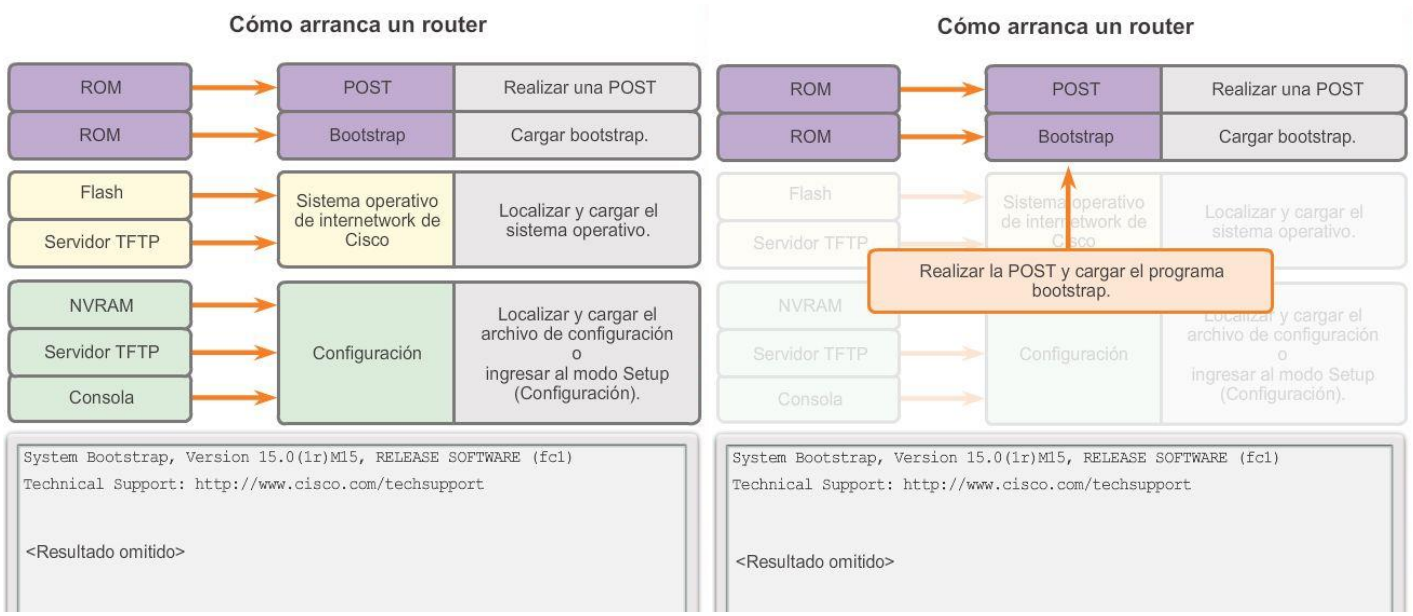
3. Localizar y cargar el archivo de configuración (figura 4)

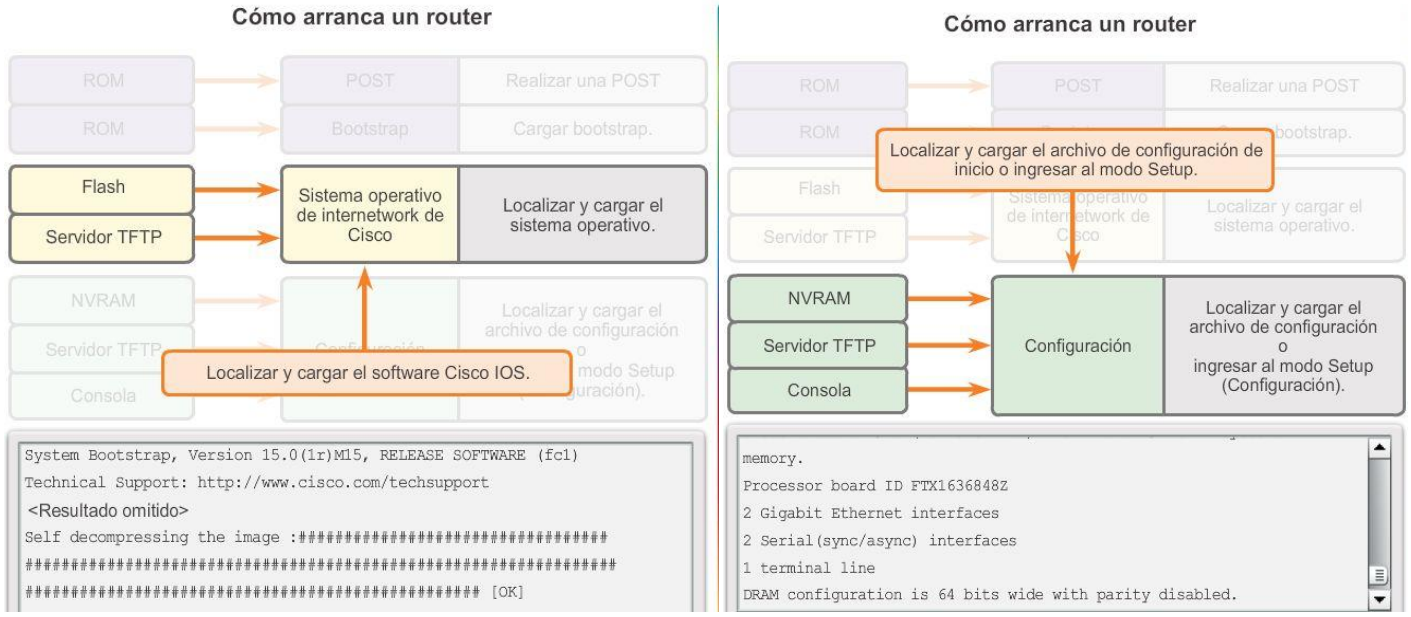
A continuación, el programa bootstrap busca el archivo de configuración de inicio (también conocido como “startup-config”) en la NVRAM. El archivo contiene los parámetros y comandos de configuración guardados anteriormente. Si existe, se copia en la RAM como archivo de configuración en ejecución o “running-config”. El archivo running-config contiene direcciones de interfaz, inicia los procesos de enrutamiento, configura las contraseñas del router y define otras características del dispositivo.

Si el archivo startup-config no existe en la NVRAM, el router puede buscar un servidor de protocolo trivial de transferencia de archivos (TFTP). Si el router detecta que tiene un enlace activo a otro router configurado, envía un broadcast en busca de un archivo de configuración a través del enlace activo.

Si no se encuentra un servidor TFTP, el router muestra la petición de entrada del modo Setup. El modo Setup consiste en una serie de preguntas que solicitan al usuario información de configuración básica. El modo Setup no tiene como fin utilizarse para ingresar a configuraciones complejas del router y los administradores de red normalmente no lo usan.

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





Capítulo 6: Capa de Red 6.3.2.4 Resultado de show versión

El comando show version se puede utilizar para revisar y resolver problemas de algunos de los componentes básicos de hardware y software del router. Este comando muestra información sobre la versión del software Cisco IOS que se encuentra en ejecución en el router, la versión del programa bootstrap y datos sobre la configuración de hardware, incluida la cantidad de memoria del sistema.

El resultado del comando show version incluye lo siguiente:

- Versión de IOS: la versión del software Cisco IOS que se encuentra en la RAM y que utiliza el router.
- Programa bootstrap en la ROM: muestra la versión del software bootstrap del sistema almacenado en la ROM que se utilizó inicialmente para arrancar el router.
- Ubicación del IOS: muestra dónde se encuentra el programa boostrap y dónde cargó el Cisco IOS, además del nombre de archivo completo de la imagen de IOS.
- CPU y cantidad de RAM: en la primera parte de esta línea, se muestra el tipo de CPU del router en cuestión. La última parte de esta línea muestra la cantidad de DRAM. Algunas series de routers, como el ISR Cisco 1941, utilizan una parte de la DRAM como memoria de paquetes. La memoria de paquetes se usa para paquetes de almacenamiento intermedio. Para determinar la cantidad total de DRAM en el router, se deben sumar ambos números.
- Interfaces: muestra las interfaces físicas del router. En este ejemplo, el ISR Cisco 1941 tiene dos interfaces Gigabit Ethernet y dos interfaces seriales de baja velocidad.
- Cantidad de memoria NVRAM y flash: esta es la cantidad de memoria NVRAM y flash del router. La memoria NVRAM se utiliza para almacenar el archivo startup-config, y la memoria flash se utiliza para almacenar Cisco IOS de forma permanente.

En la última línea del comando show version, se muestra el valor configurado actualmente del registro de configuración del software en sistema hexadecimal. Si se muestra un segundo valor entre paréntesis, indica el valor del registro de configuración que se utilizará durante la siguiente recarga.

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

```
Router#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M),
Version 15.2(4)M1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 19:34 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15,
RELEASE SOFTWARE (fc1)

Router uptime is 10 hours, 9 minutes
System returned to ROM by power-on
System image file is
"flash0:c1900-universalk9-mz.SPA.152-4.M1.bin"
Last reload type: Normal Reload
Last reload reason: power-on

<Resultado omitido>
```

Capítulo 6: Capa de Red 6.4.1.1 Pasos de configuración del 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 durante su implementación en una red son idénticos para ambos dispositivos.

De modo similar a lo que sucede al configurar un switch, se deben completar los siguientes pasos al configurar los parámetros iniciales de un router:

1. Asignar un nombre de dispositivo mediante el comando de configuración global hostname (figura 1).

2. Establecer contraseñas. (Figura 2).

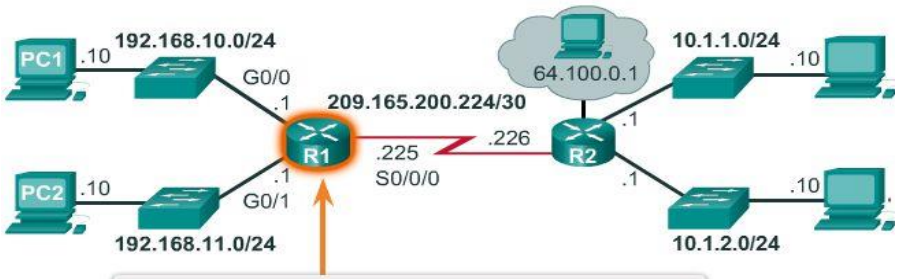
- Proteger el acceso al modo EXEC privilegiado mediante el comando enable secret.
- Proteger el acceso al modo EXEC con el comandologin en el puerto de consola, y el comandopassword para establecer la contraseña.
- Proteger el acceso virtual. Esto se realiza de forma similar a la protección del acceso al modo EXEC, excepto que se lleva a cabo en el puerto de teletipo virtual (VTY).
- Utilizar el comando de configuración globalservice password-encryption para evitar que las contraseñas se muestren como texto no cifrado en el archivo de configuración.

3. Proporcionar notificaciones legales mediante el comando de configuración global de mensaje del día (MOTD) banner motd (figura 3).

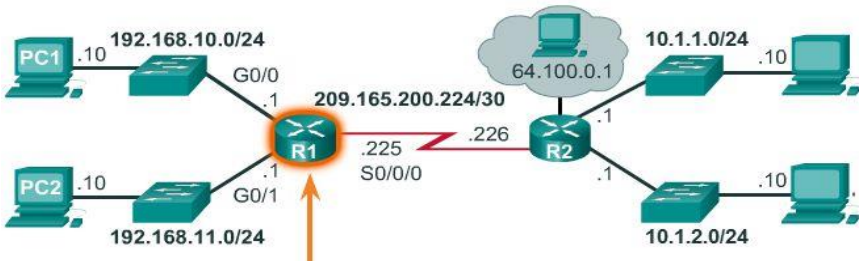
4. Guardar la configuración mediante el comando copy run start (figura 4).

5. Verificar la configuración mediante el comando show run.

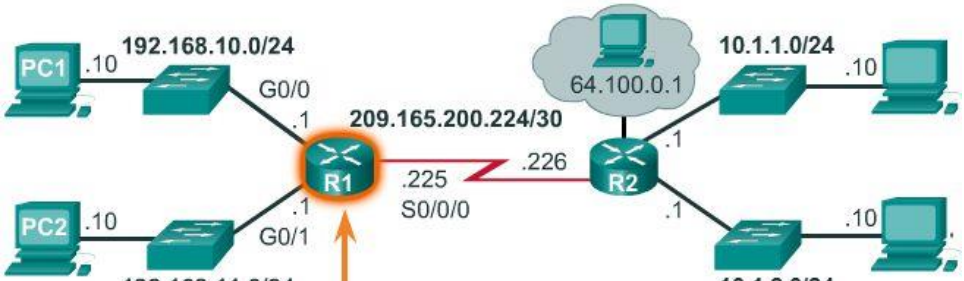
En la figura 5, se proporciona un verificador de sintaxis que le permite practicar estos pasos de configuración.



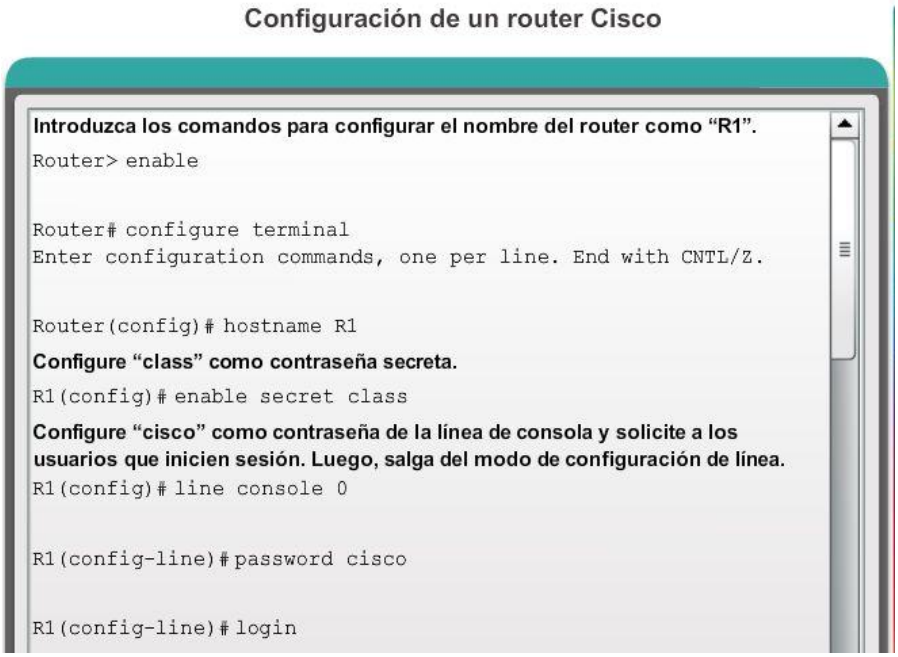

```
R1(config)#enable secret class
R1(config)#
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
R1(config)#service password-encryption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

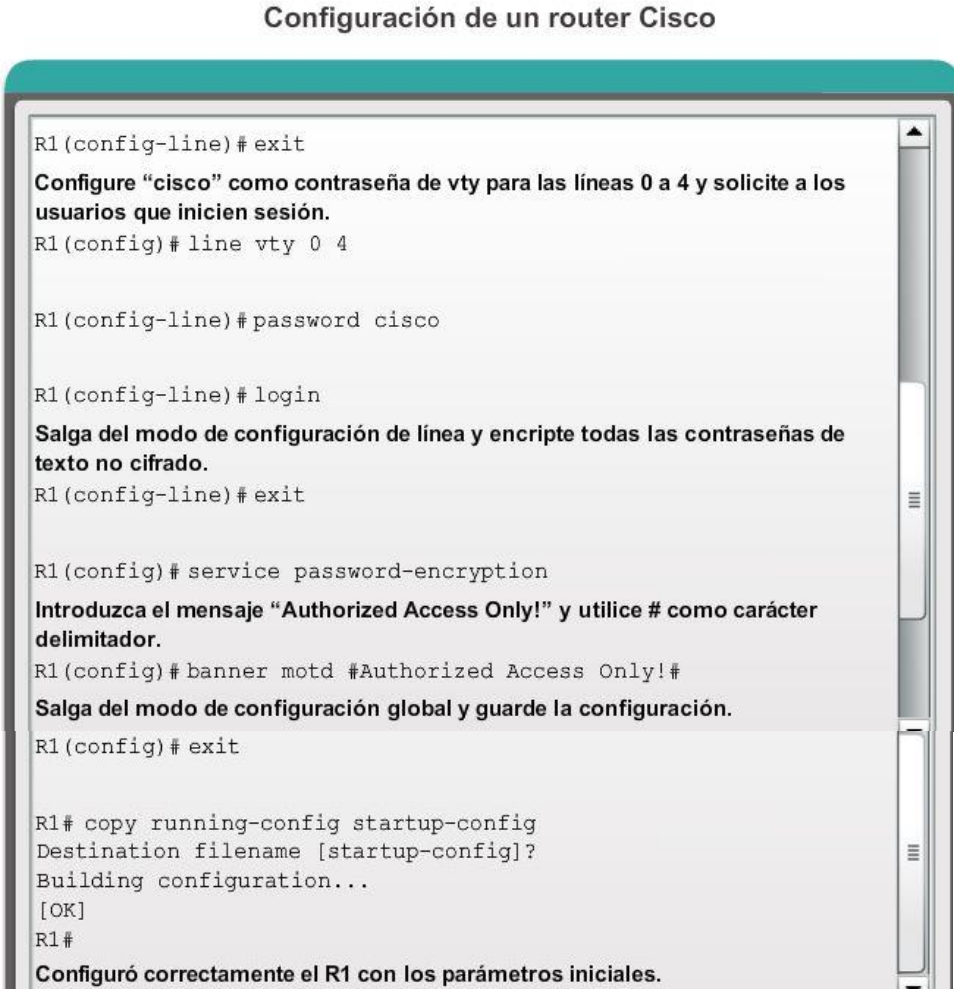



```
R1(config)#banner motd #
Enter TEXT message.  End with the character '#'.

**********************************************
      WARNING: Unauthorized access is
prohibited!

**********************************************
#

R1(config)#
```




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





Capítulo 6: Capa de Red 6.4.2.1 Configure las interfaces de LAN.

Para que los routers sean accesibles, se deben configurar sus interfaces. Por lo tanto, para habilitar una interfaz específica, ingrese al modo de configuración de interfaz con el comando del modo de configuración global interface *tipo-y-número*.

Existen varios tipos de interfaces diferentes disponibles en los routers Cisco. En este ejemplo, el router Cisco 1941 cuenta con dos interfaces Gigabit Ethernet y una tarjeta de interfaz WAN (WIC) serial que consta de dos interfaces. Las interfaces se denominan de la siguiente manera:

- Gigabit Ethernet 0/0 (G0/0)
- Gigabit Ethernet 0/1 (G0/1)
- Serial 0/0/0 (S0/0/0)
- Serial 0/0/1 (S0/0/1)

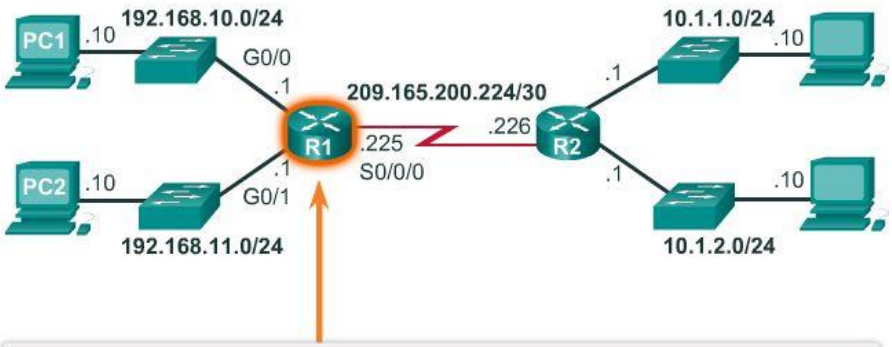
Para habilitar una interfaz del router, configure lo siguiente:

- Dirección IPv4 y máscara de subred: configura la dirección IP y la máscara de subred mediante el comando del modo de configuración de interfaz ip address *dirección máscara-de-subred*.
- Active la interfaz: de manera predeterminada, las interfaces LAN y WAN no están activadas. La interfaz se debe activar mediante el comando no shutdown. Es como encender 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.

Si bien no es necesario, es aconsejable configurar una descripción en cada interfaz para ayudar a registrar la información de la red. 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 suministra información con respecto al tipo de red a la que está conectada la interfaz y si hay otros routers en esa red. Si la interfaz se conecta a un ISP o un proveedor de servicios de telefonía móvil, resulta útil introducir la información de contacto y de conexión de dichos terceros.

En la figura 1, se muestra la configuración de las interfaces LAN conectadas al R1. En la figura 2, practique la configuración de una interfaz LAN.

Nota: para la configuración de Gigabit Ethernet 0/1 se utilizan abreviaturas de comandos.




```
R1#conf t
Enter configuration commands, one per line.
End with CNTL/Z.
R1(config)#
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#description Link to LAN-10
R1(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface GigabitEthernet0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0,changed state to up
R1(config-if)#exit
R1(config)#
R1(config)#int g0/1
R1(config-if)#ip add 192.168.11.1 255.255.255.0
R1(config-if)#des Link to LAN-11
R1(config-if)#no shut
%LINK-5-CHANGED: Interface GigabitEthernet0/1,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)#exit
R1(config)#
```

Capítulo 6: Capa de Red 6.4.2.2 Verificación de configuración de interfaz

Existen varios comandos que se pueden utilizar para verificar la configuración de interfaz. El más útil de ellos esshow ip interface brief. En el resultado generado, se muestran todas las interfaces, sus direcciones IP y su estado actual. Las interfaces configuradas y conectadas deben mostrar el valor "up" (conectado) en Status (Estado) y en Protocol (Protocolo). Cualquier otro valor indicaría un problema con la configuración o el cableado.

Puede verificar la conectividad desde la interfaz mediante el comando ping. Los routers Cisco envían cinco pings consecutivos y miden los tiempos de ida y vuelta mínimos, medios y máximos. Los signos de exclamación verifican la conectividad.

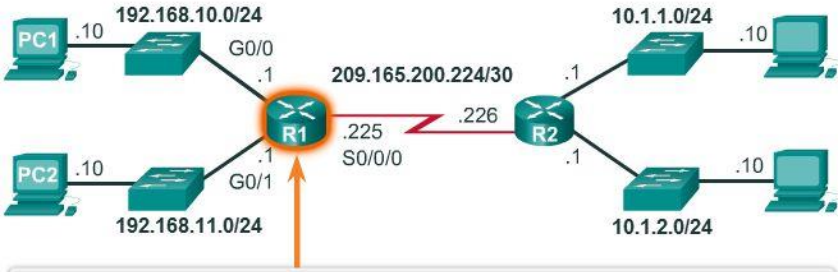
En la figura 1, se muestran los resultados del comandoshow ip interface brief, que revelan que las interfaces LAN y el enlace WAN están activos y operativos. Observe que el comando ping generó cinco signos de exclamación que verifican la conectividad al R2.

Otros comandos de verificación de interfaz incluyen los siguientes:

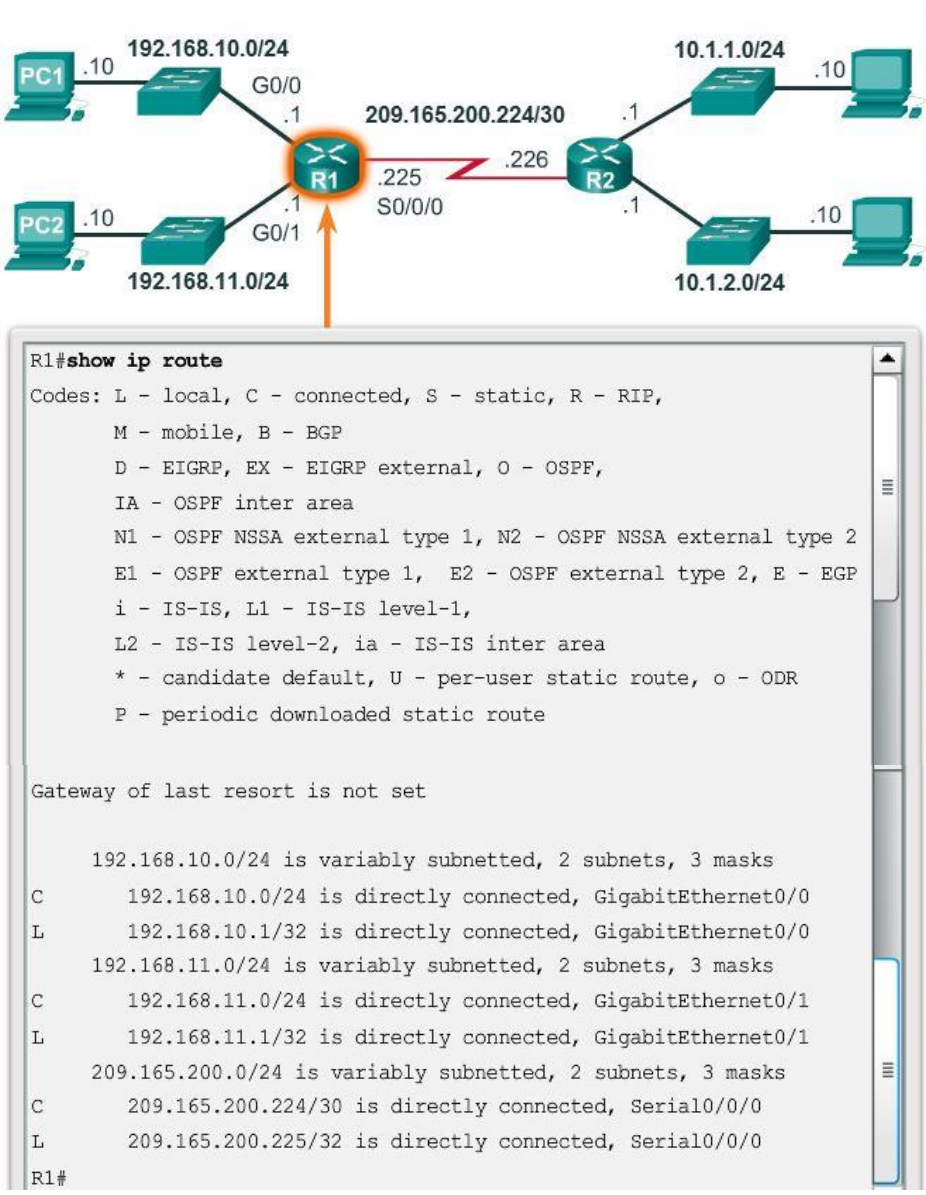
- show ip route : muestra el contenido de la tabla de enrutamiento IPv4 almacenada en la RAM.
- show interfaces - muestra estadísticas de todas las interfaces del dispositivo.
- show ip interface : muestra las estadísticas de IPv4 de todas las interfaces de un router.

En la figura 2, se muestra el resultado del comando show ip route. Observe las tres entradas de redes conectadas directamente y las entradas de las interfaces de enlace local.

Recuerde guardar la configuración mediante el comandocopy running-config startup-config.




```
R1#show ip interface brief
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
Serial0/0/1            unassigned      YES  NVRAM  administratively do
Vlan1                  unassigned      YES  NVRAM  administratively do
R1#
R1#ping 209.165.200.226
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 1/2/9 ms
R1#
```



Capítulo 6: Capa de Red 6.4.3.1 Gateway predeterminado en un host

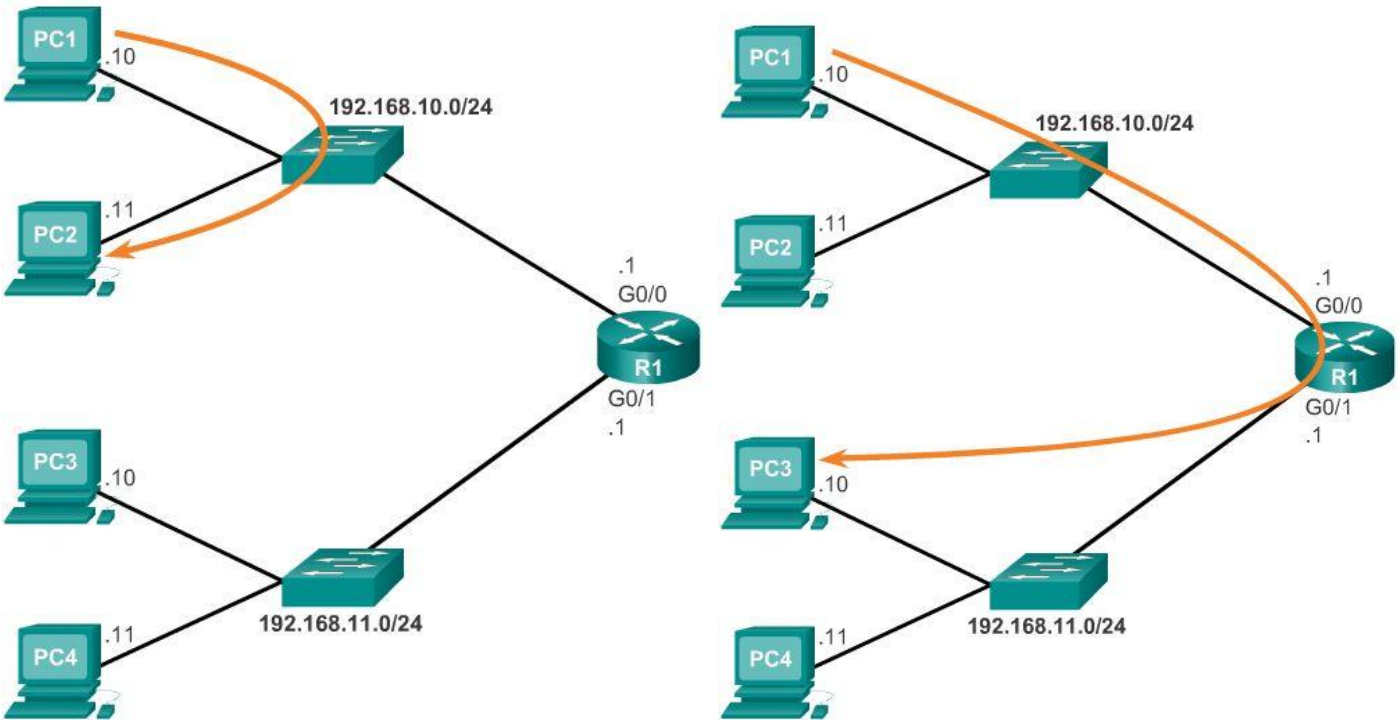
La mayoría de los routers tiene, como mínimo, dos interfaces. Cada interfaz se configura con una dirección IP distinta en una red diferente.

Para que un dispositivo final se comunique a través de la red, se debe configurar con la información de dirección IP correcta, incluida la dirección de gateway predeterminado. El gateway predeterminado se utiliza solo cuando el host desea enviar un paquete a un dispositivo en otra red. Por lo general, la dirección de gateway predeterminado es la dirección de la interfaz del router asociada a la red local del host. Si bien no importa qué dirección se configura realmente en la interfaz del router, la dirección IP del dispositivo host y la dirección de la interfaz del router deben estar en la misma red.

En las ilustraciones, se muestra la topología de un router con dos interfaces independientes. Cada interfaz está conectada a una red diferente. G0/0 está conectada a la red 192.168.10.0, mientras que G0/1 está conectada a la red 192.168.11.0. Cada dispositivo host está configurado con la dirección de gateway predeterminado correspondiente.

En la figura 1, la PC1 envía un paquete a la PC2. En este ejemplo, el gateway predeterminado no se utiliza; en cambio, la PC1 dirige el paquete con la dirección IP de la PC2 y reenvía el paquete directamente a dicha PC a través del switch.

En la figura 2, la PC1 envía un paquete a la PC3. En este ejemplo, la PC1 dirige el paquete con la dirección IP de la PC3, pero luego lo reenvía al router. El router acepta el paquete, accede a la tabla de rutas para determinar la interfaz de salida adecuada según la dirección de destino y reenvía el paquete por la interfaz apropiada para llegar a la PC3.



Capítulo 6: Capa de Red 6.4.3.2 Gateway predeterminado en un switch

Todos los dispositivos que requieren el uso de un router utilizan un gateway predeterminado para precisar el mejor camino hacia un destino remoto. Los dispositivos finales requieren direcciones de gateway predeterminado, pero también las requieren los dispositivos intermediarios, como los switches Cisco IOS.

La información de dirección IP en un switch solo se necesita para administrar el switch de forma remota. Es decir, para acceder al switch mediante Telnet, este debe tener una dirección IP a la cual se pueda acceder mediante dicho sistema. Si se accede al switch solamente desde dispositivos dentro de la red local, solo se requiere una dirección IP.

La configuración de la dirección IP en un switch se realiza en la interfaz virtual de switch (SVI):

S1(config)# interface vlan1

S1(config-vlan)# ip address 192.168.10.50 255.255.255.0

S1(config-vlan)# no shut

Sin embargo, si dispositivos de otra red deben acceder al switch, este se debe configurar con una dirección de gateway predeterminado, ya que los paquetes que se originan en el switch se manejan como los paquetes

que se originan en un dispositivo host. Por lo tanto, los paquetes que se originan en el switch y están destinados a un dispositivo en la misma red se reenvían directamente al dispositivo apropiado.

Los paquetes que se originan en el switch y están destinados a un dispositivo en una red remota se deben reenviar al gateway predeterminado para precisar la ruta.

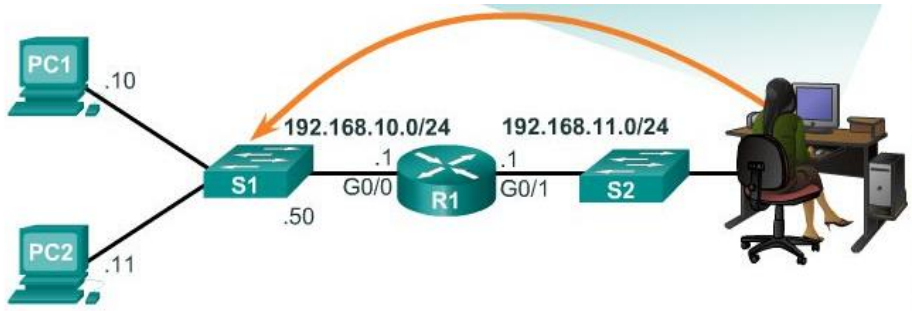
Para configurar un gateway predeterminado en un switch, utilice el siguiente comando de configuración global:

S1(config)# ip default-gateway 192.168.10.1

En la figura 1, se muestra un administrador que se conecta a un switch en una red remota. Para que el switch reenvíe los paquetes de respuesta al administrador, se debe configurar el gateway predeterminado.

Un concepto erróneo frecuente es que el switch utiliza la dirección de gateway predeterminado configurada para determinar adónde reenviar los paquetes que se originan en los hosts conectados al switch y que están destinados a los hosts en una red remota. En realidad, la información de dirección IP y de gateway predeterminado solo se utiliza para los paquetes que se originan en el switch. Los paquetes que se originan en los hosts conectados al switch ya deben tener configurada la información de gateway predeterminado para comunicarse en redes remotas. En la figura 2, practique la configuración de un gateway predeterminado en un switch.

```
S1#show running-config
Building configuration...
!
<resultado omitido>
service password-encryption
!
hostname S1
!
Interface Vlan1
ip address 192.168.10.50
!
ip default-gateway 192.168.10.1
<resultado omitido>
```



Si no se configurara el gateway predeterminado en el S1, los paquetes de respuesta del S1 no podrían llegar al administrador en 192.168.11.10. El administrador no podría administrar el dispositivo de manera remota.

Configuración de un gateway predeterminado en un switch

Ingrese al modo de configuración global y configure 192.168.10.1 como gateway predeterminado para el S1.

```
S1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

S1(config)# ip default-gateway 192.168.10.1
S1(config)#
```

Configuró correctamente el gateway predeterminado en el S1.

Capítulo 6: Capa de Red 6.5.1.1 Actividad de clase: ¿Puede leer este mapa?

¿Puede leer este mapa?

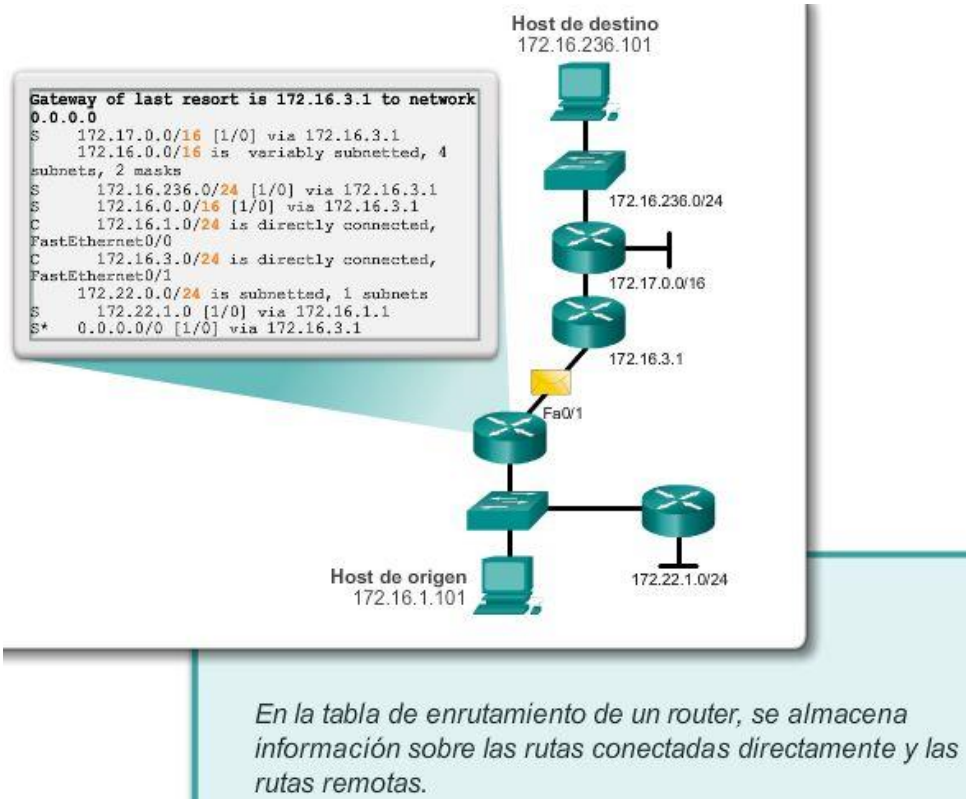
Nota: se sugiere que los estudiantes trabajan de a dos; no obstante, si así lo prefieren, pueden completar esta actividad en forma individual.

El instructor le proporcionará los resultados generados por el comando show ip route de un router. Utilice Packet Tracer para armar un modelo de topología con esta información de enrutamiento.

Como mínimo, en el modelo de topología se deben utilizar los componentes siguientes:

- 1 switch Catalyst 2960
- 1 router serie 1941 de Cisco con una tarjeta modular de puerto de conmutación HWIC-4ESW y IOS versión 15.1 o superior
- 3 PC (pueden ser servidores, PC genéricas, computadoras portátiles, etcétera).

Utilice la herramienta de notas de Packet Tracer para indicar las direcciones de las interfaces del router y las posibles direcciones para los dispositivos finales que eligió para el modelo. Rotule todos los dispositivos finales, los puertos y las direcciones que se establecieron a partir de la información de la tabla de enrutamiento y el resultado del comando show ip route en el archivo de Packet Tracer. Haga una copia impresa del trabajo o guarde una copia del archivo para compartirlo con la clase.



Capítulo 6: Capa de Red 6.5.1.3 Resumen

La capa de red, o la capa 3 de OSI, proporciona servicios que permiten que los dispositivos finales intercambien datos a través de la red. Para lograr este transporte de extremo a extremo, la capa de red utiliza cuatro procesos básicos: el direccionamiento IP para dispositivos finales, la encapsulación, el enrutamiento y la desencapsulación.

Internet se basa en gran medida en IPv4, que continua siendo el protocolo de capa de red que más se utiliza. Un paquete IPV4 contiene el encabezado IP y el contenido. Sin embargo, IPv4 dispone de una cantidad limitada de direcciones IP públicas exclusivas. Esto condujo al desarrollo de IP versión 6 (IPv6). El encabezado de IPv6 simplificado ofrece varias ventajas respecto de IPv4, como una mayor eficacia de enrutamiento, encabezados de extensión simplificados y capacidad de proceso por flujo. Además, las direcciones IPv6 se basan en un direccionamiento jerárquico de 128 bits, mientras que en IPv4 es de 32 bits. El número de direcciones IP disponibles aumenta drásticamente.

Además del direccionamiento jerárquico, la capa de red también es responsable del enrutamiento.

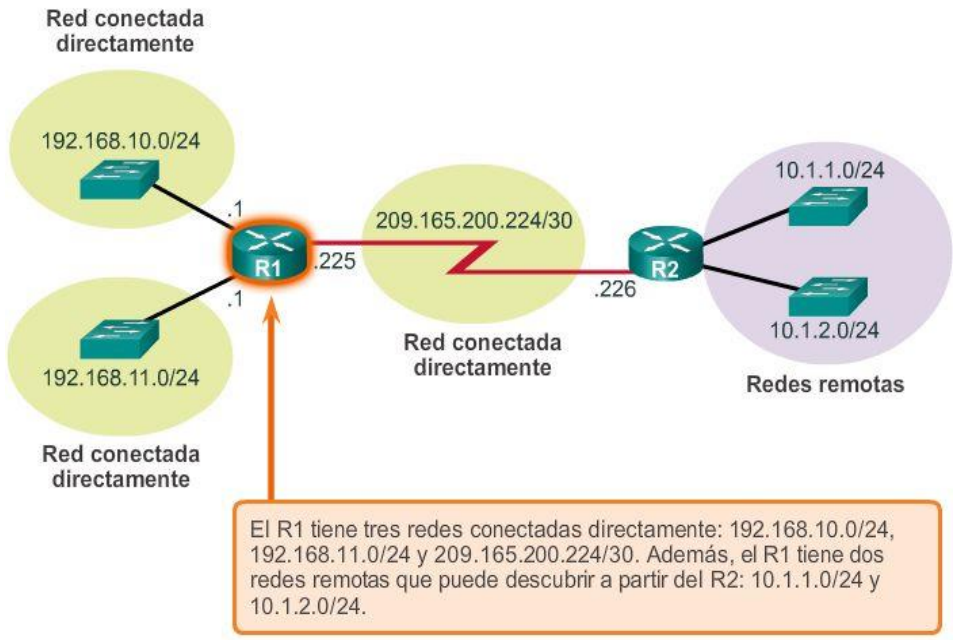
Los hosts requieren una tabla de enrutamiento local para asegurarse de que los paquetes se dirijan a la red de destino correcta. Por lo general, la tabla local de un host contiene la conexión directa, la ruta de red local y la ruta predeterminada local. La ruta predeterminada local es la ruta al gateway predeterminado.

El gateway predeterminado es la dirección IP de una interfaz de router conectado a la red local. Cuando un host necesita reenviar un paquete a una dirección de destino que no está en la misma red que el host, el paquete se envía al gateway predeterminado para su procesamiento posterior.

Cuando un router, como el gateway predeterminado, recibe un paquete, examina la dirección IP de destino para determinar la red de destino. En la tabla de enrutamiento de un router se almacena información sobre las rutas conectadas directamente y las rutas remotas a redes IP. Si el router tiene una entrada para la red de destino en la tabla de enrutamiento, reenvía el paquete. Si no existe ninguna entrada de enrutamiento, es posible que el router reenvíe el paquete a su propia ruta predeterminada, si hay una configurada. En caso contrario, descartará el paquete.

Las entradas de la tabla de enrutamiento se pueden configurar manualmente en cada router para proporcionar enrutamiento estático, o los routers pueden comunicar la información de la ruta de manera dinámica entre ellos utilizando un protocolo de enrutamiento.

Para que los routers se puedan alcanzar, se debe configurar la interfaz del router. Para habilitar una interfaz específica, ingrese al modo de configuración de interfaz con el comando del modo de configuración global interface *tipo-y-número*.



Capítulo 7: Capa de Transporte 7.0.1.1 Introducción

Las redes de datos e Internet brindan soporte a la red humana por medio del suministro de comunicación confiable entre personas. En un único dispositivo, las personas pueden utilizar varias aplicaciones y diversos servicios, como correo electrónico, la Web y la mensajería instantánea, para enviar mensajes o recuperar información.

Las aplicaciones, como los clientes de correo electrónico, los exploradores Web y los clientes de mensajería instantánea, permiten que las personas usen PC y redes para enviar mensajes y encontrar información.

Los datos de cada una de estas aplicaciones se empaquetan, se transportan y se entregan a la aplicación correspondiente en el dispositivo de destino. Los procesos que se describen en la capa de transporte del modelo OSI aceptan los datos de la capa de aplicación y los preparan para el direccionamiento en la capa de red. La capa de transporte prepara los datos para transmitirlos a través de la red. La PC de origen se comunica con una PC receptora para decidir cómo dividir los datos en segmentos, cómo asegurarse de que ninguno de los segmentos se pierda y cómo verificar si llegan todos los segmentos. Al considerar la capa de transporte, imagínese un departamento de envíos que prepara un único pedido de varios paquetes para entregar.

En este capítulo, se examina el rol de la capa de transporte en el encapsulamiento de datos de aplicación que utiliza la capa de red. La capa de transporte incluye también las siguientes funciones:

- Permite que varias aplicaciones, como el envío de correo electrónico y las redes sociales, se puedan comunicar a través la red al mismo tiempo en un único dispositivo.
- Asegura que, si es necesario, la aplicación correcta reciba todos los datos con confianza y en orden.
- Emplea mecanismos de manejo de errores.

Objetivos de aprendizaje

Al completar este capítulo, usted podrá:

- Explicar la necesidad de la capa de transporte.
- Identificar la función de la capa de transporte a medida que provee la transferencia de datos de extremo a extremo entre las aplicaciones.
- Describir la función de dos protocolos de la capa de transporte TCP/IP: TCP y UDP.
- Explicar las funciones clave de la capa de transporte, incluso la confiabilidad, el direccionamiento de puerto y la segmentación.
- Explicar cómo cada TCP y UDP maneja las funciones clave.
- Identificar cuándo es apropiado usar TCP o UDP y proveer ejemplos de aplicaciones que usan cada protocolo.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Describa el propósito de la capa de transporte en la administración del transporte de datos en la comunicación de extremo a extremo.
- Describa las características de los protocolos TCP y UDP, incluidos los números de puerto y sus usos.
- Explique la forma en que los procesos de establecimiento y finalización de sesión TCP promueven una comunicación confiable.
- Explique la forma en que se transmiten y se reconocen las unidades de datos del protocolo TCP para garantizar la entrega.
- Describa los procesos de cliente UDP para establecer la comunicación con un servidor.
- Determine cuáles son las transmisiones más adecuadas para aplicaciones comunes: las transmisiones TCP de alta confiabilidad o las transmisiones UDP no garantizadas.

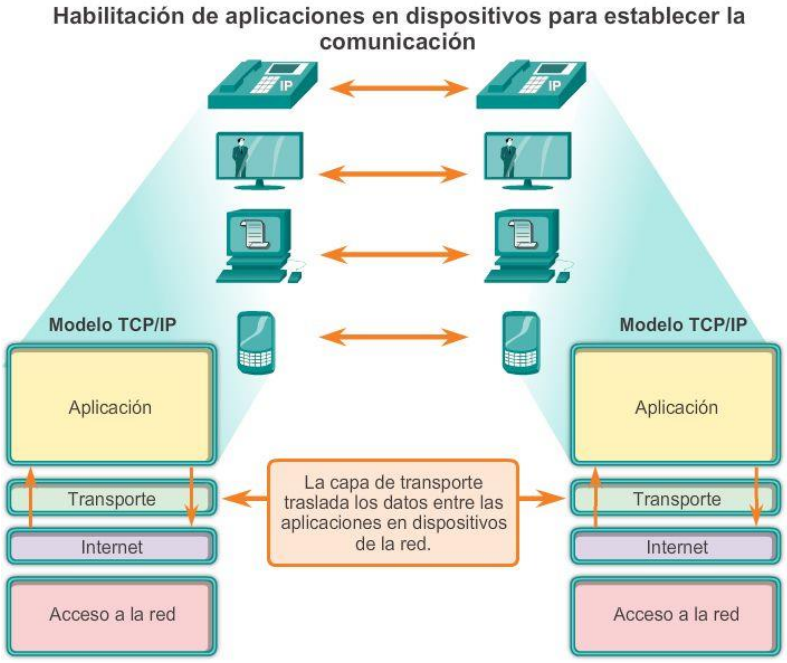
Capítulo 7: Capa de Transporte 7.1.1.1 El rol de la capa de transporte

La capa de transporte es responsable de establecer una sesión de comunicación temporal entre dos aplicaciones y de transmitir datos entre ellas. Las aplicaciones generan los datos que se envían de una aplicación en un host de origen a una aplicación a un host de destino, independientemente del tipo de host de destino, el tipo de medios a través de los que deben viajar los datos, la ruta que toman los datos, la congestión en un enlace o el tamaño de la red. Como se muestra en la ilustración, la capa de transporte es el enlace entre la capa de aplicación y las capas inferiores que son responsables de la transmisión a través de la red.

La capa de transporte proporciona un método para entregar datos a través de la red de una manera que garantiza que estos se puedan volver a unir correctamente en el extremo receptor. La capa de transporte permite la segmentación de datos y proporciona el control necesario para rearmar estos segmentos en los distintos streams de comunicación. En el protocolo TCP/IP, estos procesos de segmentación y rearmado se pueden lograr utilizando dos protocolos muy diferentes de la capa de transporte: el protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP).

Las principales responsabilidades de los protocolos de la capa de transporte son las siguientes:

- Rastreo de comunicación individual entre aplicaciones en los hosts de origen y destino
- División de los datos en segmentos para su administración y reunificación de los datos segmentados en streams de datos de aplicación en el destino
- Identificación de la aplicación correspondiente para cada stream de comunicación



Capítulo 7: Capa de Transporte 7.1.1.2 Función de la capa de transporte (cont.)

Rastreo de conversaciones individuales

En la capa de transporte, cada conjunto de datos particular que fluye entre una aplicación de origen y una de destino se conoce como “conversación” (figura 1). Un host puede tener varias aplicaciones que se comunican a través de la red de forma simultánea. Cada una de estas aplicaciones se comunica con una o más aplicaciones en uno o más hosts remotos. Es responsabilidad de la capa de transporte mantener y hacer un seguimiento de todas estas conversaciones.

Segmentación de datos y rearmado de segmentos

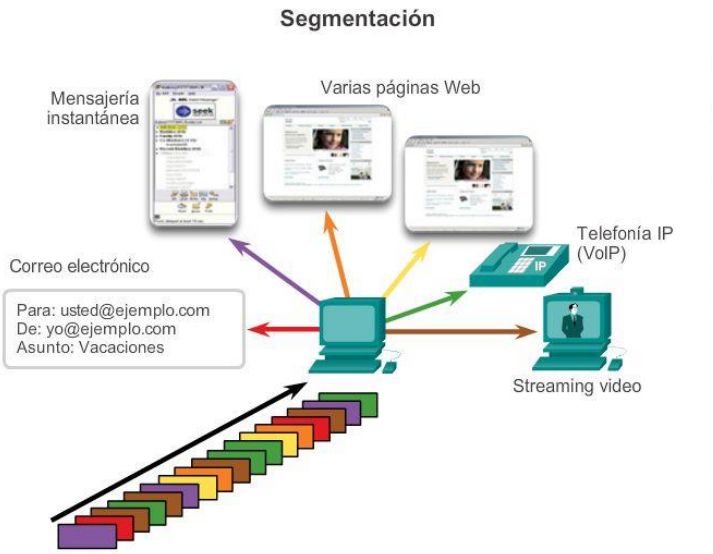
Se deben preparar los datos para el envío a través de los medios en partes manejables. La mayoría de las redes tienen un límite de la cantidad de datos que se puede incluir en un solo paquete. Los protocolos de la capa de transporte tienen servicios que segmentan los datos de aplicación en bloques de datos de un tamaño apropiado (figura 2). Estos servicios incluyen la encapsulación necesaria en cada porción de datos. Se agrega un encabezado a cada bloque de datos para el rearmado. Este encabezado se utiliza para hacer un seguimiento del stream de datos.

En el destino, la capa de transporte debe poder reconstruir las porciones de datos en un stream de datos completo que sea útil para la capa de aplicación. Los protocolos en la capa de transporte describen cómo se utiliza la información del encabezado de dicha capa para rearmar las porciones de datos en streams para pasarlos a la capa de aplicación.

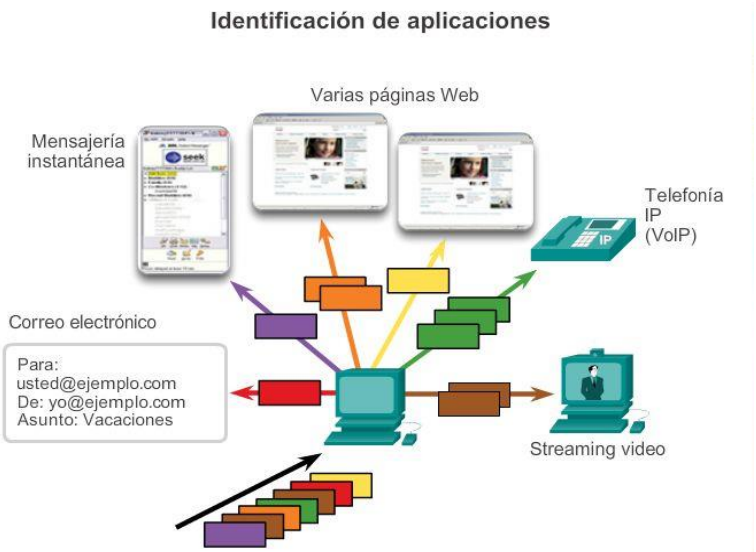
Identificación de aplicaciones

Puede haber muchas aplicaciones o servicios que se ejecutan en cada host de la red. Para pasar streams de datos a las aplicaciones adecuadas, la capa de transporte debe identificar la aplicación objetivo (figura 3). Para lograr esto, la capa de transporte asigna un identificador a cada aplicación. Este identificador se denomina “número de puerto”. A todos los procesos de software que requieran acceder a la red se les asigna un número de puerto exclusivo en ese host. La capa de transporte utiliza puertos para identificar la aplicación o el servicio.

La capa de transporte hace un seguimiento de cada conversación individual que fluye entre una aplicación de origen y una aplicación de destino por separado.



La capa de transporte divide los datos en segmentos, que son más fáciles de administrar y transportar.



La capa de transporte garantiza que aunque sean varias las aplicaciones se ejecutan en un dispositivo, todas reciban los datos correctos.

Capítulo 7: Capa de Transporte 7.1.1.3 Multiplexación de conversaciones

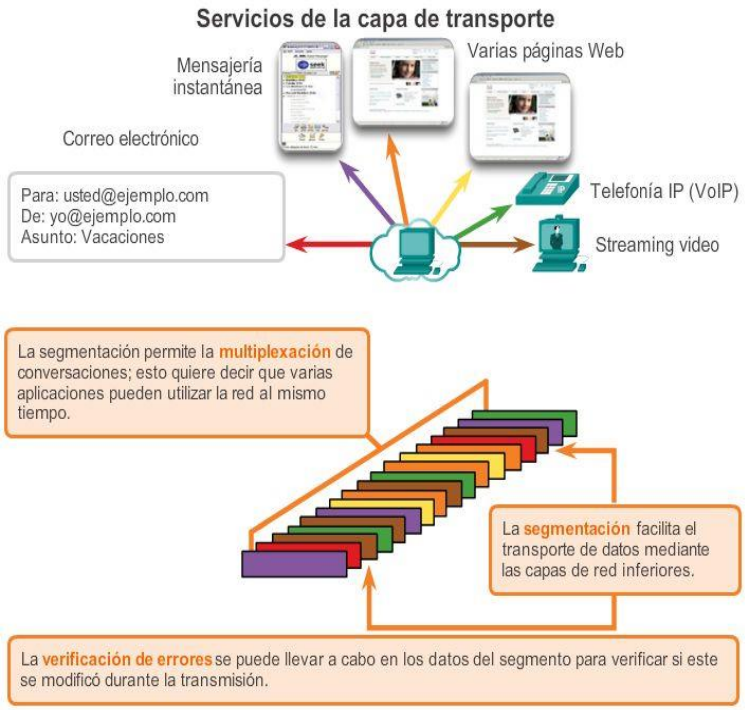
Multiplexación de conversaciones

El envío de algunos tipos de datos (por ejemplo, un streaming video) a través de una red, como un stream completo de comunicación, podría utilizar todo el ancho de banda disponible e impedir que se produzcan otras comunicaciones al mismo tiempo. También dificulta la recuperación de errores y la retransmisión de datos dañados.

En la ilustración, se muestra que la segmentación de los datos en partes más pequeñas permite que se entrelacen (multiplexen) varias comunicaciones de distintos usuarios en la misma red. La segmentación de los datos según los protocolos de la capa de transporte también proporciona los medios para enviar y recibir datos cuando se ejecutan varias aplicaciones a la vez en una PC.

Sin la segmentación, solo podría recibir datos una aplicación. Por ejemplo, con un streaming video, los medios se consumirían por completo por ese stream de comunicación en lugar de compartirse. No podría recibir correos electrónicos, chatear por mensajería instantánea o visitar páginas Web mientras mira el video.

Para identificar cada segmento de datos, la capa de transporte agrega al segmento un encabezado que contiene datos binarios. Este encabezado contiene campos de bits. Los valores de estos campos permiten que los distintos protocolos de la capa de transporte lleven a cabo diferentes funciones de administración de la comunicación de datos.



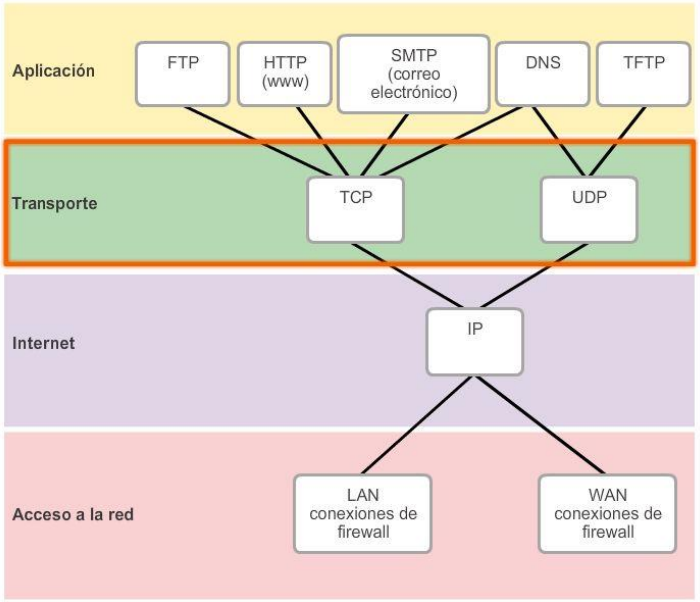
Capítulo 7: Capa de Transporte 7.1.1.4 Confiabilidad de la capa de transporte

La capa de transporte también es responsable de administrar los requisitos de confiabilidad de las conversaciones. Las diferentes aplicaciones tienen diferentes requisitos de confiabilidad de transporte.

IP se ocupa solo de la estructura, el direccionamiento y el enrutamiento de paquetes. IP no especifica la manera en que se lleva a cabo la entrega o el transporte de los paquetes.

Los protocolos de transporte especifican la manera en que se transfieren los mensajes entre los hosts. TCP/IP proporciona dos protocolos de la capa de transporte: el protocolo de control de transmisión (TCP) y el protocolo de datagramas de usuario (UDP), como se muestra en la ilustración. IP utiliza estos protocolos de transporte para habilitar la comunicación y la transferencia de datos entre los hosts.

TCP se considera un protocolo de la capa de transporte confiable y completo, lo que garantiza que todos los datos lleguen al destino. En cambio, UDP es un protocolo de la capa de transporte muy simple que no proporciona confiabilidad.



Capítulo 7: Capa de Transporte 7.1.1.5 TCP

Como se indicó anteriormente, TCP se considera un protocolo de transporte confiable, lo que significa que incluye procesos para garantizar la entrega confiable entre aplicaciones mediante el uso de entrega con acuse de recibo. La función del protocolo de transporte TCP es similar al envío de paquetes de los que se hace un seguimiento de origen a destino. Si se divide un pedido de FedEx en varios envíos, el cliente puede revisar en línea el orden de la entrega.

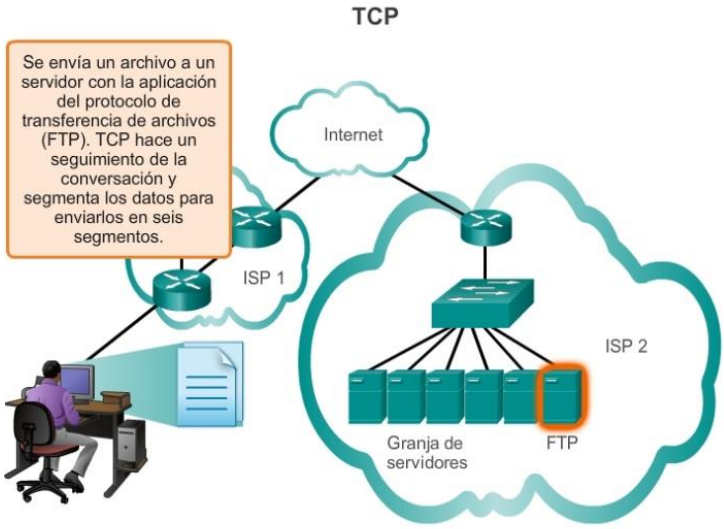
Con TCP, las tres operaciones básicas de confiabilidad son las siguientes:

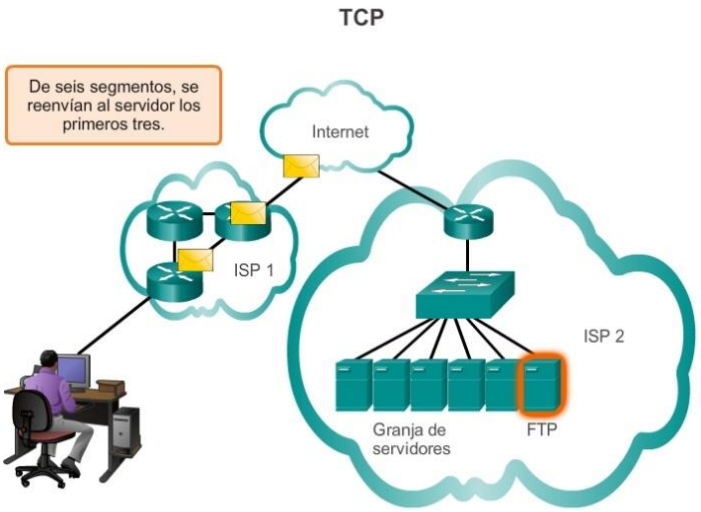
- Seguimiento de segmentos de datos transmitidos
- Acuse de recibo de datos
- Retransmisión de cualquier dato sin acuse de recibo

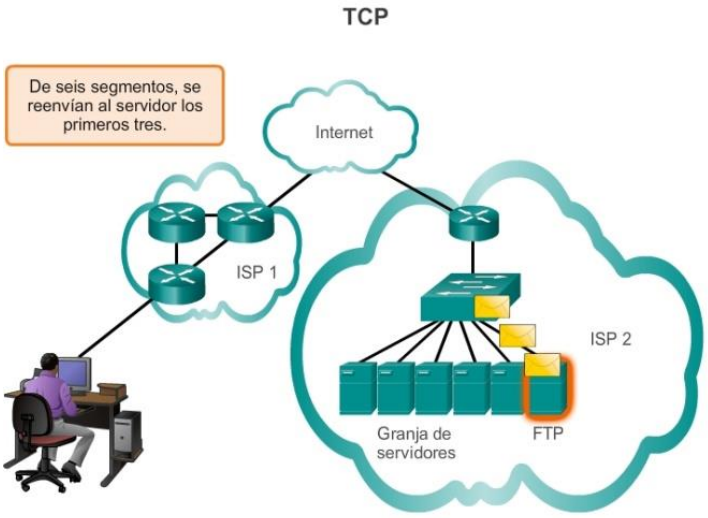
TCP divide el mensaje en partes pequeñas, conocidas como segmentos. Los segmentos se numeran en secuencia y se pasan al proceso IP para armarse en paquetes. TCP realiza un seguimiento del número de segmentos que se enviaron a un host específico desde una aplicación específica. Si el emisor no recibe un acuse de recibo antes del transcurso de un período determinado, supone que los segmentos se perdieron y los vuelve a transmitir. Sólo se vuelve a enviar la parte del mensaje que se perdió, no todo el mensaje. En el host receptor, TCP se encarga de rearmar los segmentos del mensaje y de pasarlos a la aplicación. El protocolo de transferencia de archivos (FTP) y el protocolo de transferencia de hipertexto (HTTP) son ejemplos de las aplicaciones que utilizan TCP para garantizar la entrega de datos.

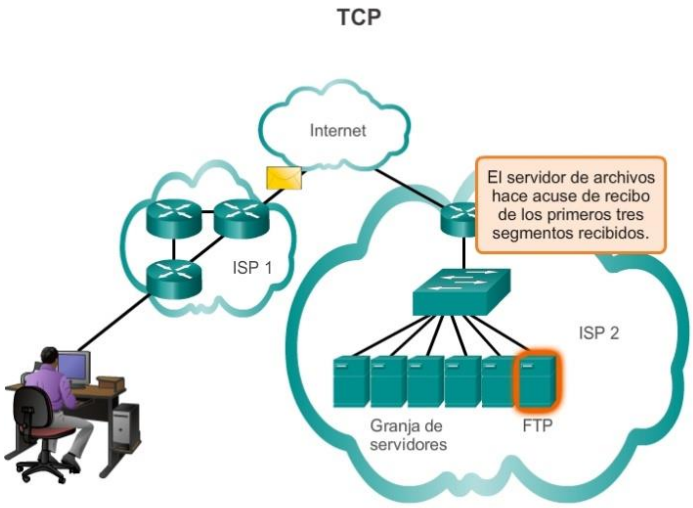
Haga clic en el botón Reproducir en la ilustración para ver una animación de los segmentos TCP que se transmiten del emisor al receptor.

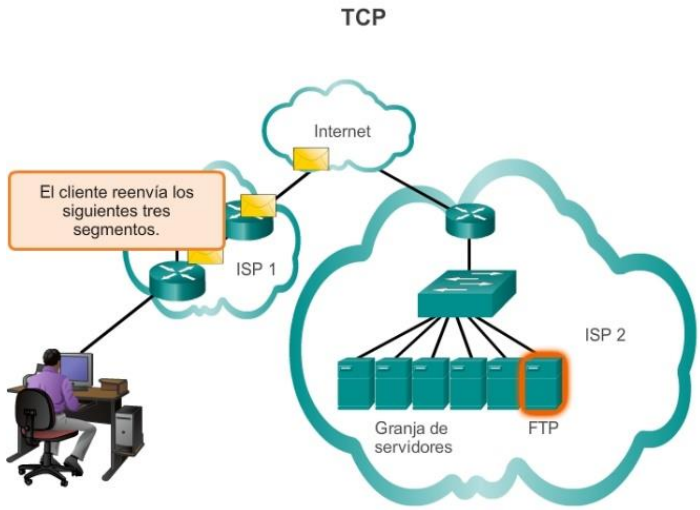
Estos procesos de confiabilidad generan una sobrecarga adicional en los recursos de la red debido a los procesos de acuse de recibo, rastreo y retransmisión. Para admitir estos procesos de confiabilidad, se intercambian más datos de control entre los hosts emisores y receptores. Esta información de control está incluida en un encabezado TCP.

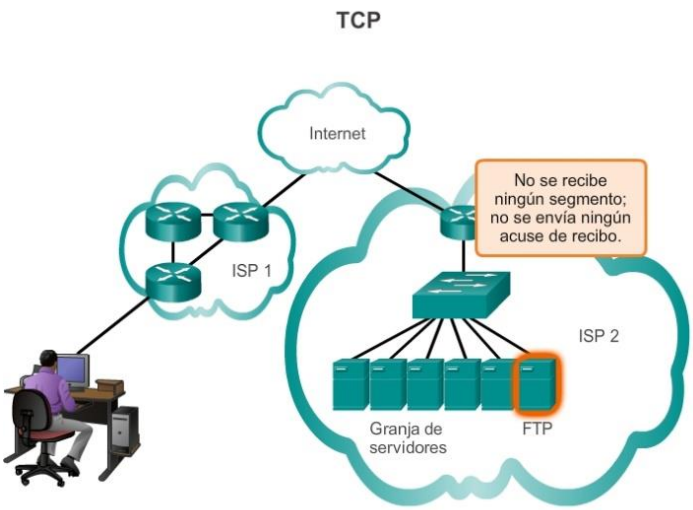

TCP
Se envía un archivo a un servidor con la aplicación del protocolo de transferencia de archivos (FTP). TCP hace un seguimiento de la conversación y segmenta los datos para enviarlos en seis segmentos.
Internet
ISP 1
ISP 2
Granja de servidores
FTP

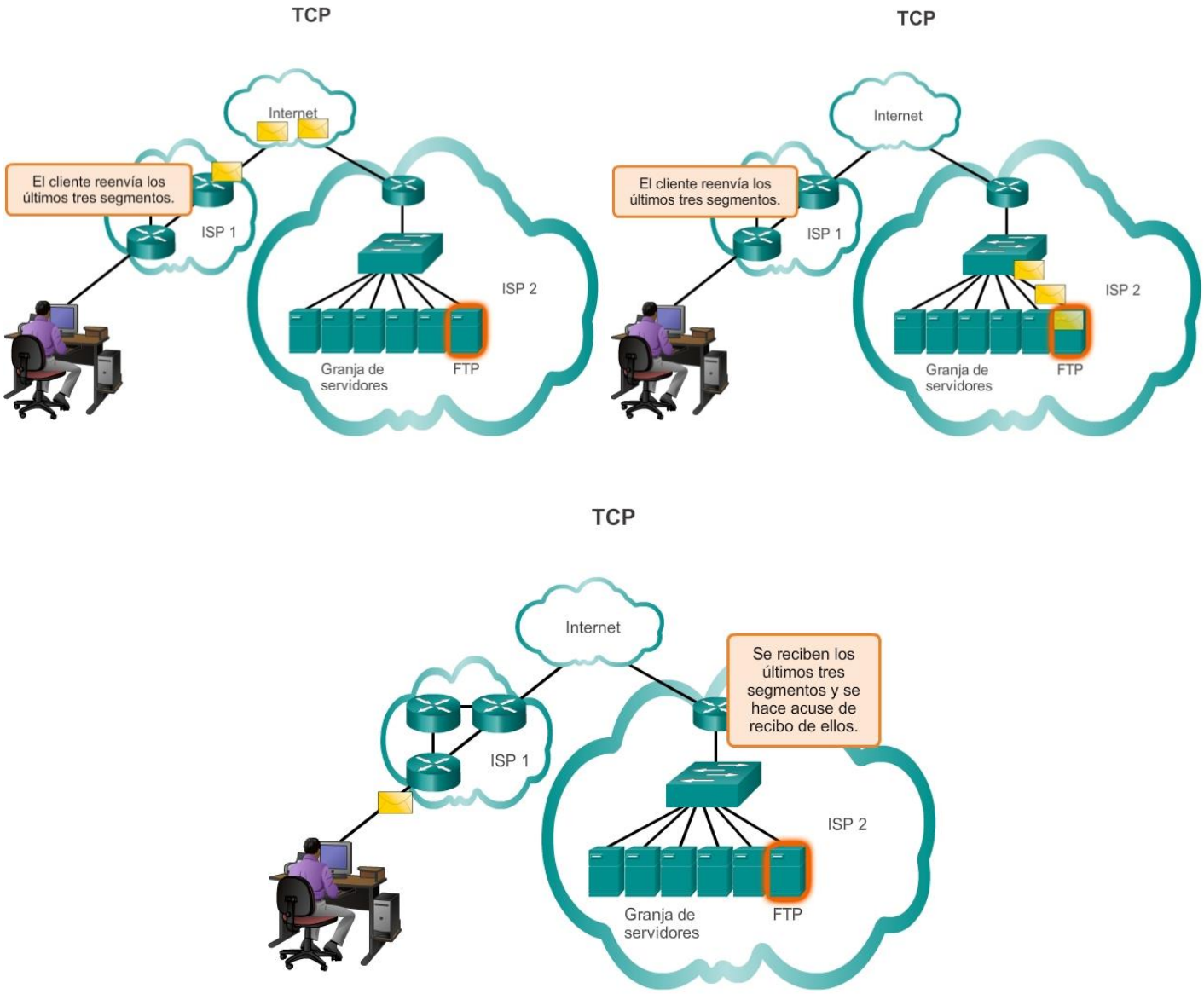

TCP
De seis segmentos, se reenvían al servidor los primeros tres.
Internet
ISP 1
ISP 2
Granja de servidores
FTP


TCP
De seis segmentos, se reenvían al servidor los primeros tres.
Internet
ISP 1
ISP 2
Granja de servidores
FTP


TCP
Internet
El servidor de archivos hace acuse de recibo de los primeros tres segmentos recibidos.
ISP 1
ISP 2
Granja de servidores
FTP


TCP
Internet
El cliente reenvía los siguientes tres segmentos.
ISP 1
ISP 2
Granja de servidores
FTP


TCP
Internet
No se recibe ningún segmento; no se envía ningún acuse de recibo.
ISP 1
ISP 2
Granja de servidores
FTP



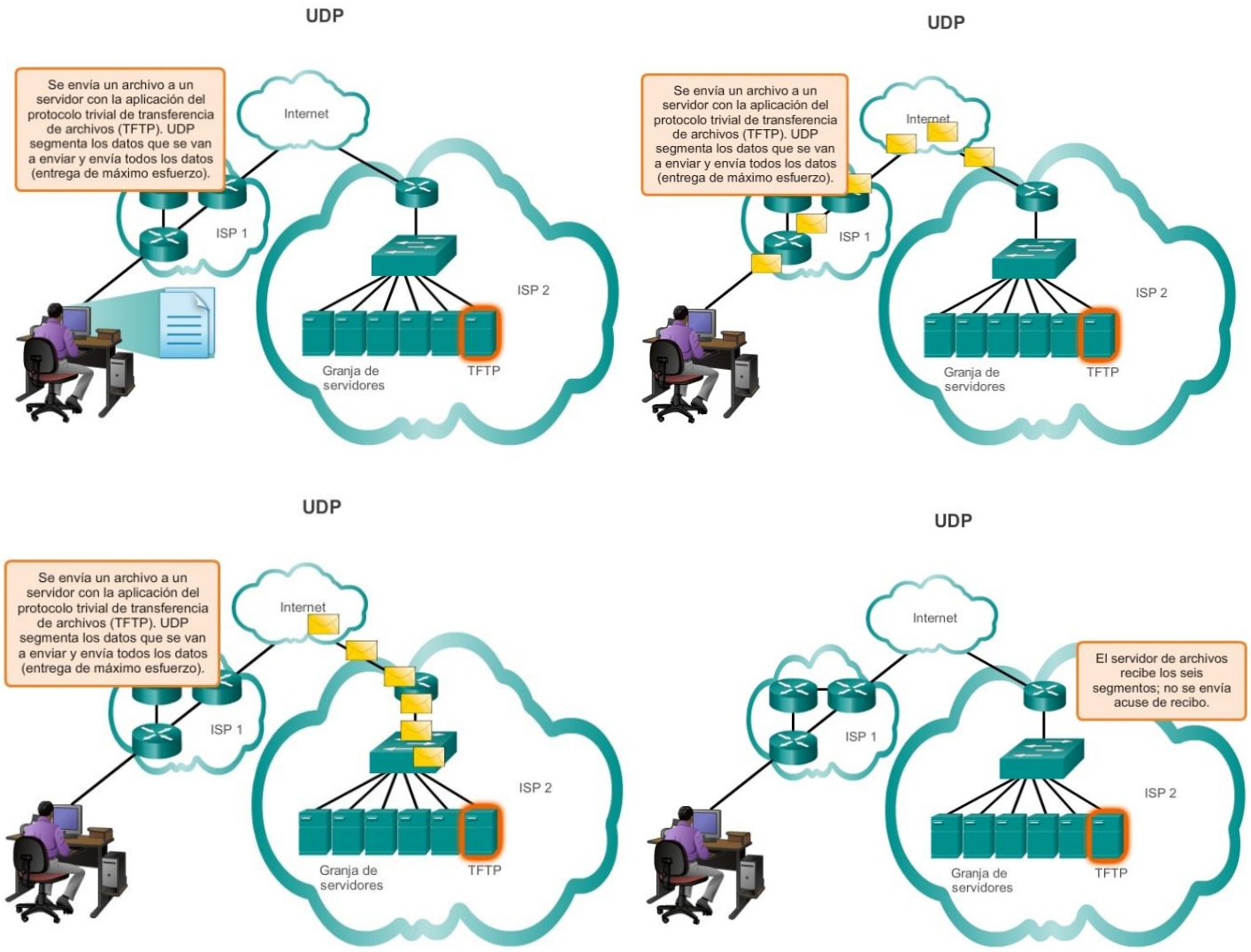
Capítulo 7: Capa de Transporte 7.1.1.6 UDP

Si bien las funciones de confiabilidad de TCP proporcionan una comunicación más sólida entre aplicaciones, también representan una sobrecarga adicional y pueden provocar demoras en la transmisión. Existe una compensación entre el valor de la confiabilidad y la carga que implica para los recursos de la red. La imposición de sobrecarga para garantizar la confiabilidad para algunas aplicaciones podría reducir la utilidad a la aplicación e incluso ser perjudicial para esta. En estos casos, UDP es un protocolo de transporte mejor.

UDP proporciona solo las funciones básicas para entregar segmentos de datos entre las aplicaciones adecuadas, con muy poca sobrecarga y revisión de datos. El protocolo UDP se conoce como protocolo de entrega de máximo esfuerzo. En el contexto de redes, la entrega de máximo esfuerzo se denomina “poco confiable”, porque no hay acuse de recibo que indique que los datos se recibieron en el destino. Con UDP, no existen procesos de capa de transporte que informen al emisor si la entrega se produjo correctamente.

El proceso de UDP es similar al envío por correo de una carta simple sin registrar. El emisor de la carta no sabe si el receptor está disponible para recibir la carta ni la oficina de correos es responsable de hacer un seguimiento de la carta o de informar al emisor si esta no llega a destino.

Haga clic en el botón Reproducir en la ilustración para ver una animación de los segmentos UDP que se transmiten del emisor al receptor.



Capítulo 7: Capa de Transporte 7.1.1.7 Protocolo de la capa de transporte correcto para la aplicación adecuada

Tanto TCP como UDP son protocolos de transporte válidos. Según los requisitos de la aplicación, se puede utilizar uno de estos protocolos de transporte y, en ocasiones, se pueden utilizar ambos. Los desarrolladores de aplicaciones deben elegir qué tipo de protocolo de transporte es adecuado según los requisitos de las aplicaciones.

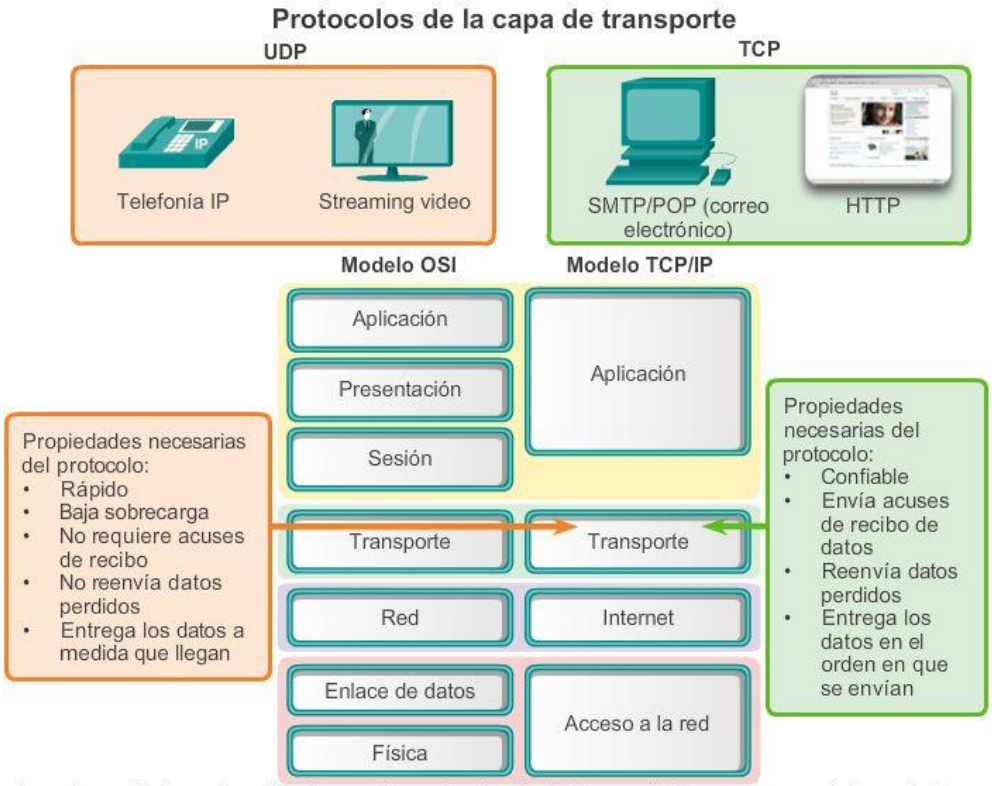
Para algunas aplicaciones, los segmentos deben llegar en una secuencia muy específica para que se puedan procesar correctamente. Con otras aplicaciones, todos los datos se deben recibir en forma completa para poder considerarse útiles. En ambos casos, se utiliza TCP como protocolo de transporte. Por ejemplo, las aplicaciones, como las bases de datos, los exploradores Web y los clientes de correo electrónico, requieren que todos los datos que se envían lleguen a destino en su formato original. Todos los datos perdidos pueden corromper una comunicación y dejarla incompleta o ilegible. Por lo tanto, estas aplicaciones están diseñadas para utilizar TCP. Los gastos de red adicionales se consideran necesarios para estas aplicaciones.

En otros casos, una aplicación puede tolerar cierta pérdida de datos durante la transmisión a través de la red, pero no se admiten retrasos en la transmisión.

UDP es la mejor opción para estas aplicaciones, ya que se requiere menos sobrecarga de red. Con aplicaciones como streaming audio, video y voz sobre IP (VoIP), es preferible utilizar UDP. Los acuses de recibo reducirían la velocidad de la entrega, y las retransmisiones no son recomendables.

Por ejemplo, si uno o dos segmentos de un stream de video no llegan al destino, se interrumpe momentáneamente el stream. Esto puede representar distorsión en la imagen, pero quizá ni el usuario lo note. Por otro lado, la imagen en un streaming video se degradaría en gran medida si el dispositivo de destino tuviera que dar cuenta de los datos perdidos y demorar el stream mientras espera las retransmisiones. En este caso, es mejor producir el mejor video posible con los segmentos recibidos y prescindir de la confiabilidad.

La radio a través de Internet es otro ejemplo de aplicación que utiliza UDP. Si parte del mensaje se pierde durante su transmisión por la red, no se vuelve a transmitir. Si se pierden algunos paquetes, el oyente podrá escuchar una breve interrupción en el sonido. Si se utilizara TCP y se volvieran a enviar los paquetes perdidos, la transmisión haría una pausa para recibirlos, y la interrupción sería más notoria.



Los desarrolladores de aplicaciones eligen el protocolo de la capa de transporte apropiado según la naturaleza de la aplicación.

Capítulo 7: Capa de Transporte 7.1.2.1 Presentación de TCP

Para entender con propiedad las diferencias entre TCP y UDP, es importante comprender la manera en que cada protocolo implementa las funciones específicas de confiabilidad y la forma en que realizan el seguimiento de las comunicaciones.

Protocolo de control de transmisión (TCP)

TCP se describió inicialmente en RFC 793. Además de admitir funciones básicas de segmentación y rearmado de datos, TCP, como se muestra en la ilustración, también proporciona lo siguiente:

- Conversaciones orientadas a la conexión mediante el establecimiento de sesiones
- Entrega confiable
- Reconstrucción de datos ordenada
- Control del flujo

Establecimiento de una sesión

TCP es un protocolo orientado a la conexión. Un protocolo orientado a la conexión es uno que negocia y establece una conexión (o sesión) permanente entre los dispositivos de origen y de destino antes de reenviar tráfico. El establecimiento de sesión prepara los dispositivos para que se comuniquen entre sí. Mediante el establecimiento de sesión, los dispositivos negocian la cantidad de tráfico que se puede reenviar en un momento determinado, y los datos que se comunican entre ambos se pueden administrar detenidamente. La sesión se termina solo cuando se completa toda la comunicación.

Entrega confiable

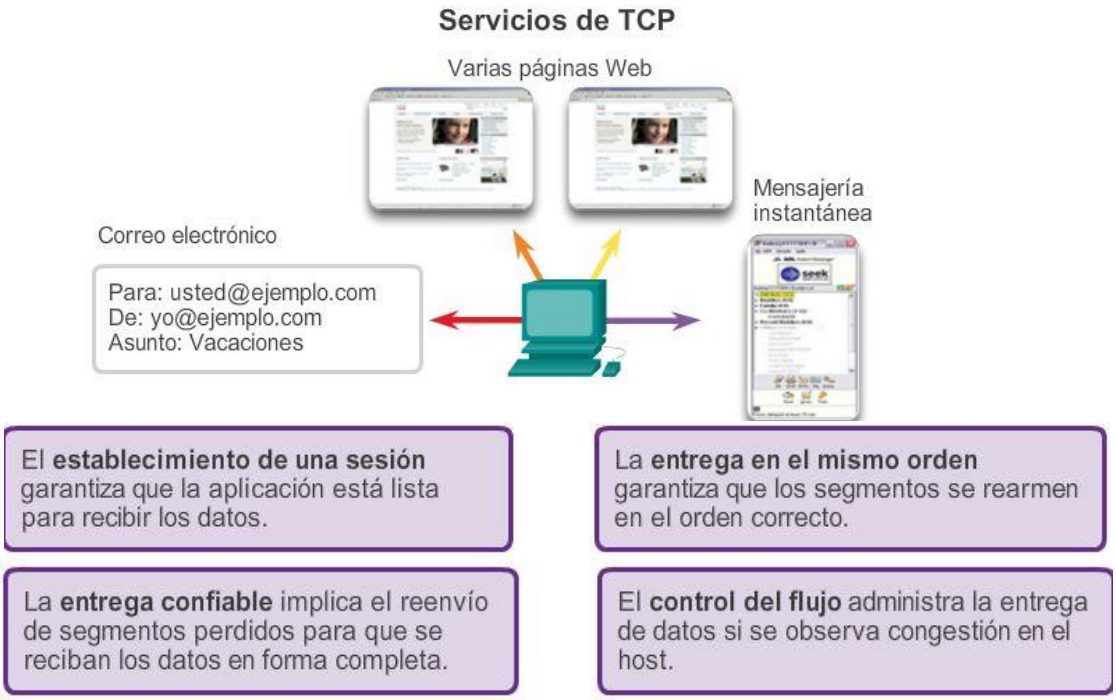
TCP puede implementar un método para garantizar la entrega confiable de los datos. En términos de redes, confiabilidad significa asegurar que cada sección de datos que envía el origen llegue al destino. Por varias razones, es posible que una sección de datos se corrompa o se pierda por completo a medida que se transmite a través de la red. TCP puede asegurar que todas las partes lleguen a destino al hacer que el dispositivo de origen retransmita los datos perdidos o dañados.

Entrega en el mismo orden

Los datos pueden llegar en el orden equivocado, debido a que las redes pueden proporcionar varias rutas que pueden tener diferentes velocidades de transmisión. Al numerar y secuenciar los segmentos, TCP puede asegurar que estos se rearmen en el orden correcto.

Control de flujo

Los hosts de la red cuentan con recursos limitados, como memoria o ancho de banda. Cuando TCP advierte que estos recursos están sobrecargados, puede solicitar que la aplicación emisora reduzca la velocidad del flujo de datos. Esto lo lleva a cabo TCP, que regula la cantidad de datos que transmite el origen. El control de flujo puede evitar la pérdida de segmentos en la red y evitar la necesitad de la retransmisión.



Capítulo 7: Capa de Transporte 7.1.2.2 Rol del TCP

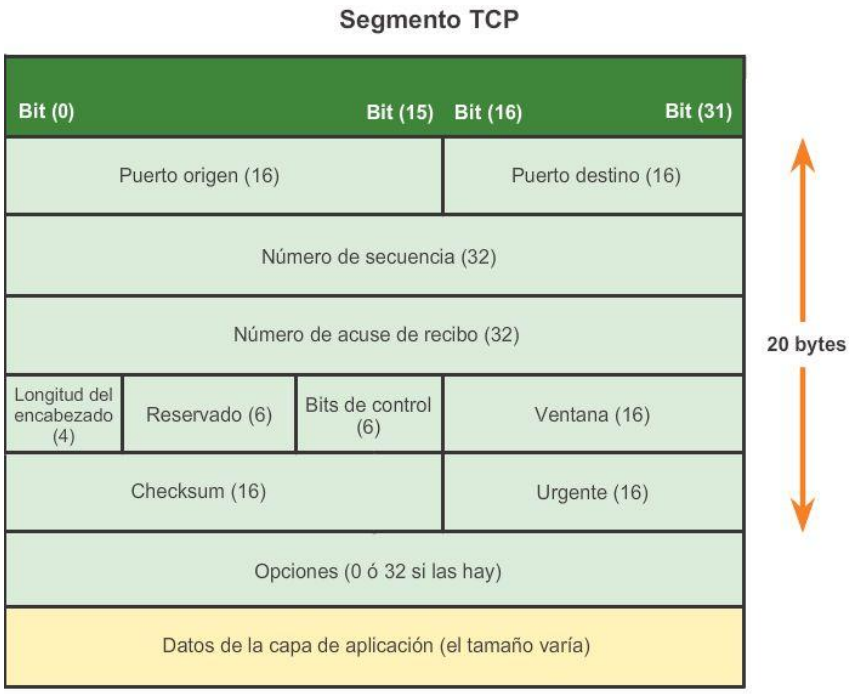
Una vez que TCP establece una sesión, puede hacer un seguimiento de la conversación dentro de esa sesión. Debido a la capacidad de TCP de hacer un seguimiento de conversaciones reales, se lo considera un protocolo con estado. Un protocolo con estado es un protocolo que realiza el seguimiento del estado de la sesión de comunicación. Por ejemplo, cuando se transmiten datos mediante TCP, el emisor espera que el destino acuse recibo de los datos. TCP hace un seguimiento de la información que se envió y de la que se acusó de recibo. Si no se acusa recibo de los datos, el emisor supone que no llegaron y los vuelve a enviar. La sesión con estado comienza con el establecimiento de sesión y finaliza cuando se cierra la sesión con terminación de sesión.

Nota: el mantenimiento de esta información de estado requiere recursos que no son necesarios para un protocolo sin estado, como UDP.

TCP genera sobrecarga adicional para obtener estas funciones. Como se muestra en la ilustración, cada segmento TCP tiene 20 bytes de sobrecarga en el encabezado que encapsula los datos de la capa de aplicación. Este tipo de segmento es mucho más largo que un segmento UDP, que solo tiene 8 bytes de sobrecarga. La sobrecarga adicional incluye lo siguiente:

- Número de secuencia (32 bits): se utiliza para rearmar datos.
- Número de acuse de recibo (32 bits): indica los datos que se recibieron.
- Longitud del encabezado (4 bits): conocido como “desplazamiento de datos”. Indica la longitud del encabezado del segmento TCP.
- Reservado (6 bits): este campo está reservado para el futuro.
- Bits de control (6 bits): incluye códigos de bit, o indicadores, que indican el propósito y la función del segmento TCP.
- Tamaño de la ventana (16 bits): indica la cantidad de segmentos que se puedan aceptar por vez.
- Checksum (16 bits): se utiliza para la verificación de errores en el encabezado y los datos del segmento.
- Urgente (16 bits): indica si la información es urgente.

Algunos ejemplos de aplicaciones que utilizan TCP son los exploradores Web, el correo electrónico y las transferencias de archivos.



Capítulo 7: Capa de Transporte 7.1.2.3 Presentación de UDP

Protocolo de datagramas de usuario (UDP)

UDP se considera un protocolo de transporte de máximo esfuerzo, descrito en RFC 768. UDP es un protocolo de transporte liviano que ofrece la misma segmentación y rearmado de datos que TCP, pero sin la confiabilidad y el control del flujo de TCP. UDP es un protocolo tan simple que, por lo general, se lo describe en términos de lo que no hace en comparación con TCP.

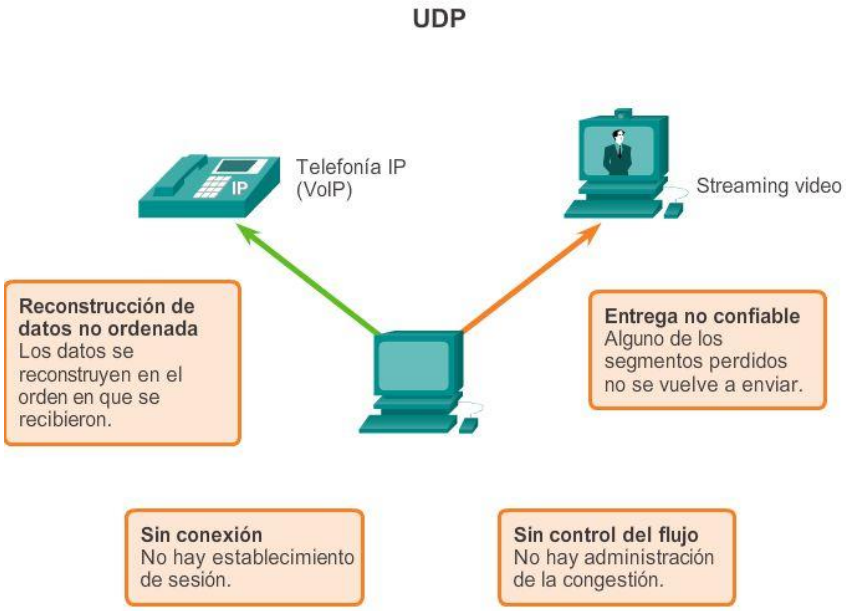
Como se muestra en la ilustración, las siguientes características describen a UDP:

- Sin conexión: UDP no establece una conexión entre los hosts antes de que se puedan enviar y recibir datos.

- Entrega no confiable: UDP no proporciona servicios para asegurar que los datos se entreguen con confianza. UDP no cuenta con procesos que hagan que el emisor vuelva a transmitir los datos que se pierden o se dañan.

- Reconstrucción de datos no ordenada: en ocasiones, los datos se reciben en un orden distinto del de envío. UDP no proporciona ningún mecanismo para rearmar los datos en su secuencia original. Los datos simplemente se entregan a la aplicación en el orden en que llegan.

- Sin control del flujo: UDP no cuenta con mecanismos para controlar la cantidad de datos que transmite el dispositivo de origen para evitar la saturación del dispositivo de destino. El origen envía los datos. Si los recursos en el host de destino se sobrecargan, es probable que dicho host descarte los datos enviados hasta que los recursos estén disponibles. A diferencia de TCP, en UDP no hay un mecanismo para la retransmisión automática de datos descartados.



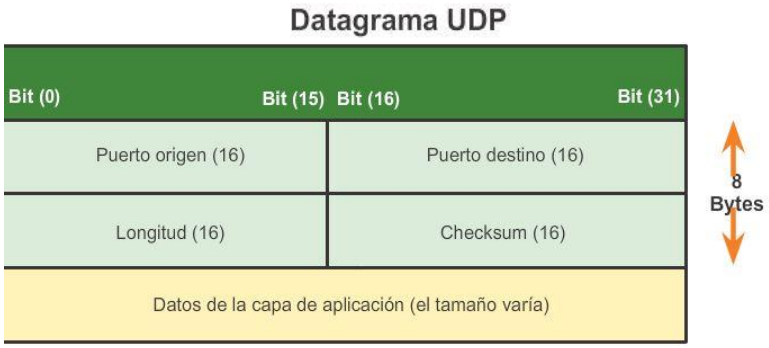
Capítulo 7: Capa de Transporte 7.1.2.4 Rol del UDP

Aunque UDP no incluye la confiabilidad y los mecanismos de control del flujo de TCP, como se muestra en la ilustración, la entrega de datos de baja sobrecarga de UDP lo convierte en un protocolo de transporte ideal para las aplicaciones que pueden tolerar cierta pérdida de datos. Las porciones de comunicación en UDP se llaman datagramas.

El protocolo de la capa de transporte envía estos datagramas como máximo esfuerzo. Algunas aplicaciones que utilizan UDP son el Sistema de nombres de dominios (DNS), el streaming de video y la voz sobre IP (VoIP).

Uno de los requisitos más importantes para transmitir video en vivo y voz a través de la red es que los datos fluyan rápidamente. Las aplicaciones de video y de voz pueden tolerar cierta pérdida de datos con un efecto mínimo o imperceptible, y se adaptan perfectamente a UDP.

UDP es un protocolo sin estado, lo cual significa que ni el cliente ni el servidor están obligados a hacer un seguimiento del estado de la sesión de comunicación. Como se muestra en la ilustración, UDP no se ocupa de la confiabilidad ni del control del flujo. Los datos se pueden perder o recibir fuera de secuencia sin ningún mecanismo de UDP que pueda recuperarlos o reordenarlos. Si se requiere confiabilidad al utilizar UDP como protocolo de transporte, esta la debe administrar la aplicación.



Capítulo 7: Capa de Transporte 7.1.2.5 Separación de comunicaciones múltiples

La capa de transporte debe poder separar y administrar varias comunicaciones con diferentes necesidades de requisitos de transporte. Tome como ejemplo un usuario conectado a una red en un dispositivo final.

El usuario envía y recibe correo electrónico y mensajes instantáneos, visita sitios Web y realiza una llamada telefónica de voz sobre IP (VoIP) simultáneamente.

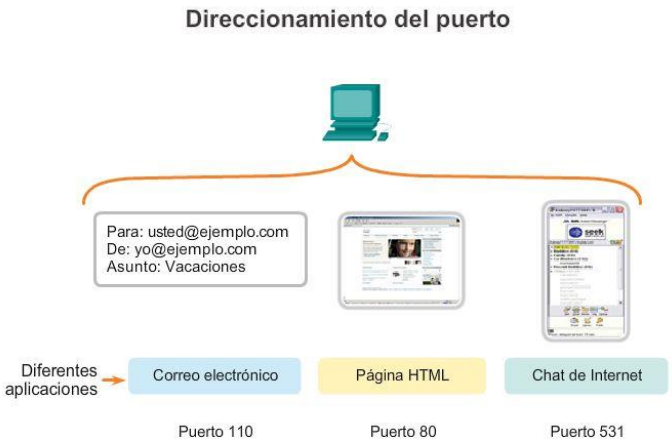
Cada una de estas aplicaciones envía y recibe datos a través de la red al mismo tiempo, a pesar de los diferentes requisitos de confiabilidad.

Además, los datos de la llamada telefónica no están dirigidos al explorador Web y el texto de un mensaje instantáneo no aparece en un correo electrónico.

Por motivos de confiabilidad, los usuarios necesitan que un correo electrónico o una página Web se reciba y presente por completo para que la información se considere útil. Por lo general, se permiten leves retrasos en la carga de correo electrónico o de páginas Web, siempre y cuando el producto final se muestre en su totalidad y de forma correcta. En este ejemplo, la red administra el reenvío o reemplazo de la información que falta y no muestra el producto final hasta que se hayan recibido y armado todos los datos.

En cambio, la pérdida ocasional de partes pequeñas de una conversación telefónica se puede considerar aceptable. Incluso si se descartan partes pequeñas de algunas palabras, se puede deducir el audio que falta del contexto de la conversación o solicitar que la otra persona repita lo que dijo. Si la red administrara y reenviara segmentos faltantes, se prefiere lo mencionado anteriormente a los retrasos que se producen. En este ejemplo, es el usuario y no la red quien administra el reenvío o reemplazo de la información que falta.

Como se muestra en la ilustración, para que TCP y UDP administren estas conversaciones simultáneas con diversos requisitos, los servicios basados en UDP y TCP deben hacer un seguimiento de las diversas aplicaciones que se comunican. Para diferenciar los segmentos y datagramas para cada aplicación, tanto TCP como UDP cuentan con campos de encabezado que pueden identificar de manera exclusiva estas aplicaciones. Estos identificadores únicos son números de puertos.



Capítulo 7: Capa de Transporte 7.1.2.6 Direccionamiento de puertos TCP y UDP

En el encabezado de cada segmento o datagrama, hay un puerto origen y uno de destino. El número de puerto de origen es el número para esta comunicación asociado con la aplicación que origina la comunicación en el host local. Como se muestra en la ilustración, el número de puerto de destino es el número para esta comunicación relacionada con la aplicación de destino en el host remoto.

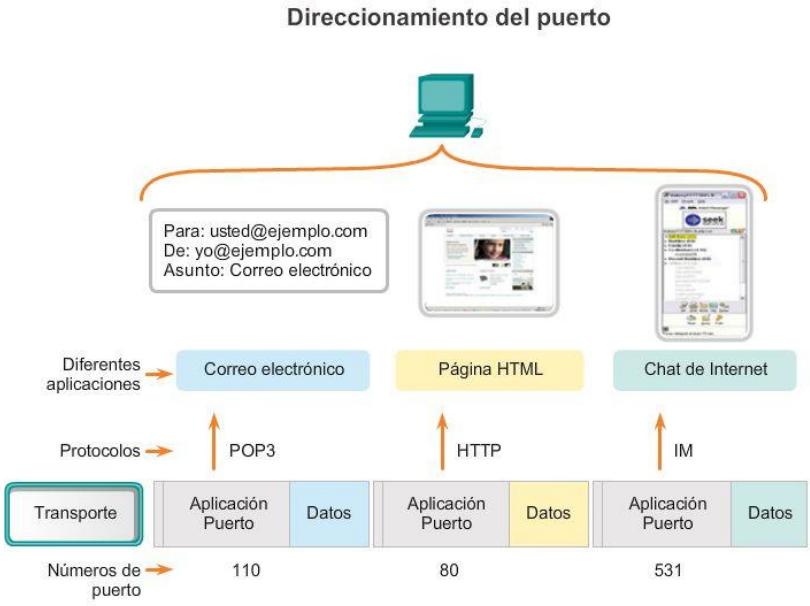
Cuando se envía un mensaje utilizando TCP o UDP, los protocolos y servicios solicitados se identifican con un número de puerto. Un puerto es un identificador numérico de cada segmento, que se utiliza para realizar un seguimiento de conversaciones específicas y de servicios de destino solicitados. Cada mensaje que envía un host contiene un puerto de origen y un puerto de destino.

Puerto de destino

El cliente coloca un número de puerto de destino en el segmento para informar al servidor de destino el servicio solicitado. Por ejemplo: el puerto 80 se refiere a HTTP o al servicio Web. Cuando un cliente especifica el puerto 80 en el puerto de destino, el servidor que recibe el mensaje sabe que se solicitan servicios Web. Un servidor puede ofrecer más de un servicio simultáneamente. Por ejemplo, puede ofrecer servicios Web en el puerto 80 al mismo tiempo que ofrece el establecimiento de una conexión FTP en el puerto 21.

Puerto de origen

El número de puerto de origen es generado de manera aleatoria por el dispositivo emisor para identificar una conversación entre dos dispositivos. Esto permite establecer varias conversaciones simultáneamente. En otras palabras, un dispositivo puede enviar varias solicitudes de servicio HTTP a un servidor Web al mismo tiempo. El seguimiento de las conversaciones por separado se basa en los puertos de origen.



Capítulo 7: Capa de Transporte 7.1.2.7 Direccionamiento de puertos TCP y UDP (cont.)

Los puertos de origen y de destino se colocan dentro del segmento. Los segmentos se encapsulan dentro de un paquete IP. El paquete IP contiene la dirección IP de origen y de destino. La combinación de las direcciones IP de origen y de destino y de los números de puerto de origen y de destino se conoce como “socket”. El socket se utiliza para identificar el servidor y el servicio que solicita el cliente. Miles de hosts se comunican a diario con millones de servidores diferentes. Los sockets identifican esas comunicaciones.

La combinación del número de puerto de la capa de transporte y de la dirección IP de la capa de red del host identifica de manera exclusiva un proceso de aplicación en particular que se ejecuta en un dispositivo host individual. Esta combinación se denomina socket. Un par de sockets, que consiste en las direcciones IP de

origen y destino y los números de puertos, también es exclusivo e identifica la conversación específica entre los dos hosts.

Un socket de cliente puede ser parecido a esto, donde 1099 representa el número de puerto de origen: 192.168.1.5:1099

El socket en un servidor Web podría ser el siguiente: 192.168.1.7:80

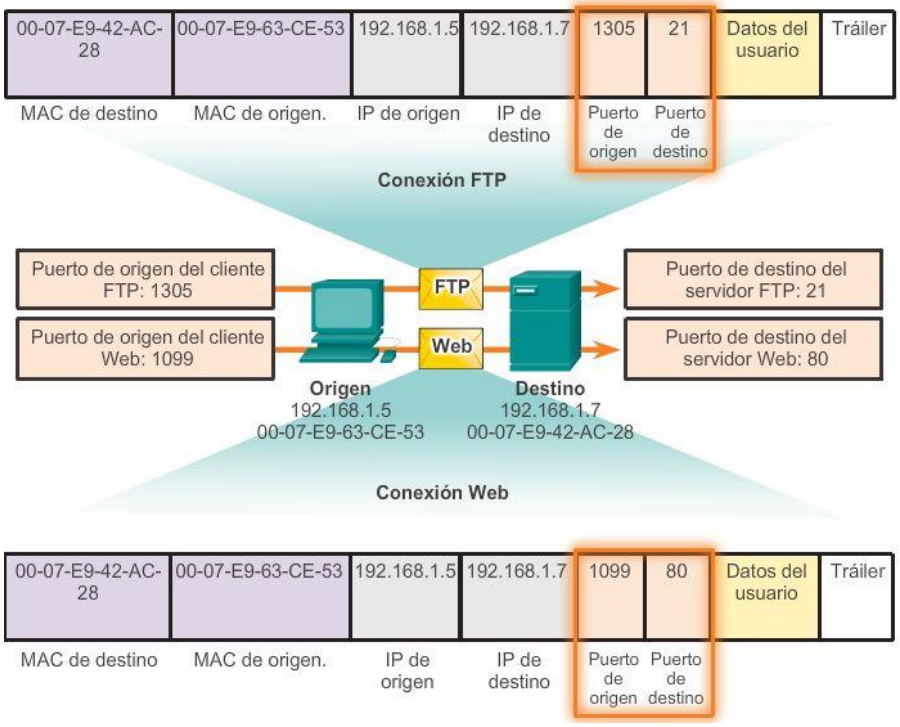
Juntos, estos dos sockets se combinan para formar un par de sockets: 192.168.1.5:1099, 192.168.1.7:80

Con la creación de sockets, se conocen los extremos de la comunicación, de modo que los datos puedan moverse desde una aplicación en un host hacia una aplicación en otro host.

Los sockets permiten que los procesos múltiples que se ejecutan en un cliente se distingan entre sí. También permiten la diferenciación de múltiples conexiones a un proceso de servidor.

El puerto de origen de la solicitud de un cliente se genera de manera aleatoria. El número de puerto actúa como dirección de retorno para la aplicación que realiza la solicitud. La capa de transporte hace un seguimiento de este puerto y de la aplicación que generó la solicitud de manera que cuando se devuelva una respuesta, esta se envíe a la aplicación correcta.

El número de puerto de la aplicación que realiza la solicitud se utiliza como número de puerto de destino en la respuesta que vuelve del servidor.



Capítulo 7: Capa de Transporte 7.1.2.8 Direccionamiento de puertos TCP y UDP (cont.)

La Agencia de asignación de números por Internet (IANA) asigna números de puerto. IANA es un organismo normativo responsable de asegurar diferentes estándares de direccionamiento.

Existen diferentes tipos de números de puerto, como se muestra en la figura 1:

- Puertos bien conocidos (números del 0 al 1023):estos números se reservan para servicios y aplicaciones. Se utilizan comúnmente para aplicaciones como HTTP (servidor Web), protocolo de acceso a mensajes de Internet (IMAP) o protocolo simple de transferencia de correo (SMTP) (servidor de correo electrónico) y Telnet. Al definir estos puertos bien conocidos para las aplicaciones de los servidores, las aplicaciones cliente se pueden programar para solicitar una conexión a ese puerto en particular y el servicio relacionado.

- Puertos registrados (números del 1024 al 49151):estos números de puerto se asignan a procesos o aplicaciones del usuario. Principalmente, estos procesos son aplicaciones individuales que el usuario elige instalar en lugar de aplicaciones comunes que recibiría un número de puerto bien conocido.

  Cuando no se utilizan para un recurso del servidor, un cliente puede seleccionar estos puertos de forma dinámica como su puerto de origen.

- Puertos dinámicos o privados (números 49152 a 65535): también conocidos como puertos efímeros, generalmente se los asigna de forma dinámica a las aplicaciones cliente cuando el cliente inicia una conexión a un servicio.

  El puerto dinámico suele utilizarse para identificar la aplicación cliente durante la comunicación, mientras que el cliente utiliza el puerto bien conocido para identificar el servicio que se solicita en el servidor y conectarse a dicho servicio.

  No es común que un cliente se conecte a un servicio mediante un puerto dinámico o privado (aunque algunos programas de intercambio de archivos punto a punto lo hacen).

En la figura 2, se muestran algunos puertos bien conocidos y registrados comunes en TCP. En la figura 3, se muestran algunos puertos bien conocidos y registrados comunes en UDP.

Uso de TCP y UDP

Algunas aplicaciones pueden utilizar tanto TCP como UDP (figura 4). Por ejemplo, el bajo gasto de UDP permite que DNS atienda rápidamente varias solicitudes de clientes. Sin embargo, a veces el envío de la información solicitada puede requerir la confiabilidad de TCP. En este caso, el número de puerto bien conocido (53) lo utilizan ambos protocolos con este servicio.

Hay una lista de números de puerto y de aplicaciones asociadas en el sitio Web organizacional de la IANA.

Números de puerto

Rango de números de puerto	Grupo de puertos
Entre 0 y 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Números de puerto

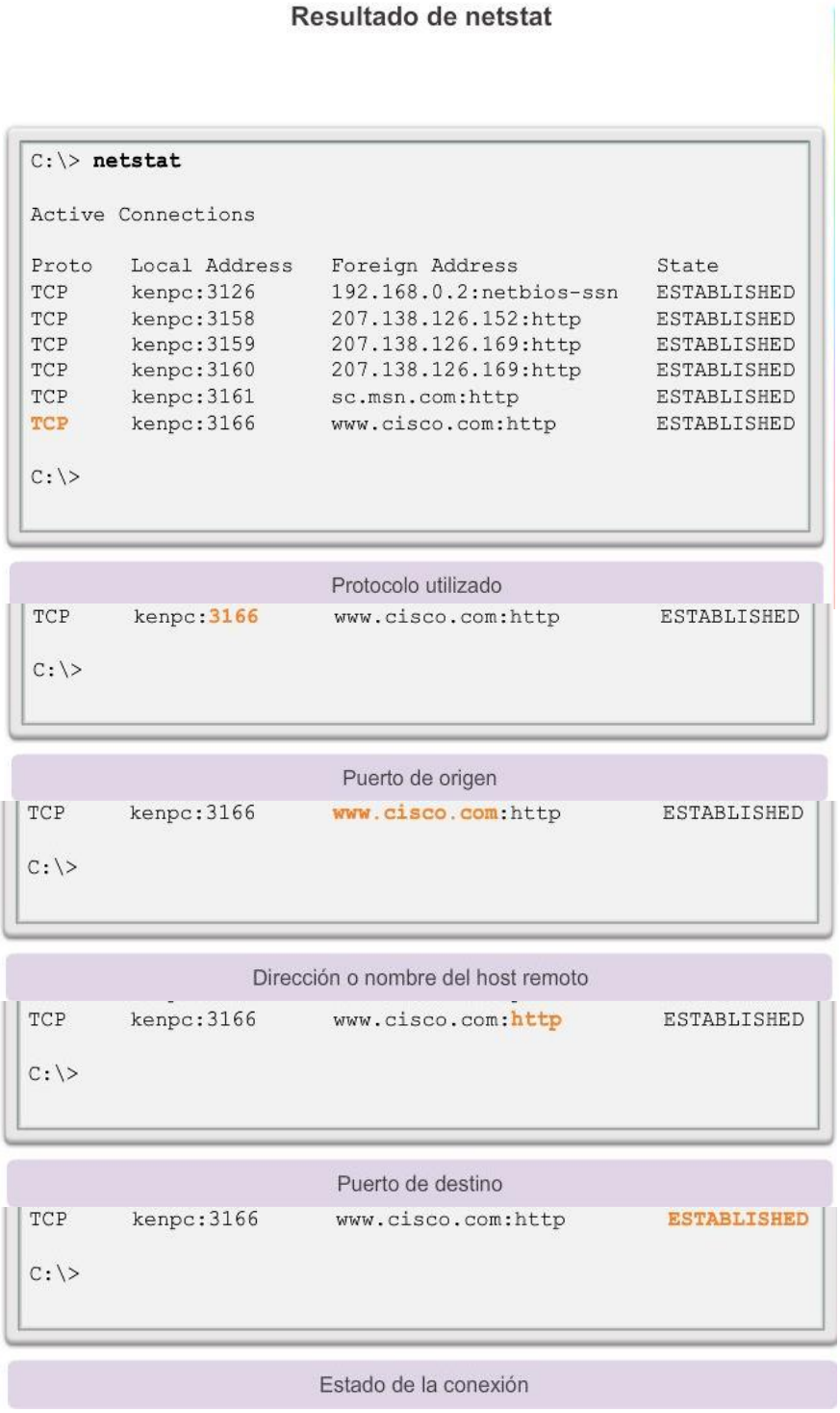
Rango de números de puerto	Grupo de puertos
Entre 0 y 1023	Puertos bien conocidos
de 1024 a 49151	Puertos registrados
de 49152 a 65535	Puertos privados y/o dinámicos

Capítulo 7: Capa de Transporte 7.1.2.9 Direccionamiento de puertos TCP y UDP (cont.)

A veces es necesario conocer las conexiones TCP activas que están abiertas y en ejecución en el host de red. Netstat es una utilidad de red importante que puede usarse para verificar esas conexiones. Netstat indica el protocolo que se está usando, la dirección y el número de puerto locales, la dirección y el número de puerto externos y el estado de la conexión.

Las conexiones TCP desconocidas pueden presentar una amenaza de seguridad grave, ya que pueden indicar que hay algo o alguien conectado al host local. Además, las conexiones TCP innecesarias pueden consumir recursos valiosos del sistema y, por lo tanto, enlentecer el rendimiento del host. Netstat debe utilizarse para examinar las conexiones abiertas de un host cuando el rendimiento parece estar comprometido.

Existen muchas opciones útiles para el comandonetstat. Haga clic en los botones en las figuras 1 a 5 para conocer la información que se muestra en los diferentes resultados del comando netstat.



Capítulo 7: Capa de Transporte 7.1.2.10 Segmentación TCP y UDP

En un capítulo anterior, se explicó la forma en que se construyen las unidades de datos del protocolo (PDU) mediante la transmisión de datos de una aplicación a través de los diversos protocolos para crear una PDU que después se transmita en el medio. En el host de destino, este proceso se revierte hasta que los datos se puedan transferir a la aplicación.

Algunas aplicaciones transmiten grandes cantidades de datos; en algunos casos, muchos gigabytes. Resultaría poco práctico enviar todos estos datos en una sola gran sección. No puede transmitirse ningún otro tráfico de red mientras se envían estos datos. Una gran sección de datos puede tardar minutos y hasta horas en enviarse. Además, si hubiese errores, se perdería el archivo de datos completo o habría que volver a

enviarlo. Los dispositivos de red no cuentan con buffers de memoria lo suficientemente grandes como para almacenar esa cantidad de datos durante la transmisión o recepción. El límite varía según la tecnología de red y el medio físico específico en uso.

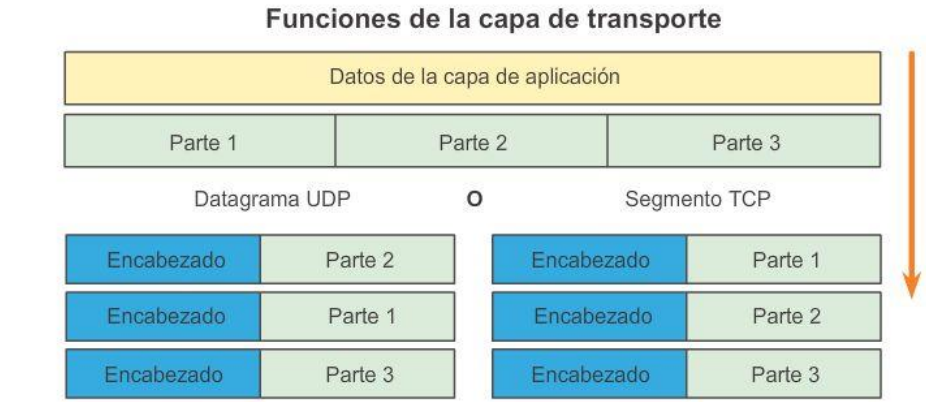
La división de datos de aplicación en segmentos asegura que estos se transmitan dentro de los límites de los medios y que los datos de diferentes aplicaciones se puedan multiplexar en los medios.

TCP y UDP: manejo distinto de la segmentación

Como se muestra en la ilustración, cada encabezado del segmento TCP contiene un número de secuencia que permite que las funciones de la capa de transporte en el host de destino vuelvan a armar segmentos en el orden en que se transmitieron. Esto asegura que la aplicación de destino tiene los datos en la misma forma que el emisor la planeó.

Aunque los servicios que utilizan UDP rastrean también las conversaciones entre las aplicaciones, no se encargan del orden en que se transmite la información ni de mantener una conexión. No existe número de secuencia en el encabezado UDP. UDP es un diseño simple y genera menos carga que TCP, lo que produce una transferencia de datos más rápida.

La información puede llegar en un orden distinto del de la transmisión, ya que los distintos paquetes pueden tomar diferentes rutas a través de la red. Una aplicación que utiliza UDP debe tolerar el hecho de que los datos no lleguen en el orden en el que fueron enviados.



La capa de transporte divide los datos en partes y agrega un encabezado para la entrega a través de la red.

Haga clic en los cuadros de encabezado azules para obtener más información.

Capítulo 7: Capa de Transporte 7.2.1.2 Procesos del servidor TCP

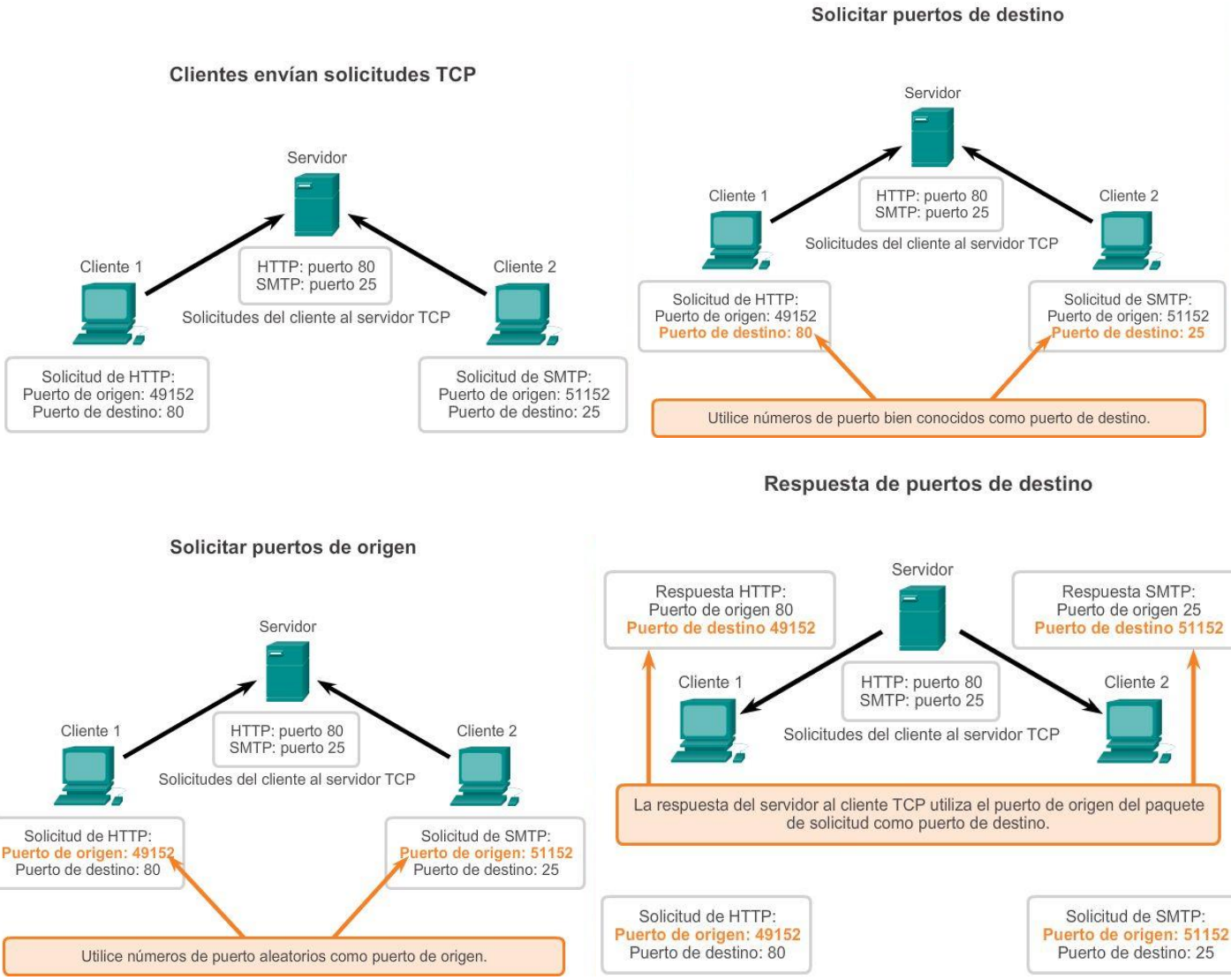
Los procesos de las aplicaciones se ejecutan en los servidores. Un único servidor puede ejecutar varios procesos de aplicaciones al mismo tiempo. Estos procesos esperan hasta que el cliente inicia comunicación con una solicitud de información u otros servicios.

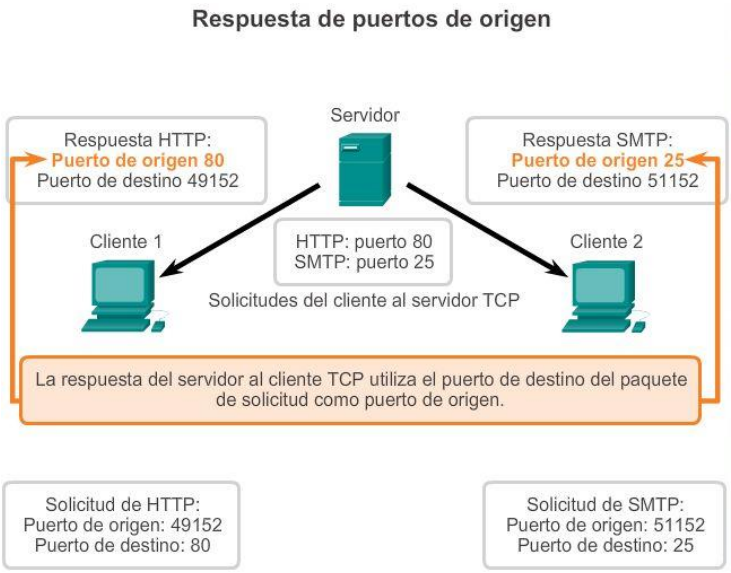
Cada proceso de aplicación que se ejecuta en el servidor se configura para utilizar un número de puerto, ya sea predeterminado o de forma manual por el administrador del sistema. Un servidor individual no puede tener dos servicios asignados al mismo número de puerto dentro de los mismos servicios de la capa de transporte. Un host que ejecuta una aplicación de servidor Web y una de transferencia de archivos no puede configurar ambas para utilizar el mismo puerto (por ejemplo, el puerto TCP 8.080). Una aplicación de servidor activa asignada a un puerto específico se considera abierta, lo que significa que la capa de transporte acepta y

procesa los segmentos dirigidos a ese puerto. Toda solicitud entrante de un cliente direccionada al socket correcto es aceptada y los datos se envían a la aplicación del servidor. Pueden existir varios puertos simultáneos abiertos en un servidor, uno para cada aplicación de servidor activa. Es común que un servidor proporcione más de un servicio al mismo tiempo, como un servidor Web y un servidor FTP.

Una manera de mejorar la seguridad en un servidor es restringir el acceso al servidor únicamente a aquellos puertos relacionados con los servicios y las aplicaciones a los que deben poder acceder los solicitantes autorizados.

Consulte las figuras 1 a 5 para ver la asignación típica de puertos de origen y de destino en las operaciones TCP de cliente y servidor.





Capítulo 7: Capa de Transporte 7.2.1.3 Establecimiento y finalización de la conexión TCP

En algunas culturas, cuando dos personas se conocen, generalmente se saludan dándose la mano. Ambas culturas entienden el acto de darse la mano como señal de un saludo amigable. Las conexiones en la red son similares. El primer enlace solicita la sincronización. El segundo enlace acusa recibo de la solicitud de sincronización inicial y sincroniza los parámetros de conexión en la dirección opuesta. El tercer segmento de enlace es un acuse de recibo que se utiliza para informarle al destino que ambos lados están de acuerdo en que se estableció una conexión.

Cuando dos hosts se comunican utilizando TCP, se establece una conexión antes de que puedan intercambiarse los datos. Luego de que se completa la comunicación, se cierran las sesiones y la conexión finaliza. Los mecanismos de conexión y sesión habilitan la función de confiabilidad de TCP. Vea en la figura los pasos para establecer y terminar una conexión del TCP.

Los hosts hacen un seguimiento de cada segmento de datos dentro de una sesión e intercambian información sobre qué datos se reciben mediante la información del encabezado TCP. TCP es un protocolo full-duplex, en el que cada conexión representa dos streams de comunicación unidireccionales, o sesiones. Para establecer la conexión los hosts realizan un protocolo de enlace de tres vías. Los bits de control en el encabezado TCP indican el progreso y estado de la conexión. Enlace de tres vías:

- Establece que el dispositivo de destino se presente en la red
- Verifica que el dispositivo de destino tenga un servicio activo y que acepte solicitudes en el número de puerto de destino que el cliente de origen intenta utilizar para la sesión
- Informa al dispositivo de destino que el cliente de origen intenta establecer una sesión de comunicación en dicho número de puerto

En las conexiones TCP, el cliente del host establece la conexión con el servidor. Los tres pasos en el establecimiento de una conexión TCP son:

Paso 1. El cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.

Paso 2. El servidor acusa recibo de la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.

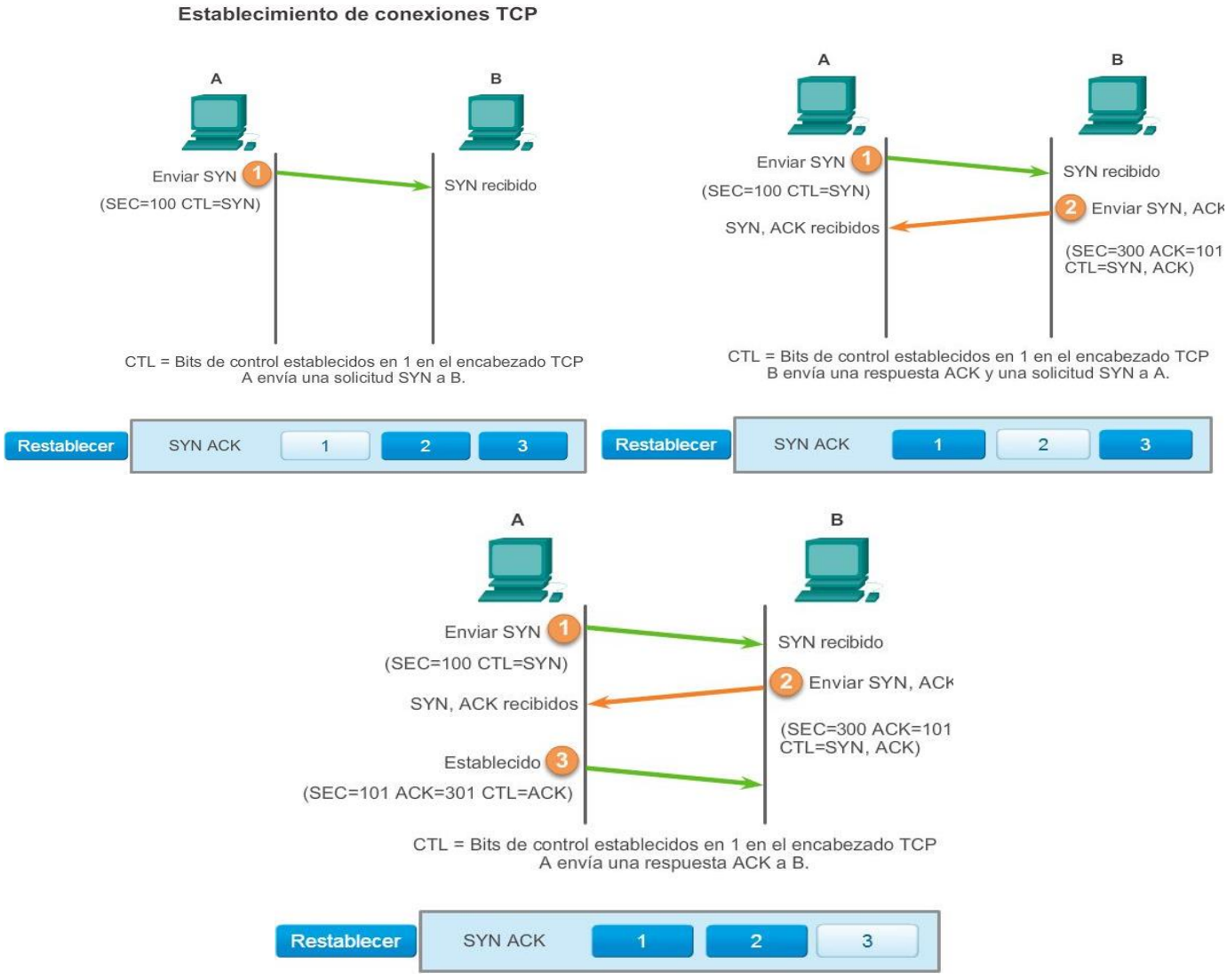
Paso 3. El cliente de origen acusa recibo de la sesión de comunicación de servidor a cliente.

En la ilustración, haga clic en los botones 1 a 3 para ver el establecimiento de la conexión TCP.

Para comprender el proceso de enlace de tres vías, observe los diversos valores que intercambian ambos hosts. Dentro del encabezado del segmento TCP, existen seis campos de 1 bit que contienen información de control utilizada para gestionar los procesos de TCP. Estos campos son los siguientes:

- URG: campo indicador urgente importante
- ACK: campo de acuse de recibo importante
- PSH: función de empuje
- RST: restablecer la conexión
- SYN: sincronizar números de secuencia
- FIN: no hay más datos del emisor

Los campos ACK y SYN son importantes para el análisis del protocolo de enlace de tres vías.



Capítulo 7: Capa de Transporte 7.2.1.4 Análisis del protocolo TCP de enlace de tres vías: paso 1

Mediante el resultado del software de análisis de protocolos, como los resultados de Wireshark, se puede examinar la operación del protocolo TCP de enlace de tres vías:

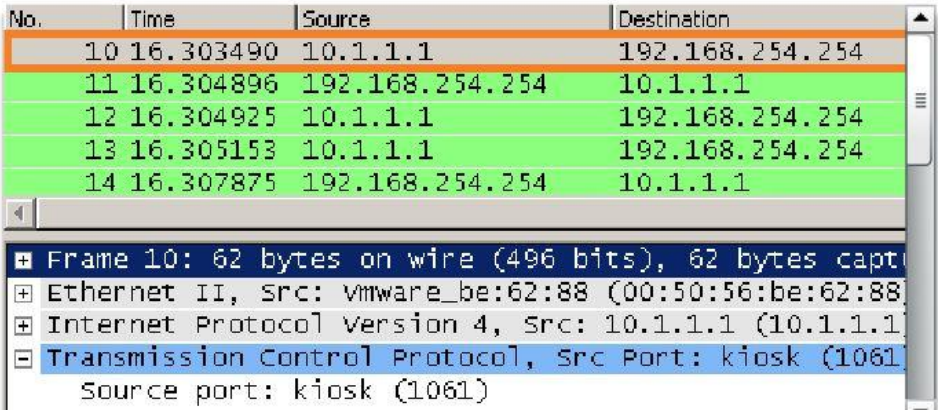
Paso 1: El cliente de origen solicita una sesión de comunicación de cliente a servidor con el servidor.

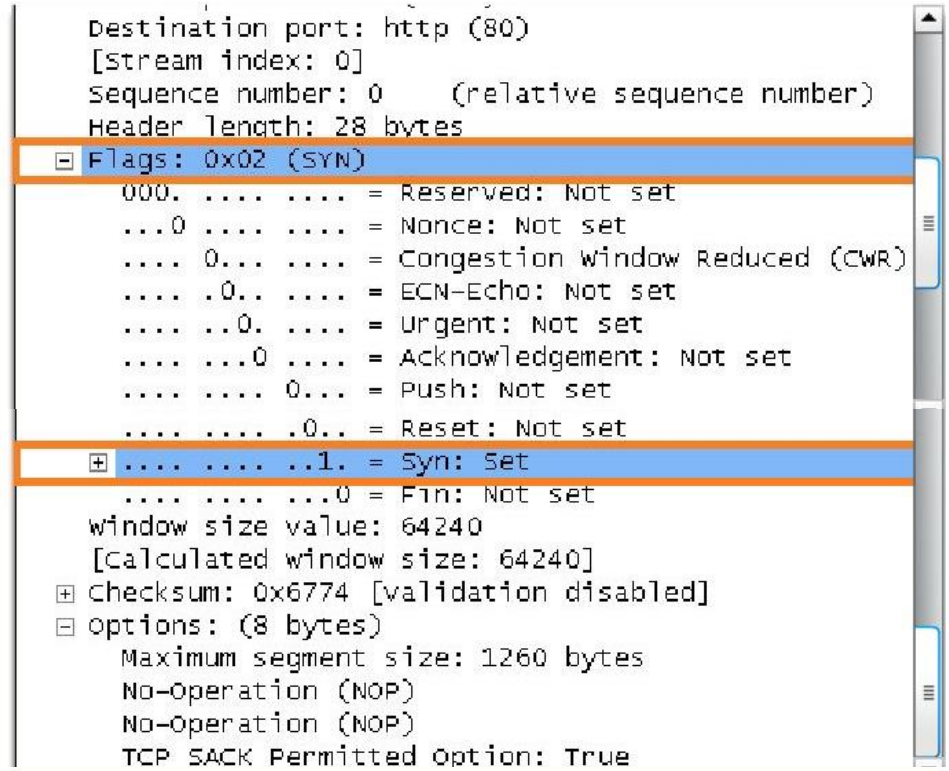
Un cliente TCP inicia un protocolo de enlace de tres vías al enviar un segmento con el indicador de control de sincronizar números de secuencia (SYN) establecido, lo que indica un valor inicial en el campo de número de secuencia en el encabezado. Este valor inicial para el número de secuencia, conocido como número de secuencia inicial (ISN), se elige de manera aleatoria y se utiliza para comenzar a rastrear el flujo de datos de esta sesión desde el cliente hasta el servidor. El ISN en el encabezado de cada segmento se incrementa en uno por cada byte de datos enviados desde el cliente hacia el servidor mientras continúa la conversación de datos.

Como se muestra en la figura, el resultado de un analizador de protocolos muestra el señalizador de control SYN y el número de secuencia relativa.

El indicador de control SYN está establecido y el número de secuencia relativa está en 0. Aunque el analizador de protocolos en el gráfico indique los valores relativos para los números de secuencia y de acuse de recibo, los verdaderos valores son números binarios de 32 bits. En la ilustración, se muestran los cuatro bytes representados en un valor hexadecimal.

Protocolo TCP de enlace de tres vías (SYN)





Un analizador de protocolos muestra la solicitud del cliente inicial para la sesión en la trama 10

En el segmento TCP de esta trama se muestra lo siguiente:

- El indicador SYN está establecido para validar un número de secuencia inicial.
- El número de secuencia seleccionado aleatoriamente es válido (el valor relativo es 0).
- El puerto de origen aleatorio es 1061.
- El puerto de destino bien conocido es 80 (puerto HTTP); indica el servidor Web (httpd).

Capítulo 7: Capa de Transporte 7.2.1.5 Análisis del protocolo TCP de enlace de tres vías:

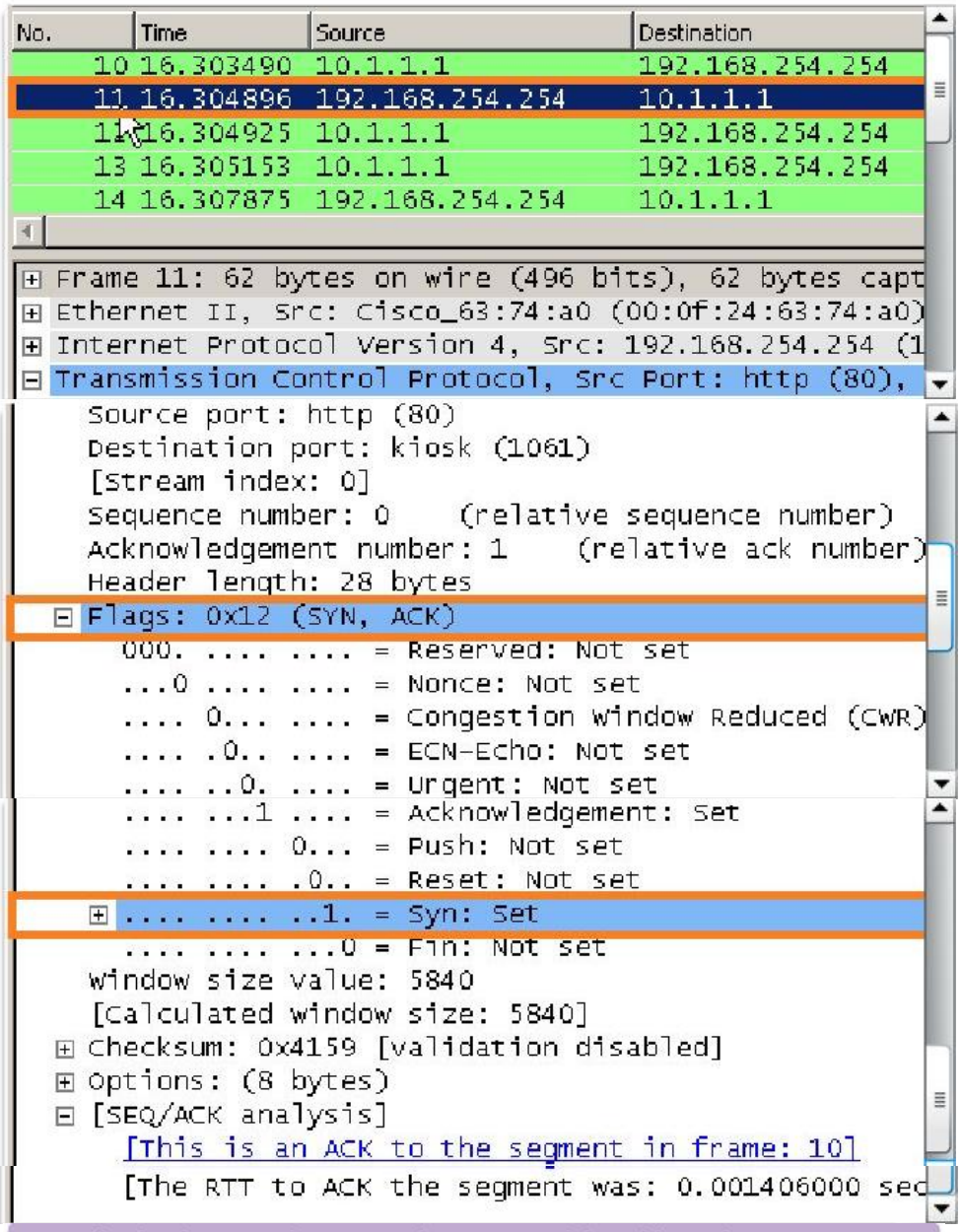
Paso 2: El servidor reconoce la sesión de comunicación de cliente a servidor y solicita una sesión de comunicación de servidor a cliente.

El servidor TCP debe dar acuse de recibo del segmento SYN del cliente para establecer la sesión de cliente a servidor. Para hacerlo, el servidor envía un segmento al cliente con el indicador de acuse de recibo (ACK) establecido que indica que el número de acuse de recibo es significativo. Con este señalizador establecido en el segmento, el cliente interpreta esto como acuse de recibo de que el servidor ha recibido el SYN del cliente TCP.

El valor del campo de número de acuse de recibo es igual al ISN más 1. Esto establece una sesión del cliente al servidor. El indicador ACK permanece establecido para mantener el equilibrio de la sesión. Recuerde que la conversación entre el cliente y el servidor son, en realidad, dos sesiones unidireccionales: una del cliente al servidor y otra del servidor al cliente. En este segundo paso del protocolo de enlace de tres vías, el servidor debe iniciar la respuesta al cliente. Para comenzar esta sesión, el servidor utiliza el señalizador SYN de la misma manera en que lo hizo el cliente. Establece el señalizador de control SYN en el encabezado para establecer una sesión del servidor al cliente. El señalizador SYN indica que el valor inicial del campo de número de secuencia se encuentra en el encabezado. Este valor se utiliza para hacer un seguimiento del flujo de datos en esta sesión del servidor al cliente.

Como se muestra en la ilustración, el resultado del analizador de protocolos muestra que se establecieron los indicadores de control ACK y SYN y que se muestran los números de acuse de recibo y de secuencia relativa.

Protocolo TCP de enlace de tres vías (SYN, ACK)



Un analizador de protocolos muestra la respuesta del servidor en la trama 11

- El indicador ACK está establecido para indicar un número válido de acuse de recibo.
- Respuesta de número de acuse de recibo al número de secuencia inicial como valor relativo de 1.
- El indicador SYN está establecido para indicar el número de secuencia inicial de la sesión de servidor a cliente.
- El número de puerto de destino 1061 corresponde al puerto de origen del cliente.
- El número de puerto de origen 80 (HTTP) indica el servicio del servidor Web (httpd).

Capítulo 7: Capa de Transporte 7.2.1.6 Análisis del protocolo TCP de enlace de tres vías:

Paso 3: El cliente de origen reconoce la sesión de comunicación de servidor a cliente.

Por último, el cliente TCP responde con un segmento que contiene un ACK que actúa como respuesta al SYN de TCP enviado por el servidor. No existen datos de usuario en este segmento. El valor del campo de número

de acuse de recibo contiene uno más que el ISN recibido del servidor. Una vez que se establecen ambas sesiones entre el cliente y el servidor, todos los segmentos adicionales que se intercambian en esta comunicación tendrán establecido el indicador ACK.

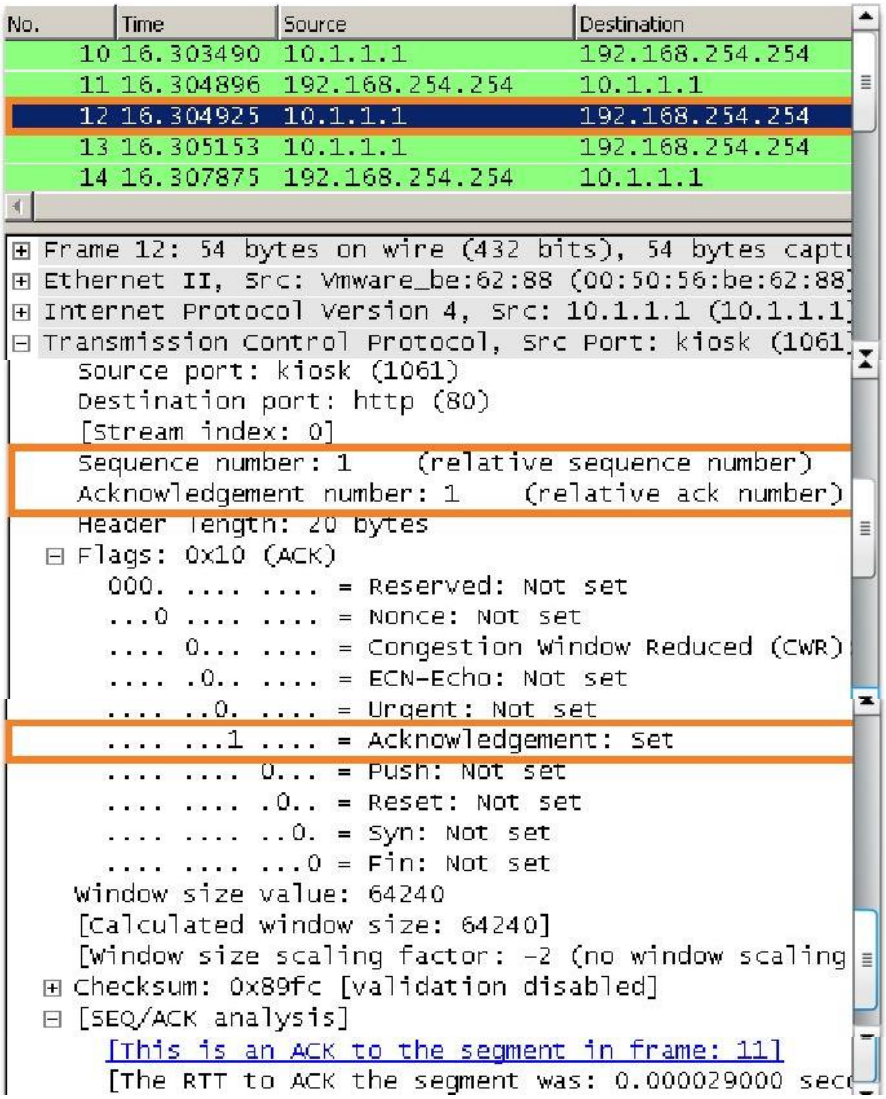
Como se muestra en la ilustración, el resultado del analizador de protocolos muestra el indicador de control ACK establecido y los números de acuse de recibo y de secuencia relativa.

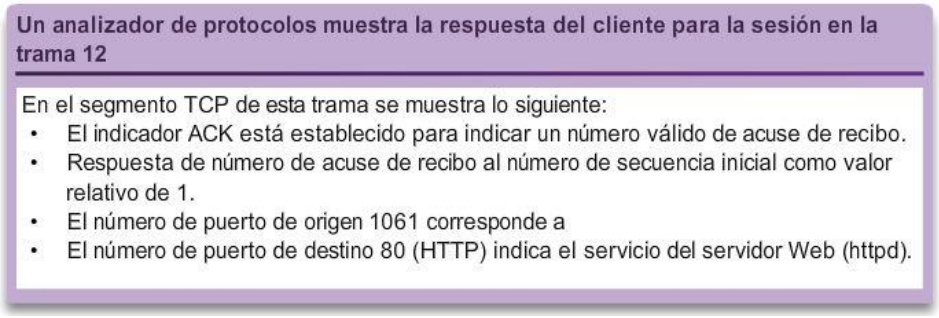
Se puede añadir seguridad a la red de datos de la siguiente manera:

- Denegar el establecimiento de sesiones del TCP
- Permitir sólo sesiones que se establezcan para servicios específicos
- Permitir sólo tráfico como parte de sesiones ya establecidas

Estas medidas de seguridad se pueden implementar para todas las sesiones TCP o solo para las sesiones seleccionadas.

Protocolo TCP de enlace de tres vías (ACK)





Capítulo 7: Capa de Transporte 7.2.1.7 Análisis de terminación de sesión TCP

Para cerrar una conexión, se debe establecer el indicador de control finalizar (FIN) en el encabezado del segmento. Para finalizar todas las sesiones TCP de una vía, se utiliza un enlace de dos vías, que consta de un segmento FIN y un segmento ACK.

Por lo tanto, para terminar una única conversación que admite TCP, se requieren cuatro intercambios para finalizar ambas sesiones, como se muestra en la figura 1.

Nota: en esta explicación, los términos “cliente” y “servidor” se utilizan como referencia con fines de simplificación, pero el proceso de finalización lo pueden iniciar dos hosts cualesquiera que tengan una sesión abierta:

Paso 1: cuando el cliente no tiene más datos para enviar en el stream, envía un segmento con el indicador FIN establecido.

Paso 2: el servidor envía un ACK para acusar recibo del FIN y terminar la sesión de cliente a servidor.

Paso 3: el servidor envía un FIN al cliente para terminar la sesión de servidor a cliente.

Paso 4: el cliente responde con un ACK para dar acuse de recibo del FIN desde el servidor.

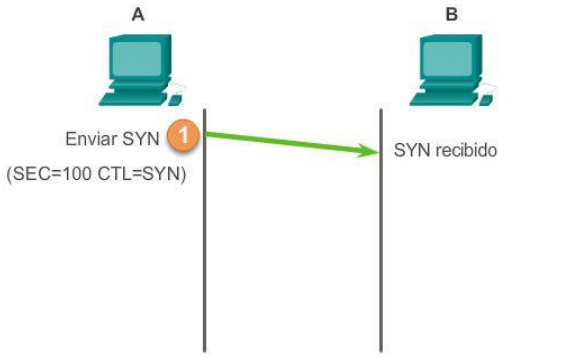
Cuando el cliente no tiene más datos que transferir, establece el indicador FIN en el encabezado de un segmento. A continuación, el extremo servidor de la conexión envía un segmento normal que contiene datos con el indicador ACK establecido utilizando el número de acuse de recibo, lo que confirma que se recibieron todos los bytes de datos. Cuando se dio acuse de recibo de todos los segmentos, la sesión se cierra.

La sesión en la otra dirección se cierra con el mismo proceso. El receptor indica que no existen más datos para enviar estableciendo el señalizador FIN en el encabezado del segmento enviado al origen. Un acuse de recibo devuelto confirma que todos los bytes de datos se recibieron y que la sesión, a su vez, finalizó.

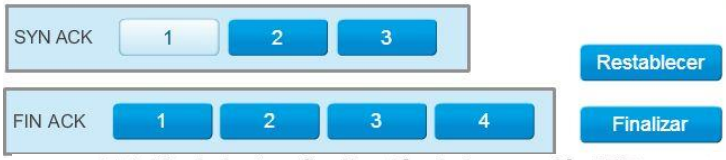
Consulte las figuras 2 y 3 para ver los indicadores de control FIN y ACK establecidos en el encabezado del segmento, lo que finaliza la sesión HTTP.

También es posible terminar la conexión por medio de un enlace de tres vías. Cuando el cliente no posee más datos para enviar, envía un señalizador FIN al servidor. Si el servidor tampoco tiene más datos para enviar, puede responder con los señalizadores FIN y ACK, combinando dos pasos en uno. A continuación, el cliente responde con un ACK.

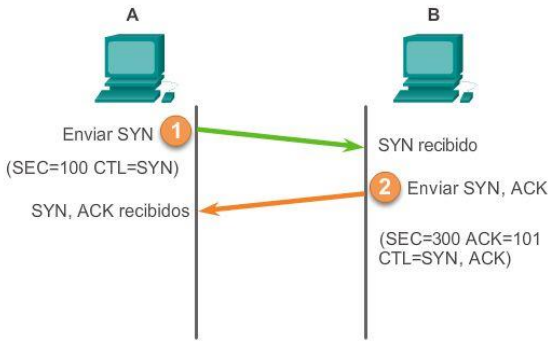
Establecimiento y finalización de la conexión TCP



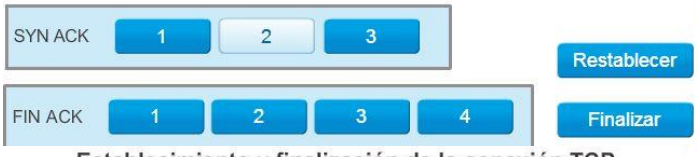
CTL = Bits de control establecidos en 1 en el encabezado TCP
A envía una solicitud SYN a B.



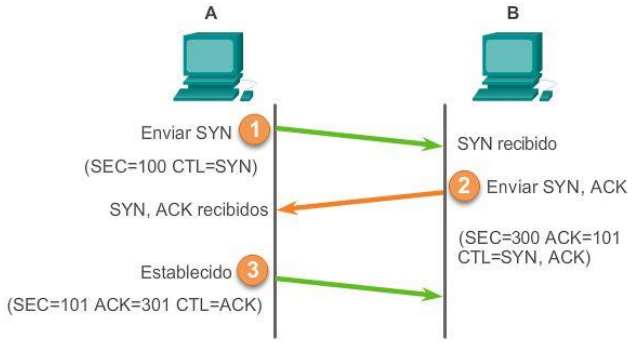
Establecimiento y finalización de la conexión TCP



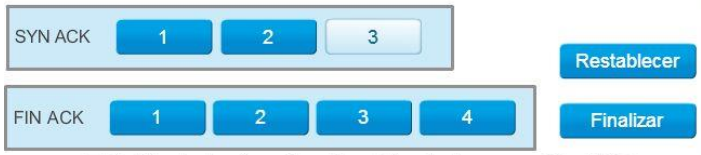
CTL = Bits de control establecidos en 1 en el encabezado TCP
B envía una respuesta ACK y una solicitud SYN a A.



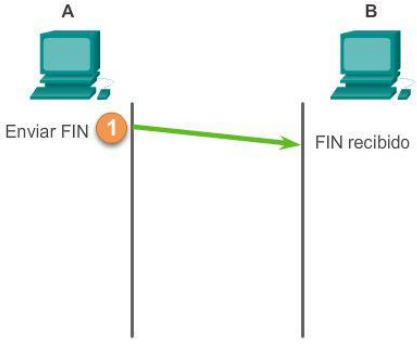
Establecimiento y finalización de la conexión TCP



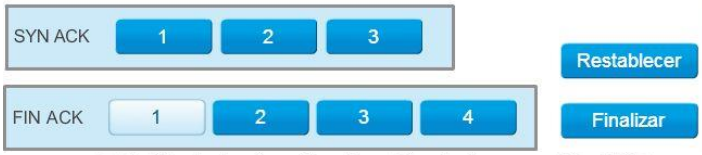
CTL = Bits de control establecidos en 1 en el encabezado TCP
A envía una respuesta ACK a B.



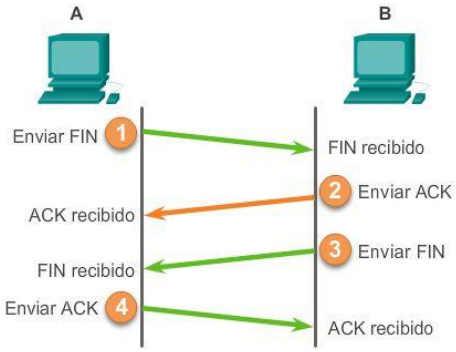
Establecimiento y finalización de la conexión TCP



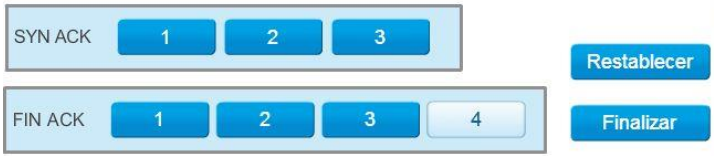
A envía una solicitud FIN a B.



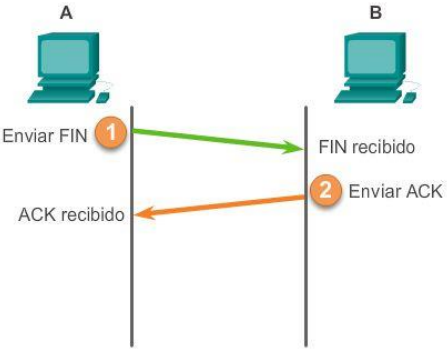
Establecimiento y finalización de la conexión TCP

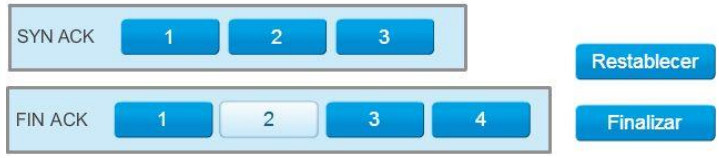


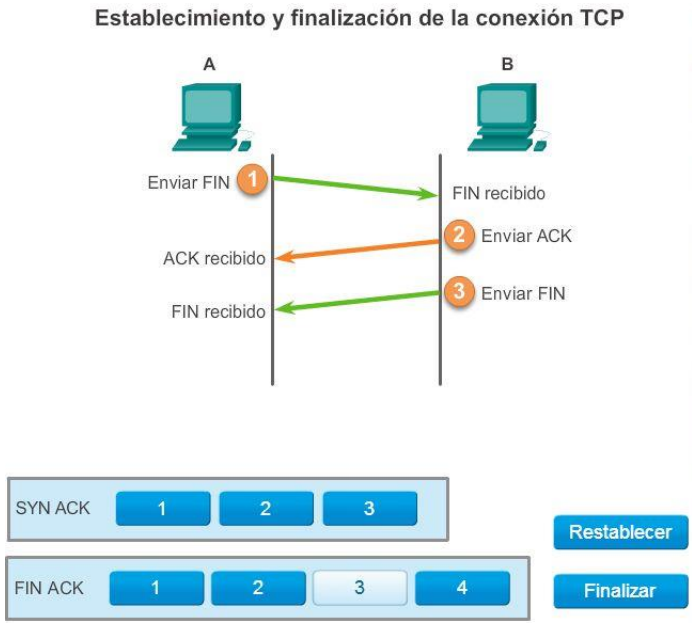
A envía una respuesta ACK a B.



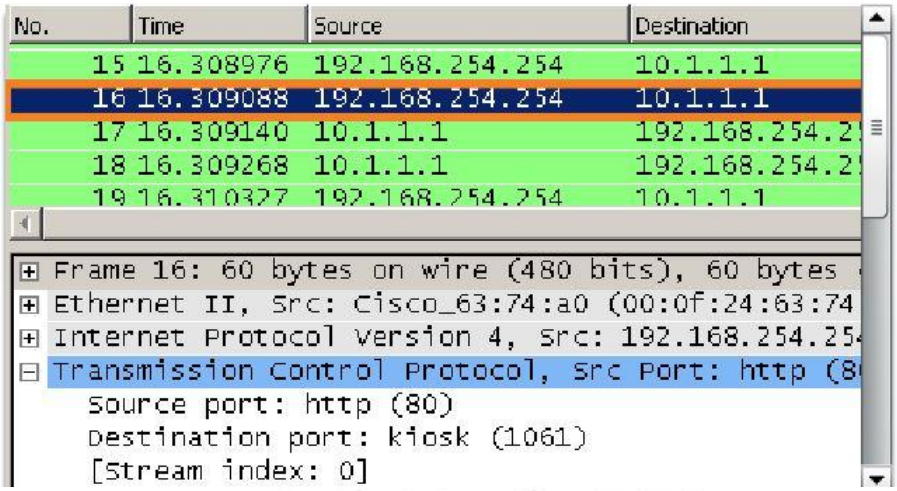
Establecimiento y finalización de la conexión TCP



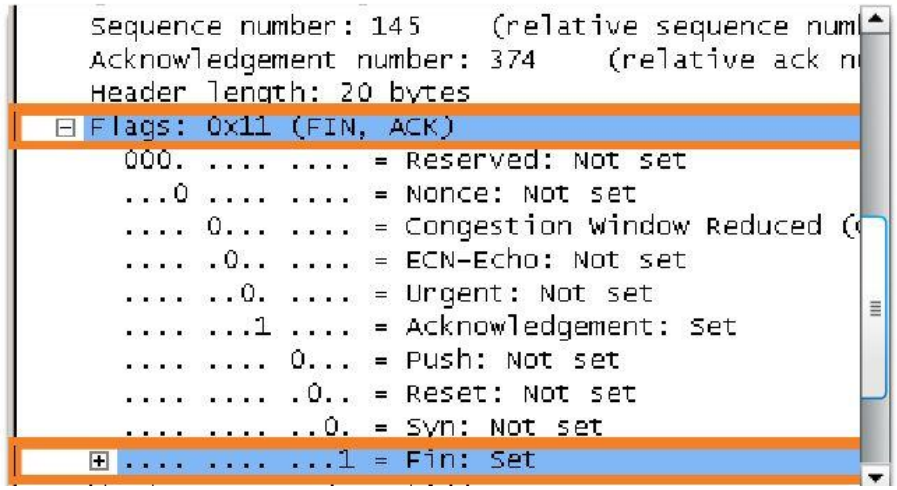


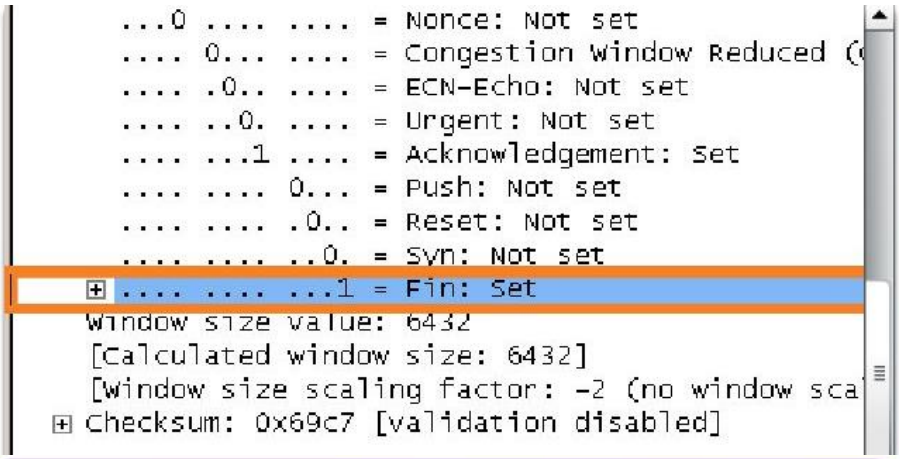


Terminación de la sesión TCP (FIN)



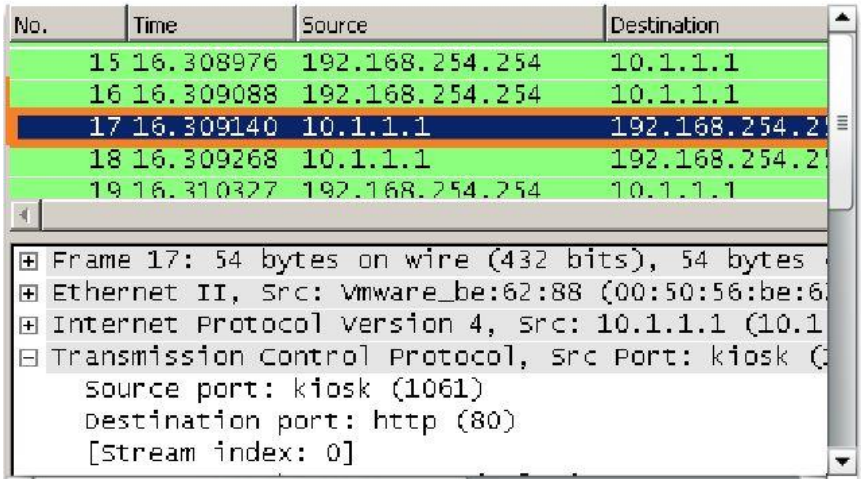
Terminación de la sesión TCP (FIN)



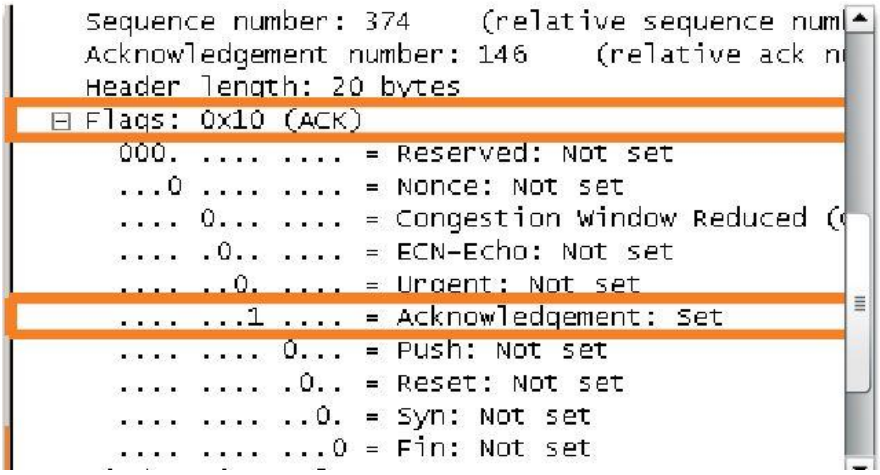


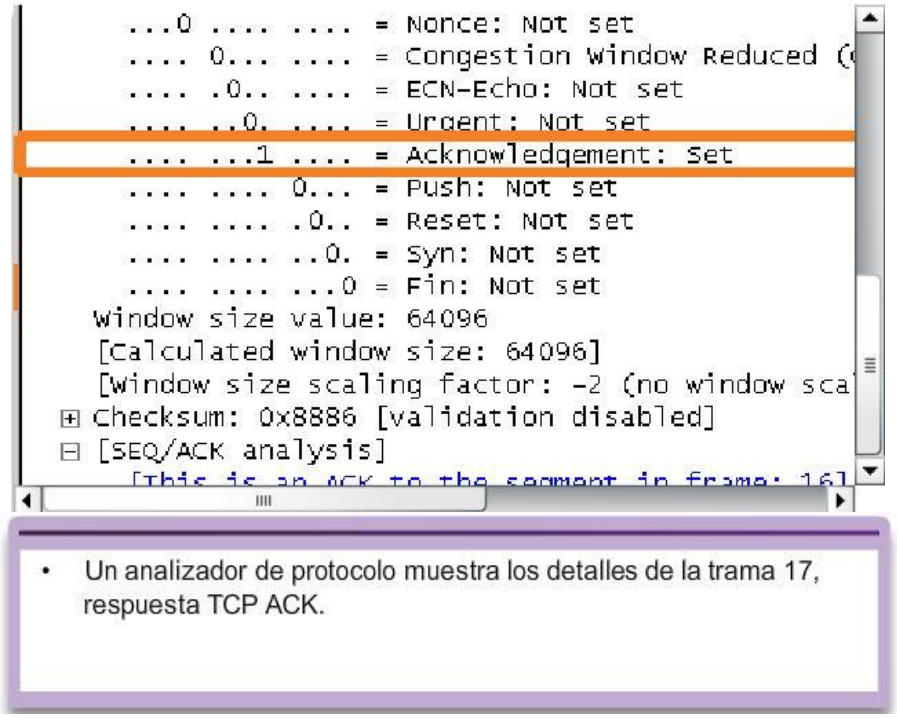
- Un analizador de protocolo muestra los detalles de la trama 16, solicitud TCP FIN.

Terminación de la sesión TCP (ACK)



Terminación de la sesión TCP (ACK)





Capítulo 7: Capa de Transporte 7.2.2.1 Confiabilidad de TCP: entrega ordenada

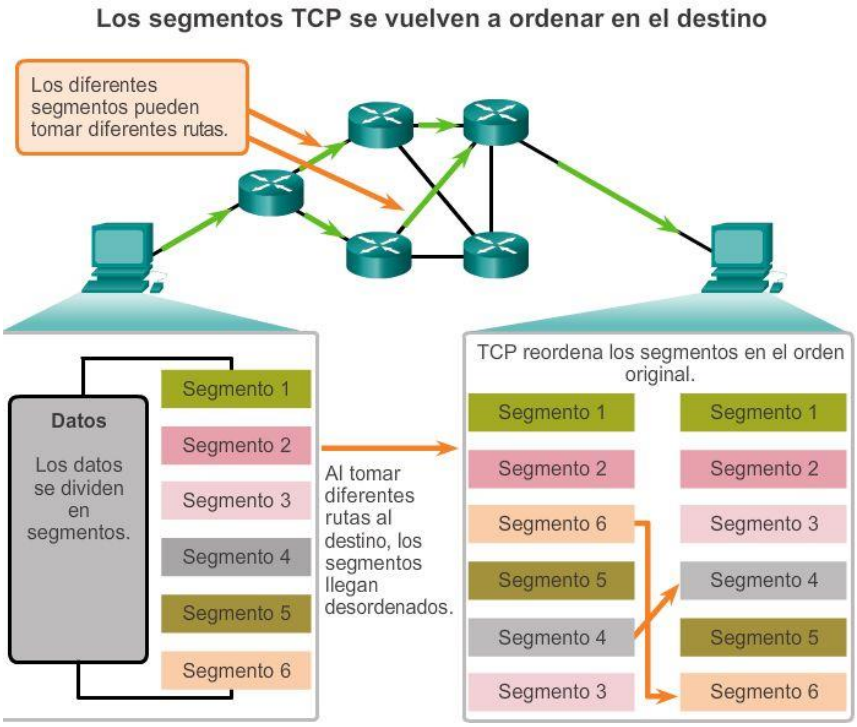
Reordenamiento de segmentos

Cuando los servicios envían datos mediante el TCP, los segmentos pueden llegar a su destino en desorden. Para que el receptor comprenda el mensaje original, los datos en estos segmentos se reensamblan en el orden original. Para lograr esto, se asignan números de secuencia en el encabezado de cada paquete.

Durante la configuración de la sesión, se establece un número de secuencia inicial (ISN). Este ISN representa el valor inicial para los bytes para esta sesión que se transmite a la aplicación receptora. A medida que se transmiten los datos durante la sesión, el número de secuencia se incrementa en el número de bytes que se han transmitido. Este seguimiento de bytes de datos permite identificar y dar acuse de recibo de cada segmento de manera exclusiva. Se pueden identificar segmentos perdidos.

Los números de secuencia de segmento habilitan la confiabilidad al indicar cómo rearmar y reordenar los segmentos recibidos, como se muestra en la ilustración.

El proceso TCP receptor coloca los datos del segmento en un búfer de recepción. Los segmentos se colocan en el orden de número de secuencia correcto y se pasan a la capa de aplicación cuando se rearman. Todos los segmentos que llegan con números de secuencia no contiguos se mantienen para su posterior procesamiento. A continuación, cuando llegan los segmentos con bytes faltantes, tales segmentos se procesan en orden.



Capítulo 7: Capa de Transporte 7.2.2.2 Confiabilidad de TCP: reconocimiento y tamaño de la ventana

Confirmación de recepción de segmentos

Una de las funciones de TCP es garantizar que cada segmento llegue a destino. Los servicios de TCP en el host de destino envían un acuse de recibo de los datos que recibe la aplicación de origen.

El número de secuencia (SEQ) y el número de acuse de recibo (ACK) se utilizan juntos para confirmar la recepción de los bytes de datos contenidos en los segmentos transmitidos. El número de SEQ indica la cantidad relativa de bytes que se transmitieron en esta sesión, incluso los bytes en el segmento actual. TCP utiliza el número de ACK reenviado al origen para indicar el próximo byte que el receptor espera recibir. Esto se llama acuse de recibo de expectativa.

Se le informa al origen que el destino recibió todos los bytes de este stream de datos, hasta el byte especificado por el número de ACK, pero sin incluirlo. Se espera que el host emisor envíe un segmento que utiliza un número de secuencia que es igual al número de ACK.

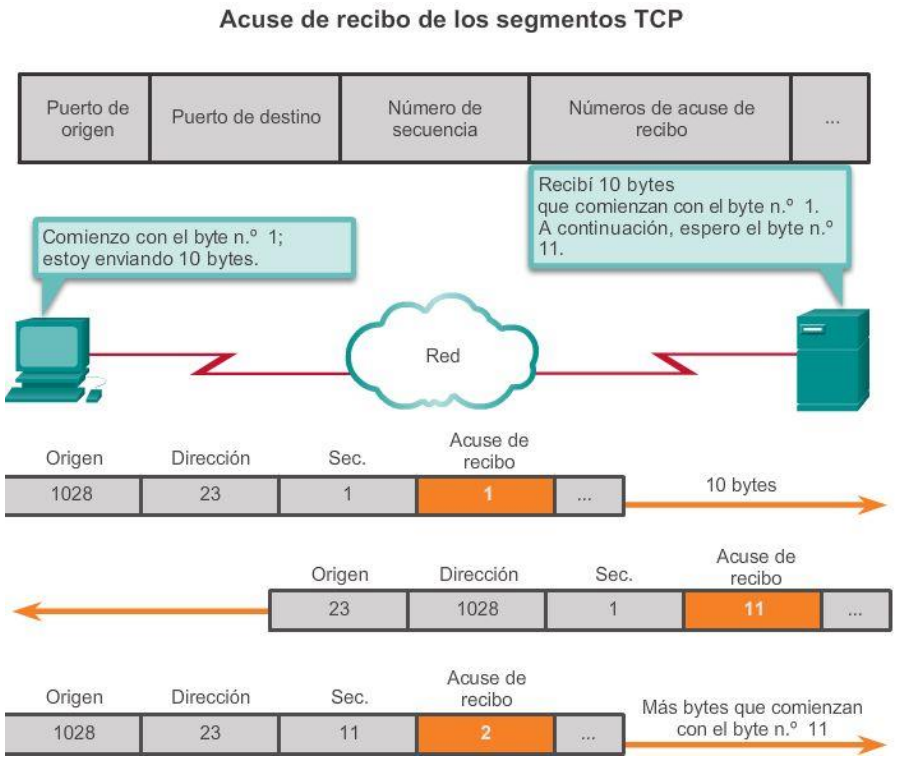
Recuerde que cada conexión son realmente dos sesiones de una vía. Los números de SEQ y ACK se intercambian en ambas direcciones.

En el ejemplo de la figura, el host de la izquierda envía datos al host de la derecha. Envía un segmento que contiene 10 bytes de datos para esta sesión y un número de secuencia igual a 1 en el encabezado.

El host receptor recibe el segmento en la capa 4 y determina que el número de secuencia es 1 y que tiene 10 bytes de datos. Luego el host envía un segmento de vuelta al host de la izquierda para acusar recibo de estos datos. En este segmento, el host establece el número de ACK en 11 para indicar que el siguiente byte de datos que espera recibir en esta sesión es el byte número 11. Cuando el host emisor recibe este acuse de recibo, puede enviar el próximo segmento que contiene datos para esta sesión a partir del byte 11.

En este ejemplo, si el host emisor tuviera que esperar el acuse de recibo de cada uno de los 10 bytes, la red tendría mucha sobrecarga. Para reducir la sobrecarga de estos acuses de recibo, pueden enviarse varios segmentos de datos y dar acuse de recibo de estos con un único mensaje de TCP en la dirección opuesta. Este acuse de recibo contiene un número de ACK que se basa en la cantidad total de bytes recibidos en la sesión. Por ejemplo, si se comienza con un número de secuencia 2000, si se reciben 10 segmentos de 1000 bytes cada uno, se devolverá al origen un número de ACK igual a 12 001.

La cantidad de datos que un origen puede transmitir antes de recibir un acuse de recibo se denomina “tamaño de la ventana”, que es un campo en el encabezado TCP que permite administrar datos perdidos y controlar el flujo.



Capítulo 7: Capa de Transporte 7.2.2.3 Confiabilidad de TCP: pérdida y retransmisión de datos

Manejo de segmentos perdidos

La pérdida de datos se produce en ocasiones, sin importar qué tan bien diseñada esté la red; por lo tanto, TCP proporciona métodos para administrar estas pérdidas de segmentos. Entre estos está un mecanismo para retransmitir segmentos con datos sin acuse de recibo.

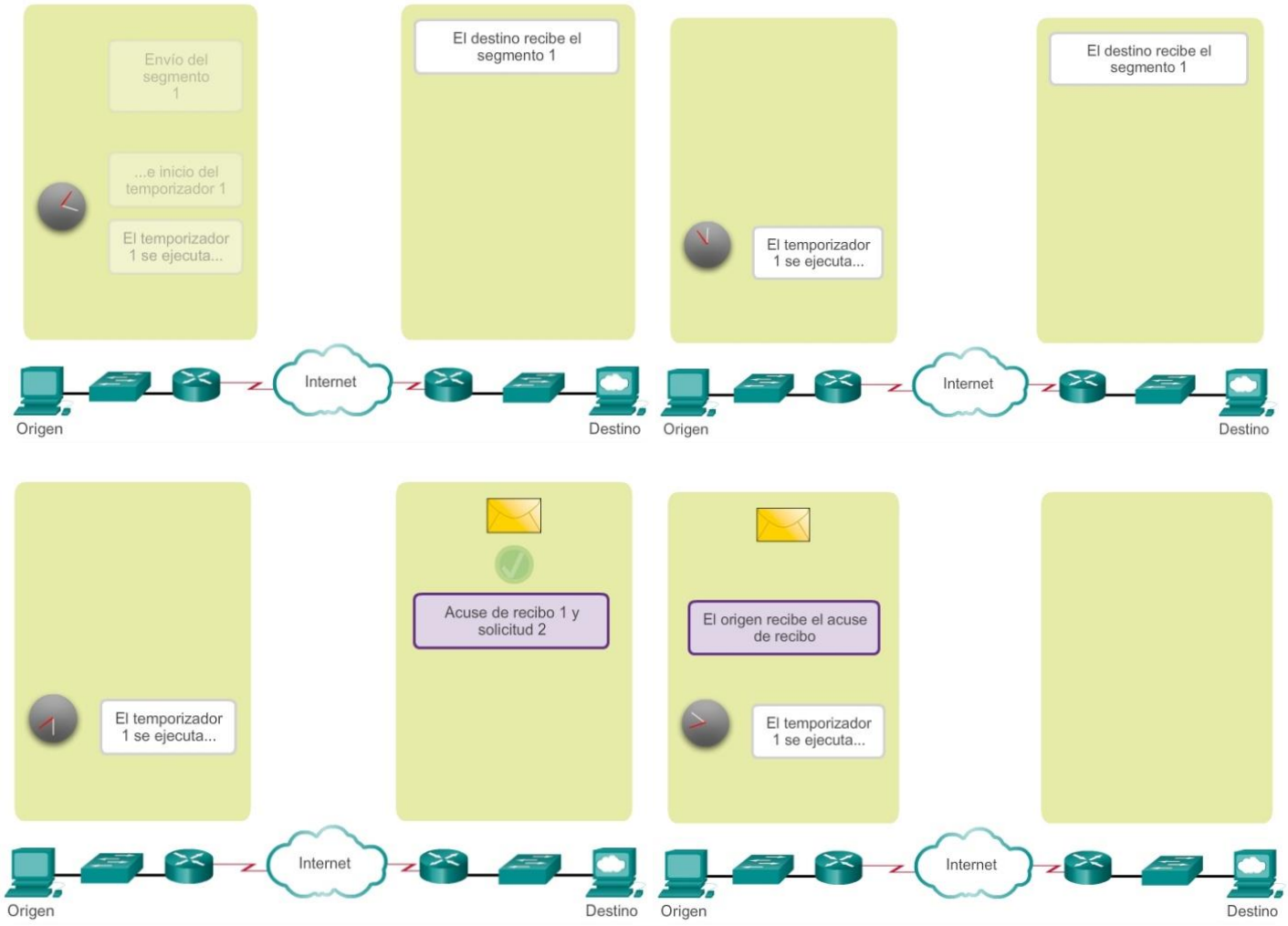
Un servicio de host de destino que utiliza TCP generalmente sólo da acuse de recibo de datos para bytes de secuencia continuos. Si faltan uno o más segmentos, solo se hace acuse de recibo de los datos en la primera secuencia contigua de bytes. Por ejemplo, si se reciben segmentos con números de secuencia de 1500 a 3000 y de 3400 a 3500, el número de ACK sería 3001. Esto se debe a que hay segmentos con números de SEQ de 3001 a 3399 que no se recibieron.

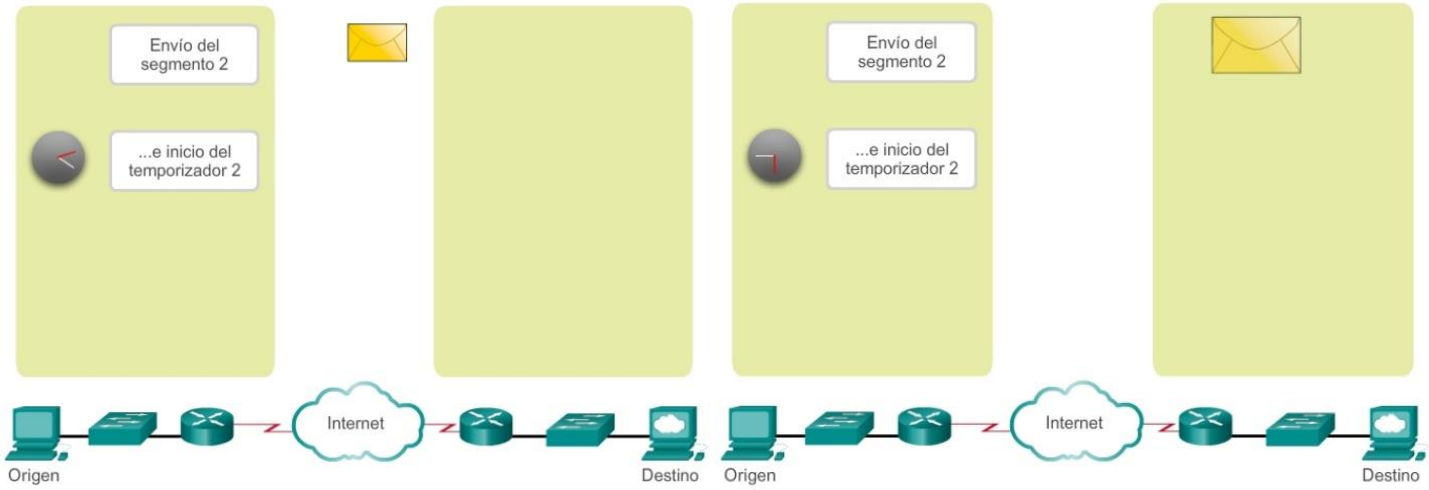
Cuando el TCP en el host de origen no recibe un acuse de recibo después de una cantidad de tiempo predeterminada, este vuelve al último número de ACK recibido y vuelve a transmitir los datos desde ese punto en adelante. La solicitud de comentarios (RFC) no especifica el proceso de retransmisión, pero se deja a criterio de la implementación particular del TCP.

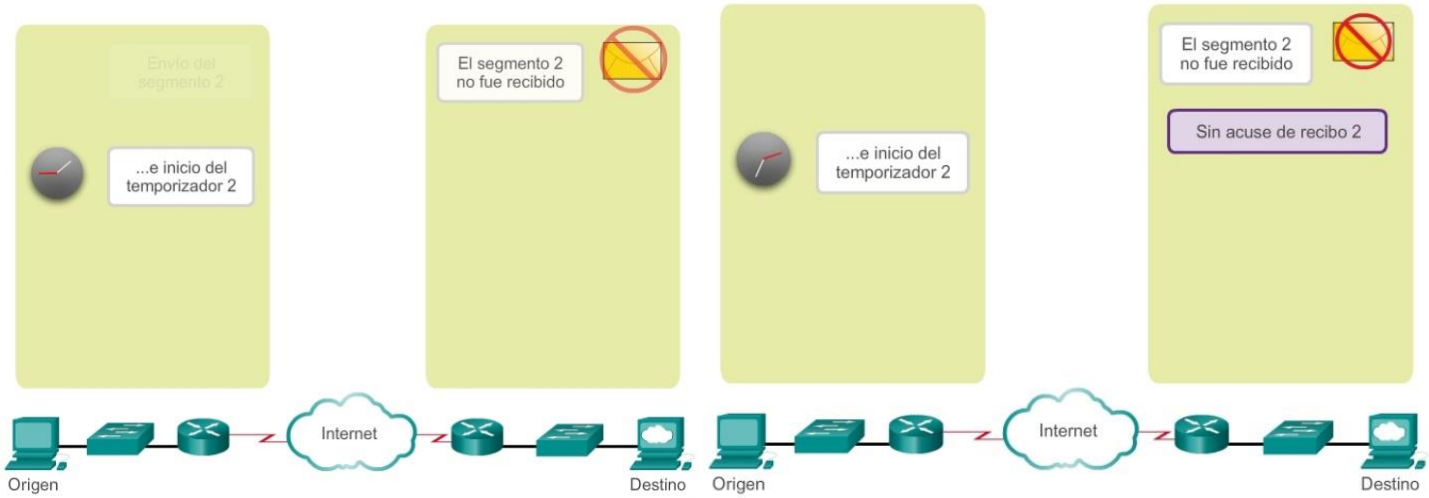
Para una implementación de TCP típica, un host puede transmitir un segmento, colocar una copia del segmento en una cola de retransmisión e iniciar un temporizador. Cuando se recibe el acuse de recibo de los datos, se elimina el segmento de la cola. Si no se recibe el acuse de recibo antes de que el temporizador venza, el segmento es retransmitido.

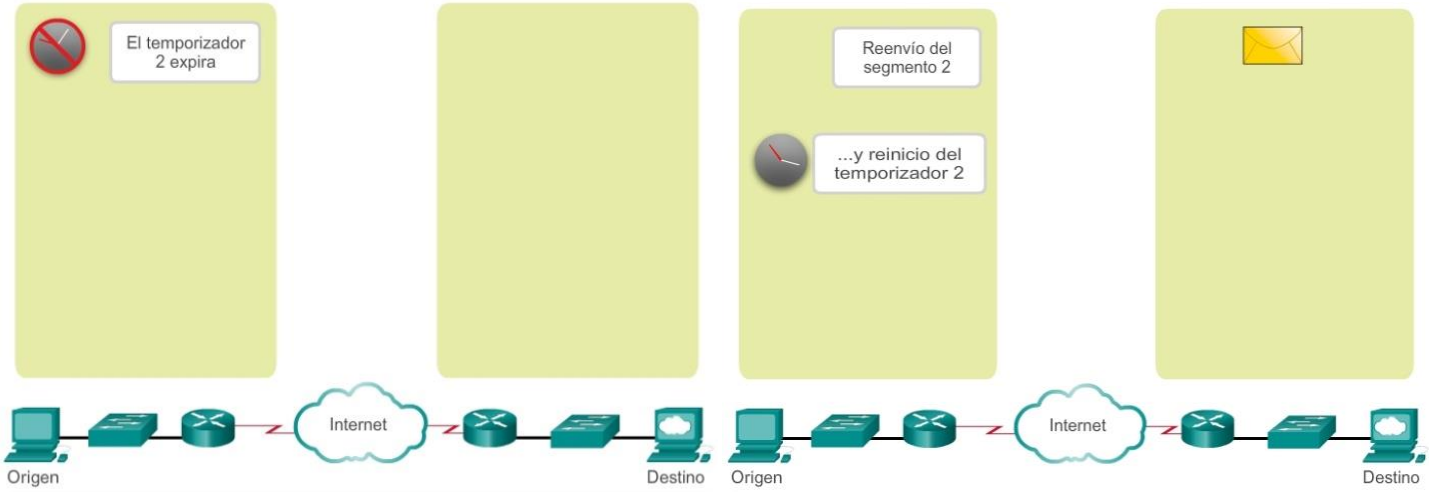
Haga clic en el botón Reproducir en la ilustración para ver una animación de la retransmisión de segmentos perdidos.

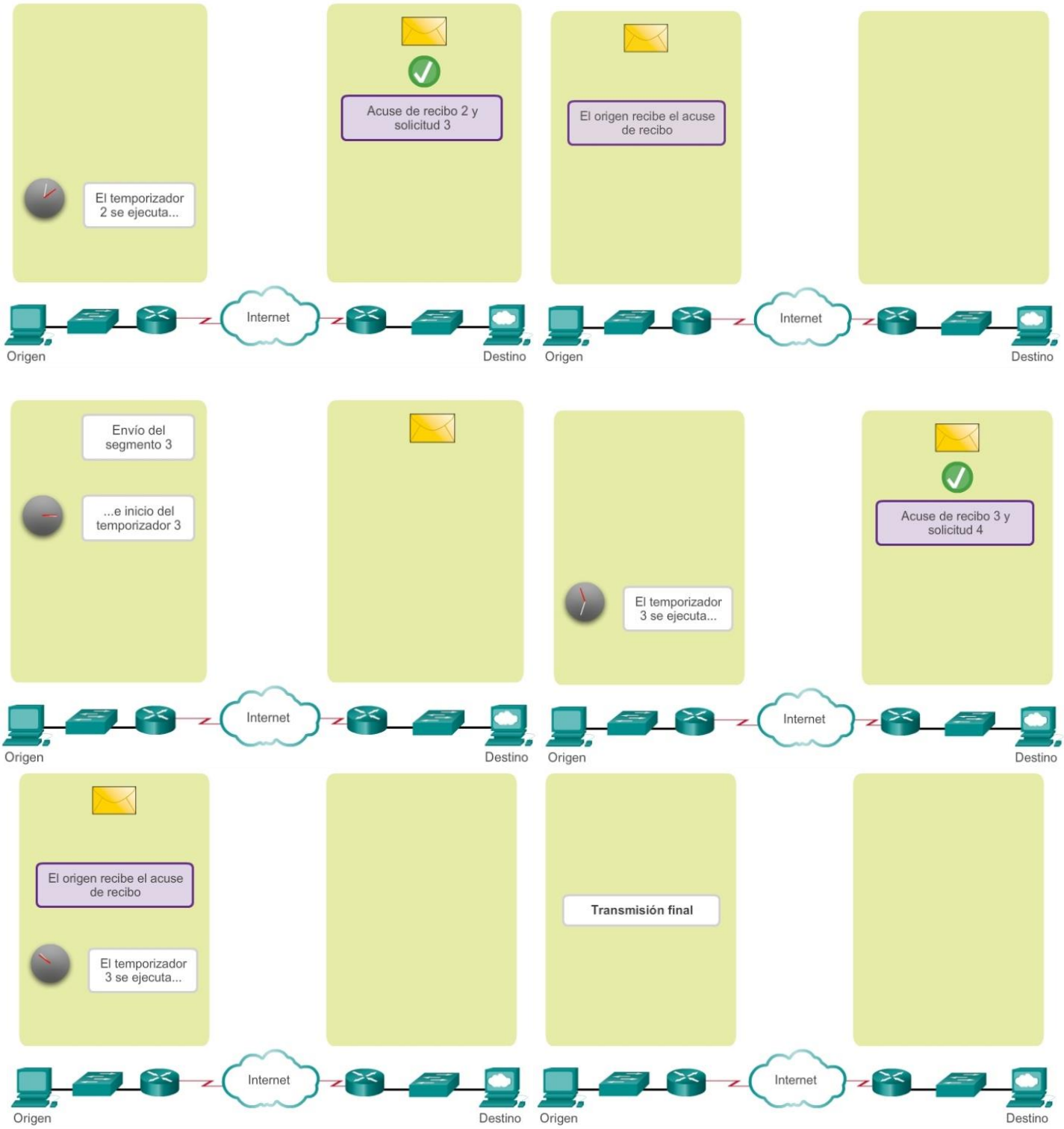
En la actualidad, los hosts pueden emplear también una característica optativa llamada “acuses de recibo selectivos” (SACK). Si ambos hosts admiten los SACK, es posible que el destino acuse recibo de los bytes de segmentos discontinuos, y el host solo necesitará volver a transmitir los datos perdidos.




Envío del segmento 2
...e inicio del temporizador 2
Internet
Origen
Destino
Envío del segmento 2
...e inicio del temporizador 2
Internet
Origen
Destino


...e inicio del temporizador 2
El segmento 2 no fue recibido
Internet
Origen
Destino
...e inicio del temporizador 2
El segmento 2 no fue recibido
Sin acuse de recibo 2
Internet
Origen
Destino


El temporizador 2 expira
Internet
Origen
Destino
Reenvío del segmento 2
...y reinicio del temporizador 2
Internet
Origen
Destino



Capítulo 7: Capa de Transporte 7.2.2.4 Control del flujo de TCP: tamaño de la ventana y acuses de recibo

Control de flujo

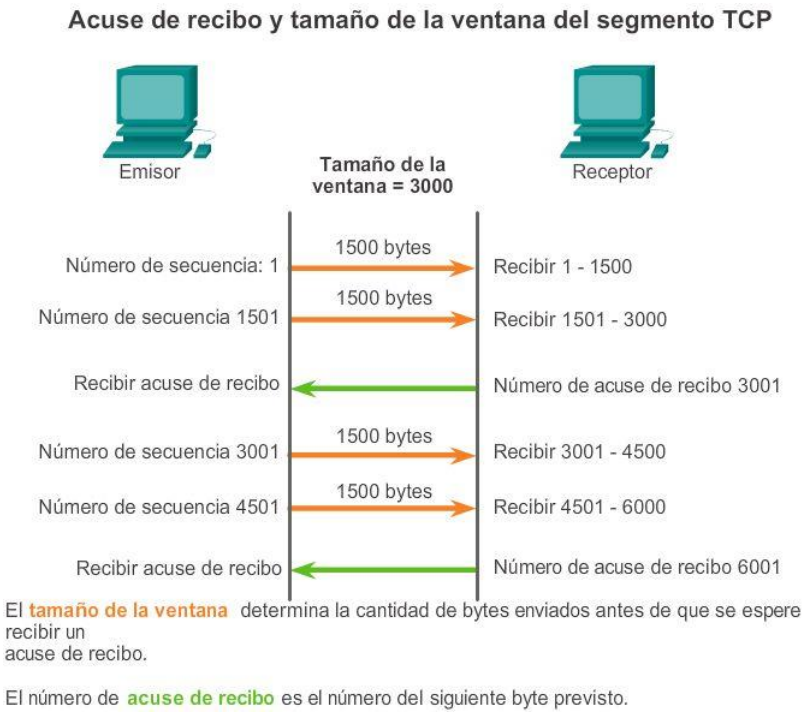
TCP también proporciona mecanismos para el control del flujo. El control del flujo permite mantener la confiabilidad de la transmisión de TCP mediante el ajuste de la velocidad del flujo de datos entre el origen y el destino para una sesión dada. El control del flujo se logra limitando la cantidad de segmentos de datos que se envían al mismo tiempo y solicitando acuses de recibo antes de enviar más segmentos.

Para lograr el control del flujo, lo primero que determina TCP es la cantidad de segmentos de datos que puede aceptar el dispositivo de destino. El encabezado TCP incluye un campo de 16 bits llamado “tamaño de la ventana”. Esta es la cantidad de bytes que el dispositivo de destino de una sesión TCP puede aceptar y procesar al mismo tiempo. El tamaño inicial de la ventana se acuerda durante el inicio de sesión entre el origen y el destino por medio del protocolo de enlace de tres vías. Una vez acordado el tamaño, el dispositivo de origen debe limitar la cantidad de segmentos de datos enviados al dispositivo de destino sobre la base del tamaño de la ventana. El dispositivo de origen puede continuar enviando más datos para la sesión solo cuando obtiene un acuse de recibo de los segmentos de datos recibidos.

Durante el retraso en la recepción del acuse de recibo, el emisor no envía ningún otro segmento. En los períodos en los que la red está congestionada o los recursos del host receptor están exigidos, la demora puede aumentar. A medida que aumenta esta demora, disminuye la tasa de transmisión efectiva de los datos para esta sesión. La disminución de velocidad en la transmisión de datos de cada sesión ayuda a reducir el conflicto de recursos en la red y en el dispositivo de destino cuando se ejecutan varias sesiones.

Ver la figura para obtener una representación simplificada del tamaño de la ventana y los acuses de recibo. En este ejemplo, el tamaño de la ventana inicial para una sesión TCP representada se establece en 3000 bytes. Cuando el emisor transmite 3000 bytes, espera por un acuse de recibo de los mismos antes de transmitir más segmentos para esta sesión. Una vez que el emisor obtiene este acuse de recibo del receptor, puede transmitir 3000 bytes adicionales.

TCP utiliza tamaños de ventana para tratar de aumentar la velocidad de transmisión hasta el flujo máximo que la red y el dispositivo de destino pueden admitir y, al mismo tiempo, minimizar las pérdidas y las retransmisiones.



Capítulo 7: Capa de Transporte 7.2.2.5 Control del flujo de TCP: prevención de congestiones

Reducción del tamaño de la ventana

Otra forma de controlar el flujo de datos es utilizar tamaños de ventana dinámicos. Cuando los recursos de la red son limitados, TCP puede reducir el tamaño de la ventana para lograr que los segmentos recibidos sean

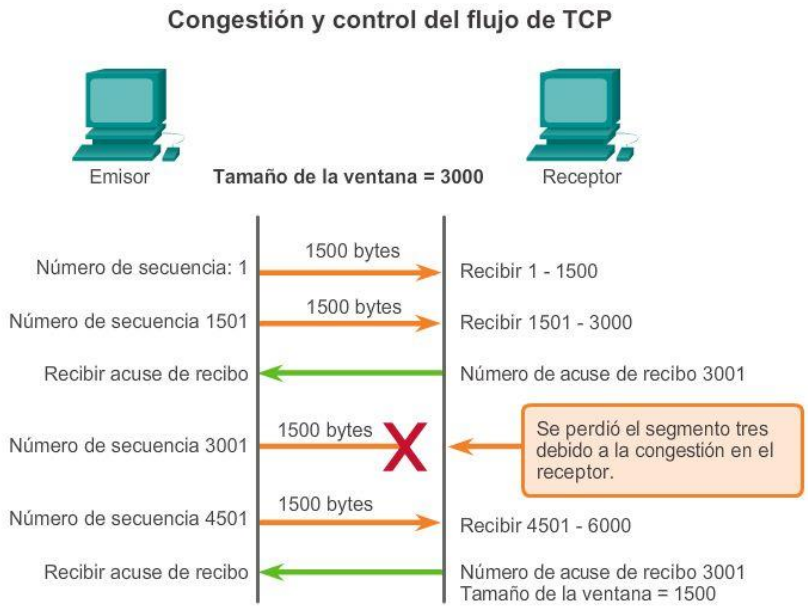
reconocidos con mayor frecuencia. Esto reduce de forma efectiva la velocidad de transmisión porque el origen espera que se de acuse de recibo de los datos con más frecuencia.

El host receptor envía el valor del tamaño de la ventana al host emisor para indicar la cantidad de bytes que puede recibir. Si el destino necesita disminuir la velocidad de comunicación debido, por ejemplo, a una memoria de búfer limitada, puede enviar un valor más pequeño del tamaño de la ventana al origen como parte del acuse de recibo.

Como se muestra en la ilustración, si un host receptor está congestionado, puede responder al host emisor con un segmento que especifique un tamaño reducido de la ventana. En esta ilustración, se muestra que se produjo la pérdida de uno de los segmentos. El receptor cambió el campo de la ventana en el encabezado TCP de los segmentos devueltos en esta conversación de 3000 a 1500. Esto hizo que el emisor redujera el tamaño de la ventana a 1500.

Después de un período de transmisión sin pérdidas de datos ni recursos limitados, el receptor comienza a aumentar el campo de la ventana, lo que reduce la sobrecarga en la red, ya que se deben enviar menos acuses de recibo. El tamaño de la ventana sigue aumentando hasta que se produce la pérdida de datos, lo que provoca que disminuya el tamaño de la ventana.

Este aumento y disminución dinámicos del tamaño de la ventana es un proceso continuo en TCP. En redes altamente eficaces, los tamaños de la ventana pueden ser muy grandes, porque no se pierden datos. En redes en las que la infraestructura subyacente está bajo presión, es probable que el tamaño de la ventana se mantenga pequeño...



Si se pierden los segmentos debido a la congestión, el receptor acusará recibo del último segmento secuencial recibido y responderá con un tamaño de ventana reducido.

Capítulo 7: Capa de Transporte 7.2.3.1 Comparación de baja sobrecarga y confiabilidad de UDP

UDP es un protocolo simple que proporciona las funciones básicas de la capa de transporte. Tiene una sobrecarga mucho menor que TCP, ya que no está orientado a la conexión y no proporciona los mecanismos sofisticados de retransmisión, secuenciación y control del flujo que ofrecen confiabilidad.

Esto no significa que las aplicaciones que utiliza UDP sean siempre poco confiables ni que UDP sea un protocolo inferior. Solo quiere decir que estas funciones no las proporciona el protocolo de la capa de transporte, y se deben implementar aparte, si fuera necesario.

Pese a que es relativamente baja la cantidad total de tráfico UDP que puede encontrarse en una red típica, los protocolos clave de la capa de aplicación que utilizan UDP incluyen lo siguiente:

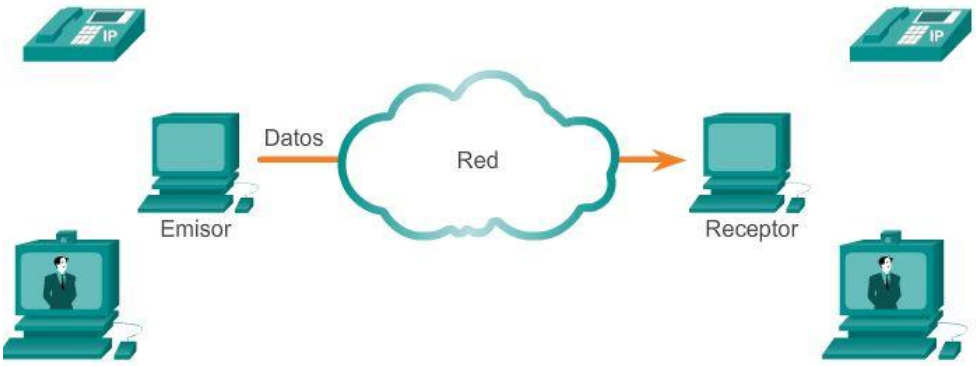
- Sistema de nombres de dominio (DNS)

- Protocolo simple de administración de red (SNMP, Simple Network Management Protocol)
- Protocolo de configuración dinámica de host (DHCP)
- Protocolo de información de enrutamiento (RIP)
- Protocolo de transferencia de archivos trivial (TFTP)
- Telefonía IP o voz sobre IP (VoIP)
- Juegos en línea

Algunas aplicaciones, como los juegos en línea o VoIP, pueden tolerar cierta pérdida de datos. Si estas aplicaciones utilizaran TCP, experimentarían largas demoras, ya que TCP detecta la pérdida de datos y los retransmite. Estas demoras serían más perjudiciales para el rendimiento de la aplicación que las pequeñas pérdidas de datos. Algunas aplicaciones, como DNS, simplemente reintentan el envío de la solicitud si no reciben ninguna respuesta; por lo tanto, no necesitan que TCP garantice la entrega de mensajes.

La baja sobrecarga del UDP es deseada por dichas aplicaciones.

Transporte de datos con baja sobrecarga de UDP



UDP no establece ninguna conexión antes de enviar datos.

UDP proporciona transporte de datos con baja sobrecarga, debido a que posee un encabezado de datagrama pequeño sin tráfico de administración de red.

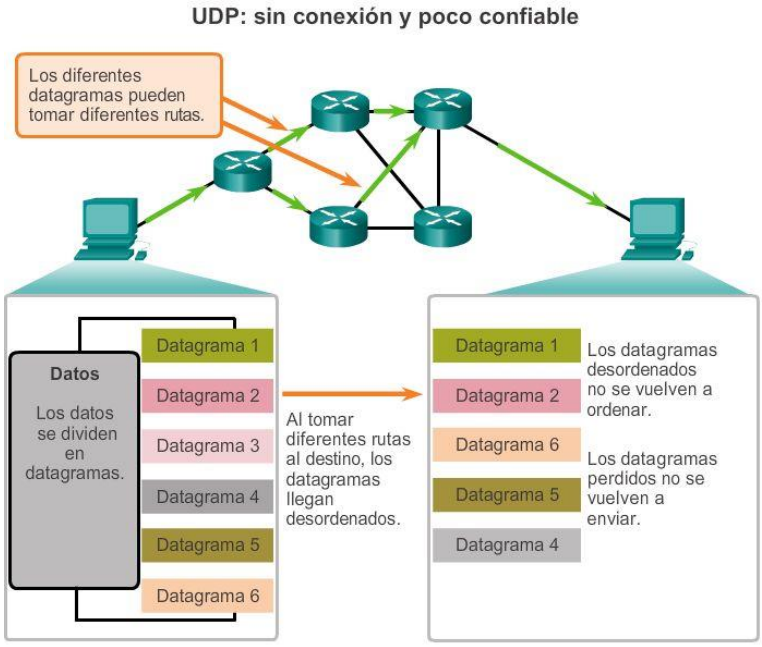
Capítulo 7: Capa de Transporte 7.2.3.2 Reensamblaje de datagramas de UDP

Ya que UDP opera sin conexión, las sesiones no se establecen antes de que se lleve a cabo la comunicación, como sucede con TCP. Se dice que UDP está basado en las transacciones; es decir, cuando una aplicación tiene datos para enviar, simplemente los envía.

Muchas aplicaciones que utilizan UDP envían pequeñas cantidades de datos que pueden ajustarse en un segmento. Sin embargo, algunas aplicaciones envían cantidades de datos más grandes que deben dividirse en varios segmentos. La PDU del UDP se conoce como un “datagrama”, aunque los términos “segmento” y “datagrama” se utilizan algunas veces de forma intercambiable para describir una PDU de la capa de transporte.

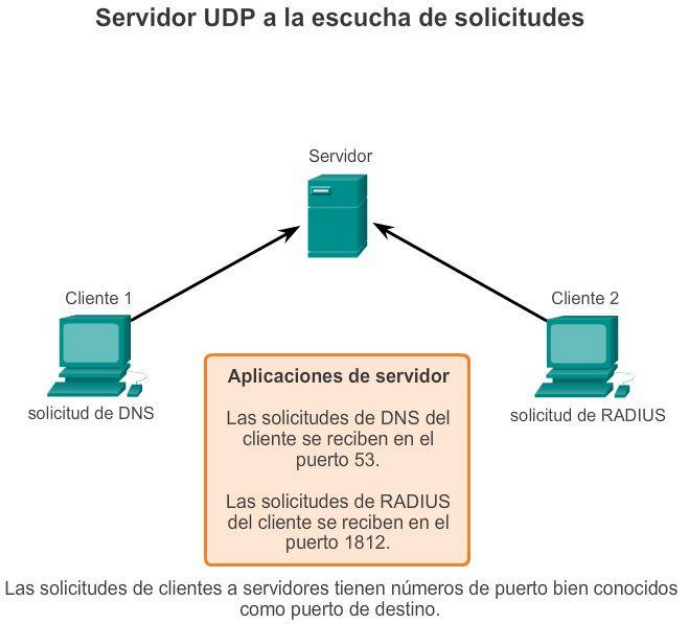
Cuando se envían datagramas múltiples a un destino, pueden tomar diferentes rutas y llegar en el orden equivocado. UDP no realiza un seguimiento de los números de secuencia de la manera en que lo hace TCP. UDP no tiene forma de reordenar datagramas en el orden en que se transmiten, como se muestra en la ilustración.

Por lo tanto, UDP simplemente reensambla los datos en el orden en que se recibieron y los envía a la aplicación. Si la secuencia de datos es importante para la aplicación, esta debe identificar la secuencia adecuada y determinar cómo se deben procesar los datos.



Capítulo 7: Capa de Transporte 7.2.3.3 Procesos y solicitudes del servidor UDP

Al igual que las aplicaciones basadas en TCP, a las aplicaciones de servidor basadas en UDP se les asignan números de puerto bien conocido o registrado. Cuando estas aplicaciones o estos procesos se ejecutan en un servidor, aceptan los datos que coinciden con el número de puerto asignado. Cuando UDP recibe un datagrama destinado a uno de esos puertos, envía los datos de aplicación a la aplicación adecuada en base a su número de puerto.



Capítulo 7: Capa de Transporte 7.2.3.4 Procesos de cliente UDP

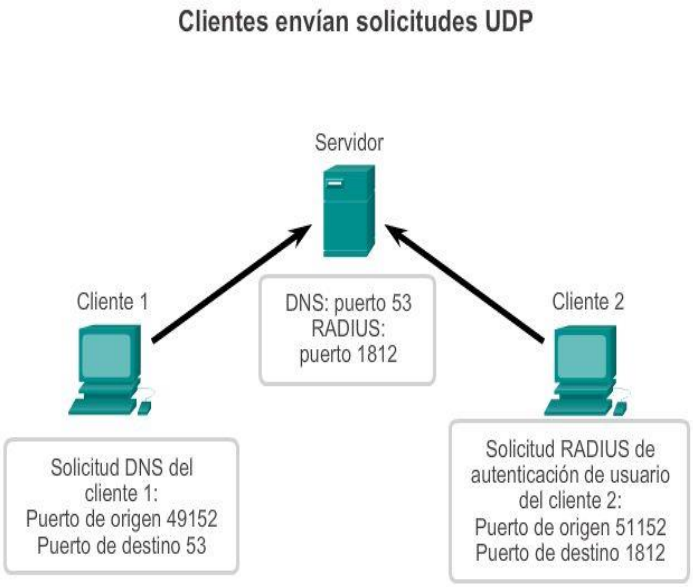
Como en TCP, la comunicación cliente/servidor la inicia una aplicación cliente que solicita datos de un proceso de servidor. El proceso de cliente UDP selecciona al azar un número de puerto del rango de números de puerto dinámicos y lo utiliza como puerto de origen para la conversación. Por lo general, el puerto de destino es el número de puerto bien conocido o registrado que se asigna al proceso de servidor.

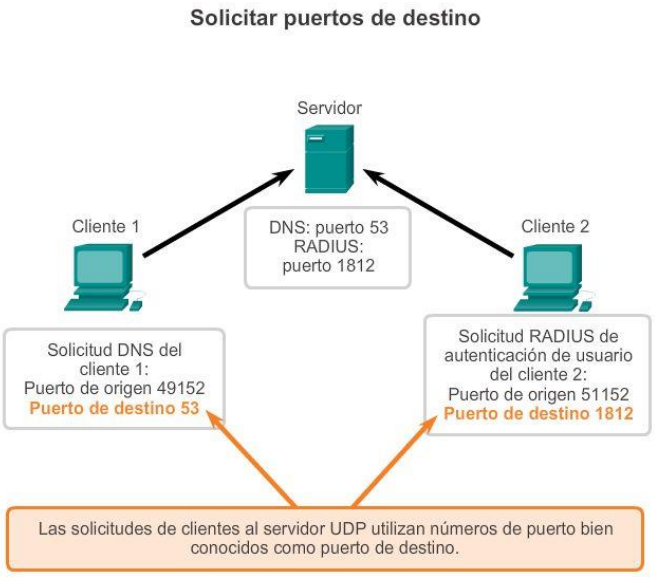
Los números de puerto de origen seleccionados al azar colaboran con la seguridad. Si existe un patrón predecible para la selección del puerto de destino, un intruso puede simular el acceso a un cliente de manera más sencilla intentando conectarse al número de puerto que tenga mayor posibilidad de estar abierto.

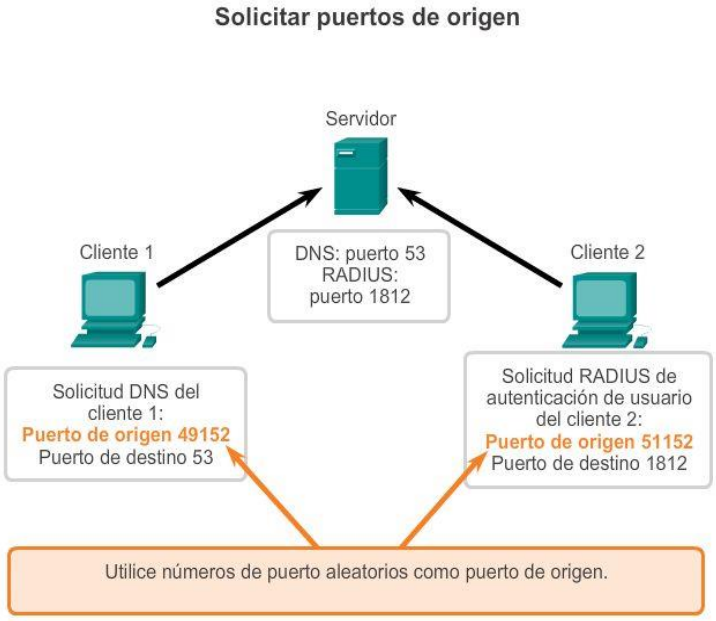
Dado que no se crean sesiones con UDP, no bien los datos están listos para enviarse y los puertos están identificados, UDP puede formar los datagramas y pasarlos a la capa de red para direccionarlos y enviarlos a la red.

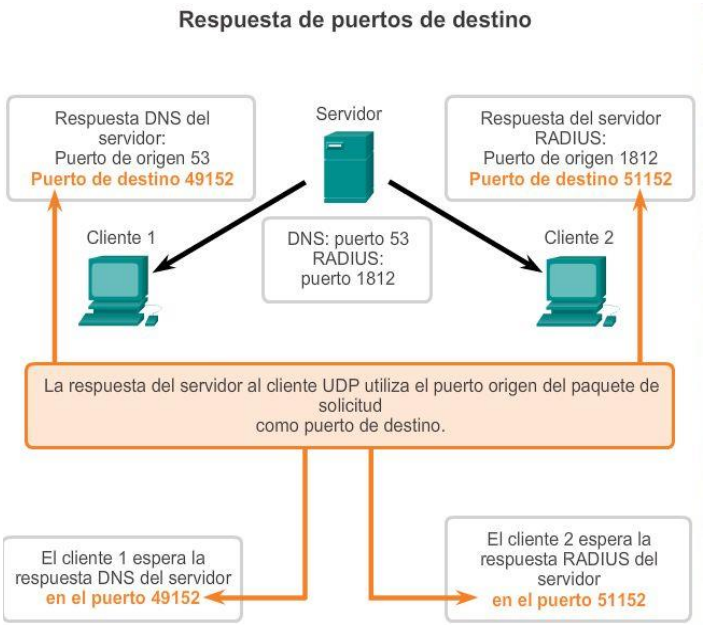
Una vez que el cliente selecciona los puertos de origen y de destino, este mismo par de puertos se utiliza en el encabezado de todos los datagramas que se utilizan en la transacción. Para la devolución de datos del servidor al cliente, se invierten los números de puerto de origen y destino en el encabezado del datagrama.

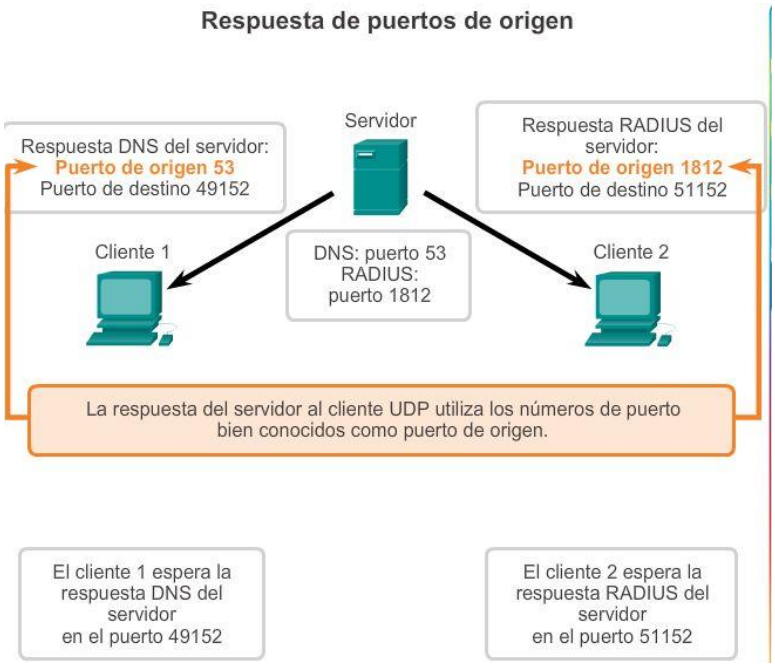
Desplácese por las ilustraciones a la derecha para ver los detalles de los procesos de cliente UDP.


Clientes envían solicitudes UDP
Servidor
Cliente 1
Cliente 2
DNS: puerto 53
RADIUS:
puerto 1812
Solicitud DNS del
cliente 1:
Puerto de origen 49152
Puerto de destino 53
Solicitud RADIUS de
autenticación de usuario
del cliente 2:
Puerto de origen 51152
Puerto de destino 1812


Solicitar puertos de destino
Servidor
Cliente 1
Cliente 2
DNS: puerto 53
RADIUS:
puerto 1812
Solicitud DNS del
cliente 1:
Puerto de origen 49152
Puerto de destino 53
Solicitud RADIUS de
autenticación de usuario
del cliente 2:
Puerto de origen 51152
Puerto de destino 1812
Las solicitudes de clientes al servidor UDP utilizan números de puerto bien
conocidos como puerto de destino.


Solicitar puertos de origen
Servidor
Cliente 1
Cliente 2
DNS: puerto 53
RADIUS:
puerto 1812
Solicitud DNS del
cliente 1:
Puerto de origen 49152
Puerto de destino 53
Solicitud RADIUS de
autenticación de usuario
del cliente 2:
Puerto de origen 51152
Puerto de destino 1812
Utilice números de puerto aleatorios como puerto de origen.


Respuesta de puertos de destino
Respuesta DNS del
servidor:
Puerto de origen 53
Puerto de destino 49152
Servidor
Respuesta del servidor
RADIUS:
Puerto de origen 1812
Puerto de destino 51152
Cliente 1
Cliente 2
DNS: puerto 53
RADIUS:
puerto 1812
La respuesta del servidor al cliente UDP utiliza el puerto origen del paquete de
solicitud
como puerto de destino.
El cliente 1 espera la
respuesta DNS del servidor
en el puerto 49152
El cliente 2 espera la
respuesta RADIUS del
servidor
en el puerto 51152



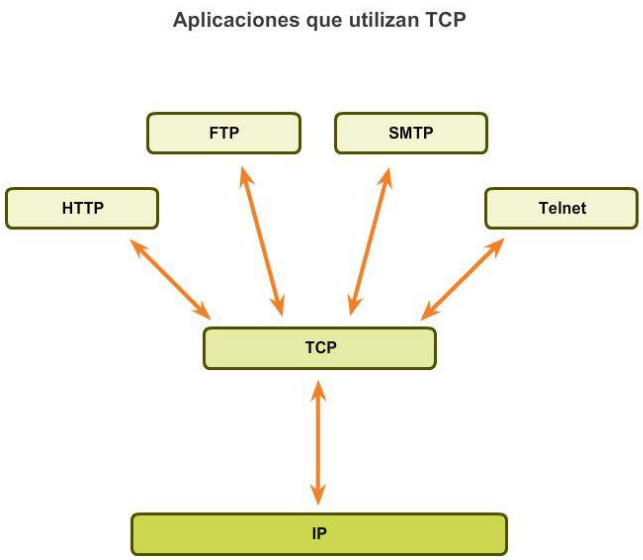
Capítulo 7: Capa de Transporte 7.2.4.1 Aplicaciones que utilizan TCP

Muchas aplicaciones requieren confiabilidad y otros servicios que proporciona TCP. Estas son aplicaciones que pueden tolerar cierto grado de demora o pérdida de rendimiento debido a la sobrecarga que impone TCP.

Esto hace que TCP sea más adecuado para las aplicaciones que necesitan transporte confiable y que pueden tolerar cierta demora. TCP es un excelente ejemplo de cómo las diferentes capas del suite de protocolos TCP/IP tienen funciones específicas. Debido a que el protocolo de la capa de transporte TCP maneja todas las tareas asociadas con la segmentación del stream de datos, la confiabilidad, el control del flujo y el reordenamiento de segmentos, este libera a la aplicación de la tarea de administrar cualquiera de estas tareas. La aplicación simplemente puede enviar el stream de datos a la capa de transporte y utilizar los servicios de TCP.

Como se muestra en la ilustración, algunos ejemplos de aplicaciones bien conocidas que utilizan TCP incluyen las siguientes:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo de transferencia de archivos (FTP)
- Protocolo simple de transferencia de correo (SMTP)
- Telnet



Capítulo 7: Capa de Transporte 7.2.4.2 Aplicaciones que utilizan UDP

Existen tres tipos de aplicaciones que son las más adecuadas para UDP:

- Aplicaciones que pueden tolerar cierta pérdida de datos, pero requieren retrasos cortos o que no haya retrasos
- Aplicaciones con transacciones de solicitud y respuesta simples
- Comunicaciones unidireccionales donde no se requiere confiabilidad o donde la aplicación la pueda administrar

Muchas aplicaciones de video y multimedia, como VoIP y la televisión por protocolo de Internet (IPTV), utilizan UDP. Estas aplicaciones pueden tolerar cierta pérdida de datos con un efecto mínimo o imperceptible. Los mecanismos de confiabilidad de TCP presentan cierto grado de demora que se puede percibir en la calidad de sonido o video que se recibe.

Otros tipos de aplicaciones adecuadas para UDP son las que utilizan transacciones de solicitud y respuesta simples. Esto se da cuando un host envía una solicitud y existe la posibilidad de que reciba una respuesta o no. Estos tipos de aplicaciones incluyen las siguientes:

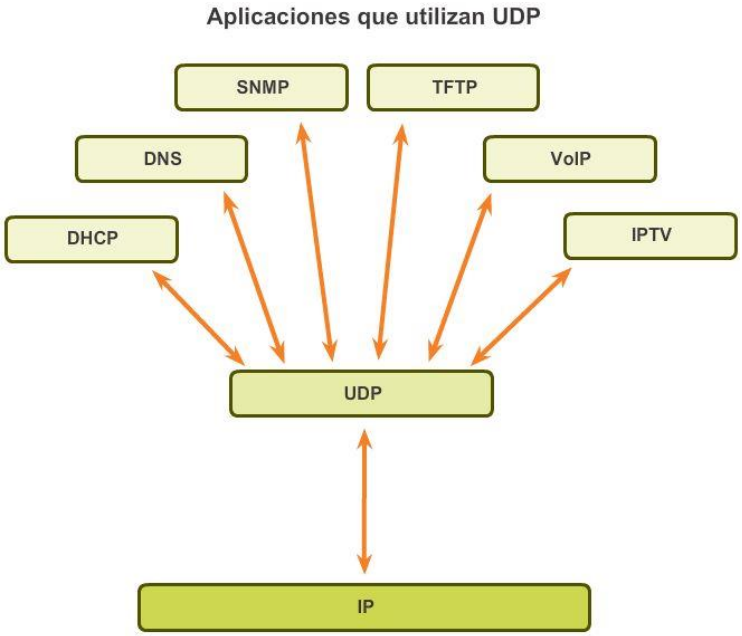
- DHCP
- DNS: también puede utilizar TCP
- SNMP
- TFTP

Algunas aplicaciones se ocupan de la confiabilidad por sí mismas. Estas aplicaciones no necesitan los servicios de TCP y pueden utilizar mejor UDP como protocolo de capa de transporte. TFTP es un ejemplo de este tipo de protocolo. TFTP tiene sus propios mecanismos para el control del flujo, la detección de errores, los acuses de recibo y la recuperación de errores. Este protocolo no necesita depender de TCP para esos servicios.

Capítulo 7: Capa de Transporte 7.2.4.3 Práctica de laboratorio: Uso de Wireshark para examinar capturas de FTP y TFTP

En esta práctica de laboratorio se cumplirán los siguientes objetivos:

- Parte 1: Identificar campos de encabezado y operación TCP mediante una captura de sesión FTP de Wireshark
- Parte 2: Identificar campos de encabezado y operación UDP mediante una captura de sesión TFTP de Wireshark



Capítulo 7: Capa de Transporte 7.3.1.1 Actividad de clase: Tenemos que hablar nuevamente (juego)

Tenemos que hablar nuevamente

Nota: es importante que los estudiantes hayan completado la actividad de creación de modelos introductoria de este capítulo. Conviene realizar esta actividad en grupos medianos de seis a ocho estudiantes.

El instructor susurrará un mensaje complejo al primer estudiante de un grupo. Por ejemplo, el mensaje puede ser: “Se espera una tormenta de nieve mañana”. Se espera que suceda por la mañana, por lo que el horario de clases se retrasará dos horas. Por lo tanto, traigan la tarea”.

Ese estudiante le susurrará el mensaje al siguiente estudiante del grupo. Todos los grupos siguen este proceso hasta que todos los miembros de cada grupo hayan oído el mensaje susurrado.

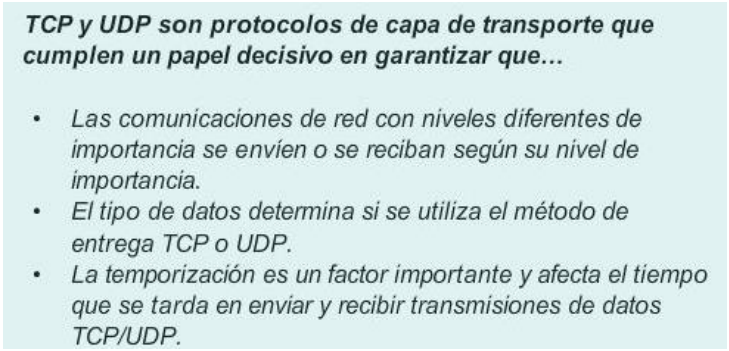
Las reglas que debe seguir son las siguientes:

- Puede susurrarle el mensaje al compañero junto a usted por partes Y TAMBIÉN puede repetir las partes del mensaje después de verificar que ese compañero escuchó el mensaje correctamente.

- Se pueden verificar y repetir partes del mensaje (hacia la derecha O hacia la izquierda para asegurar la precisión de las partes del mensaje) en susurros. A un estudiante se le asignará la tarea de medir el tiempo total de la actividad.

- Cuando se haya transmitido el mensaje a todo el grupo, el último estudiante que escuchó el mensaje lo dirá en voz alta. Las pequeñas partes del mensaje se pueden repetir (es decir, se pueden reenviar) y el proceso se puede volver a iniciar para asegurarse de que TODAS las partes del mensaje se hayan entregado en forma completa y correcta.

- El instructor repetirá el mensaje original para comprobar que el mensaje se haya entregado correctamente.



Capítulo 7: Capa de Transporte 7.3.1.2 Simulación de Packet Tracer: comunicaciones de TCP y UDP

El objetivo de esta actividad de simulación es proporcionar una base para comprender en detalle los protocolos TCP y UDP. El modo de simulación permite ver la funcionalidad de los diferentes protocolos.

A medida que los datos se trasladan por la red, se dividen en partes más pequeñas y se identifican de forma tal que se puedan volver a juntar. A cada una de estas partes se le asigna un nombre específico (unidad de datos del protocolo [PDU, protocol data unit]) y se la asocia a una capa específica. El modo de simulación de Packet Tracer le permite al usuario ver cada uno de los protocolos y las PDU asociadas. Los pasos que se detallan a continuación guían al usuario en el proceso de solicitud de servicios mediante diversas aplicaciones disponibles en una PC cliente.

Esta actividad proporciona la oportunidad de explorar la funcionalidad de los protocolos TCP y UDP, la multiplexación y la función que cumplen los números de puerto para determinar qué aplicación local solicita o envía los datos.

Capítulo 7: Capa de Transporte 7.3.1.3 Resumen

La capa de transporte proporciona servicios relacionados con el transporte de las siguientes maneras:

- La división en segmentos de los datos que se reciben de una aplicación
- La adición de un encabezado para identificar y administrar cada segmento
- El uso de la información del encabezado para reensamblar los segmentos de nuevo en datos de aplicación
- El paso de los datos ensamblados hacia la aplicación correcta

UDP y TCP son protocolos de la capa de transporte comunes.

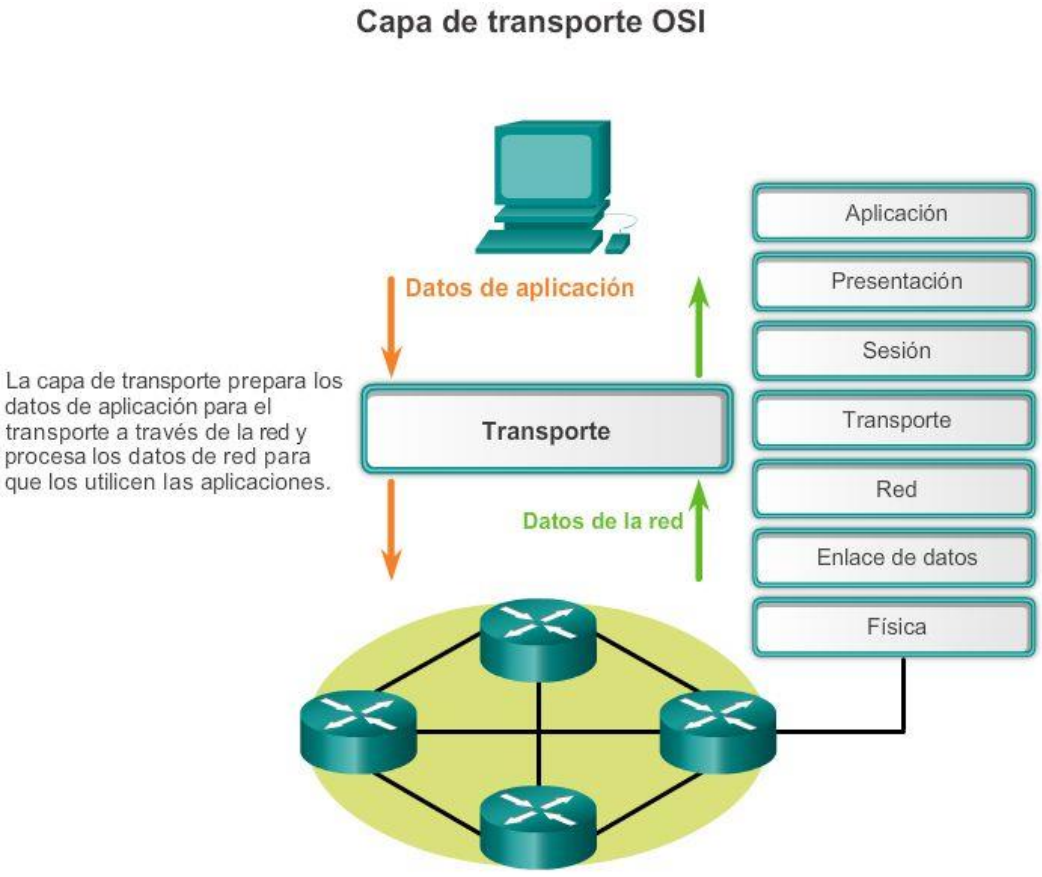
Los datagramas de UDP y los segmentos TCP tienen encabezados que se agregan delante de los datos, los cuales incluyen un número de puerto de origen y un número de puerto de destino. Estos números de puerto permiten que los datos se dirijan a la aplicación correcta que se ejecuta en la computadora de destino.

El TCP pasa datos a la red hasta que conoce el destino y está listo para recibirlo. Luego TCP administra el flujo de datos y reenvía todos los segmentos de datos de los que recibió acuse a medida que se reciben en el destino. TCP utiliza mecanismos de enlace, temporizadores, mensajes de acuse de recibo y control del flujo mediante mecanismo ventana dinámico para lograr la confiabilidad. El proceso de confiabilidad, sin embargo, impone una sobrecarga en la red en términos de encabezados de segmentos mucho más grandes y más tráfico de la red entre el origen y el destino.

Si se deben entregar los datos de aplicación a través de la red de manera rápida, o si el ancho de banda de la red no admite la sobrecarga de mensajes de control que se intercambian entre los sistemas de origen y destino, UDP es el protocolo de la capa de transporte preferido por los desarrolladores.

Esto es así porque UDP no rastrea ni acusa recibo de datagramas en el destino (solo envía los datagramas recibidos a la capa de aplicación a medida que llegan) ni reenvía datagramas perdidos. Sin embargo, esto no significa necesariamente que la comunicación misma no sea confiable; puede haber mecanismos en los protocolos de la capa de aplicación y servicios que procesen datagramas perdidos o retrasados si la aplicación tiene estos requisitos.

El desarrollador de la aplicación decide cuál es el protocolo de capa de transporte que más se ajusta a los requisitos de la aplicación. Es importante recordar que el resto de las capas cumplen una función en las comunicaciones de red de datos y afectan el rendimiento de estas.

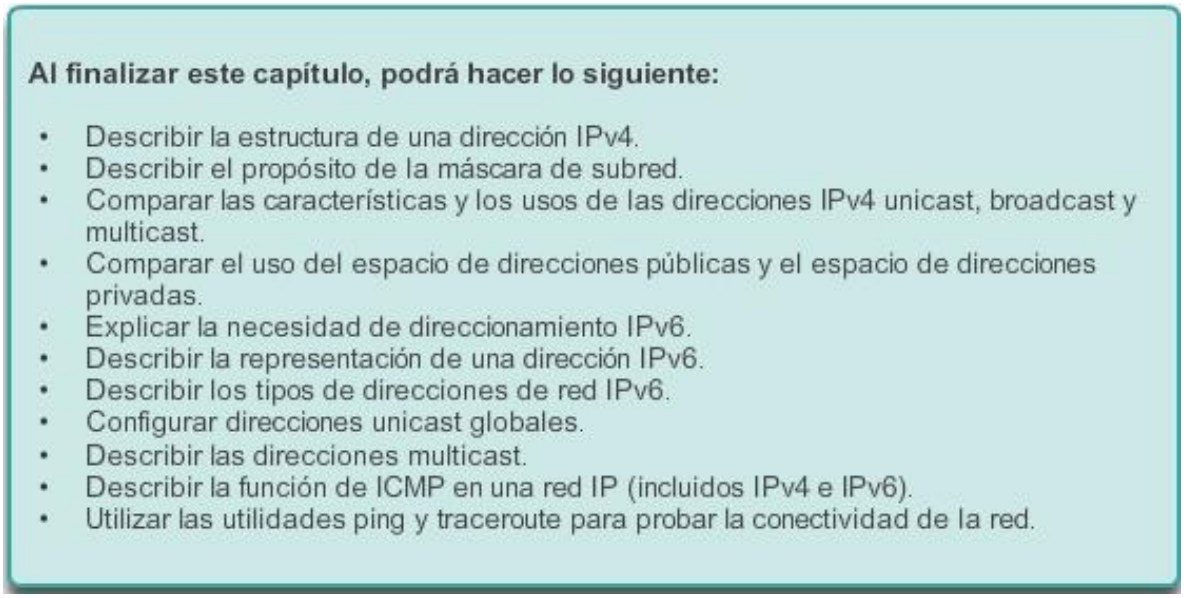


Capítulo 8: Asignación de direcciones IP 8.0.1.1 Introducción

El direccionamiento es una función clave de los protocolos de capa de red que permite la comunicación de datos entre hosts, independientemente de si los hosts se encuentran en la misma red o en redes diferentes. Tanto el protocolo de Internet versión 4 (IPv4) como el protocolo de Internet versión 6 (IPv6) proporcionan direccionamiento jerárquico para los paquetes que transportan datos.

El diseño, la implementación y la administración de un plan de direccionamiento IP eficaz asegura que las redes puedan operar de manera eficaz y eficiente.

En este capítulo, se examina detalladamente la estructura de las direcciones IP y su aplicación en la construcción y la puesta a prueba de redes y subredes IP.



Capítulo 8: Asignación de direcciones IP 8.0.1.2 Actividad: Internet de todo (IdT)

Internet de todo (IdT)

Si la naturaleza, el tráfico, el transporte, las redes y la exploración espacial dependen del intercambio de información digital, ¿de qué forma se identifica dicha información de origen a destino?

En esta actividad, comenzará a pensar no solo en lo que se identificará en el mundo de IdT, sino también en cómo se direccionarán todos esos aspectos en ese mundo.

- Lea el blog o la fuente de noticias proporcionada por John Chambers con respecto a Internet de todo (IdT) http://blogs.cisco.com/news/internet-of-everything-2. Vea el video que se encuentra en la mitad de la página.
- A continuación, vaya a la página principal de IdT:http://www.cisco.com/web/tomorrow-starts-here/index.html. Haga clic en una categoría que le interese.
- Vea el video, el blog o el .pdf que pertenece a la categoría de IdT de interés.
- Escriba cinco preguntas o comentarios sobre lo que vio o leyó, y compártalos con la clase.

"En la actualidad, más del 99% del mundo está desconectado. Mañana, conectaremos todo".

¿De qué forma utilizará IdT los servicios de direccionamiento IP para la comunicación de red?

Capítulo 8: Asignación de direcciones IP 8.1.1.1 Notación binaria

Para comprender el funcionamiento de los dispositivos en una red, debemos observar las direcciones y otros datos de la misma manera en que lo hacen los dispositivos: en notación binaria.

La notación binaria es una representación de la información mediante unos y ceros solamente. Las PC se comunican mediante datos binarios. Los datos binarios se pueden utilizar para representar muchas formas distintas de datos. Por ejemplo, al pulsar letras en un teclado, esas letras aparecen en la pantalla de una manera que el usuario puede leer y comprender. Sin embargo, la PC traduce cada letra a una serie de dígitos binarios para su almacenamiento y transporte. Para traducir esas letras, la PC utiliza el Código Estadounidense Estándar para el Intercambio de Información (ASCII).

Mediante ASCII, la letra "A" se representa en forma de bit como "01000001", mientras que la "a" minúscula se representa en forma de bit como "01100001". Utilice el traductor de ASCII en la figura 1 para convertir los caracteres ASCII al sistema binario.

Si bien, por lo general, las personas no deben preocuparse por la conversión binaria de letras, es necesario comprender el uso del sistema binario para el direccionamiento IP. Cada dispositivo en una red se debe identificar de forma exclusiva mediante una dirección binaria. En redes IPv4, esta dirección se representa mediante una cadena de 32 bits (unos y ceros). A continuación, en la capa de red, los paquetes incluyen esta información de identificación única para los sistemas de origen y de destino. Por lo tanto, en una red IPv4, cada paquete incluye una dirección de origen de 32 bits y una dirección de destino de 32 bits en el encabezado de capa 3.

Para la mayoría de las personas, una cadena de 32 bits es difícil de interpretar e incluso más difícil de recordar. Por este motivo, representamos las direcciones IPv4 mediante el formato decimal punteado en lugar del binario.

Esto significa que vemos a cada byte (octeto) como número decimal en el rango de 0 a 255. Para entender cómo funciona esto, es necesario tener aptitudes para la conversión de sistema binario a decimal.

Notación de posición

Aprender a convertir el sistema binario a decimal requiere el conocimiento de los fundamentos matemáticos de un sistema de numeración denominado notación de posición. "Notación de posición" significa que un dígito representa diferentes valores según la posición que ocupa. En un sistema de notación de posición, la base numérica se denomina "raíz". En el sistema de base 10, la raíz es 10. En el sistema binario, se utiliza una raíz de 2. Los términos "raíz" y "base" se pueden utilizar de manera indistinta. Más específicamente, el valor que un dígito representa es el valor multiplicado por la potencia de la base o raíz representado por la posición que el dígito ocupa. Algunos ejemplo ayudarán a aclarar cómo funciona este sistema.

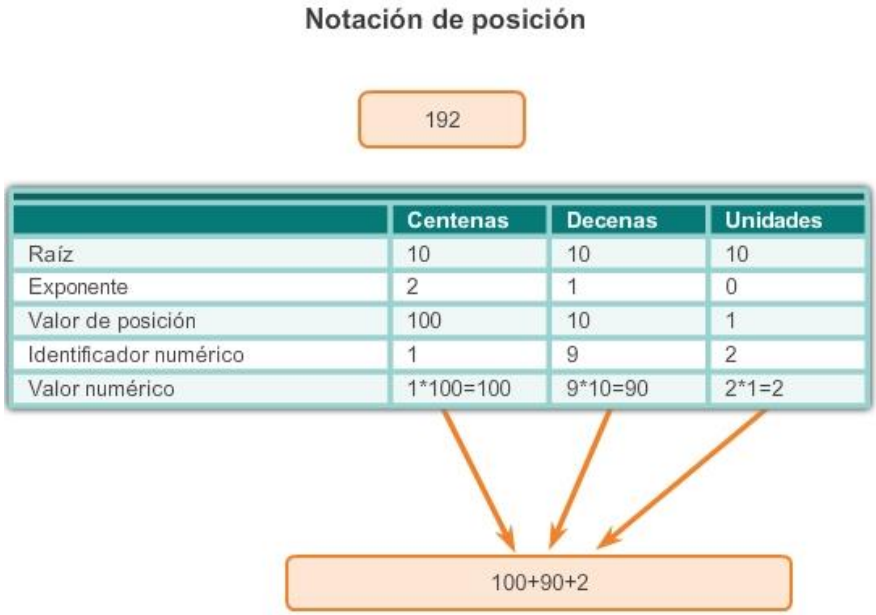
Para el número decimal 192, el valor que el 1 representa es 1*10^2 (1 multiplicado por 10 elevado a la segunda potencia). El 1 se encuentra en lo que comúnmente llamamos la posición "100". La notación de posición se refiere a esta posición como posición base^2 porque la base o raíz es 10 y la potencia es 2. El 9 representa 9*10^1 (9 multiplicado por 10 elevado a la primera potencia). En la figura 2, se muestra la notación de posición para el número decimal 192.

Usando la notación de posición en el sistema de numeración con base 10, 192 representa:

192 = (1 * 10^2) + (9 * 10^1) + (2 * 10^0)

o

192 = (1 * 100) + (9 * 10) + (2 * 1)



Capítulo 8: Asignación de direcciones IP 8.1.1.2 Sistema de numeración binario

En IPv4, las direcciones son números binarios de 32 bits. Sin embargo, para facilitar el uso por parte de las personas, los patrones binarios que representan direcciones IPv4 se expresan en formato decimal punteado. Esto primero se logra separando cada byte (8 bits) del patrón binario de 32 bits, llamado “octeto”, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

La dirección binaria:

11000000 10101000 00001010 00001010

se expresa como decimal punteada de la siguiente manera:

192.168.10.10

En la figura 1, seleccione cada botón para ver cómo se representa la dirección binaria de 32 bits en octetos decimales punteados.

¿Pero de qué forma se determinan los equivalentes decimales reales?

Sistema de numeración binaria

En el sistema de numeración binaria la raíz es 2. Por lo tanto, cada posición representa aumentos en potencias de 2. En números binarios de 8 bits, las posiciones representan estas cantidades:

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

El sistema de numeración de base 2 solo tiene dos dígitos: 0 y 1.

Cuando se interpreta un byte como un número decimal, se obtiene la cantidad que esa posición representa si el dígito es 1, y no se obtiene la cantidad si el dígito es 0, como se muestra en la figura 1.

En la figura 2, se ilustra la representación del número decimal 192 en sistema binario. Un 1 en una determinada posición significa que se agrega ese valor al total. Un 0 significa que no se agrega ese valor. El número binario 11000000 tiene un 1 en la posición 2^7 (valor decimal 128) y un 1 en la posición 2^6 (valor decimal 64). Los bits restantes son todos 0, de modo que no se agregan los valores decimales correspondientes. El resultado de agregar 128 + 64 es 192, el equivalente decimal de 11000000.

A continuación, se proporcionan dos ejemplos más:

Ejemplo 1: un octeto compuesto solo por unos, 11111111

Un 1 en cada posición significa que sumamos el valor para esa posición al total. Todos 1 significa que se incluyen los valores de cada posición en el total; por lo tanto, el valor de todos 1 en un octeto es 255.

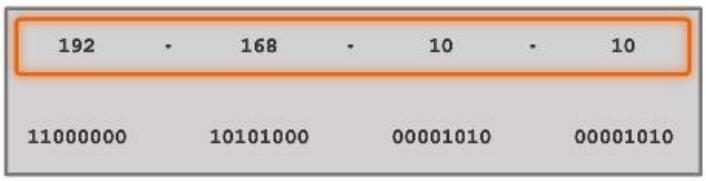
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

Ejemplo 2: un octeto compuesto solo por ceros, 00000000

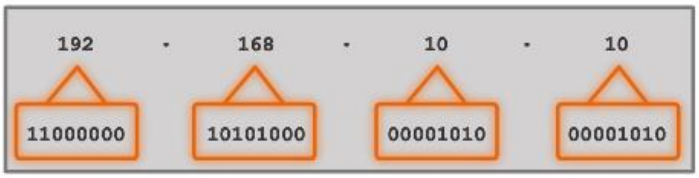
Un 0 en cada posición indica que no se incluye el valor para esa posición en el total. Un 0 en cada posición produce un total de 0.

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

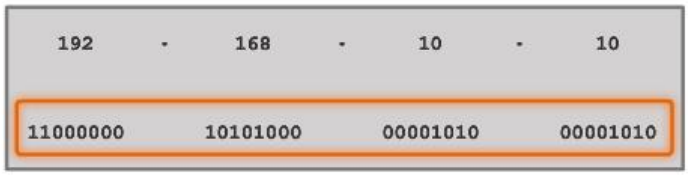
Una combinación distinta de unos y ceros arroja un valor decimal diferente.



192.168.10.10 es una dirección IP asignada a una PC.



Esta dirección está formada por cuatro octetos diferentes.



La PC almacena la dirección como el stream de datos de 32 bits completo.

Capítulo 8: Asignación de direcciones IP 8.1.1.3 Conversión de una dirección binaria a decimal

Cada octeto está compuesto por 8 bits y cada bit tiene un valor, 0 o 1. Los cuatro grupos de 8 bits tienen el mismo conjunto de valores válidos en el rango de 0 a 255 inclusive. El valor de cada ubicación de bits, de derecha a izquierda, es 1, 2, 4, 8, 16, 32, 64 y 128.

Determine el valor del octeto sumando los valores de las posiciones cada vez que haya un 1 binario presente.

- Si en esa posición hay un 0, no sume el valor.
- Si los 8 bits son 0, 00000000, el valor del octeto es 0.
- Si los 8 bits son 1, 11111111, el valor del octeto es 255 (128 + 64 + 32 + 16 + 8 + 4 + 2 + 1).
- Si los 8 bits están combinados, los valores se agregan juntos. Por ejemplo, el octeto 00100111 tiene un valor de 39 (32 + 4 + 2 + 1).

Por lo tanto, el valor de cada uno de los cuatro octetos puede ir de 0 a un máximo de 255.

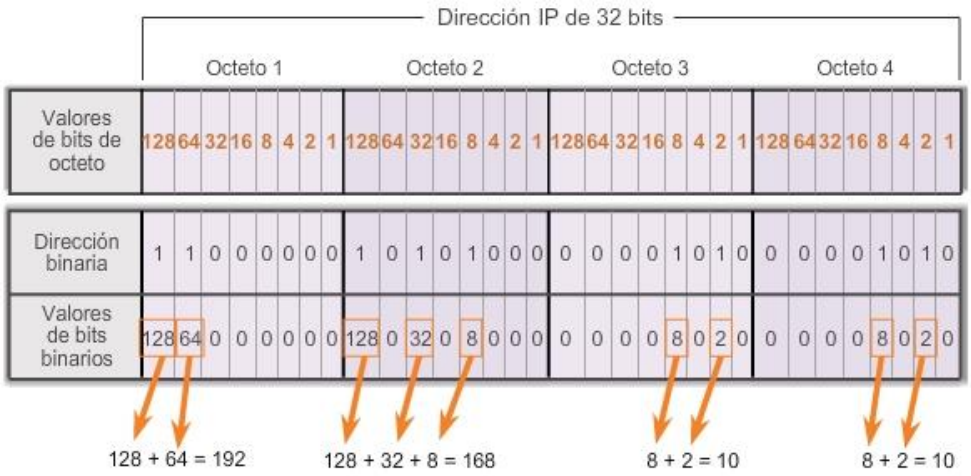
Utilizando la dirección IPv4 de 32 bits 11000000101010000000101000001010, convierta la representación binaria en decimal punteada mediante los siguientes pasos:

Paso 1. Divida los 32 bits en 4 octetos.

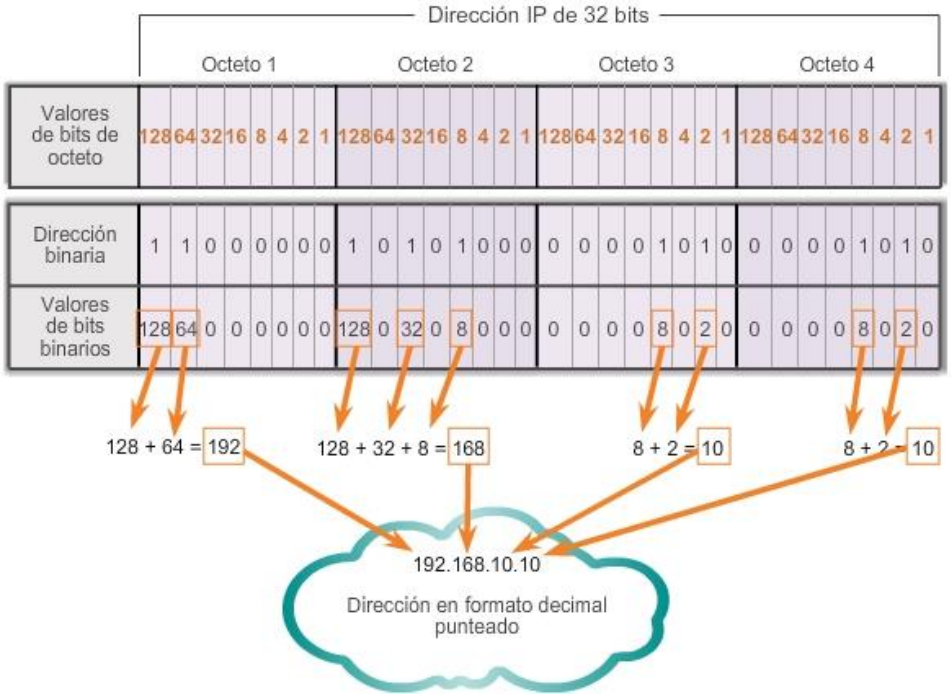
Paso 2. Convierta cada octeto a decimal.

Paso 3. Agregue un "punto" entre cada decimal.

Haga clic en Reproducir en la ilustración para ver cómo se convierte una dirección binaria en decimal punteada.



Sume los valores de bits binarios.



Capítulo 8: Asignación de direcciones IP 8.1.1.5 Conversión de decimal en binario

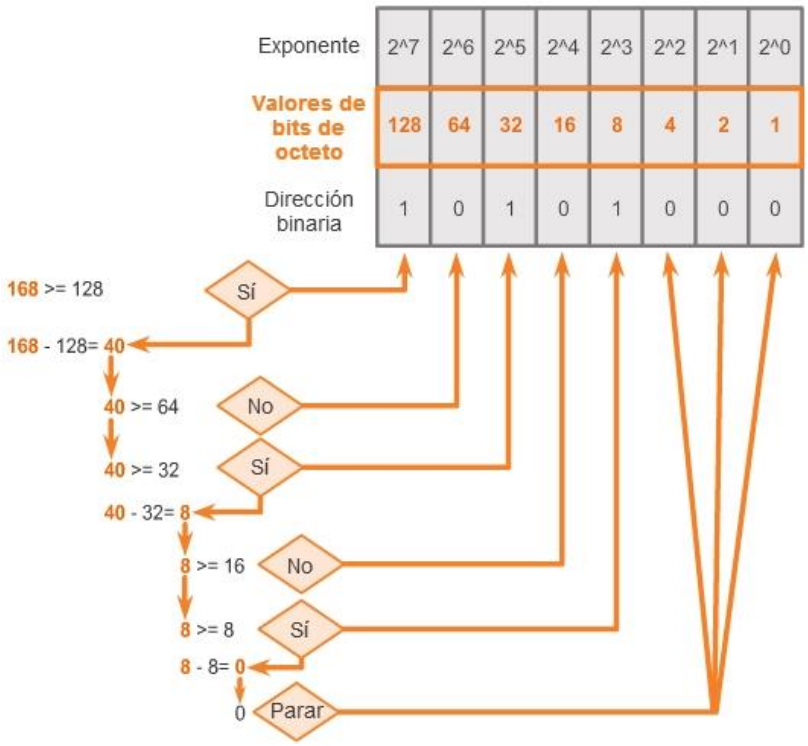
Además de poder convertir de sistema binario a decimal, también es necesario comprender cómo convertir de decimal a binario.

Dado que representamos las direcciones IPv4 mediante el formato decimal punteado, solo es necesario analizar el proceso de conversión de valores binarios de 8 bits a valores decimales de 0 a 255 para cada octeto en una dirección IPv4.

Para comenzar el proceso de conversión, empezaremos determinando si el número decimal es igual a o mayor que nuestro valor decimal más grande representado por el bit más significativo. En la posición más alta, se determina si el número de octeto es igual o superior a 128. Si el número de octeto es inferior a 128, se coloca un 0 en la posición de bit para el valor decimal 128 y se avanza a la posición de bit para el valor decimal 64.

Si el número de octeto en la posición de bit para el valor decimal 128 es mayor o igual que 128, se coloca un 1 en la posición de bit para el valor decimal 128 y se resta 128 del número de octeto que se está convirtiendo. A continuación, comparamos el resto de esta operación con el siguiente valor más pequeño, 64. Continuamos este proceso para todas las posiciones de bits restantes.

Haga clic en las figuras 1 a 6 para ver el proceso de conversión de 168 al equivalente binario de 10101000.



Capítulo 8: Asignación de direcciones IP 8.1.1.6 Conversión de decimal en binario (cont.)

Siga los pasos de conversión que se detallan en las ilustraciones para ver cómo se convierte una dirección IP a binaria.

Figura 1: Convertir 192 a binario

Figura 2: Convertir 168 a binario

Figura 3: Convertir 10 a binario

Figura 4: Convertir 10 a binario

Figura 5: Combinar los octetos convertidos comenzando con el primer octeto

Convertir de decimal a binario

192.168.10.10

11000000

	128	64	32	16	8	4	2	1
192 > 128, colocar un 1 en la posición 128 -128 restar 128	1							
64 = 64, colocar un 1 en la posición 64 -64 restar 64	1	1						
0 colocar un 0 en todas las posiciones restantes. Listo. Resultado	1	1	0	0	0	0	0	0

Convertir de decimal a binario

192.168.10.10

11000000 10101000

	128	64	32	16	8	4	2	1
168 > 128, colocar un 1 en la posición 128 -128 restar 128	1							
40 < 64, colocar un 0 en la posición 64 no restar	1	0						
40 > 32, colocar un 1 en la posición 32 -32 restar 32	1	0	1					
8 < 16, colocar un 0 en la posición 16 no restar	1	0	1	0				
8 = 8, colocar un 1 en la posición 8 restar 8	1	0	1	0	1			
0 colocar un 0 en todas las posiciones restantes Listo. Resultado	1	0	1	0	1	0	0	0

Convertir de decimal a binario

192.168.10.10

11000000 10101000 00001010

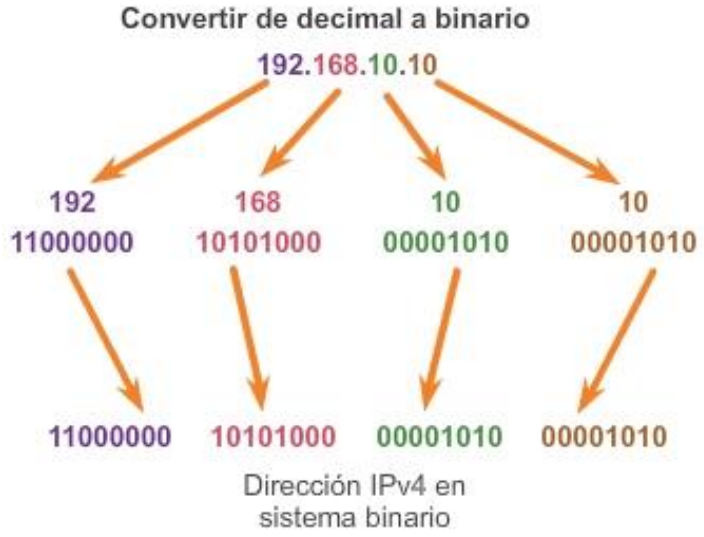
	128	64	32	16	8	4	2	1
10 < 128, colocar un 0 en la posición 128 no restar	0	0	0	0	1	0	1	0
10 < 64, colocar un 0 en la posición 64 no restar	0	0	0	0	1	0	1	0
10 < 32, colocar un 0 en la posición 32 no restar	0	0	0	0	1	0	1	0
10 < 16, colocar un 0 en la posición 16 no restar	0	0	0	0	1	0	1	0
10 > 8, colocar un 1 en la posición 8 restar 8	0	0	0	0	1	0	1	0
2 < 4, colocar un 0 en la posición 4 no restar	0	0	0	0	1	0	1	0
2 = 2, colocar un 1 en la posición 2 -2 restar 2	0	0	0	0	1	0	1	0
0 colocar un 0 en todas las posiciones restantes Listo. Resultado	0	0	0	0	1	0	1	0

Convertir de decimal a binario

192.168.10.10

11000000 10101000 00001010 00001010

	128	64	32	16	8	4	2	1
10 < 128, colocar un 0 en la posición 128 no restar	0	0	0	0	1	0	1	0
10 < 64, colocar un 0 en la posición 64 no restar	0	0	0	0	1	0	1	0
10 < 32, colocar un 0 en la posición 32 no restar	0	0	0	0	1	0	1	0
10 < 16, colocar un 0 en la posición 16 no restar	0	0	0	0	1	0	1	0
10 > 8, colocar un 1 en la posición 8 restar 8	0	0	0	0	1	0	1	0
2 < 4, colocar un 0 en la posición 4 no restar	0	0	0	0	1	0	1	0
2 = 2, colocar un 1 en la posición 2 -2 restar 2	0	0	0	0	1	0	1	0
0 colocar un 0 en todas las posiciones restantes Listo. Resultado	0	0	0	0	1	0	1	0



Dirección IPv4 en sistema binario

Capítulo 8: Asignación de direcciones IP 8.1.2.1 Porción de red y porción de host de una dirección IPv4

Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Recuerde que una dirección IP es una dirección jerárquica que consta de dos partes: una porción de red y una porción de host. Pero al determinar la porción de red en comparación con la porción de host, es necesario analizar el stream de 32 bits, y no el valor decimal. Dentro del stream de 32 bits, una parte de los bits constituye la red y una porción de los bits constituye el host.

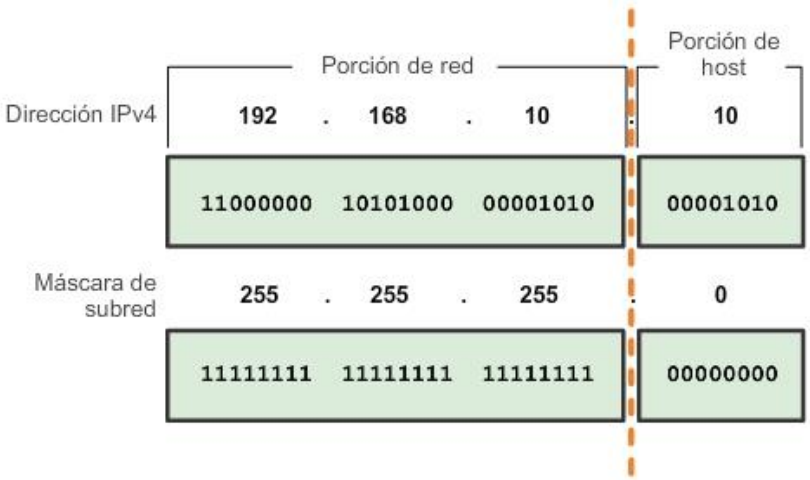
Los bits dentro de la porción de red de la dirección deben ser idénticos para todos los dispositivos que residen en la misma red. Los bits dentro de la porción de host de la dirección deben ser únicos para identificar un host específico dentro de una red. Independientemente de si los números decimales entre dos direcciones IPv4 coinciden, si dos hosts tienen el mismo patrón de bits en la porción de red especificada del stream de 32 bits, esos dos hosts residen en la misma red.

¿Pero cómo saben los hosts qué porción de los 32 bits es red y qué porción es host? Esa tarea le corresponde a la máscara de subred.

Cuando se configura un host IP, se asigna una máscara de subred junto con una dirección IP. Como sucede con la dirección IP, la máscara de subred tiene una longitud de 32 bits. La máscara de subred identifica qué parte de la dirección IP corresponde a la red y cuál al host.

La máscara de subred se compara con la dirección IP, de izquierda a derecha, bit por bit. Los 1 en la máscara de subred representan la porción de red, los 0 representan la porción de host. Como se muestra en la figura 1, la máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host. Se debe tener en cuenta que la máscara de subred no contiene en efecto la porción de red o de host de una dirección IPv4, sino que simplemente le dice a la PC dónde buscar estas porciones en una dirección IPv4 dada.

Como sucede con las direcciones IPv4, la máscara de subred se representa en formato decimal punteado por cuestiones de facilidad de uso. La máscara de subred se configura en un dispositivo host, junto con la dirección IPv4, y es necesaria para que el host pueda determinar a qué red pertenece. En la figura 2, se muestran las máscaras de subred válidas para un octeto IPv4.



Máscaras de subred válidas

Valor de subred	Valor de bit							
	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Capítulo 8: Asignación de direcciones IP 8.1.2.2 Análisis de la duración de prefijo

Prefijos de red

La duración de prefijo es otra forma de expresar la máscara de subred. La duración de prefijo es la cantidad de bits establecidos en 1 en la máscara de subred. Se escribe en “notación con barras”, una “/” seguida de la cantidad de bits establecidos en 1. Por ejemplo, si la máscara de subred es 255.255.255.0, hay 24 bits establecidos en 1 en la versión binaria de la máscara de subred, de modo que la duración de prefijo es 24 bits o /24. El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

No siempre se asigna un prefijo /24 a las redes. El prefijo asignado puede variar de acuerdo con la cantidad de hosts de la red. Tener un número de prefijo diferente cambia el rango de host y la dirección de broadcast para cada red.

En las ilustraciones, se muestran distintos prefijos que utilizan la misma dirección 10.1.1.0. En la figura 1, se ilustran los prefijos /24 a /26. En la figura 2, se ilustran los prefijos /27 a /28.

Observe que la dirección de red puede permanecer igual, pero el rango de host y la dirección de broadcast son diferentes para las diferentes duraciones de prefijos. En las ilustraciones, puede ver que la cantidad de hosts que se pueden direccionar en la red también cambia.

	Decimal punteada	Bits importantes mostrados en sistema binario
Dirección de red	**10.1.1.0/24**	**10.1.1.00000000**
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.254	10.1.1.11111110
Dirección de broadcast	10.1.1.255	10.1.1.11111111
Cantidad de hosts: 2^8 – 2 = 254 hosts		

Dirección de red	**10.1.1.0/25**	**10.1.1.00000000**
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.126	10.1.1.01111110
Dirección de broadcast	10.1.1.127	10.1.1.01111111
Cantidad de hosts: 2^7 – 2 = 126 hosts		

Dirección de red	10.1.1.0/26	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.62	10.1.1.00111110
Dirección de broadcast	10.1.1.63	10.1.1.00111111
Cantidad de hosts: 2^6 – 2 = 62 hosts		

	Decimal punteada	Bits importantes mostrados en sistema binario
Dirección de red	**10.1.1.0/27**	**10.1.1.00000000**
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.30	10.1.1.00011110
Dirección de broadcast	10.1.1.31	10.1.1.00011111
Cantidad de hosts: 2^5 – 2 = 30 hosts		

Dirección de red	10.1.1.0/28	10.1.1.00000000
Primera dirección de host	10.1.1.1	10.1.1.00000001
Última dirección de host	10.1.1.14	10.1.1.00001110
Dirección de broadcast	10.1.1.15	10.1.1.00001111
Cantidad de hosts: 2^4 – 2 = 14 hosts		

Capítulo 8: Asignación de direcciones IP 8.1.2.3 Direcciones de red, de host y de broadcast IPv4

Hay tres tipos de direcciones dentro del rango de direcciones de cada red IPv4:

- Dirección de red
- Dirección de host
- Dirección de broadcast

Dirección de red

La dirección de red es una manera estándar de hacer referencia a una red. Al referirse a la dirección de red, también es posible utilizar la máscara de subred o la duración de prefijo. Por ejemplo, la red que se muestra en la figura 1 podría indicarse como la red 10.1.1.0, la red 10.1.1.0 255.255.255.0 o la red 10.1.1.0/24. Todos los hosts en la red 10.1.1.0/24 tendrán los mismos bits de porción de red.

Como se muestra en la figura 2, dentro del rango de direcciones IPv4 de una red, la primera dirección se reserva para la dirección de red. Esta dirección tiene un 0 para cada bit de host en la porción de host de la dirección. Todos los hosts dentro de la red comparten la misma dirección de red.

Dirección de host

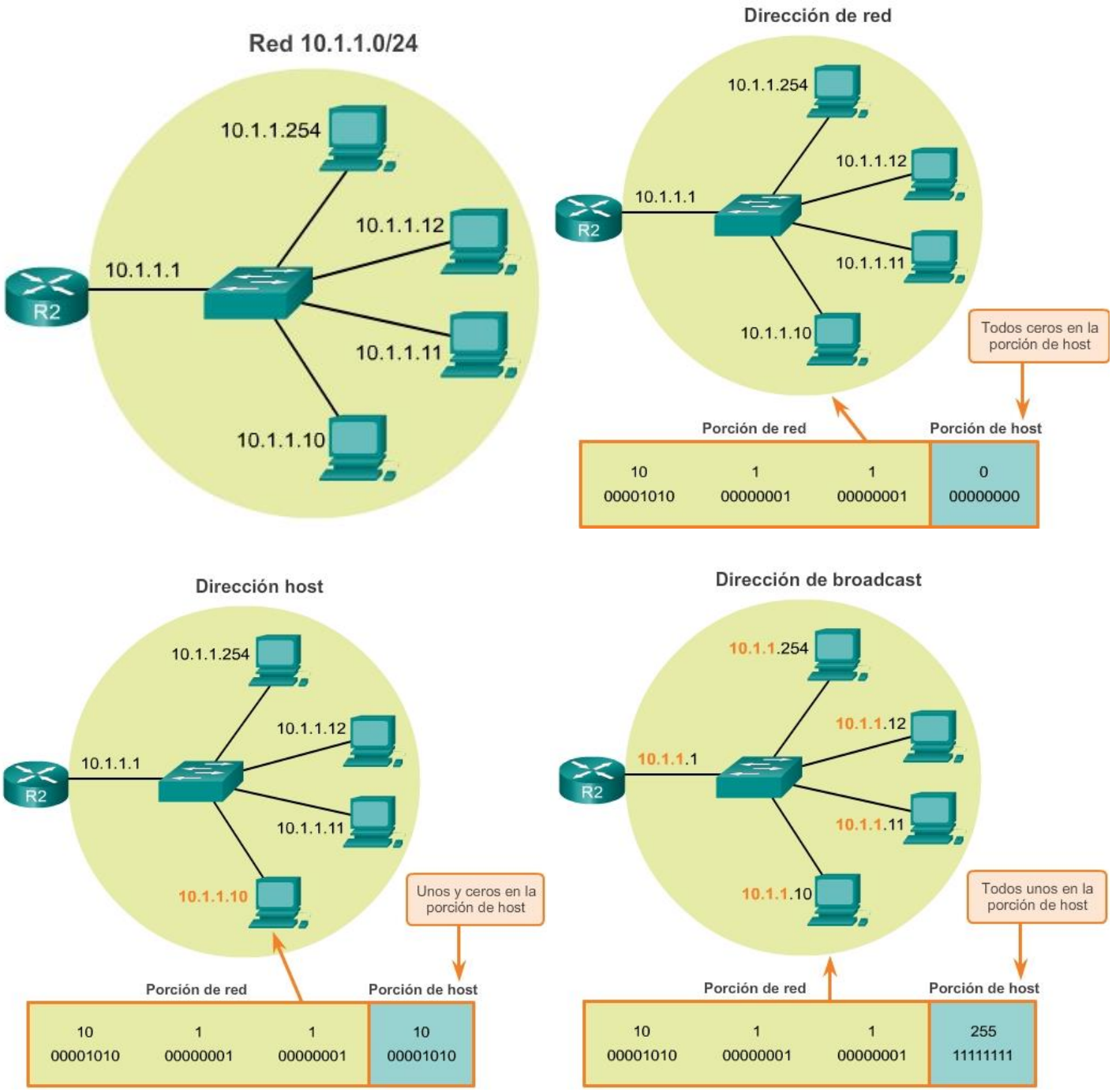
Cada dispositivo final requiere una dirección única para comunicarse en la red. En direcciones IPv4, los valores entre la dirección de red y la dirección de broadcast se pueden asignar a los dispositivos finales en una red. Como se muestra en la figura 3, esta dirección tiene cualquier combinación de bits 0 y bits 1 en la porción de host de la dirección, pero no puede contener todos bits 0 o todos bits 1.

Dirección de broadcast

La dirección de broadcast IPv4 es una dirección especial para cada red que permite la comunicación a todos los host en esa red. Para enviar datos a todos los hosts en una red a la vez, un host puede enviar un único

paquete dirigido a la dirección de broadcast de la red, y cada host en la red que recibe este paquete procesa su contenido.

La dirección de broadcast utiliza la dirección más alta en el rango de la red. Ésta es la dirección en la cual los bits de la porción de host son todos 1. Todos 1 en un octeto en forma binaria es igual al número 255 en forma decimal. Por lo tanto, como se muestra en la figura 4, para la red 10.1.1.0/24, en la cual se utiliza el último octeto para la porción de host, la dirección de broadcast sería 10.1.1.255. Observe que la porción de host no siempre es un octeto entero. A esta dirección se la conoce como broadcast dirigido.



Capítulo 8: Asignación de direcciones IP 8.1.2.4 Primera y última dirección de host

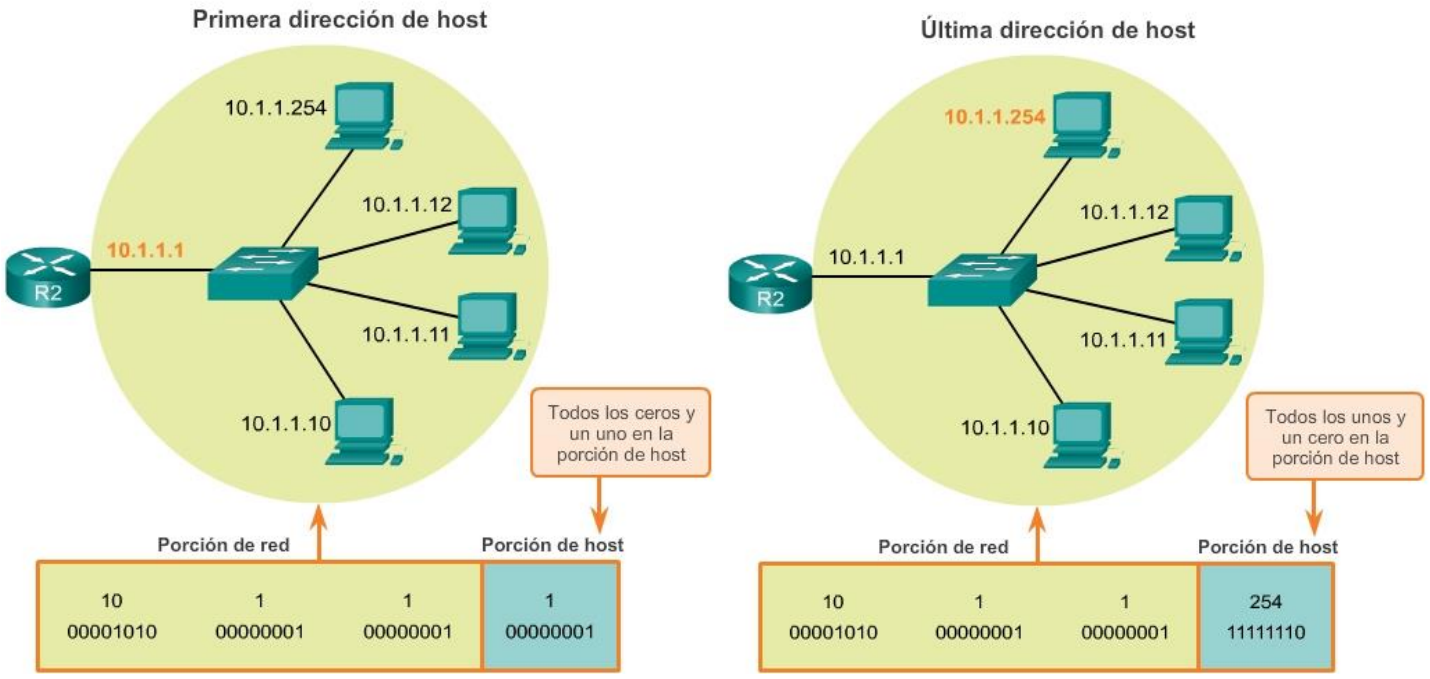
Para asegurarse de que a todos los hosts en una red se les asigne una dirección IP única dentro de ese rango de red, es importante identificar la primera y la última dirección de host. Se pueden asignar direcciones IP dentro de este rango a los hosts dentro de una red.

Primera dirección de host

Como se observa en la figura 1, la porción de host de la primera dirección de host contiene todos bits 0 con un bit 1 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre un número mayor que la dirección de red. En este ejemplo, la primera dirección de host en la red 10.1.1.0/24 es 10.1.1.1. En muchos esquemas de direccionamiento, es común utilizar la primera dirección de host del router o la dirección de gateway predeterminado.

Última dirección de host

La porción de host de la última dirección de host contiene todos bits 1, con un bit 0 que representa el bit de orden más bajo o el bit que está más a la derecha. Esta dirección es siempre una menos que la dirección de broadcast. Como se observa en la figura 2, la última dirección de host en la red 10.1.1.0/24 es 10.1.1.254.



Capítulo 8: Asignación de direcciones IP 8.1.2.5 Operación AND bit a bit

Cuando se asigna una dirección IPv4 a un dispositivo, ese dispositivo utiliza la máscara de subred para determinar a qué dirección de red pertenece. La dirección de red es la dirección que representa todos los dispositivos en la misma red.

Al enviar datos de red, el dispositivo utiliza esta información para determinar si puede enviar paquetes localmente o si debe enviarlos a un gateway predeterminado para la entrega remota. Cuando un host envía un paquete, compara la porción de red de su propia dirección IP con la porción de red de la dirección IP de destino, sobre la base de las máscaras de subred.

Si los bits de la red coinciden, tanto el host de origen como el de destino se encuentran en la misma red, y el paquete puede ser enviado localmente. Si no coinciden, el host emisor reenvía el paquete al gateway predeterminado para que se envíe a otra red.

La operación AND

AND es una de las tres operaciones binarias básicas que se utilizan en la lógica digital. Las otras dos son OR y NOT.

Mientras que las tres se usan en redes de datos, AND se usa para determinar la dirección de red. Por lo tanto, sólo se tratará aquí la lógica AND. La lógica AND es la comparación de dos bits que produce los siguientes resultados:

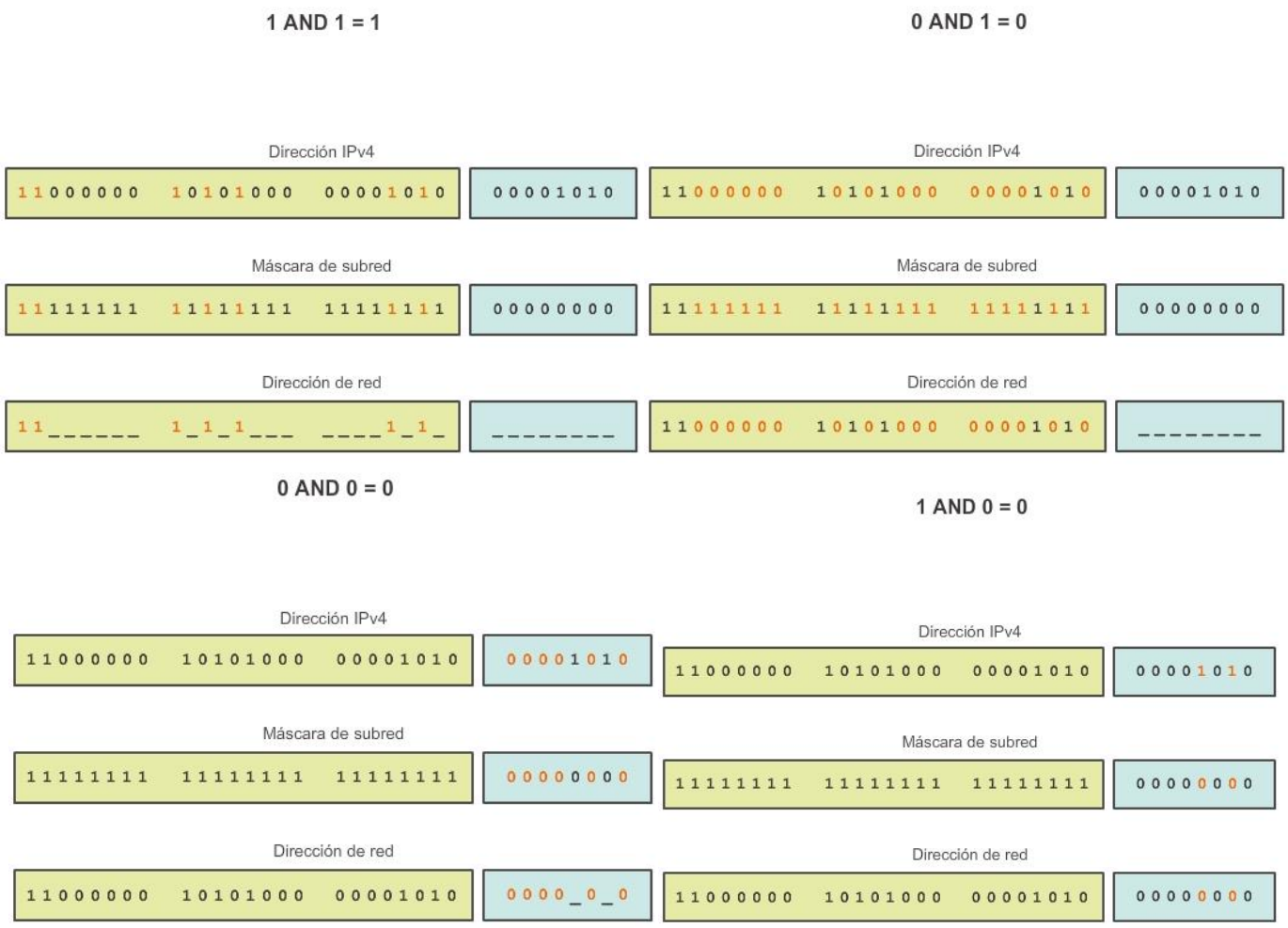
1 AND 1 = 1 (figura 1)

0 AND 1 = 0 (figura 2)

0 AND 0 = 0 (figura 3)

1 AND 0 = 0 (figura 4)

Se aplica la lógica AND a la dirección de host IPv4, bit a bit, con su máscara de subred, para determinar la dirección de red a la cual se asocia el host. Cuando se aplica esta lógica AND bit a bit entre la dirección y la máscara de subred, el resultado que se produce es la dirección de red.



Capítulo 8: Asignación de direcciones IP 8.1.2.6 Importancia de la operación AND

Si se aplica la lógica AND a cualquier bit de la dirección con valor de bit de 1 de la máscara de subred, da como resultado el valor de bit original de la dirección. Entonces, un 0 (de la dirección IPv4) AND 1 (de la máscara de subred) es 0. Un 1 (de la dirección IPv4) AND 1 (de la máscara de subred) es 1. Por lo tanto, el resultado de la aplicación de AND con un 0 en cualquier caso es 0. Estas propiedades de la operación AND se utilizan con la máscara de subred para “enmascarar” los bits de host de una dirección IPv4. Se aplica la lógica AND a cada bit de la dirección con el bit de máscara de subred correspondiente.

Debido a que todos los bits de la máscara de subred que representan bits de host son 0, la porción de host de la dirección de red resultante está formada por todos 0. Recuerde que una dirección IPv4 con todos 0 en la porción de host representa la dirección de red.

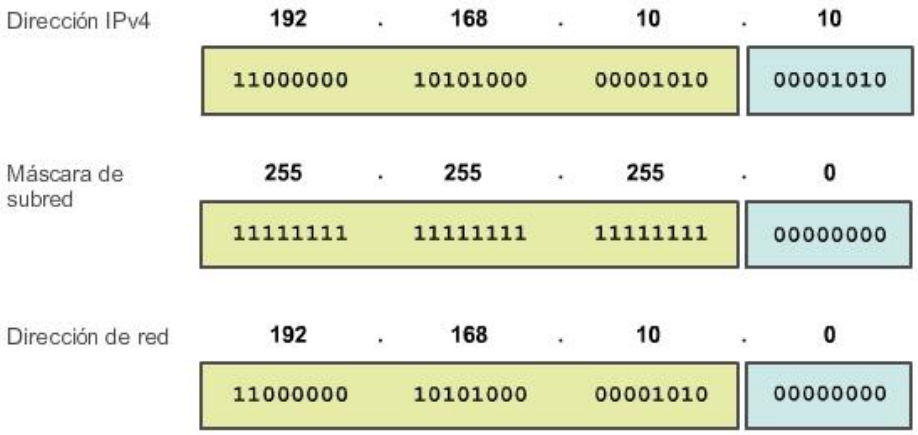
Asimismo, todos los bits de la máscara de subred que indican la porción de red son 1. Cuando se aplica la lógica AND a cada uno de estos 1 con el bit correspondiente de la dirección, los bits resultantes son idénticos a los bits de la dirección original.

Como se muestra en la ilustración, los bits 1 en la máscara de subred hacen que la porción de red de la dirección de red tenga los mismos bits que la porción de red del host. La porción de host de la dirección de red da como resultado todos 0.

En una dirección IP dada y su subred, se puede utilizar la operación AND para determinar a qué subred pertenece la dirección, así como qué otras direcciones pertenecen a la misma subred. Se debe tener en

cuenta que si dos direcciones están en la misma red o subred, se considera que son locales una respecto de la otra y, por consiguiente, pueden comunicarse directamente entre sí. Las direcciones que no se encuentran en la misma red o subred se consideran remotas respecto de sí y, por lo tanto, deben tener un dispositivo de capa 3 (como un router o un switch de capa 3) entre ellas para comunicarse.

En la verificación o resolución de problemas de red, con frecuencia es necesario determinar si dos hosts se encuentran en la misma red local. Es necesario tomar esta determinación desde el punto de vista de los dispositivos de red. Debido a una configuración incorrecta, un host puede encontrarse en una red que no era la planificada. Esto puede hacer que el funcionamiento parezca irregular, a menos que se realice el diagnóstico mediante el análisis de los procesos de aplicación de AND utilizados por el host.



Capítulo 8: Asignación de direcciones IP 8.1.3.1 Asignación de una dirección IPv4 estática a un host

Direcciones para dispositivos de usuario

En la mayoría de las redes de datos, la mayor población de hosts incluye dispositivos finales, como PC, tablet PC, smartphones, impresoras y teléfonos IP. Debido a que esta población representa la mayor cantidad de dispositivos en una red, debe asignarse la mayor cantidad de direcciones a estos hosts. A estos hosts se les asignan direcciones IP del rango de direcciones disponibles en la red. Estas direcciones IP pueden asignarse de manera estática o dinámica.

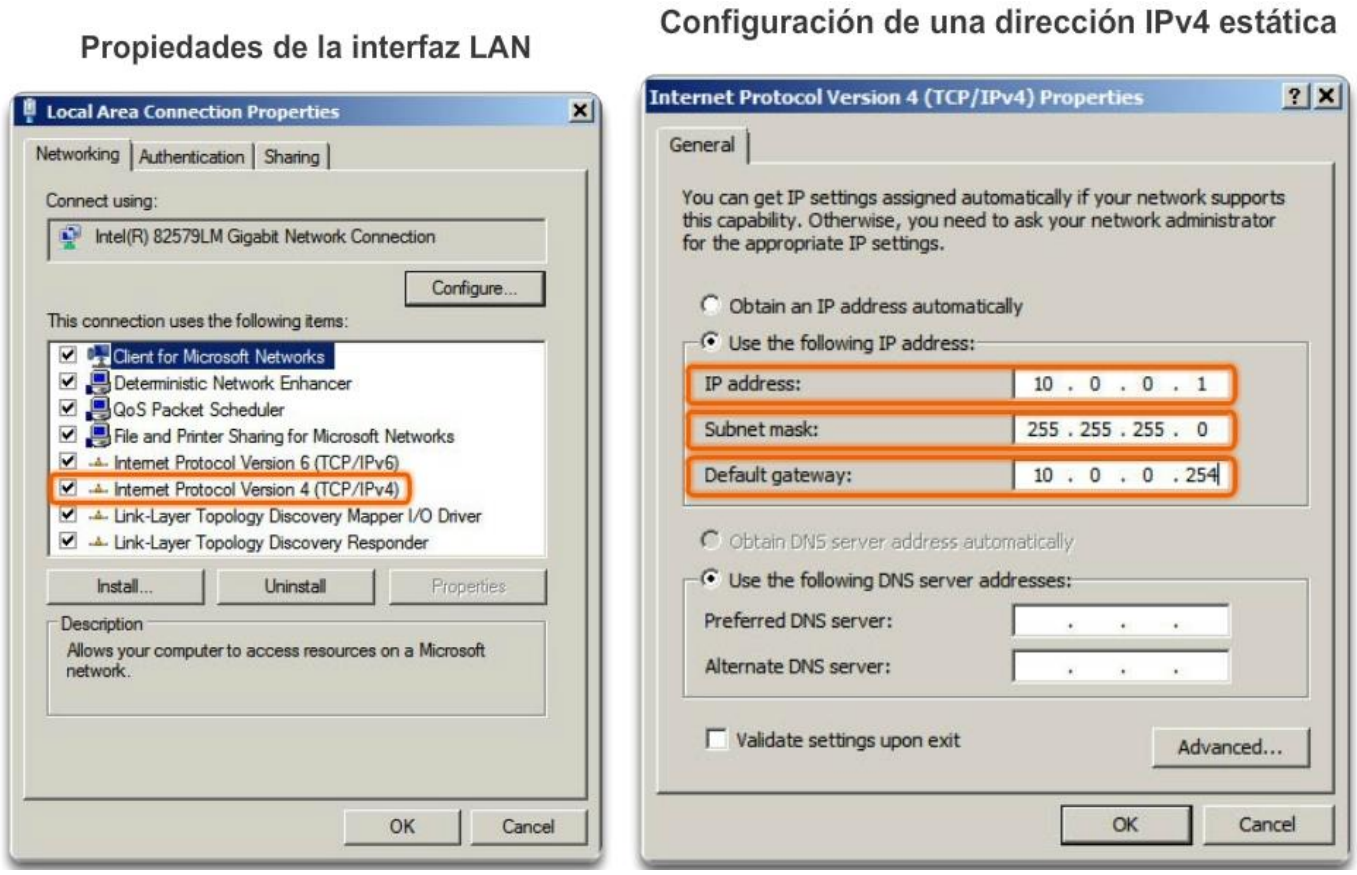
Asignación estática

Con una asignación estática, el administrador de red debe configurar manualmente la información de red para un host. En la figura 1, se muestra la ventana de las propiedades del adaptador de red. Para configurar una dirección IPv4 estática, elija IPv4 en la pantalla del adaptador de red y, a continuación, introduzca la dirección estática, la máscara de subred y el gateway predeterminado. En la figura 2, se muestra la configuración estática mínima: la dirección IP, la máscara de subred y el gateway predeterminado del host.

El direccionamiento estático tiene varias ventajas. Por ejemplo, es útil para impresoras, servidores y otros dispositivos de red que no suelen cambiar la ubicación y que deben ser accesibles para los clientes en la red sobre la base de una dirección IP fija. Si los hosts normalmente acceden a un servidor en una dirección IP en particular, esto provocaría problemas si se cambiara esa dirección. Además, la asignación estática de información de direccionamiento puede proporcionar un mayor control de los recursos de red.

Por ejemplo, es posible crear filtros de acceso sobre la base del tráfico desde y hacia una dirección IP específica. Sin embargo, introducir el direccionamiento estático en cada host puede llevar mucho tiempo.

Al utilizar direccionamiento IP estático, es necesario mantener una lista precisa de las direcciones IP asignadas a cada dispositivo. Éstas son direcciones permanentes y normalmente no vuelven a utilizarse.



Capítulo 8: Asignación de direcciones IP 8.1.3.2 Asignación de una dirección IPv4 dinámica a un host

Asignación dinámica

En las redes locales, es habitual que la población de usuarios cambie frecuentemente. Se agregan nuevos usuarios con computadoras portátiles, y esos usuarios requieren una conexión. Otros tienen estaciones de trabajo nuevas u otros dispositivos de red, como smartphones, que deben conectarse. En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más simple que las direcciones IP se asignen automáticamente. Esto se realiza mediante un protocolo conocido como Protocolo de configuración dinámica de host (DHCP), como se muestra en la figura 1.

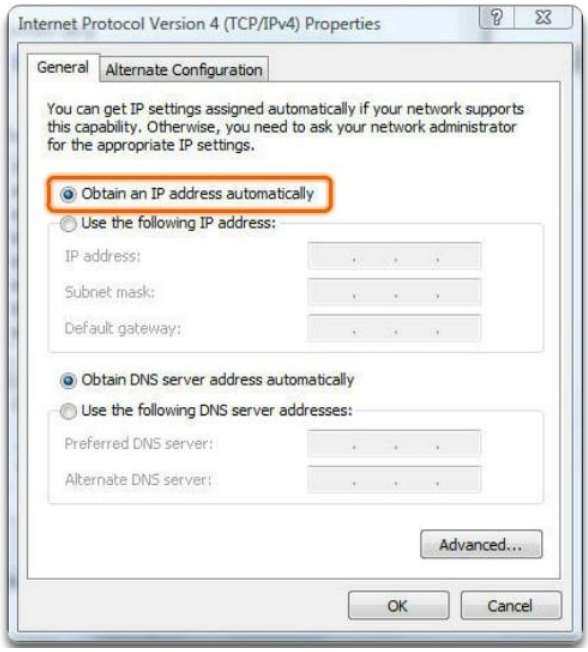
El DHCP permite la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración. La configuración del servidor de DHCP requiere que se utilice un bloque de direcciones, denominado “conjunto de direcciones”, para la asignación a los clientes DHCP en una red. Las direcciones asignadas a este conjunto deben planificarse de modo que excluyan cualquier dirección estática que utilicen otros dispositivos.

DHCP es generalmente el método preferido para asignar direcciones IPv4 a los hosts de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

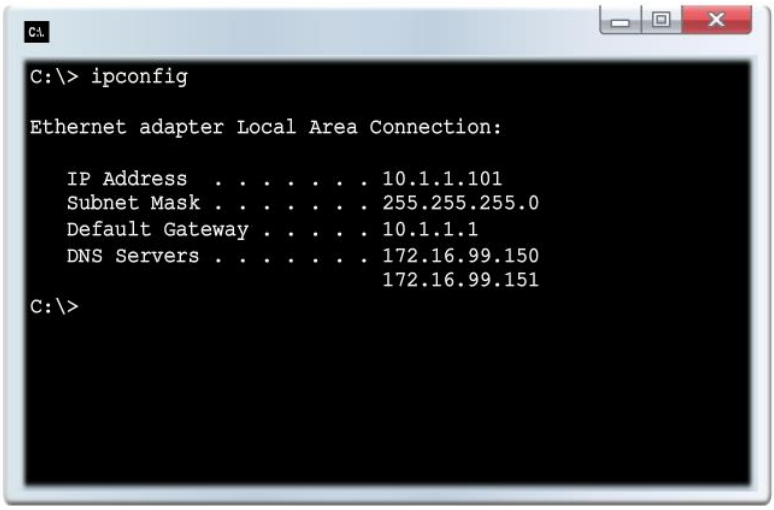
Otro beneficio de DHCP es que no se asigna de manera permanente una dirección a un host, sino que sólo se la "alquila" durante un tiempo. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esta función es muy útil para los usuarios móviles que entran y salen de la red.

Si se habilita DHCP en un dispositivo host, se puede utilizar el comando ipconfig para ver la información de la dirección IP que asigna el servidor de DHCP, como se muestra en la figura 2.

Asignación de una dirección IPv4 dinámica



Verificación de una dirección IPv4 dinámica



Capítulo 8: Asignación de direcciones IP 8.1.3.3 Transmisión de unidifusión

En una red IPv4, los hosts pueden comunicarse de una de tres maneras:

- Unicast: proceso por el cual se envía un paquete de un host a un host individual.
- Broadcast: proceso por el cual se envía un paquete de un host a todos los hosts en la red.
- Multicast: proceso por el cual se envía un paquete de un host a un grupo seleccionado de hosts, posiblemente en redes distintas.

Estos tres tipos de comunicación se utilizan con distintos objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

Tráfico unicast

La comunicación unicast se usa para la comunicación normal de host a host, tanto en redes cliente/servidor como en redes punto a punto. Los paquetes unicast utilizan las direcciones del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork.

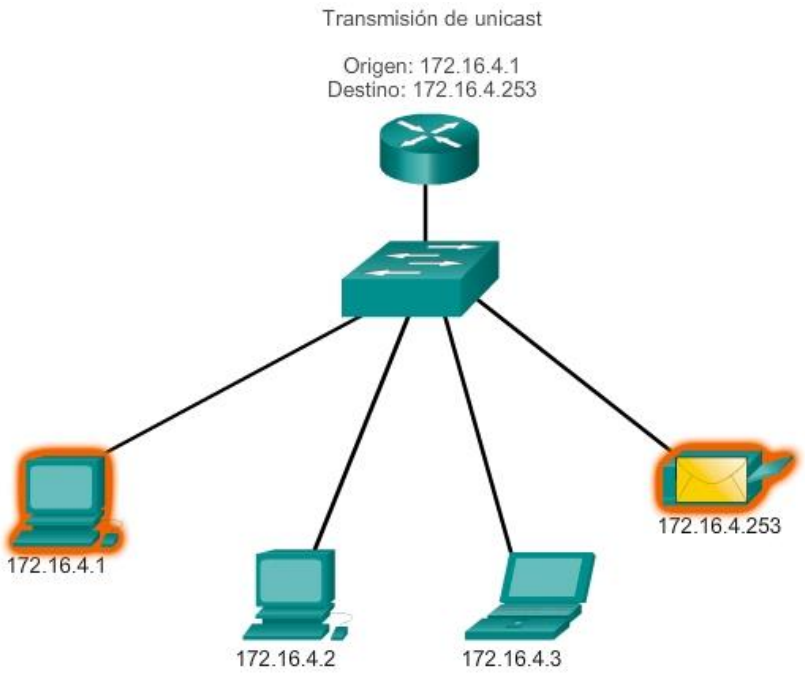
Reproduzca la animación para ver un ejemplo de transmisión unicast.

En una red IPv4, la dirección unicast aplicada a un dispositivo final se denomina “dirección de host”. En la comunicación unicast, las direcciones asignadas a dos dispositivos finales se usan como las direcciones IPv4

de origen y de destino. Durante el proceso de encapsulación, el host de origen coloca su dirección IPv4 en el encabezado del paquete unicast como la dirección de origen y la dirección IPv4 del host de destino en el encabezado del paquete como la dirección de destino. Independientemente de si el destino especificado para un paquete es unicast, broadcast o multicast, la dirección de origen de cualquier paquete es siempre la dirección unicast del host de origen.

Nota: en este curso, todas las comunicaciones entre dispositivos son comunicaciones unicast, a menos que se indique lo contrario.

Las direcciones de host IPv4 son direcciones unicast y se encuentran en el rango de direcciones de 0.0.0.0 a 223.255.255.255. Sin embargo, dentro de este rango existen muchas direcciones reservadas para fines específicos. Estas direcciones con fines específicos se analizarán más adelante en este capítulo.



Capítulo 8: Asignación de direcciones IP 8.1.3.4 Transmisión de broadcast

Transmisión de broadcast

El tráfico de broadcast se utiliza para enviar paquetes a todos los hosts en la red usando la dirección de broadcast para la red. Para broadcast, el paquete contiene una dirección IP de destino con todos unos (1) en la porción de host. Esto significa que todos los hosts de esa red local (dominio de broadcast) recibirán y verán el paquete. Muchos protocolos de red, como DHCP, utilizan broadcasts.

Cuando un host recibe un paquete enviado a la dirección de broadcast de red, el host procesa el paquete de la misma manera en la que procesaría un paquete dirigido a su dirección unicast.

Algunos ejemplos para utilizar una transmisión de broadcast son:

- Asignar direcciones de capa superior a direcciones de capa inferior
- Solicitar una dirección
- A diferencia de unicast, donde los paquetes pueden ser enrutados por toda la internetwork, los paquetes de broadcast normalmente se restringen a la red local.

Esta restricción depende de la configuración del router del gateway y del tipo de broadcast. Existen dos tipos de broadcasts: broadcast dirigido y broadcast limitado.

Broadcast dirigido

Un broadcast dirigido se envía a todos los hosts de una red específica. Este tipo de broadcast es útil para enviar un broadcast a todos los hosts de una red local. Por ejemplo, para que un host fuera de la red 172.16.4.0/24 se comunique con todos los hosts dentro de esa red, la dirección de destino del paquete sería 172.16.4.255. Aunque los routers no reenvían broadcasts dirigidos de manera predeterminada, se les puede configurar para que lo hagan.

Broadcast limitado

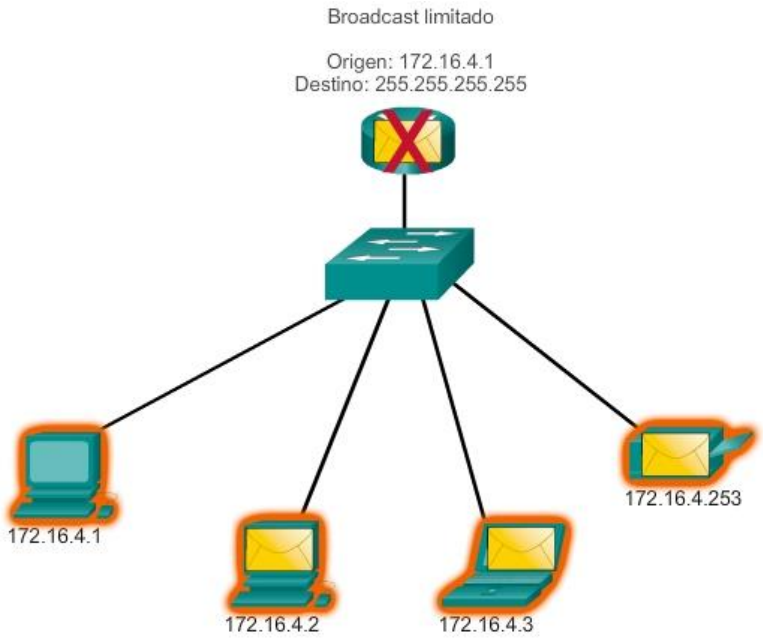
El broadcast limitado se usa para la comunicación que está limitada a los hosts en la red local. Estos paquetes siempre utilizan la dirección IPv4 de destino 255.255.255.255.

Los routers no reenvían broadcasts limitados. Por esta razón, también se hace referencia a una red IPv4 como un dominio de broadcast. Los routers son dispositivos fronterizos para un dominio de broadcast.

A modo de ejemplo, un host dentro de la red 172.16.4.0/24 transmitiría a todos los hosts en su red utilizando un paquete con una dirección de destino 255.255.255.255.

Reproduzca la animación para ver un ejemplo de transmisión de broadcast limitado.

Cuando se transmite un paquete, utiliza recursos en la red y hace que cada host receptor en la red procese el paquete. Por lo tanto, el tráfico de broadcast debe limitarse para que no afecte negativamente el rendimiento de la red o de los dispositivos. Debido a que los routers separan dominios de broadcast, subdividir las redes con tráfico de broadcast excesivo puede mejorar el rendimiento de la red.



Capítulo 8: Asignación de direcciones IP 8.1.3.5 Transmisión de multicast

Transmisión de multicast

La transmisión de multicast está diseñada para conservar el ancho de banda de las redes IPv4. Reduce el tráfico al permitir que un host envíe un único paquete a un conjunto seleccionado de hosts que forman parte de un grupo multicast suscrito. Para alcanzar hosts de destino múltiples mediante la comunicación unicast, sería necesario que el host de origen envíe un paquete individual dirigido a cada host. Con multicast, el host de origen puede enviar un único paquete que llegue a miles de hosts de destino. La responsabilidad de la internetwork es reproducir los flujos multicast en un modo eficaz para que alcancen solamente a los destinatarios.

Algunos ejemplos de transmisión de multicast son:

- Transmisiones de video y de audio
- Intercambio de información de enrutamiento por medio de protocolos de enrutamiento
- Distribución de software
- Juegos remotes

Direcciones multicast

IPv4 tiene un bloque de direcciones reservadas para direccionar grupos multicast. Este rango de direcciones va de 224.0.0.0 a 239.255.255.255. El rango de direcciones multicast está subdividido en distintos tipos de direcciones: direcciones de enlace local reservadas y direcciones agrupadas globalmente. Un tipo adicional de dirección multicast son las direcciones agrupadas administrativamente, también llamadas direcciones de agrupamiento limitado.

Las direcciones IPv4 multicast de 224.0.0.0 a 224.0.0.255 son direcciones de enlace local reservadas. Estas direcciones se utilizarán con grupos multicast en una red local. Un router conectado a la red local reconoce que estos paquetes están dirigidos a un grupo multicast de enlace local y nunca los reenvía nuevamente. Un uso común de las direcciones de link-local reservadas se da en los protocolos de enrutamiento usando transmisión multicast para intercambiar información de enrutamiento.

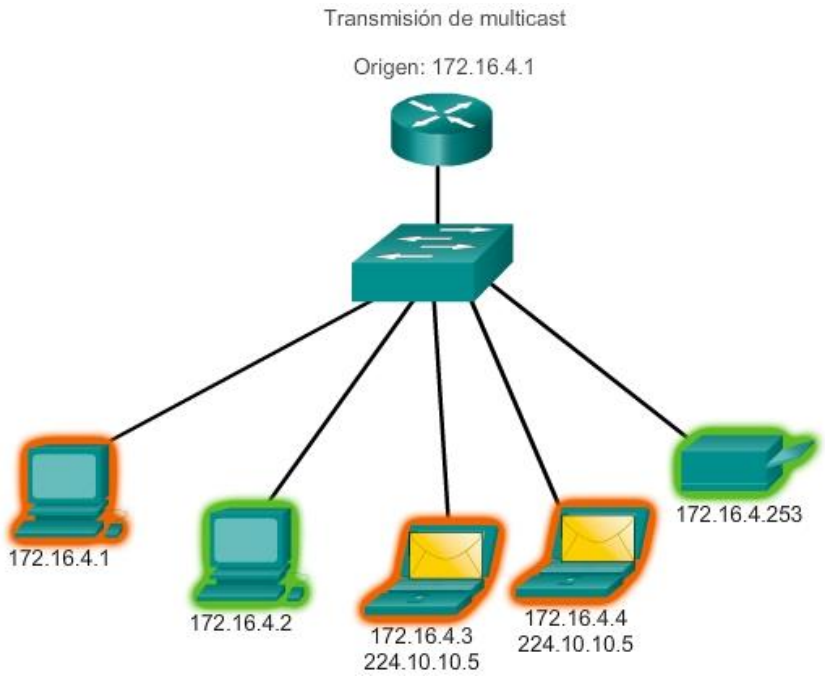
Las direcciones agrupadas globalmente son de 224.0.1.0 a 238.255.255.255. Se les puede usar para transmitir datos en Internet mediante multicast. Por ejemplo, se reservó 224.0.1.1 para que el protocolo de hora de red (NTP) sincronice los relojes con la hora del día de los dispositivos de red.

Clientes multicast

Los hosts que reciben datos multicast específicos se denominan “clientes multicast”. Los clientes multicast utilizan servicios solicitados por un programa cliente para subscribirse al grupo multicast.

Cada grupo multicast está representado por una sola dirección IPv4 de destino multicast. Cuando un host IPv4 se suscribe a un grupo multicast, el host procesa paquetes dirigidos a esta dirección multicast y paquetes dirigidos a su dirección unicast asignada exclusivamente.

La animación muestra clientes que aceptan paquetes multicast.



Capítulo 8: Asignación de direcciones IP 8.1.3.8 Packet Tracer: investigación del tráfico unidifusión, difusión y multidifusión

En esta actividad, se examina el comportamiento de unicast, broadcast y multicast. La mayoría del tráfico de una red es unicast. Cuando una PC envía una solicitud de eco ICMP a un router remoto, la dirección de origen en el encabezado del paquete IP es la dirección IP de la PC emisora. La dirección de destino en el encabezado del paquete IP es la dirección IP de la interfaz del router remoto. El paquete se envía sólo al destino deseado.

Mediante el comando ping o la característica Add Complex PDU (Agregar PDU compleja) de Packet Tracer, puede hacer ping directamente a las direcciones de broadcast para ver el tráfico de broadcast.

Para el tráfico de multicast, consultará el tráfico de EIGRP. Los routers Cisco utilizan EIGRP para intercambiar información de enrutamiento entre routers.

Los routers que utilizan EIGRP envían paquetes a la dirección multicast 224.0.0.10, que representa el grupo de routers EIGRP. Si bien estos paquetes son recibidos por otros dispositivos, todos los dispositivos (excepto los routers EIGRP) los descartan en la capa 3, sin requerir otro procesamiento.

Capítulo 8: Asignación de direcciones IP 8.1.4.1 Direcciones IPv4 públicas y privadas

Aunque la mayoría de las direcciones IPv4 de host son direcciones públicas designadas para uso en redes a las que se accede desde Internet, existen bloques de direcciones que se utilizan en redes que requieren o no acceso limitado a Internet. Estas direcciones se denominan direcciones privadas.

Direcciones privadas

Los bloques de direcciones privadas son:

10.0.0.0 a 10.255.255.255 (10.0.0.0/8)

172.16.0.0 a 172.31.255.255 (172.16.0.0/12)

192.168.0.0 a 192.168.255.255 (192.168.0.0/16)

Las direcciones privadas se definen en RFC 1918, Asignación de direcciones para redes de Internet privadas, y en ocasiones se hace referencia a ellas como direcciones RFC 1918. Los bloques de direcciones de espacio privado, como se muestra en la ilustración, se utilizan en redes privadas. Los hosts que no requieren acceso a Internet pueden utilizar direcciones privadas. Sin embargo, dentro de la red privada, los hosts aún requieren direcciones IP únicas dentro del espacio privado.

Hosts en distintas redes pueden utilizar las mismas direcciones de espacio privado. Los paquetes que utilizan estas direcciones como la dirección de origen o de destino no deberían aparecer en la Internet pública.

El router o el dispositivo de firewall del perímetro de estas redes privadas deben bloquear o convertir estas direcciones. Incluso si estos paquetes fueran a llegar hasta Internet, los routers no tendrían rutas para reenviarlos a la red privada correcta.

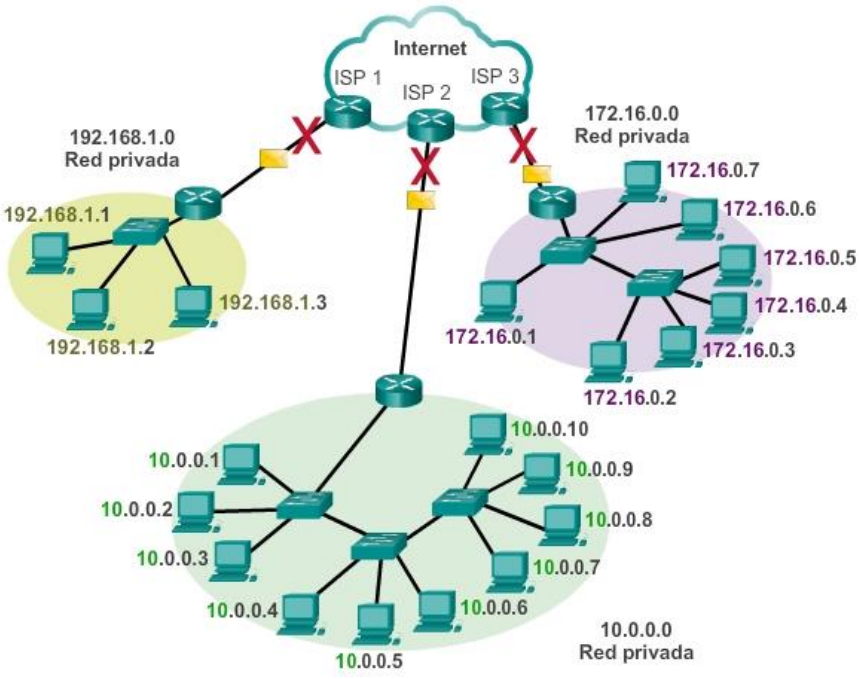
En RFC 6598, IANA reservó otro grupo de direcciones conocidas como “espacio de dirección compartido”. Como sucede con el espacio de dirección privado definido en RFC 1918, las direcciones del espacio de dirección compartido no son enrutables globalmente.

Sin embargo, el propósito de estas direcciones es solamente ser utilizadas en redes de proveedores de servicios. El bloque de direcciones compartido es 100.64.0.0/10.

Direcciones públicas

La amplia mayoría de las direcciones en el rango de host unicast IPv4 son direcciones públicas. Estas direcciones están diseñadas para ser utilizadas en los hosts de acceso público desde Internet. Aun dentro de estos bloques de direcciones IPv4, existen muchas direcciones designadas para otros fines específicos.

Las direcciones privadas no se pueden enrutar a través de Internet.



Capítulo 8: Asignación de direcciones IP 8.1.4.3 Direcciones IPv4 de uso especial

Existen determinadas direcciones que no pueden asignarse a los hosts. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones respecto de la forma en que dichos hosts pueden interactuar dentro de la red.

Direcciones de red y de broadcast

Como se explicó anteriormente, no es posible asignar la primera ni la última dirección a hosts dentro de cada red. Éstas son, respectivamente, la dirección de red y la dirección de broadcast.

Loopback

Una de estas direcciones reservadas es la dirección de loopback IPv4 127.0.0.1. La dirección de loopback es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos.

La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores del stack de TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local.

A pesar de que sólo se usa la dirección única 127.0.0.1, se reservan las direcciones 127.0.0.0 a 127.255.255.255. Cualquier dirección dentro de este bloque producirá un loop back al host local. Las direcciones dentro de este bloque no deben figurar en ninguna red.

Direcciones link-local

Las direcciones IPv4 del bloque de direcciones que va de 169.254.0.0 a 169.254.255.255 (169.254.0.0/16) se designan como direcciones link-local.

El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se pueden utilizar en una red punto a punto pequeña o para un host que no pudo obtener una dirección de un servidor de DHCP automáticamente.

La comunicación mediante direcciones link-local IPv4 sólo es adecuada para comunicarse con otros dispositivos conectados a la misma red, como se muestra en la figura. Un host no debe enviar un paquete con una dirección de destino link-local IPv4 a ningún router para ser reenviado, y debería establecer el tiempo de vida (TLL) de IPv4 para estos paquetes en 1.

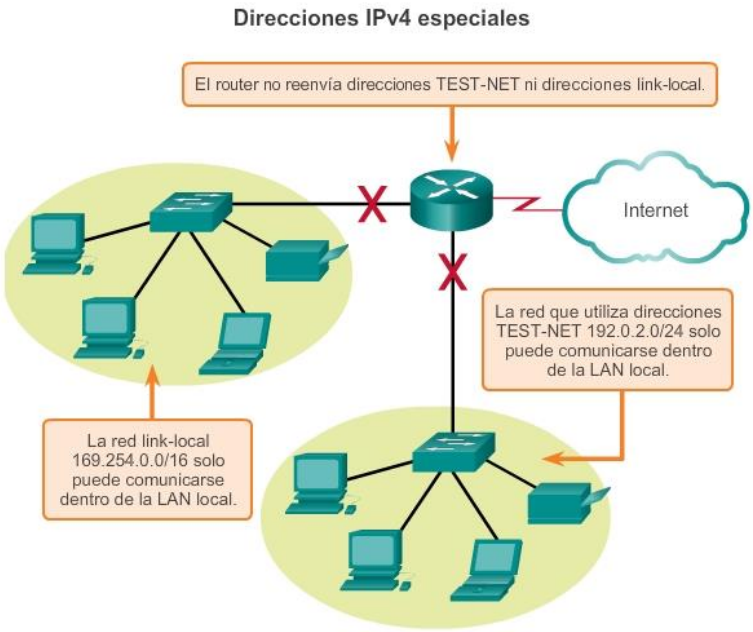
Las direcciones link-local no proporcionan servicios fuera de la red local. Sin embargo, muchas aplicaciones de cliente/servidor y punto a punto funcionarán correctamente con direcciones de enlace local IPv4.

Direcciones TEST-NET

El bloque de direcciones que va de 192.0.2.0 a 192.0.2.255 (192.0.2.0/24) se reserva para fines de enseñanza y aprendizaje. Estas direcciones pueden usarse en ejemplos de documentación y redes. A diferencia de las direcciones experimentales, los dispositivos de red aceptarán estas direcciones en su configuración. A menudo puede encontrar que estas direcciones se usan con los nombres de dominio example.com o example.net en la documentación de las RFC, del fabricante y del protocolo. Las direcciones dentro de este bloque no deben aparecer en Internet.

Direcciones experimentales

Las direcciones del bloque que va de 240.0.0.0 a 255.255.255.254 se indican como reservadas para uso futuro (RFC 3330). En la actualidad, estas direcciones solo se pueden utilizar para fines de investigación o experimentación, y no se pueden utilizar en una red IPv4. Sin embargo, según RFC 3330, podrían, técnicamente, convertirse en direcciones utilizables en el futuro.



Capítulo 8: Asignación de direcciones IP 8.1.4.4 Direccionamiento con clase antigua

Históricamente, RFC1700, Assigned Numbers (Números asignados), agrupaba rangos unicast en tamaños específicos llamados “direcciones de clase A, de clase B y de clase C”. También definía a las direcciones de clase D (multicast) y de clase E (experimental), anteriormente tratadas. Las direcciones unicast de clases A, B y C definían redes de tamaños específicos y bloques de direcciones específicos para estas redes.

Se asignó a una compañía u organización todo un bloque de direcciones de clase A, clase B o clase C. Este uso de espacio de dirección se denomina direccionamiento con clase.

Bloques de clase A

Se diseñó un bloque de direcciones de clase A para admitir redes extremadamente grandes con más de 16 millones de direcciones host. Las direcciones IPv4 de clase A usaban un prefijo /8 fijo, donde el primer octeto indicaba la dirección de red. Los tres octetos restantes se usaban para las direcciones host. Todas las direcciones de clase A requerían que el bit más significativo del octeto de orden superior fuera un cero. Esto significaba que había solo 128 redes de clase A posibles, 0.0.0.0/8 a 127.0.0.0/8.

A pesar de que las direcciones de clase A reservaban la mitad del espacio de direcciones, debido al límite de 128 redes, sólo podían ser asignadas a aproximadamente 120 compañías u organizaciones.

Bloques de clase B

El espacio de direcciones de clase B fue diseñado para admitir las necesidades de redes de tamaño moderado a grande con hasta aproximadamente 65 000 hosts. Una dirección IP de clase B usaba los dos octetos de orden superior para indicar la dirección de red. Los dos octetos restantes especificaban las

direcciones host. Al igual que con la clase A, debía reservarse espacio de direcciones para las clases de direcciones restantes. Con las direcciones de clase B, los dos bits más significativos del octeto de orden superior eran 10. Esto restringía el bloque de direcciones para la clase B a 128.0.0.0/16 hasta 191.255.0.0/16. La clase B tenía una asignación de direcciones ligeramente más eficaz que la clase A, debido a que dividía equitativamente el 25% del total del espacio total de direcciones IPv4 entre alrededor de 16 000 redes.

Bloques de clase C

El espacio de direcciones de clase C era la clase de direcciones antiguas más comúnmente disponible. Este espacio de direcciones tenía el propósito de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts. Los bloques de direcciones de clase C utilizaban el prefijo /24. Esto significaba que una red de clase C usaba sólo el último octeto como direcciones host, con los tres octetos de orden superior para indicar la dirección de red. Los bloques de direcciones de clase C reservaban espacio de dirección utilizando un valor fijo de 110 para los tres bits más significativos del octeto de orden superior. Esto restringía el bloque de direcciones para la clase C a 192.0.0.0/24 hasta 223.255.255.0/24. A pesar de que ocupaba solo el 12,5% del total del espacio de direcciones IPv4, podía proporcionar direcciones a dos millones de redes.

En la figura 1, se ilustra cómo se dividen estas clases de direcciones.

Limitaciones del sistema basado en clases

No todos los requisitos de las organizaciones se ajustaban a una de estas tres clases. La asignación con clase de espacio de direcciones a menudo desperdiciaba muchas direcciones, lo cual agotaba la disponibilidad de direcciones IPv4. Por ejemplo: una compañía con una red con 260 hosts necesitaría que se le otorgue una dirección de clase B con más de 65.000 direcciones.

A pesar de que este sistema con clase no fue abandonado hasta finales de la década del 90, es posible ver restos de estas redes en la actualidad. Por ejemplo, cuando asigna una dirección IPv4 a una PC, el sistema operativo examina la dirección que se asigna, a fin de determinar si esta dirección es una dirección de clase A, de clase B o de clase C.

A continuación, el sistema operativo supone el prefijo utilizado por esa clase y lleva a cabo la asignación de la máscara de subred predeterminada.

Direccionamiento sin clase

El sistema que se utiliza en la actualidad se denomina “direccionamiento sin clase”. El nombre formal es “enrutamiento entre dominios sin clase” (CIDR, pronunciado “cider”). La asignación con clase de direcciones IPv4 era muy ineficaz, y permitía solo las duraciones de prefijo /8, /16 o /24, cada una de un espacio de dirección distinto. En 1993, el IETF creó un nuevo conjunto de estándares que permitía que los proveedores de servicios asignaran direcciones IPv4 en cualquier límite de bits de dirección (duración de prefijo) en lugar de solo con una dirección de clase A, B o C.

El IETF sabía que el CIDR era solo una solución temporal y que sería necesario desarrollar un nuevo protocolo IP para admitir el rápido crecimiento de la cantidad de usuarios de Internet. En 1994, el IETF comenzó a trabajar para encontrar un sucesor de IPv4, que finalmente fue IPv6.

En la figura 2, se muestran los rangos de direcciones con clase.

```
11111111.00000000.00000000.00000000   /8 (255.0.0.0) 16,777,214 direcciones de host
11111111.10000000.00000000.00000000   /9 (255.128.0.0) 8,388,606 direcciones de host
11111111.11000000.00000000.00000000  /10 (255.192.0.0) 4,194,302 direcciones de host
11111111.11100000.00000000.00000000  /11 (255.224.0.0) 2,097,150 direcciones de host
11111111.11110000.00000000.00000000  /12 (255.240.0.0) 1,048,574 direcciones de host
11111111.11111000.00000000.00000000  /13 (255.248.0.0) 524,286 direcciones de host
11111111.11111100.00000000.00000000  /14 (255.252.0.0) 262,142 direcciones de host
11111111.11111110.00000000.00000000  /15 (255.254.0.0) 131,070 direcciones de host
11111111.11111111.00000000.00000000  /16 (255.255.0.0) 65,534 direcciones de host
11111111.11111111.10000000.00000000  /17 (255.255.128.0) 32,766 direcciones de host
11111111.11111111.11000000.00000000  /18 (255.255.192.0) 16,382 direcciones de host
11111111.11111111.11100000.00000000  /19 (255.255.224.0) 8,190 direcciones de host
11111111.11111111.11110000.00000000  /20 (255.255.240.0) 4,094 direcciones de host
11111111.11111111.11111000.00000000  /21 (255.255.248.0) 2,046 direcciones de host
11111111.11111111.11111100.00000000  /22 (255.255.252.0) 1,022 direcciones de host
11111111.11111111.11111110.00000000  /23 (255.255.254.0) 510 direcciones de host
11111111.11111111.11111111.00000000  /24 (255.255.255.0) 254 direcciones de host
11111111.11111111.11111111.10000000  /25 (255.255.255.128) 126 direcciones de host
11111111.11111111.11111111.11000000  /26 (255.255.255.192) 62 direcciones de host
11111111.11111111.11111111.11100000  /27 (255.255.255.224) 30 direcciones de host
11111111.11111111.11111111.11110000  /28 (255.255.255.240) 14 direcciones de host
11111111.11111111.11111111.11111000  /29 (255.255.255.248) 6 direcciones de host
11111111.11111111.11111111.11111100  /30 (255.255.255.252) 2 direcciones de host
11111111.11111111.11111111.11111110  /31 (255.255.255.254) 0 direcciones de host
11111111.11111111.11111111.11111111  /32 (255.255.255.255) "Ruta de host"
```

Clases de direcciones IP

Clase de dirección	Rango del 1er octeto (decimal)	Bits del primer octeto (los bits verdes no cambian)	Red (N) y Host (H) partes de la dirección	Máscara de subred predeterminada (decimal y binaria)
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0
B	128-191	10000000- 10111111	N.N.H.H	255.255.0.0
C	192-223	11000000- 11011111	N.N.N.H	255.255.255.0
D	224-239	11100000- 11101111	No disponible (multicast)	
E	240-255	11110000- 11111111	No disponible (experimental)	

Nota: una combinación de todos ceros (0) o de todos unos (1) constituye direcciones de hos

Capítulo 8: Asignación de direcciones IP 8.1.4.5 Asignación de direcciones IP

Para que una compañía u organización tenga hosts de red, como servidores Web, a los que se pueda acceder desde Internet, dicha organización debe tener un bloque de direcciones públicas asignado. Se debe tener en cuenta que las direcciones públicas deben ser únicas, y el uso de estas direcciones públicas se regula y se asigna a cada organización de forma independiente. Esto es válido para las direcciones IPv4 e IPv6.

IANA y RIR

La Internet Assigned Numbers Authority (IANA) (http://www.iana.org) administra la asignación de direcciones IPv4 e IPv6. Hasta mediados de los años noventa, todo el espacio de direcciones IPv4 era directamente administrado por la IANA.

En ese entonces, se asignó el resto del espacio de direcciones IPv4 a otros diversos registros para que realicen la administración de áreas regionales o con propósitos particulares. Estas compañías de registro se llaman registros regionales de Internet (RIR), como se muestra en la figura.

Los principales registros son:

- AfriNIC (African Network Information Centre), región África http://www.afrinic.net
- APNIC (Asia Pacific Network Information Centre), región Asia/Pacífico http://www.apnic.net
- ARIN (American Registry for Internet Numbers), región América del Norte http://www.arin.net
- LACNIC (Regional Latin-American and Caribbean IP Address Registry), América Latina y algunas islas del Caribe http://www.lacnic.net
- RIPE NCC (Reseaux IP Europeans), Europa, Medio Oriente y Asia Central http://www.ripe.net

Proveedores de servicios de Internet (ISP)

Los RIR se encargan de asignar direcciones IP a los proveedores de servicios de Internet (ISP). La mayoría de las compañías u organizaciones obtiene sus bloques de direcciones IPv4 de un ISP. Un ISP generalmente suministrará una pequeña cantidad de direcciones IPv4 utilizables (6 ó 14) a sus clientes como parte de los servicios. Se pueden obtener bloques mayores de direcciones de acuerdo con la justificación de las necesidades y con un costo adicional por el servicio.

En cierto sentido, el ISP presta o alquila estas direcciones a la organización. Si se elige cambiar la conectividad de Internet a otro ISP, el nuevo ISP suministrará direcciones de los bloques de direcciones que ellos poseen, y el ISP anterior devuelve los bloques prestados a su asignación para prestarlos nuevamente a otro cliente.

Las direcciones IPv6 se pueden obtener del ISP o, en algunos casos, directamente del RIR. Las direcciones IPv6 y los tamaños típicos de los bloques de direcciones se analizarán más adelante en este capítulo.

Capítulo 8: Asignación de direcciones IP 8.1.4.6 Asignación de direcciones IP (cont.)

Servicios del ISP

Para tener acceso a los servicios de Internet, tenemos que conectar nuestra red de datos a Internet usando un proveedor de servicios de Internet (ISP).

Los ISP poseen sus propios conjuntos de redes internas de datos para administrar la conectividad a Internet y ofrecer servicios relacionados. Entre los demás servicios que los ISP suelen proporcionar a sus clientes se encuentran los servicios DNS, los servicios de correo electrónico y un sitio Web. Dependiendo del nivel de servicio requerido y disponible, los clientes usan diferentes niveles de un ISP.

Niveles del ISP

Los ISP se designan mediante una jerarquía basada en su nivel de conectividad al backbone de Internet. Cada nivel inferior obtiene conectividad al backbone por medio de la conexión a un ISP de nivel superior, como se muestra en las ilustraciones.

Nivel 1

Como se muestra en la figura 1, en la cima de la jerarquía de ISP se encuentran los ISP de nivel 1.

Estos son grandes ISP a nivel nacional o internacional que se conectan directamente al backbone de Internet. Los clientes de ISP de nivel 1 son ISP de menor nivel o grandes compañías y organizaciones. Debido a que se encuentran en la cima de la conectividad a Internet, ofrecen conexiones y servicios altamente confiables. Entre las tecnologías utilizadas como apoyo de esta confiabilidad se encuentran múltiples conexiones al backbone de Internet.

Las principales ventajas para los clientes de ISP de nivel 1 son la confiabilidad y la velocidad.

Debido a que estos clientes están a sólo una conexión de distancia de Internet, hay menos oportunidades de que se produzcan fallas o cuellos de botella en el tráfico. La desventaja para los clientes de ISP de nivel 1 es el costo elevado.

Nivel 2

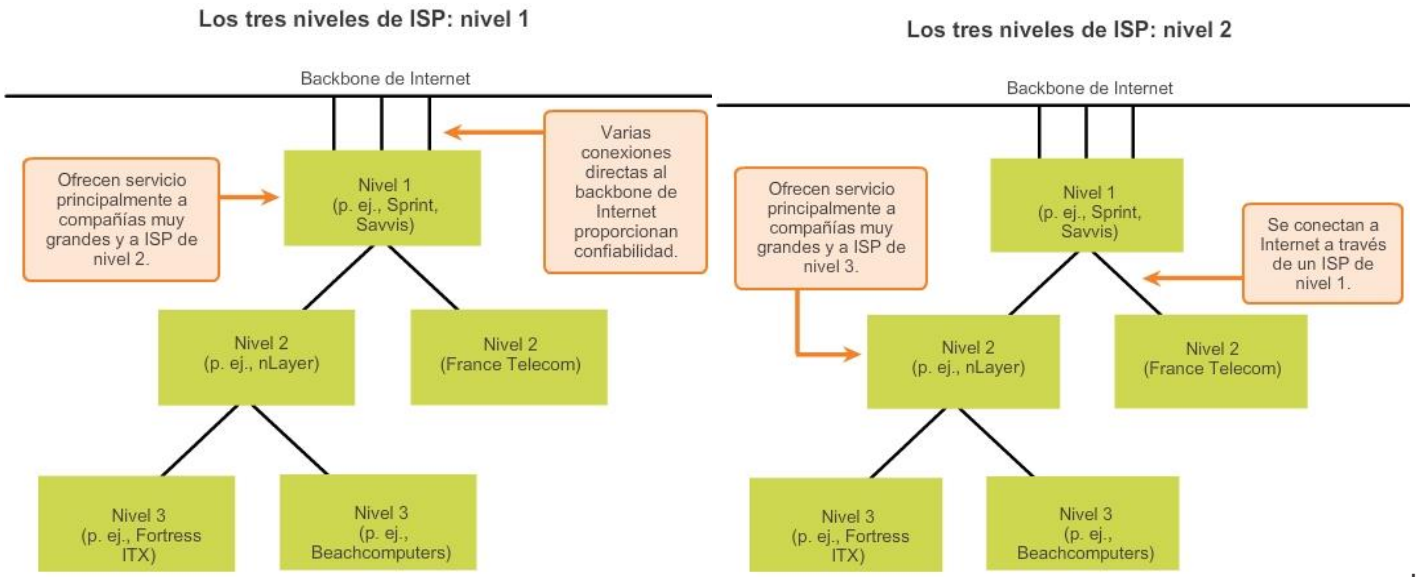
Como se muestra en la figura 2, los ISP de nivel 2 adquieren su servicio de Internet de los ISP de nivel 1. Los ISP de nivel 2 generalmente se centran en los clientes empresa. Los ISP de nivel 2 normalmente ofrecen más servicios que los ISP de los otros dos niveles. Estos ISP de nivel 2 suelen tener recursos de TI para ofrecer sus propios servicios, como DNS, servidores de correo electrónico y servidores Web. Otros servicios ofrecidos por los ISP de nivel 2 pueden incluir desarrollo y mantenimiento de sitios web, e-commerce/e-business y VoIP.

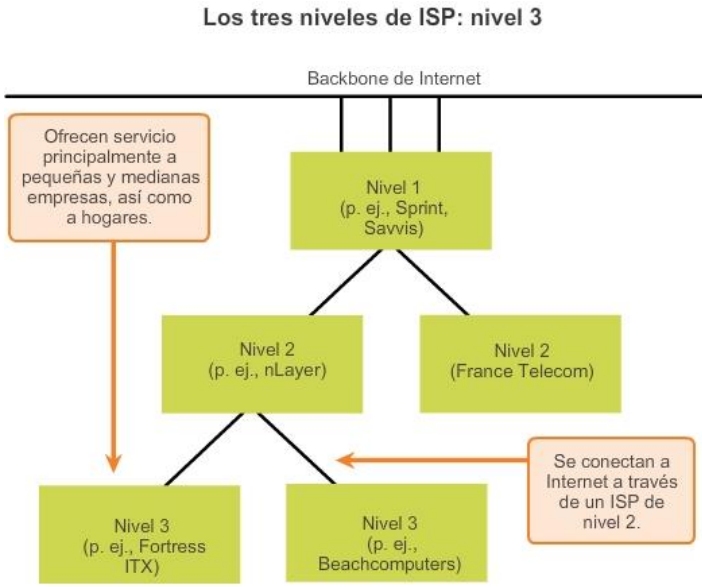
La principal desventaja de los ISP de nivel 2, comparados con los ISP de nivel 1, es el acceso más lento a Internet. Como los IPS de Nivel 2 están al menos a una conexión más lejos de la red troncal de Internet, tienden a tener menor confiabilidad que los IPS de Nivel 1.

Nivel 3

Como se muestra en la figura 3, los ISP de nivel 3 adquieren su servicio de Internet de los ISP de nivel 2. El objetivo de estos ISP son los mercados minoristas y del hogar en una ubicación específica. Típicamente, los clientes del nivel 3 no necesitan muchos de los servicios requeridos por los clientes del nivel 2. Su necesidad principal es conectividad y soporte.

Estos clientes a menudo tienen conocimiento escaso o nulo sobre computación o redes. Los ISP de nivel 3 suelen incluir la conectividad a Internet como parte del contrato de servicios de red y computación para los clientes. A pesar de que pueden tener un menor ancho de banda y menos confiabilidad que los proveedores de nivel 1 y 2, suelen ser buenas opciones para pequeñas y medianas empresas.





Capítulo 8: Asignación de direcciones IP 8.2.1.1 Necesidad de utilizar IPv6

IPv6 está diseñado para ser el sucesor de IPv4. IPv6 tiene un mayor espacio de direcciones de 128 bits, lo que proporciona 340 sextillones de direcciones. (Eso es el número 340 seguido de 36 ceros). Sin embargo, IPv6 es mucho más que una mera dirección más extensa. Cuando el IETF comenzó el desarrollo de una sucesora de IPv4, utilizó esta oportunidad para corregir las limitaciones de IPv4 e incluir mejoras adicionales. Un ejemplo es el protocolo de mensajes de control de Internet versión 6 (ICPMv6), que incluye la resolución de direcciones y la configuración automática de direcciones, las cuales no se encuentran en ICMP para IPv4 (ICMPv4). ICMPv4 e ICMPv6 se analizarán más adelante en este capítulo.

Necesidad de utilizar IPv6

El agotamiento del espacio de direcciones IPv4 fue el factor que motivó la migración a IPv6. Debido al aumento de la conexión a Internet en África, Asia y otras áreas del mundo, las direcciones IPv4 ya no son suficientes para admitir este crecimiento. El lunes 31 de enero de 2011, la IANA asignó los últimos dos bloques de direcciones IPv4 /8 a los registros regionales de Internet (RIR). Diversas proyecciones indican que

entre 2015 y 2020 se habrán acabado las direcciones IPv4 en los cinco RIR. En ese momento, las direcciones IPv4 restantes se habrán asignado a los ISP.

IPv4 tiene un máximo teórico de 4300 millones de direcciones. Las direcciones privadas definidas en RFC 1918 junto con la traducción de direcciones de red (NAT) fueron un factor determinante para retardar el agotamiento del espacio de direcciones IPv4. La NAT tiene limitaciones que obstaculizan gravemente las comunicaciones punto a punto.

Internet de las cosas

En la actualidad, Internet es significativamente distinta de como era en las últimas décadas. Hoy en día, Internet es más que correo electrónico, páginas Web y transferencia de archivos entre PC. Internet evoluciona y se está convirtiendo en una Internet de las cosas. Los dispositivos que acceden a Internet ya no serán solamente PC, tablet PC y smartphones. Los dispositivos del futuro preparados para acceder a Internet y equipados con sensores incluirán desde automóviles y dispositivos biomédicos hasta electrodomésticos y ecosistemas naturales. Imagine una reunión en la ubicación de un cliente que se programa en forma automática en la aplicación de calendario para que comience una hora antes de la hora en que normalmente comienza a trabajar. Esto podría ser un problema importante, en especial si olvida revisar el calendario o ajustar el despertador según corresponda.

Ahora imagine que la aplicación de calendario comunica esta información directamente al despertador para usted y su automóvil. El automóvil calienta automáticamente para derretir el hielo del limpiaparabrisas antes de que usted ingrese y cambia la ruta hacia el lugar de la reunión.

Con una creciente población de Internet, un espacio limitado de direcciones IPv4, problemas con la NAT y con Internet de las cosas, llegó el momento de iniciar la transición a IPv6.

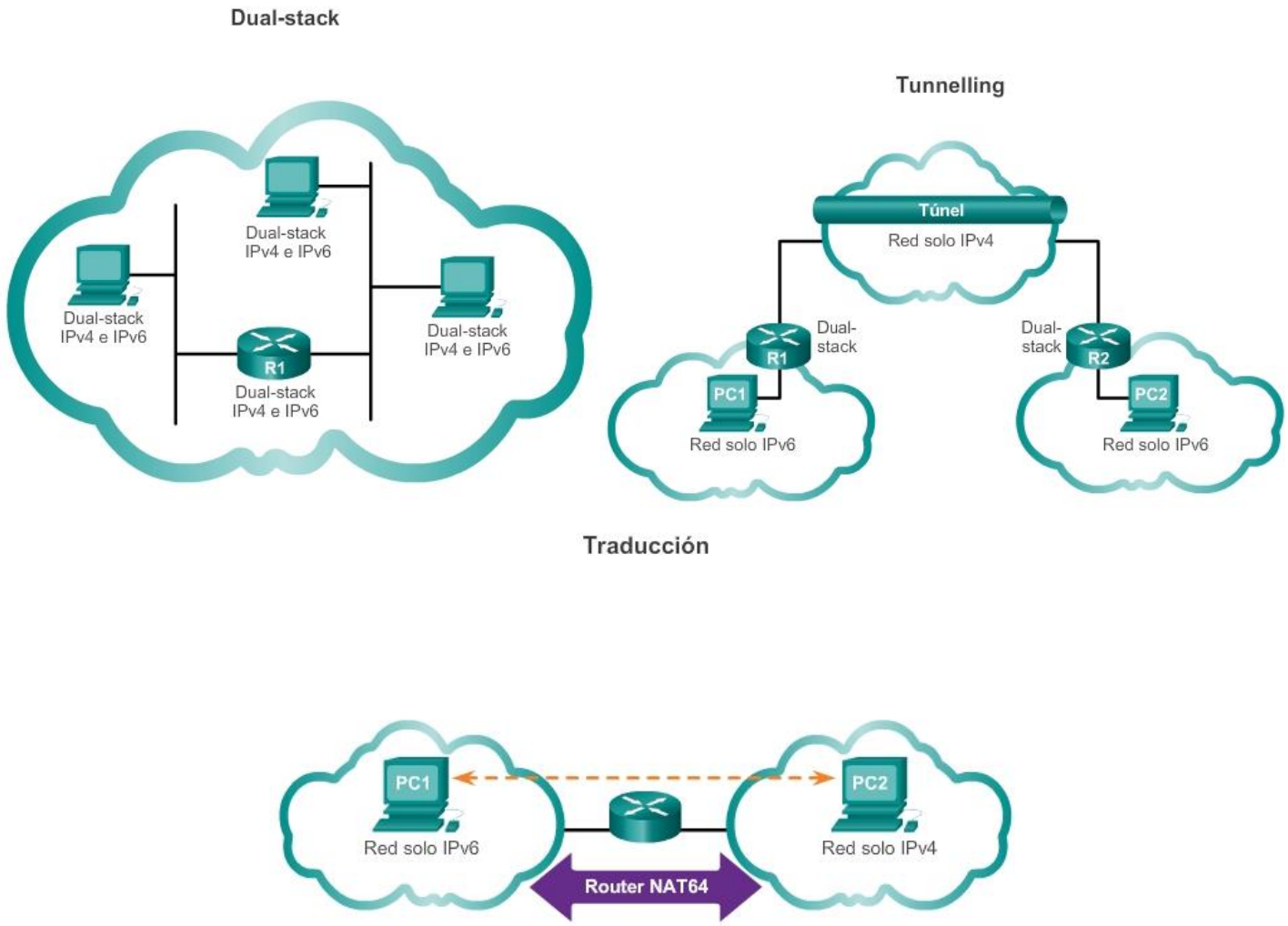
Capítulo 8: Asignación de direcciones IP 8.2.1.2 Coexistencia de IPv4 e IPv6

No hay una única fecha para realizar la transición a IPv6. En un futuro cercano, IPv4 e IPv6 coexistirán. Se espera que la transición demore años. El IETF creó diversos protocolos y herramientas para ayudar a los administradores de red a migrar las redes a IPv6. Las técnicas de migración pueden dividirse en tres categorías:

- Dual-stack: como se muestra en la figura 1, la técnica dual-stack permite que IPv4 e IPv6 coexistan en la misma red. Los dispositivos dual-stack ejecutan stacks de protocolos IPv4 e IPv6 de manera simultánea.

- Tunneling: como se muestra en la figura 2, tunneling es un método para transportar paquetes IPv6 a través de redes IPv4. El paquete IPv6 se encapsula dentro de un paquete IPV4, de manera similar a lo que sucede con otros tipos de datos.

- Traducción: como se muestra en la figura 3, la traducción de direcciones de red 64 (NAT64) permite que los dispositivos con IPv6 habilitado se comuniquen con dispositivos con IPv4 habilitado mediante una técnica de traducción similar a la NAT para IPv4. Un paquete IPv6 se traduce en un paquete IPV4, y viceversa.



Capítulo 8: Asignación de direcciones IP 8.2.2.1 Sistema numérico hexadecimal

A diferencia de las direcciones IPv4, que se expresan en notación decimal punteada, las direcciones IPv6 se representan mediante valores hexadecimales. Usted observó que el formato hexadecimal se utiliza en el panel Packets Byte (Byte del paquete) de Wireshark. En Wireshark, el formato hexadecimal se utiliza para representar los valores binarios dentro de tramas y paquetes. El formato hexadecimal también se utiliza para representar las direcciones de control de acceso al medio (MAC) de Ethernet.

Numeración hexadecimal

El método hexadecimal ("Hex") es una manera conveniente de representar valores binarios. Así como el sistema de numeración decimal es un sistema de base diez y el binario es un sistema de base dos, el sistema hexadecimal es un sistema de base dieciséis.

El sistema de numeración de base 16 utiliza los números del 0 al 9 y las letras de la A a la F. En la figura 1, se muestran los valores hexadecimales, binarios y decimales equivalentes. Existen 16 combinaciones únicas de cuatro bits, de 0000 a 1111. El sistema hexadecimal de16 dígitos es el sistema de numeración perfecto para utilizar, debido a que cuatro bits cualesquiera se pueden representar con un único valor hexadecimal.

Comprensión de los bytes

Dado que 8 bits (un byte) es una agrupación binaria común, los binarios 00000000 hasta 11111111 pueden representarse en valores hexadecimales como el intervalo 00 a FF. Se pueden mostrar los ceros iniciales para completar la representación de 8 bits. Por ejemplo, el valor binario 0000 1010 se muestra en valor hexadecimal como 0A.

Representación de valores hexadecimales

Nota: en lo que respecta a los caracteres del 0 al 9, es importante distinguir los valores hexadecimales de los decimales.

Por lo general, los valores hexadecimales se representan en forma de texto mediante el valor precedido por 0x (por ejemplo, 0x73) o un subíndice 16. Con menor frecuencia, pueden estar seguidos de una H, por ejemplo, 73H. Sin embargo, y debido a que el texto en subíndice no es reconocido en entornos de línea de comando o de programación, la representación técnica de un valor hexadecimal es precedida de "0x" (cero X). Por lo tanto, los ejemplos anteriores deberían mostrarse como 0x0A y 0x73, respectivamente.

Conversiones hexadecimales

Las conversiones numéricas entre valores decimales y hexadecimales son simples, pero no siempre es conveniente dividir o multiplicar por 16.

Con la práctica, es posible reconocer los patrones de bits binarios que coinciden con los valores decimales y hexadecimales. En la figura 2, se muestran estos patrones para valores seleccionados de 8 bits.

Representación de valores hexadecimales

Hexadecimal	Decimal	Binario
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Conversión de octetos binarios a valores hexadecimales

Hexadecimal	Decimal	Binario
00	0	00000000
01	1	00000001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	00001010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	10000000
C0	192	11000000
EC	202	1100 1010
F0	240	11110000
FF	255	11111111

Capítulo 8: Asignación de direcciones IP 8.2.2.2 Representación de dirección IPv6

Las direcciones IPv6 tienen una longitud de 128 bits y se escriben como una cadena de valores hexadecimales. Cuatro bits se representan mediante un único dígito hexadecimal, con un total de 32 valores hexadecimales. Las direcciones IPv6 no distinguen mayúsculas de minúsculas y pueden escribirse en minúscula o en mayúscula.

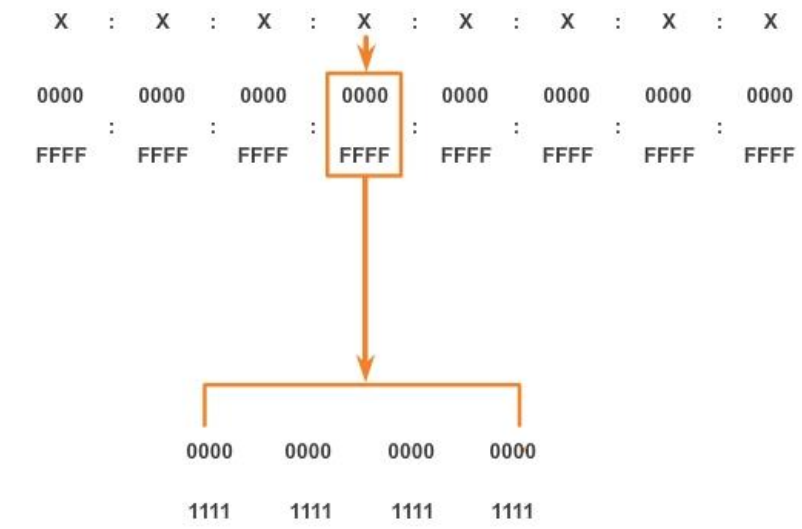
Formato preferido

Como se muestra en la figura 1, el formato preferido para escribir una dirección IPv6 es x:x:x:x:x:x:x:x, donde cada “x” consta de cuatro valores hexadecimales. Al hacer referencia a 8 bits de una dirección IPv4, utilizamos el término “octeto”.

En IPv6, un “hexteto” es el término no oficial que se utiliza para referirse a un segmento de 16 bits o cuatro valores hexadecimales. Cada “x” es un único hexteto, 16 bits o cuatro dígitos hexadecimales.

“Formato preferido” significa que la dirección IPv6 se escribe utilizando 32 dígitos hexadecimales. No significa necesariamente que es el método ideal para representar la dirección IPv6. En las siguientes páginas, veremos dos reglas que permiten reducir el número de dígitos necesarios para representar una dirección IPv6.

En la figura 2, se muestran ejemplos de direcciones IPv6 en el formato preferido.



2001	0DB8	0000	1111	0000	0000	0000	0200
2001	0DB8	0000	00A3	ABCD	0000	0000	1234
2001	0DB8	000A	0001	0000	0000	0000	0100
2001	0DB8	AAAA	0001	0000	0000	0000	0200
FE80	0000	0000	0000	0123	4567	89AB	CDEF
FE80	0000	0000	0000	0000	0000	0000	0001
FF02	0000	0000	0000	0000	0000	0000	0001
FF02	0000	0000	0000	0000	0001	FF00	0200
0000	0000	0000	0000	0000	0000	0000	0001
0000	0000	0000	0000	0000	0000	0000	0000

Capítulo 8: Asignación de direcciones IP 8.2.2.3 Regla 1: Omisión de ceros iniciales

La primera regla que permite reducir la notación de direcciones IPv6 es que se puede omitir cualquier 0 (cero) inicial en cualquier sección de 16 bits o hexteto. Por ejemplo:

- 01AB puede representarse como 1AB.
- 09F0 puede representarse como 9F0.
- 0A00 puede representarse como A00.
- 00AB puede representarse como AB.

Esta regla solo es válida para los ceros iniciales, y NO para los ceros finales; de lo contrario, la dirección sería ambigua. Por ejemplo, el hexteto “ABC” podría ser tanto “0ABC” como “ABC0”.

En las figuras 1 a 8, se muestran varios ejemplos de cómo se puede utilizar la omisión de ceros iniciales para reducir el tamaño de una dirección IPv6. Se muestra el formato preferido para cada ejemplo. Advierta cómo la

omisión de ceros iniciales en la mayoría de los ejemplos da como resultado una representación más pequeña de la dirección.

Omisión de ceros iniciales

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin 0 inicial	2001: DB8: 0:1111: 0: 0: 0: 200

Recomendado	2001:0DB8:0000:A300:ABCD:0000:0000:1234
Sin 0 inicial	2001: DB8: 0:A300:ABCD: 0: 0:1234

Recomendado	2001:0DB8:000A:1000:0000:0000:0000:0100
Sin 0 inicial	2001: DB8: A:1000: 0: 0: 0: 100

Recomendado	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Sin 0 inicial	FE80: 0: 0: 0: 123:4567:89AB:CDEF

Recomendado	FF02:0000:0000:0000:0000:0000:0000:0001
Sin 0 inicial	FF02: 0: 0: 0: 0: 0: 0: 1

Recomendado	FF02:0000:0000:0000:0000:0001:FF00:0200
Sin 0 inicial	FF02: 0: 0: 0: 0: 1:FF00: 200

Recomendado	0000:0000:0000:0000:0000:0000:0000:0001
Sin 0 inicial	0: 0: 0: 0: 0: 0: 0: 1

Recomendado	0000:0000:0000:0000:0000:0000:0000:0000
Sin 0 inicial	0: 0: 0: 0: 0: 0: 0: 0

Capítulo 8: Asignación de direcciones IP 8.2.2.4 Regla 2: Omisión de los segmentos compuestos por todos ceros

La segunda regla que permite reducir la notación de direcciones IPv6 es que los dos puntos dobles (::) pueden reemplazar cualquier cadena única y contigua de uno o más segmentos de 16 bits (hextetos) compuestos solo por ceros.

Los dos puntos dobles (::) se pueden utilizar solamente una vez dentro de una dirección; de lo contrario, habría más de una dirección resultante posible. Cuando se utiliza junto con la técnica de omisión de ceros iniciales, la notación de direcciones IPv6 generalmente se puede reducir de manera considerable. Esto se suele conocer como “formato comprimido”.

Dirección incorrecta:

- 2001:0DB8::ABCD::1234

Expansiones posibles de direcciones comprimidas ambiguas:

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

En las figuras 1 a 7, se muestran varios ejemplos de cómo el uso de los dos puntos dobles (::) y la omisión de ceros iniciales puede reducir el tamaño de una dirección IPv6.

Uso de dos puntos dobles

Recomendado	2001:0DB8:0000:1111:0000:0000:0000:0200
Sin 0 inicial	2001: DB8: 0:1111: 0: 0: 0: 200
Comprimida	2001:DB8:0:1111::200

Recomendado	2001:0DB8:0000:0000:ABCD:0000:0000:0100
Sin 0 inicial	2001: DB8: 0: 0:ABCD: 0: 0: 100
Comprimida	2001:DB8::ABCD:0:0:100
o	
Comprimida	2001:DB8:0:0:ABCD::100

Se puede utilizar solo un "::"

Recomendado	FE80:0000:0000:0000:0123:4567:89AB:CDEF
Sin 0 inicial	FE80: 0: 0: 0: 123:4567:89AB:CDEF
Comprimida	FE80::123:4567:89AB:CDEF

Recomendado	FF02:0000:0000:0000:0000:0000:0000:0001
Sin 0 inicial	FF02: 0: 0: 0: 0: 0: 0: 1
Comprimida	FF02::1

Recomendado	FF02:0000:0000:0000:0000:0001:FF00:0200
Sin 0 inicial	FF02: 0: 0: 0: 0: 1:FF00: 200
Comprimida	FF02::1:FF00:200

Recomendado	0000:0000:0000:0000:0000:0000:0000:0001
Sin 0 inicial	0: 0: 0: 0: 0: 0: 0: 1
Comprimida	::1

Recomendado	0000:0000:0000:0000:0000:0000:0000:0000
Sin 0 inicial	0: 0: 0: 0: 0: 0: 0: 0
Comprimida	::

Capítulo 8: Asignación de direcciones IP 8.2.3.1 Tipos de direcciones IPv6

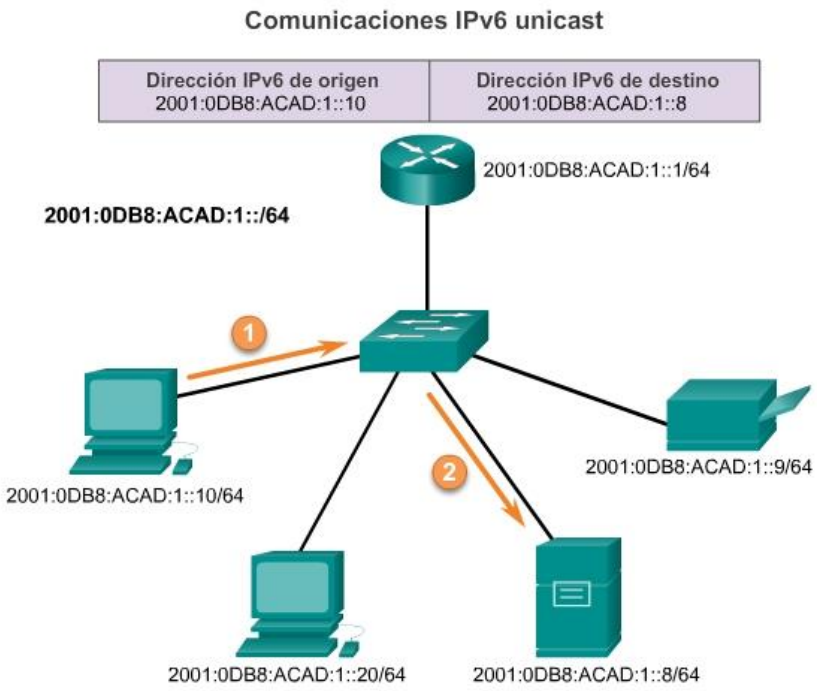
Existen tres tipos de direcciones IPv6:

- Unicast: las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Como se muestra en la ilustración, las direcciones IPv6 de origen deben ser direcciones unicast.

- Multicast: las direcciones IPv6 multicast se utilizan para enviar un único paquete IPv6 a varios destinos.

- Anycast: las direcciones IPv6 anycast son direcciones IPv6 unicast que se pueden asignar a varios dispositivos. Los paquetes enviados a una dirección anycast se enrutan al dispositivo más cercano que tenga esa dirección. En este curso, no se analizan las direcciones anycast.

A diferencia de IPv4, IPv6 no tiene una dirección de broadcast. Sin embargo, existe una dirección IPv6 multicast de todos los nodos que brinda básicamente el mismo resultado.

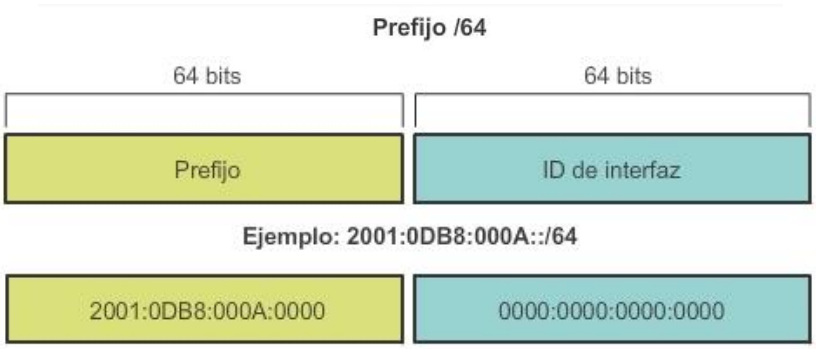


Capítulo 8: Asignación de direcciones IP 8.2.3.2 Duración de prefijo IPv6

Recuerde que es posible identificar el prefijo, o la porción de red, de una dirección IPv4 mediante una máscara de subred en formato decimal punteado o una duración de prefijo (notación con barras). Por ejemplo, la dirección IP 192.168.1.10 con la máscara de subred decimal punteada 255.255.255.0 equivale a 192.168.1.10/24.

IPv6 utiliza la duración de prefijo para representar la porción de prefijo de la dirección. IPv6 no utiliza la notación decimal punteada de máscara de subred. La duración de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el formato de dirección IPv6/duración de prefijo.

La duración de prefijo puede ir de 0 a 128. Una duración de prefijo IPv6 típica para LAN y la mayoría de los demás tipos de redes es /64. Esto significa que la porción de prefijo o de red de la dirección tiene una longitud de 64 bits, lo cual deja otros 64 bits para la ID de interfaz (porción de host) de la dirección.



Capítulo 8: Asignación de direcciones IP 8.2.3.3 Direcciones IPv6 unicast

Las direcciones IPv6 unicast identifican de forma exclusiva una interfaz en un dispositivo con IPv6 habilitado. Un paquete que se envía a una dirección unicast es recibido por la interfaz que tiene asignada esa dirección. Como sucede con IPv4, las direcciones IPv6 de origen deben ser direcciones unicast. Las direcciones IPv6 de destino pueden ser direcciones unicast o multicast.

Existen seis tipos de direcciones IPv6 unicast.

Unicast global

Las direcciones unicast globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones unicast globales pueden configurarse estáticamente o asignarse de forma dinámica. Existen algunas diferencias importantes con respecto a la forma en que un dispositivo recibe su dirección IPv6 dinámicamente en comparación con DHCP para IPv4.

Link-local

Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los routers no reenvían paquetes con una dirección de origen o de destino link-local.

Loopback

Los hosts utilizan la dirección de loopback para enviarse paquetes a sí mismos, y esta dirección no se puede asignar a una interfaz física. Al igual que en el caso de una dirección IPv4 de loopback, se puede hacer ping a una dirección IPv6 de loopback para probar la configuración de TCP/IP en el host local. La dirección IPv6 de loopback está formada por todos ceros, excepto el último bit, representado como ::1/128 o, simplemente, ::1 en el formato comprimido.

Dirección sin especificar

Una dirección sin especificar es una dirección compuesta solo por ceros representada como ::/128 o, simplemente, :: en formato comprimido. No puede asignarse a una interfaz y solo se utiliza como dirección de origen en un paquete IPv6. Las direcciones sin especificar se utilizan como direcciones de origen cuando el dispositivo aún no tiene una dirección IPv6 permanente o cuando el origen del paquete es irrelevante para el destino.

Local única

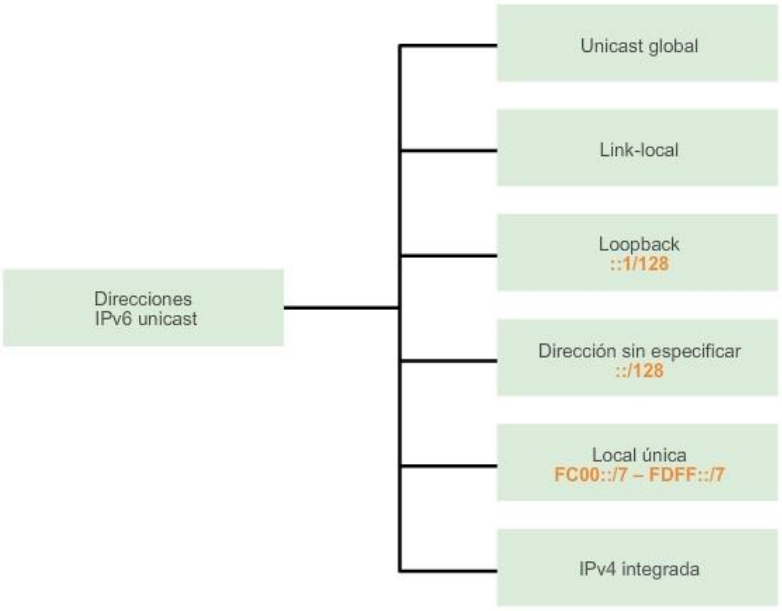
Las direcciones IPv6 locales únicas tienen cierta similitud con las direcciones privadas para IPv4 definidas en RFC 1918, pero también existen diferencias importantes. Las direcciones locales únicas se utilizan para el direccionamiento local dentro de un sitio o entre una cantidad limitada de sitios. Estas direcciones no deben ser enrutables en la IPv6 global. Las direcciones locales únicas están en el rango de FC00::/7 a FDFF::/7.

Con IPv4, las direcciones privadas se combinan con NAT/PAT para proporcionar una traducción de varios a uno de direcciones privadas a públicas. Esto se hace debido a la disponibilidad limitada de espacio de direcciones IPv4. Muchos sitios también utilizan la naturaleza privada de las direcciones definidas en RFC 1918 para ayudar a proteger u ocultar su red de posibles riesgos de seguridad. Sin embargo, este nunca fue el uso que se pretendió dar a estas tecnologías, y el IETF siempre recomendó que los sitios tomen las precauciones de seguridad adecuadas en el router con conexión a Internet. Si bien IPv6 proporciona direccionamiento de sitio específico, no tiene por propósito ser utilizado para contribuir a ocultar dispositivos internos con IPv6 habilitado de Internet IPv6. El IETF recomienda que la limitación del acceso a los dispositivos se logre implementando medidas de seguridad adecuadas y recomendadas.

Nota: en la especificación IPv6 original, se definían las direcciones locales de sitio con un propósito similar y se utilizaba el rango de prefijos FEC0::/10. La especificación contenía varias ambigüedades, y el IETF dejó en desuso las direcciones locales de sitio en favor de direcciones locales únicas.

IPv4 integrada

El último tipo de dirección unicast es la dirección IPv4 integrada. Estas direcciones se utilizan para facilitar la transición de IPv4 a IPv6. En este curso, no se analizan las direcciones IPv4 integradas.



Capítulo 8: Asignación de direcciones IP 8.2.3.4 Direcciones IPv6 unicast link-local

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.

A diferencia de las direcciones IPv4 link-local, las direcciones IPv6 link-local cumplen una función importante en diversos aspectos de la red. La dirección unicast global no constituye un requisito, pero toda interfaz de red con IPv6 habilitado debe tener una dirección link-local.

Si en una interfaz no se configura una dirección link-local de forma manual, el dispositivo crea automáticamente su propia dirección sin comunicarse con un servidor de DHCP. Los hosts con IPv6 habilitado crean una dirección IPv6 link-local incluso si no se asignó una dirección IPv6 unicast global al dispositivo. Esto permite que los dispositivos con IPv6 habilitado se comuniquen con otros dispositivos con IPv6 habilitado en la misma subred. Esto incluye la comunicación con el gateway predeterminado (router).

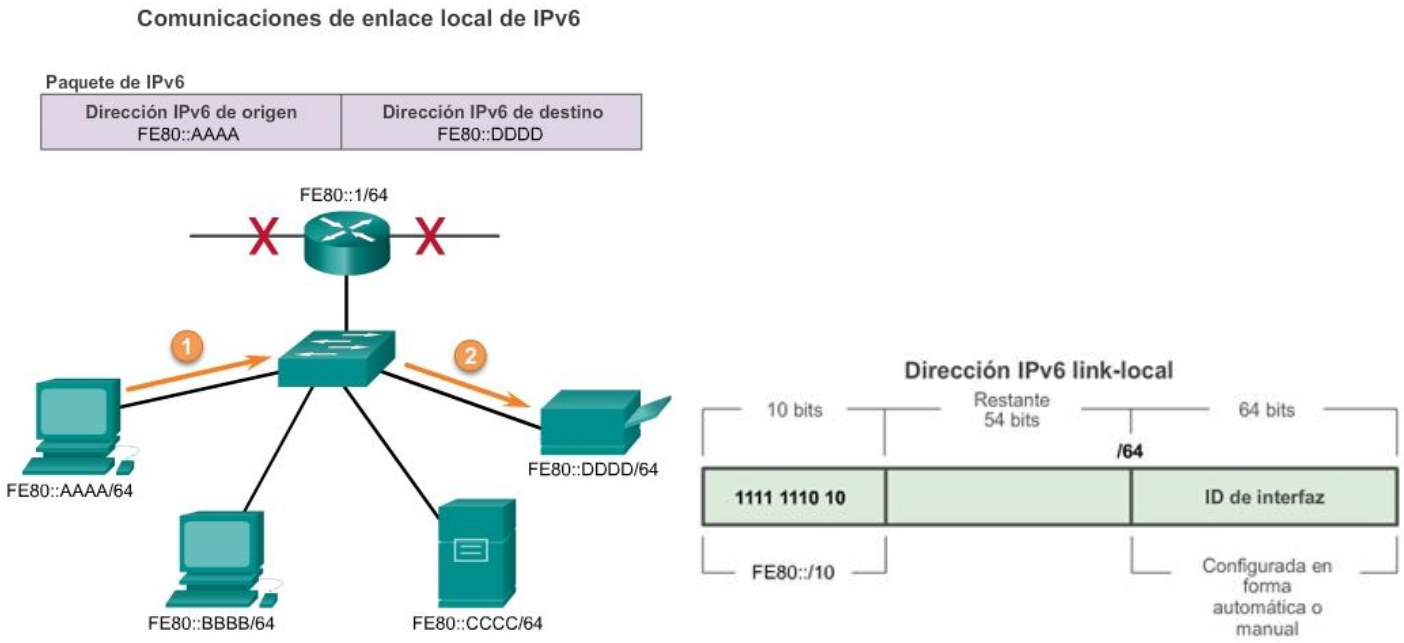
Las direcciones IPv6 link-local están en el rango de FE80::/10. /10 indica que los primeros 10 bits son 1111 1110 10xx xxxx. El primer hexteto tiene un rango de 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111(FEBF).

En la figura 1, se muestra un ejemplo de comunicación mediante direcciones IPv6 link-local.

En la figura 2, se muestra el formato de una dirección IPv6 link-local.

Los protocolos de enrutamiento IPv6 también utilizan direcciones IPv6 link-local para intercambiar mensajes y como la dirección del siguiente salto en la tabla de enrutamiento IPv6. Las direcciones link-local se analizan más detalladamente en un curso posterior.

Nota: por lo general, la dirección que se utiliza como gateway predeterminado para los otros dispositivos en el enlace es la dirección link-local del router, y no la dirección unicast global.



Capítulo 8: Asignación de direcciones IP 8.2.4.1 Estructura de una dirección IPv6 unicast global

Las direcciones IPv6 unicast globales son globalmente únicas y enrutables en Internet IPv6. Estas direcciones son equivalentes a las direcciones IPv4 públicas. La Internet Corporation for Assigned Names and Numbers (ICANN), el operador de la Internet Assigned Numbers Authority (IANA), asigna bloques de direcciones IPv6 a los cinco RIR. Actualmente, solo se asignan direcciones unicast globales con los tres primeros bits de 001 o 2000::/3. Esto solo constituye un octavo del espacio total disponible de direcciones IPv6, sin incluir solamente una parte muy pequeña para otros tipos de direcciones unicast y multicast.

Nota: la dirección 2001:0DB8::/32 se reservó para fines de documentación, incluido el uso en ejemplos.

En la figura 1, se muestra la estructura y el rango de una dirección unicast global.

Una dirección unicast global consta de tres partes:

- Prefijo de enrutamiento global
- ID de subred
- ID de interfaz

Prefijo de enrutamiento global

El prefijo de enrutamiento global es la porción de prefijo, o de red, de la dirección que asigna el proveedor (por ejemplo, un ISP) a un cliente o a un sitio. En la actualidad, los RIR asignan a los clientes el prefijo de enrutamiento global /48. Esto incluye desde redes comerciales de empresas hasta unidades domésticas Para la mayoría de los clientes, este espacio de dirección es más que suficiente.

En la figura 2, se muestra la estructura de una dirección unicast global con el prefijo de enrutamiento global /48. Los prefijos /48 son los prefijos de enrutamiento global más comunes, y se utilizarán en la mayoría de los ejemplos a lo largo de este curso.

Por ejemplo, la dirección IPv6 2001:0DB8:ACAD::/48 tiene un prefijo que indica que los primeros 48 bits (3 hextetos) (2001:0DB8:ACAD) son la porción de prefijo o de red de la dirección. Los dos puntos dobles (::) antes de la duración de prefijo /48 significan que el resto de la dirección se compone solo de ceros.

ID de subred

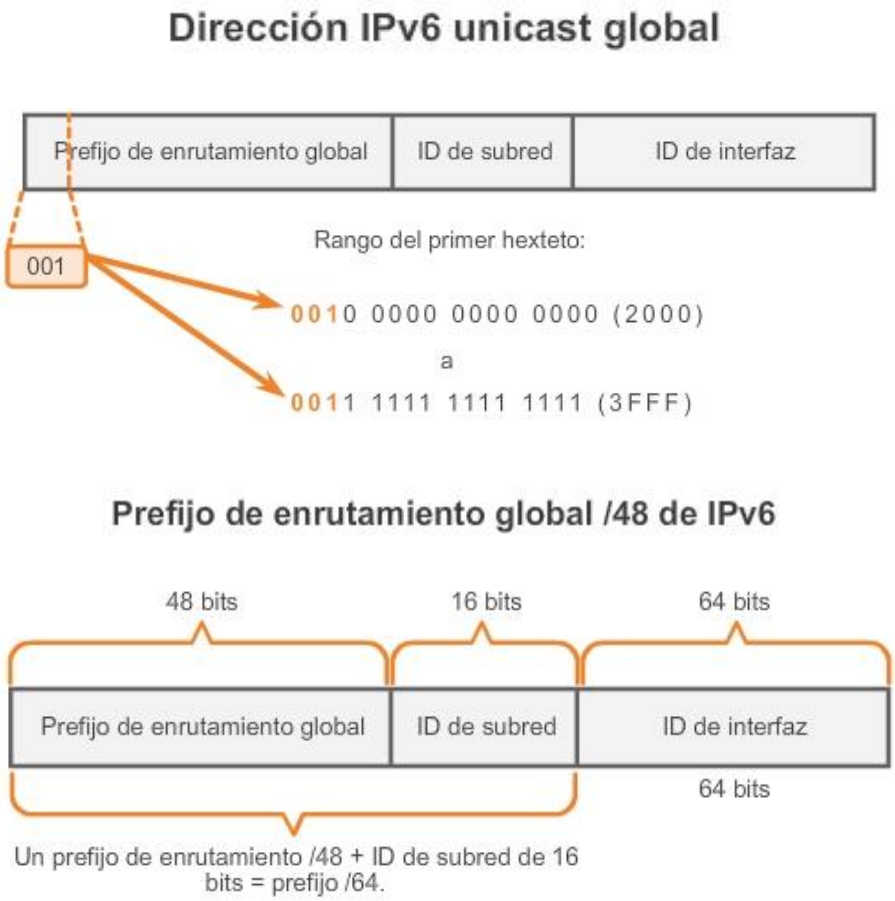
Las organizaciones utilizan la ID de subred para identificar una subred dentro de su ubicación.

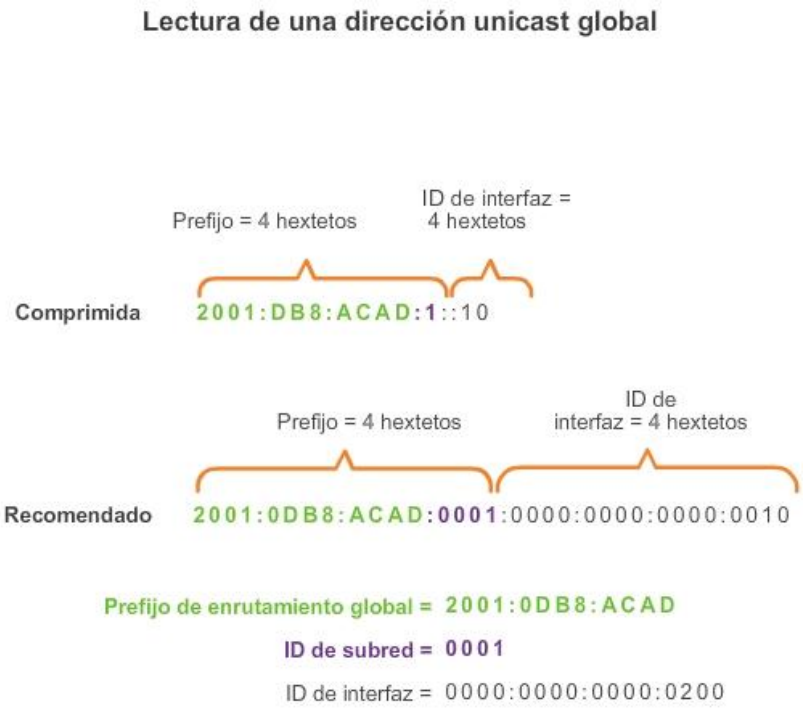
ID de interfaz

La ID de interfaz IPv6 equivale a la porción de host de una dirección IPv4. Se utiliza el término “ID de interfaz” debido a que un único host puede tener varias interfaces, cada una con una o más direcciones IPv6.

Nota: a diferencia de IPv4, en IPv6 se pueden asignar las direcciones de host compuestas solo por ceros y unos a un dispositivo. Se puede usar la dirección compuesta solo por unos debido al hecho de que en IPv6 no se usan las direcciones de broadcast. También se puede utilizar la dirección compuesta solo por ceros, pero se reserva como una dirección anycast de subred y router, y se debe asignar solo a routers.

Una forma fácil de leer la mayoría de las direcciones IPv6 es contar la cantidad de hextetos. Como se muestra en la figura 3, en una dirección unicast global /64 los primeros cuatro hextetos son para la porción de red de la dirección, y el cuarto hexteto indica la ID de subred. Los cuatro hextetos restantes son para la ID de interfaz.





Capítulo 8: Asignación de direcciones IP 8.2.4.2 Configuración estática de una dirección unicast global

Configuración del router

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

El comando interface que se utiliza para configurar una dirección IPv6 unicast global en una interfaz es ipv6 address *dirección ipv6/duración de prefijo*.

Advierta que no hay un espacio entre *dirección ipv6* y*duración de prefijo*.

En la configuración de ejemplo, se utiliza la topología que se muestra en la figura 1 y estas subredes 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)

Como se muestra en la figura 2, los comandos requeridos para configurar la dirección IPv6 unicast global en la interfaz GigabitEthernet 0/0 de R1 serían los siguientes:

Router(config)#interface GigabitEthernet 0/0

Router(config-if)#ipv6 address 2001:db8:acad:1::1/64

Router(config-if)#no shutdown

Configuración de host

Configurar la dirección IPv6 en un host de forma manual es similar a configurar una dirección IPv4.

Como se muestra en la figura 3, la dirección de gateway predeterminado configurada para PC1 es 2001:DB8:ACAD:1::1, la dirección unicast global de la interfaz GigabitEthernet de R1 en la misma red.

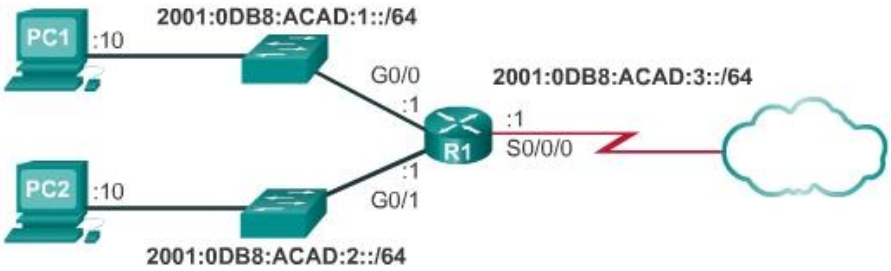
Utilice el verificador de sintaxis de la figura 4 para configurar la dirección IPv6 unicast global.

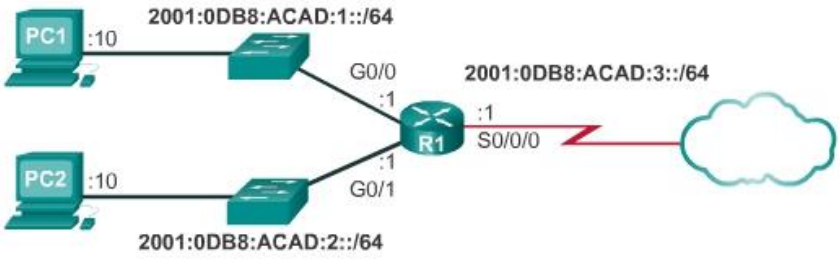
Al igual que con IPv4, la configuración de direcciones estáticas en clientes no se extiende a entornos más grandes. Por este motivo, la mayoría de los administradores de red en una red IPv6 habilitan la asignación dinámica de direcciones IPv6.

Los dispositivos pueden obtener automáticamente una dirección IPv6 unicast global de dos maneras:

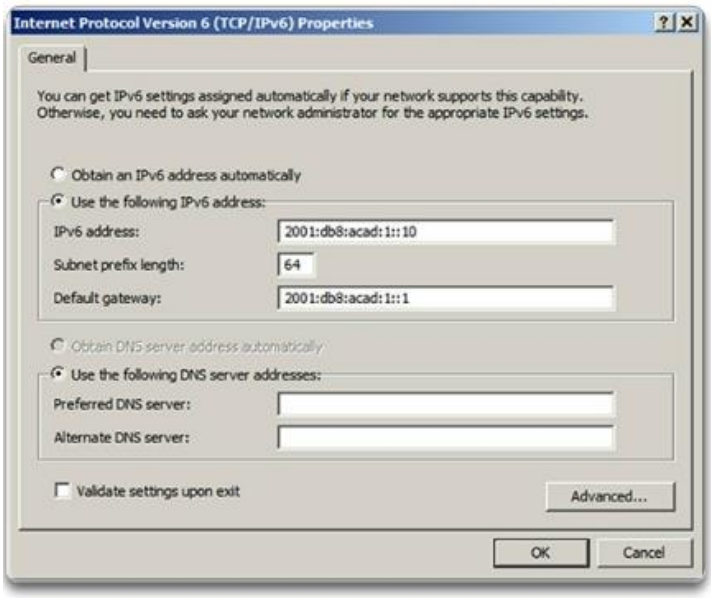
- Configuración automática de dirección sin estado (SLAAC)
- DHCPv6

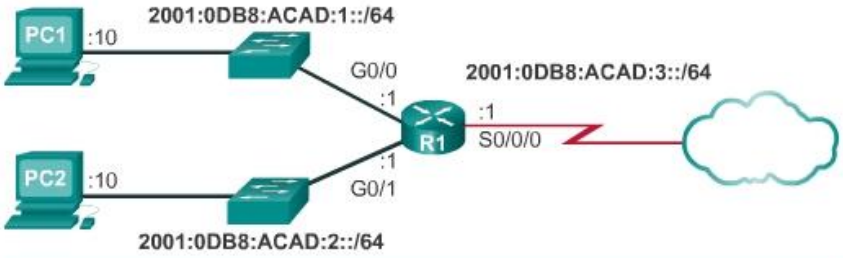
Configuración de IPv6 en un router






```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address 2001:db8:acad:2::1/64
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address 2001:db8:acad:3::1/64
R1(config-if)#clock rate 56000
R1(config-if)#no shutdown
```





Configure y active las interfaces en el siguiente orden:

- **GigabitEthernet 0/0 - 2001:db8:acad:1::1/64**
- **GigabitEthernet 0/1 - 2001:db8:acad:2::1/64**
- **Serial 0/0/0 - 2001:db8:acad:3::1/64**

Nota: no tiene que salir del modo de configuración de interfaz.

```
Router(config)# interface gigabitethernet 0/0
Router(config-if)# ipv6 address 2001:db8:acad:1::1/64
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
Router(config-if)# interface gigabitethernet 0/1
Router(config-if)# ipv6 address 2001:db8:acad:2::1/64
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
Router(config-if)# interface serial 0/0/0
Router(config-if)# ipv6 address 2001:db8:acad:3::1/64
Router(config-if)# no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to
up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
```

Configuró correctamente las interfaces del R1 con direcciones IPv6.

Capítulo 8: Asignación de direcciones IP 8.2.4.3 Configuración dinámica de una dirección unicast global mediante SLAAC

Configuración automática de dirección sin estado (SLAAC)

La configuración automática de dirección sin estado (SLAAC) es un método que permite que un dispositivo obtenga su prefijo, duración de prefijo e información de la dirección de gateway predeterminado de un *router IPv6* sin utilizar un servidor de DHCPv6. Mediante SLAAC, los dispositivos dependen de los mensajes de anuncio de router (RA) de ICMPv6 del router local para obtener la información necesaria.

Los routers IPv6 envían mensajes de anuncio de router (RA) de ICMPv6 a todos los dispositivos en la red con IPv6 habilitado de forma periódica.

De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos a la dirección IPv6 de grupo multicast de todos los nodos. Los dispositivos IPv6 en la red no tienen que esperar estos mensajes periódicos de RA. Un dispositivo puede enviar un mensaje de solicitud de router (RS) utilizando la dirección IPv6 de grupo multicast de todos los routers. Cuando un router IPv6 recibe un mensaje de RS, responde inmediatamente con un anuncio de router.

Si bien es posible configurar una interfaz en un router Cisco con una dirección IPv6, esto no lo convierte en un “router IPv6”. Un router IPv6 es un router que presenta las siguientes características:

- Reenvía paquetes IPv6 entre redes.
- Puede configurarse con rutas estáticas IPv6 o con un protocolo de enrutamiento dinámico IPv6.
- Envía mensajes RA ICMPv6.

El enrutamiento IPv6 no está habilitado de manera predeterminada. Para habilitar un router como router IPv6, se debe utilizar el comando de configuración global ipv6 unicast-routing.

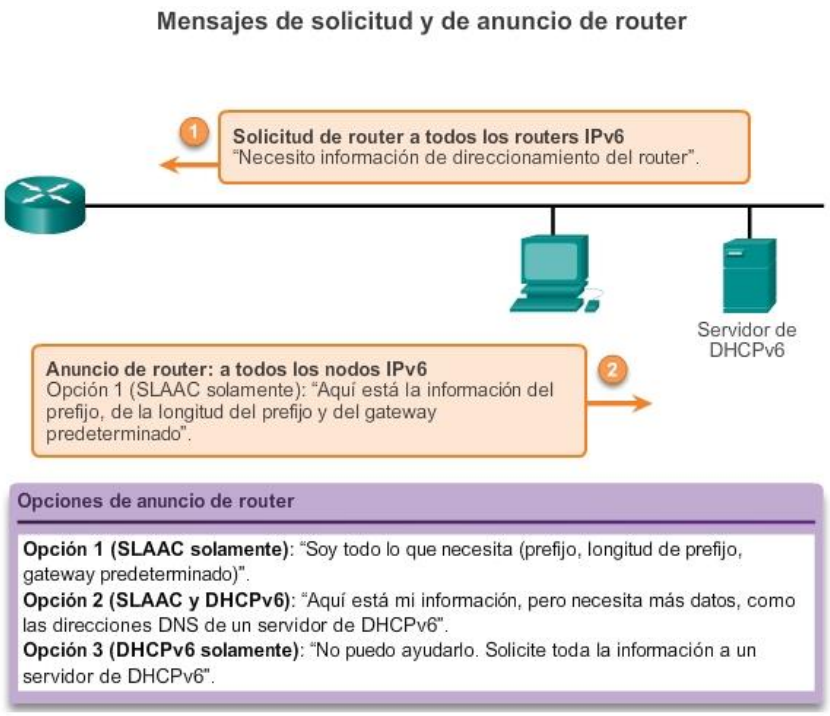
Nota: los routers Cisco están habilitados como routers IPv4 de manera predeterminada.

El mensaje de RA de ICMPv6 contiene el prefijo, la duración de prefijo y otra información para el dispositivo IPv6. El mensaje de RA también informa al dispositivo IPv6 cómo obtener la información de direccionamiento. El mensaje de RA puede contener una de las siguientes tres opciones, como se muestra en la ilustración:

- Opción 1, SLAAC solamente: el dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA. No se encuentra disponible ninguna otra información de un servidor de DHCPv6.
- Opción 2, SLAAC y DHCPv6: el dispositivo debe utilizar el prefijo, la duración de prefijo y la información de la dirección de gateway predeterminado incluida en el mensaje de RA. Existe otra información disponible de un servidor de DHCPv6, como la dirección del servidor DNS. El dispositivo obtiene esta información adicional mediante el proceso normal de descubrimiento y consulta a un servidor de DHCPv6. Esto se conoce como DHCPv6 sin estado, debido a que el servidor de DHCPv6 no necesita asignar ni realizar un seguimiento de ninguna asignación de direcciones IPv6, sino que solo proporciona información adicional, tal como la dirección del servidor DNS.
- Opción 3, DHCPv6 solamente: el dispositivo no debe utilizar la información incluida en el mensaje de RA para obtener la información de direccionamiento.

En cambio, el dispositivo utiliza el proceso normal de descubrimiento y consulta a un servidor de DHCPv6 para obtener toda la información de direccionamiento. Esto incluye una dirección IPv6 unicast global, la duración de prefijo, la dirección de gateway predeterminado y las direcciones de los servidores DNS. En este caso, el servidor de DHCPv6 actúa como un servidor de DHCP sin estado, de manera similar a DHCP para IPv4. El servidor de DHCPv6 asigna direcciones IPv6 y realiza un seguimiento de ellas, a fin de no asignar la misma dirección IPv6 a varios dispositivos.

Los routers envían mensajes de RA de ICMPv6 utilizando la dirección link-local como la dirección IPv6 de origen. Los dispositivos que utilizan SLAAC usan la dirección link-local del router como su dirección de gateway predeterminado.



Capítulo 8: Asignación de direcciones IP 8.2.4.4 Configuración dinámica de una dirección unicast global mediante DHCPv6

DHCPv6

El protocolo de configuración dinámica de host para IPv6 (DHCPv6) es similar a DHCP para IPv4. Los dispositivos pueden recibir de manera automática la información de direccionamiento, incluso una dirección unicast global, la duración de prefijo, la dirección de gateway predeterminado y las direcciones de servidores DNS, mediante los servicios de un servidor de DHCPv6.

Los dispositivos pueden recibir la información de direccionamiento IPv6 en forma total o parcial de un servidor de DHCPv6 en función de si en el mensaje de RA de ICMPv6 se especificó la opción 2 (SLAAC y DHCPv6) o la opción 3 (DHCPv6 solamente). Además, el OS host puede optar por omitir el contenido del mensaje de RA del router y obtener su dirección IPv6 y otra información directamente de un servidor de DHCPv6.

Antes de implementar dispositivos IPv6 en una red, se recomienda primero verificar si el host observa las opciones dentro del mensaje ICMPv6 de RA del router.

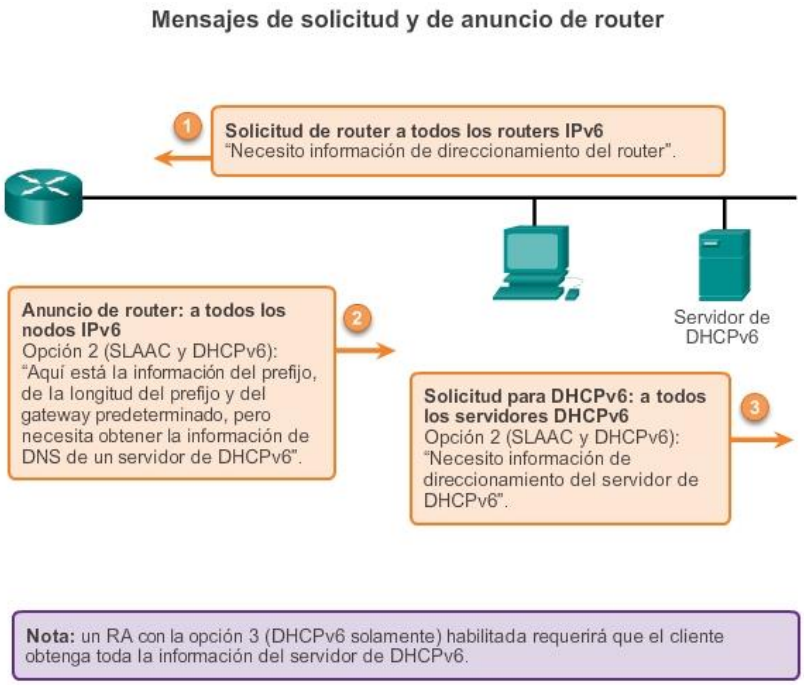
Un dispositivo puede obtener la dirección IPv6 unicast global dinámicamente y también estar configurado con varias direcciones IPv6 estáticas en la misma interfaz. IPv6 permite que varias direcciones IPv6 (que pertenecen a la misma red IPv6) se configuren en la misma interfaz.

También se puede configurar un dispositivo con más de una dirección IPv6 de gateway predeterminado. Para obtener más información sobre cómo se toma la decisión respecto de cuál es la dirección que se usa como la dirección IPv6 de origen o cuál es la dirección de gateway predeterminado que se utiliza, consulte RFC 6724, Default Address Selection for IPv6 (Selección de direcciones predeterminada para IPv6).

ID de interfaz

Si el cliente no utiliza la información incluida en el mensaje de RA y depende exclusivamente de DHCPv6, el servidor de DHCPv6 proporciona la dirección IPv6 unicast global completa, incluidos el prefijo y la ID de interfaz.

Sin embargo, si se utiliza la opción 1 (SLAAC solamente) o la opción 2 (SLAAC con DHCPv6), el cliente no obtiene la porción de ID de interfaz real de la dirección mediante este estos procesos. El dispositivo cliente debe determinar su propia ID de interfaz de 64 bits, ya sea mediante el proceso EUI-64 o generando un número aleatorio de 64 bits.



Capítulo 8: Asignación de direcciones IP 8.2.4.5 Proceso EUI-64 o de generación aleatoria

Proceso EUI-64

El IEEE definió el identificador único extendido (EUI) o proceso EUI-64 modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear una ID de interfaz de 64 bits.

Las direcciones MAC de Ethernet, por lo general, se representan en formato hexadecimal y constan de dos partes:

- Identificador único de organización (OUI): el OUI es un código de proveedor de 24 bits (seis dígitos hexadecimales) que asigna el IEEE.
- Identificador de dispositivo: el identificador de dispositivo es un valor único de 24 bits (seis dígitos hexadecimales) dentro de un OUI común.

Las ID de interfaz EUI-64 se representan en sistema binario y constan de tres partes:

- OUI de 24 bits de la dirección MAC del cliente, pero el séptimo bit (bit universal/local, U/L) se invierte. Esto significa que si el séptimo bit es un 0, se convierte en 1, y viceversa.
- Valor de 16 bits FFFE introducido (en formato hexadecimal)
- Identificador de dispositivo de 24 bits de la dirección MAC del cliente

En la figura 1, se ilustra el proceso EUI-64, con la siguiente dirección MAC de GigabitEthernet de R1: FC99:4775:CEE0.

Paso 1: Dividir la dirección MAC entre el OUI y el identificador de dispositivo
Paso 2: Insertar el valor hexadecimal FFFE, que en formato binario es: 1111 1111 1111 1110
Paso 3: Convertir los primeros dos valores hexadecimales del OUI a binario e invertir el bit U/L (séptimo bit) En este ejemplo, el 0 en el bit 7 se cambia a 1.

El resultado es una ID de interfaz de FE99:47FF:FE75:CEE0 generada mediante EUI-64.

Nota: el uso del bit U/L y los motivos para invertir su valor se analizan en RFC 5342.

La ventaja de EUI-64 es que se puede utilizar la dirección MAC de Ethernet para determinar la ID de interfaz. También permite que los administradores de red rastreen fácilmente una dirección IPv6 a un dispositivo final mediante la dirección MAC única. Sin embargo, esto generó inquietudes con respecto a la privacidad a muchos usuarios. Les preocupa que los paquetes puedan ser rastreados a la PC física real. Debido a estas inquietudes, se puede utilizar en cambio una ID de interfaz generada aleatoriamente.

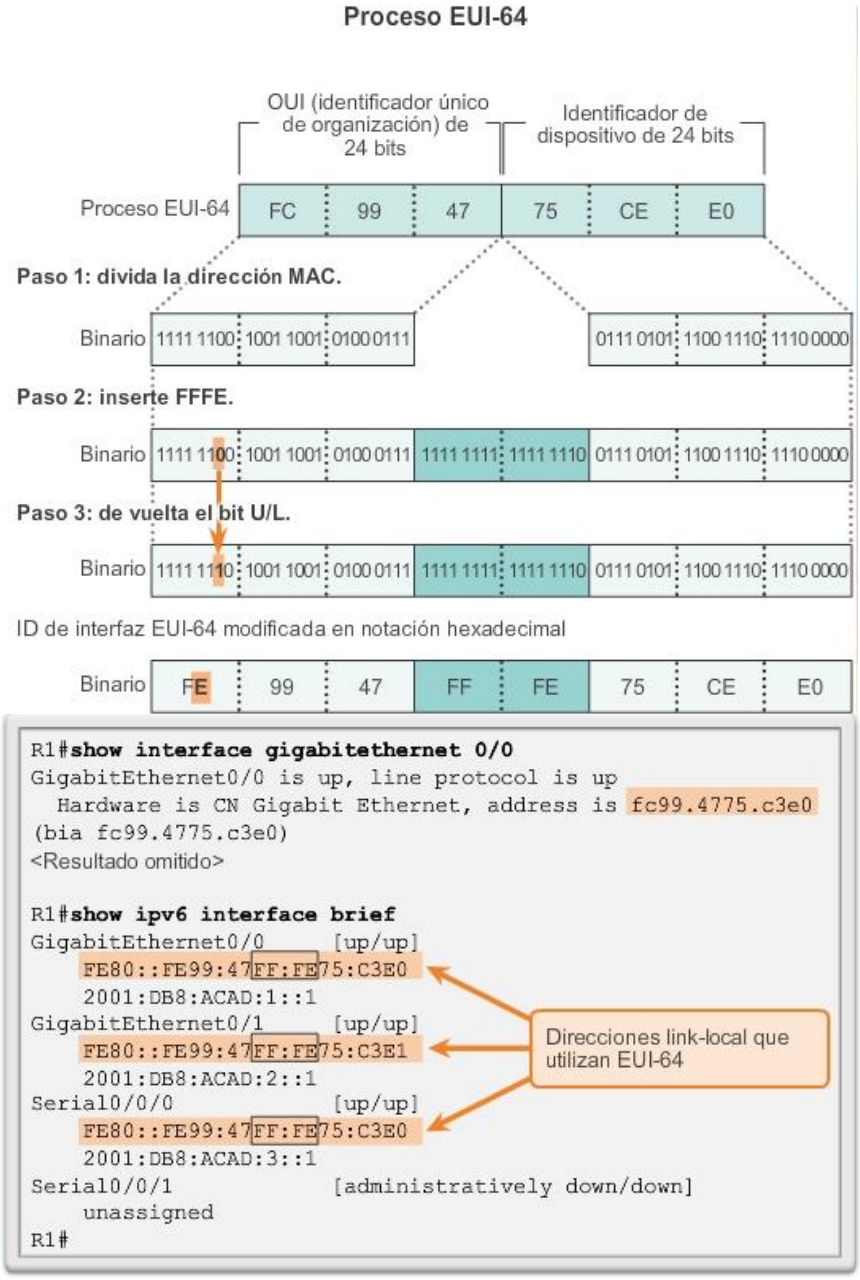
ID de interfaz generadas aleatoriamente

Según el sistema operativo, un dispositivo puede utilizar una ID de interfaz generada aleatoriamente en lugar de utilizar la dirección MAC y el proceso EUI-64. Por ejemplo, comenzando con Windows Vista, Windows utiliza una ID de interfaz generada aleatoriamente en lugar de una ID de interfaz creada mediante EUI-64. Windows XP y sistemas operativos Windows anteriores utilizaban EUI-64.

Una manera sencilla de identificar que una dirección muy probablemente se creó mediante EUI-64 es el valor FFFE ubicado en medio de la ID de interfaz, como se muestra en la figura 2.

Después de que se establece una ID de interfaz, ya sea mediante el proceso EUI-64 o mediante la generación aleatoria, se puede combinar con un prefijo IPv6 para crear una dirección unicast global o una dirección link-local.

- Dirección unicast global: al utilizar SLAAC, el dispositivo recibe su prefijo del mensaje de RA de ICMPv6 y lo combina con la ID de interfaz.
- Dirección link-local: los prefijos link-local comienzan con FE80::/10. Los dispositivos suelen utilizar FE80::/64 como prefijo o duración de prefijo, seguido de la ID de interfaz.



Capítulo 8: Asignación de direcciones IP 8.2.4.6 Direcciones link-local dinámicas

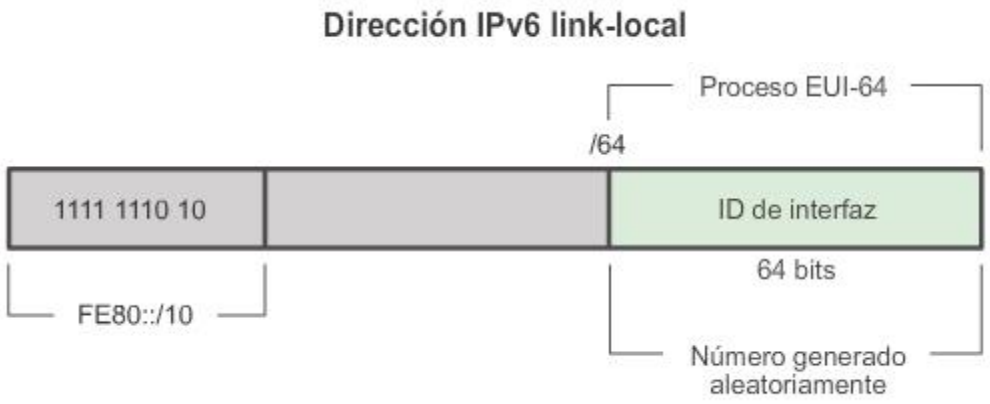
Al utilizar SLAAC (SLAAC solamente o SLAAC con DHCPV6), los dispositivos reciben el prefijo y la duración de prefijo del mensaje de RA de ICMPv6. Debido a que el mensaje de RA designa el prefijo de la dirección, el dispositivo debe proporcionar únicamente la porción de ID de interfaz de su dirección. Como se indicó anteriormente, la ID de interfaz se puede generar de forma automática mediante el proceso EUI-64, o, según el OS, se puede generar de forma aleatoria. Con la información del mensaje de RA y la ID de interfaz, el dispositivo puede establecer su dirección unicast global.

Después de que se asigna una dirección unicast global a una interfaz, el dispositivo con IPv6 habilitado genera la dirección link-local automáticamente. Los dispositivos con IPv6 habilitado deben tener, como mínimo, la dirección link-local. Recuerde que una dirección IPv6 link-local permite que un dispositivo se comunique con otros dispositivos con IPv6 habilitado en la misma subred.

Las direcciones IPv6 link-local se utilizan para diversos fines, incluidos los siguientes:

- Los hosts utilizan la dirección link-local del router local para obtener la dirección IPv6 de gateway predeterminado.
- Los routers intercambian mensajes de protocolo de enrutamiento dinámico mediante direcciones link-local.
- Las tablas de enrutamiento de los routers utilizan la dirección link-local para identificar el router del siguiente salto al reenviar paquetes IPv6.

Las direcciones link-local se pueden establecer dinámicamente o se pueden configurar de forma manual como direcciones link-local estáticas.



Dirección link-local asignada dinámicamente

La dirección link-local se crea dinámicamente mediante el prefijo FE80::/10 y la ID de interfaz.

De manera predeterminada, los routers en los que se utiliza Cisco IOS utilizan EUI-64 para generar la ID de interfaz para todas las direcciones link-local en las interfaces IPv6. Para las interfaces seriales, el router utiliza la dirección MAC de una interfaz Ethernet. Recuerde que una dirección link-local debe ser única solo en ese enlace o red. Sin embargo, una desventaja de utilizar direcciones link-local asignadas dinámicamente es su longitud, que dificulta identificar y recordar las direcciones asignadas.

Capítulo 8: Asignación de direcciones IP 8.2.4.7 Direcciones link-local estáticas

Dirección Link-Local estática

Configurar la dirección link-local de forma manual permite crear una dirección reconocible y más fácil de recordar.

Las direcciones link-local pueden configurarse manualmente mediante el mismo comando interface que se utiliza para crear direcciones IPv6 unicast globales, pero con un parámetro adicional:

Router(config-if)#ipv6 address link-local-address link-local

En la figura 1, se muestra que una dirección link-local tiene un prefijo dentro del rango FE80 a FEBF. Cuando una dirección comienza con este hexteto (segmento de 16 bits), el parámetro link-local debe seguir la dirección.

En la figura 2, se muestra la configuración de una dirección link-local mediante el comando ipv6 address interface. La dirección link-local FE80::1 se utiliza para que sea posible reconocer fácilmente que pertenece al router R1. Se configura la misma dirección IPv6 link-local en todas las interfaces de R1. Se puede configurar FE80::1 en cada enlace, debido a que solamente tiene que ser única en ese enlace.

De manera similar a R1, el router R2 se configuraría con FE80::2 como la dirección IPv6 link-local en todas sus interfaces.

Configuración de direcciones link-local en el R1

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ipv6 address fe80::1 ?
  link-local  Use link-local address

R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#
```

```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::1
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::1
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

Direcciones link-local configuradas estáticamente

Capítulo 8: Asignación de direcciones IP 8.2.4.8 Verificación de la configuración de la dirección IPv6

Como se muestra en la figura 1, el comando para verificar la configuración de la interfaz IPv6 es similar al comando que se utiliza para IPv4.

El comando show interface muestra la dirección MAC de las interfaces Ethernet. EUI-64 utiliza esta dirección MAC para generar la ID de interfaz para la dirección link-local. Además, el comando show ipv6 interface brief muestra un resultado abreviado para cada una de las interfaces. El resultado [up/up]en la misma línea que la 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.

Advierta que cada interfaz tiene dos direcciones IPv6. La segunda dirección para cada interfaz es la dirección unicast global que se configuró. La primera dirección, la que comienza con FE80, es la dirección unicast link-local para la interfaz. Recuerde que la dirección link-local se agrega automáticamente a la interfaz cuando se asigna una dirección unicast global.

Además, advierta que la dirección link-local serial 0/0/0 de R1 es igual a la interfaz GigabitEthernet 0/0. Las interfaces seriales no tienen una dirección MAC de Ethernet, de modo que Cisco IOS utiliza la dirección MAC de la primera interfaz Ethernet disponible. Esto es posible porque las interfaces link-local solo deben ser únicas en ese enlace.

La dirección link-local de la interfaz del router suele ser la dirección de gateway predeterminado para los dispositivos en ese enlace o red.

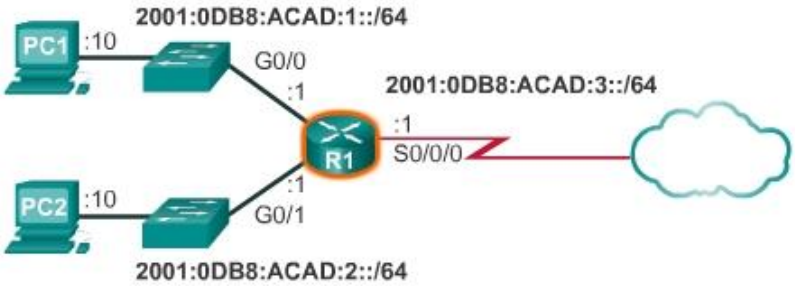
Como se muestra en la figura 2, el comando show ipv6 route puede utilizarse para verificar si las redes IPv6 y las direcciones específicas de la interfaz IPv6 se instalaron en la tabla de enrutamiento IPv6. El comandoshow ipv6 route muestra solamente redes IPv6, no redes IPv4.

Dentro de la tabla de la ruta, 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 enrutamiento utiliza las rutas locales para procesar eficazmente paquetes cuya dirección de 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 usa una dirección IPv6. Como se muestra en la figura 3, el comando se utiliza para verificar la conectividad de capa 3 entre R1 y PC1. Al hacer ping a una dirección link-local desde un router, Cisco IOS solicita al usuario la interfaz de salida. Dado que la dirección link-local de destino puede estar en uno o más de los enlaces o redes, el router debe saber qué interfaz utilizar para enviar el ping.

Utilice el verificador de sintaxis de la figura 4 para verificar la configuración de la dirección IPv6.




```
R1#show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
R1#
```

```
R1#show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static

<resultado omitido>

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
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

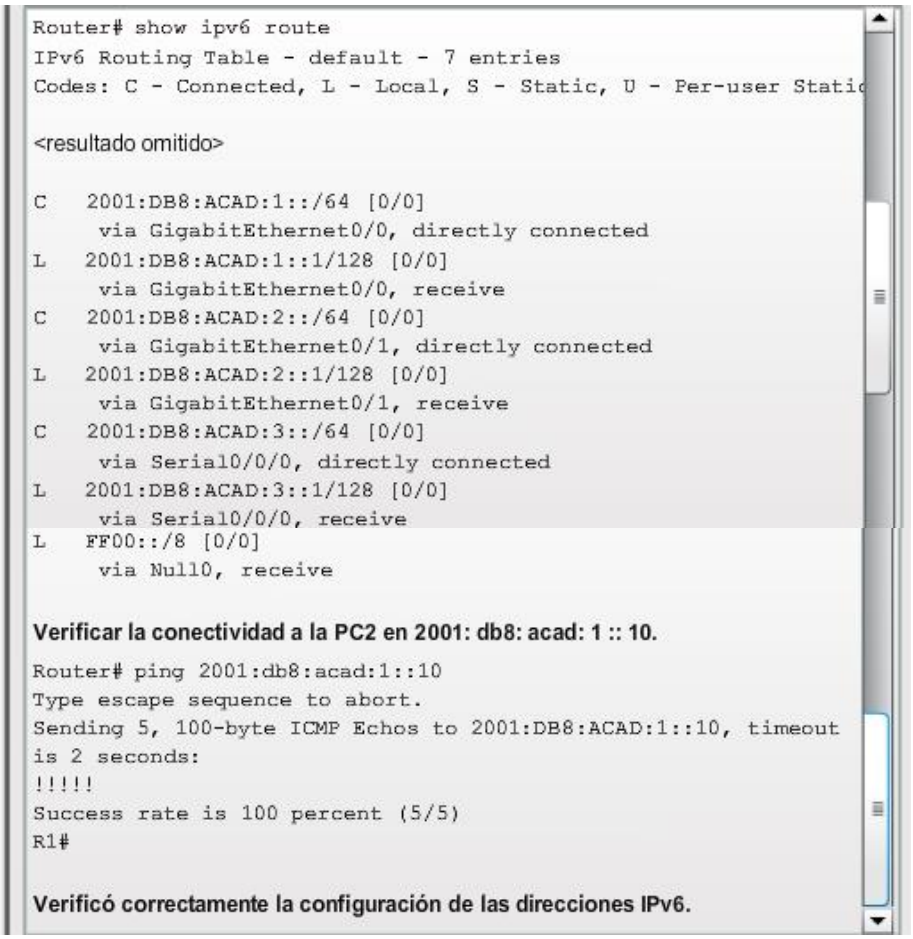
```
R1#ping 2001:db8:acad:1::10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5)
R1#
```

Verificación de la configuración de la dirección IPv6

Introduzca el comando show que le mostrará un breve resumen del estado de la interfaz IPv6.

```
Router# show ipv6 interface brief
GigabitEthernet0/0      [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:1::1
GigabitEthernet0/1      [up/up]
    FE80::FE99:47FF:FE75:C3E1
    2001:DB8:ACAD:2::1
Serial0/0/0             [up/up]
    FE80::FE99:47FF:FE75:C3E0
    2001:DB8:ACAD:3::1
Serial0/0/1             [administratively down/down]
    unassigned
```

Introduzca el comando show que le mostrará la tabla de enrutamiento IPv6.



Capítulo 8: Asignación de direcciones IP 8.2.5.1 Direcciones IPv6 multicast asignadas

Las direcciones IPv6 multicast son similares a las direcciones IPv4 multicast. Recuerde que las direcciones multicast se utilizan para enviar un único paquete a uno o más destinos (grupo multicast). Las direcciones IPv6 multicast tienen el prefijo FF00::/8.

Nota: las direcciones multicast solo pueden ser direcciones de destino, no de origen.

Existen dos tipos de direcciones IPv6 multicast:

- Dirección multicast asignada
- Dirección multicast de nodo solicitado

Dirección multicast asignada

Las direcciones multicast asignadas son direcciones multicast reservadas para grupos predefinidos de dispositivos. Una dirección multicast asignada es una única dirección que se utiliza para llegar a un grupo de dispositivos que ejecutan un protocolo o servicio común. Las direcciones multicast asignadas se utilizan en contexto con protocolos específicos, como DHCPv6.

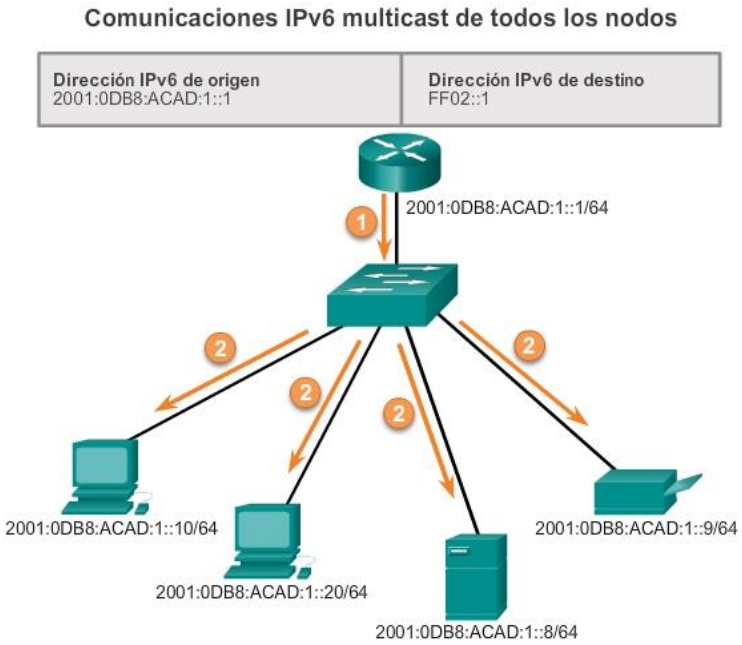
Dos grupos comunes de direcciones multicast IPv6 asignadas incluyen los siguientes:

- Grupo multicast de todos los nodos FF02::1: grupo multicast al que se unen todos los dispositivos con IPv6 habilitado. Los paquetes que se envían a este grupo son recibidos y procesados por todas las interfaces IPv6 en el enlace o en la red.

  Esto tiene el mismo efecto que una dirección de broadcast en IPv4. En la ilustración, se muestra un ejemplo de comunicación mediante la dirección multicast de todos los nodos. Un router IPv6 envía mensajes de RA de protocolo de mensajes de control de Internet versión 6 (ICMPv6) al grupo multicast de todos los nodos. El mensaje de RA proporciona a todos los dispositivos en la red con IPv6 habilitado la información de direccionamiento, como el prefijo, la duración de prefijo y el gateway predeterminado.

- Grupo multicast de todos los routers FF02::2:grupo multicast al que se unen todos los routers con IPv6 habilitado. Un router se convierte en un miembro de este grupo cuando se habilita como router IPv6 mediante el comando de configuración global ipv6 unicast-routing. Los paquetes que se envían a este grupo son recibidos y procesados por todos los routers IPv6 en el enlace o en la red.

Los dispositivos con IPv6 habilitado envían mensajes de solicitud de router (RS) de ICMPv6 a la dirección multicast de todos los routers. El mensaje de RS solicita un mensaje de RA del router IPv6 para contribuir a la configuración de direcciones del dispositivo.



Capítulo 8: Asignación de direcciones IP 8.2.5.2 Direcciones IPv6 multicast de nodo solicitado

Las direcciones multicast de nodo solicitado son similares a las direcciones multicast de todos los nodos. Recuerde que la dirección multicast de todos los nodos es esencialmente lo mismo que una dirección IPv4 de broadcast.

Todos los dispositivos en la red deben procesar el tráfico enviado a la dirección de todos los nodos. Para reducir el número de dispositivos que deben procesar tráfico, utilice una dirección multicast de nodo solicitado.

Una dirección multicast de nodo solicitado es una dirección que coincide solo con los últimos 24 bits de la dirección IPv6 unicast global de un dispositivo. Los únicos dispositivos que deben procesar estos paquetes son aquellos que tienen estos mismos 24 bits en la porción menos significativa que se encuentra más hacia la derecha de la ID de interfaz.

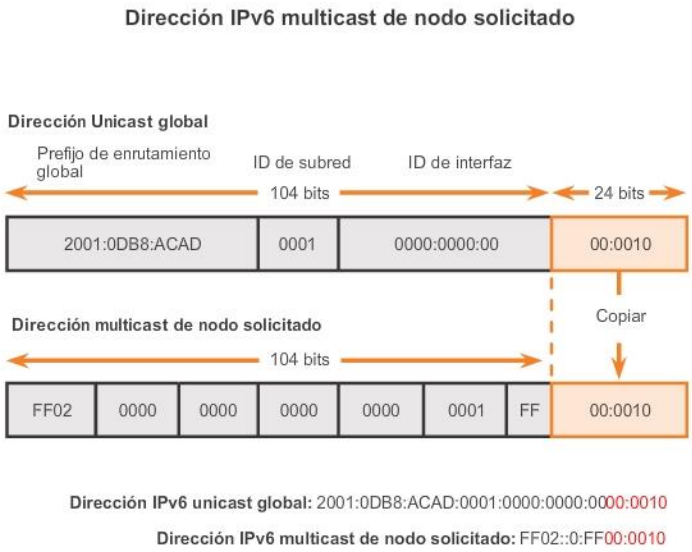
Una dirección IPv6 multicast de nodo solicitado se crea de forma automática cuando se asigna la dirección unicast global o la dirección unicast link-local. La dirección IPv6 multicast de nodo solicitado se crea combinando un prefijo especial FF02:0:0:0:0:1:FF00::/104 con los 24 bits de su dirección unicast que se encuentran en el extremo derecho.

La dirección multicast de nodo solicitado consta de dos partes:

- Prefijo multicast FF02:0:0:0:0:1:FF00::/104: los primeros 104 bits de la dirección multicast de todos los nodos solicitados.

- 24 bits menos significativos: los 24 bits finales o que se encuentran más hacia la derecha de la dirección multicast de nodo solicitado. Estos bits se copian de los 24 bits del extremo derecho de la dirección unicast global o unicast link-local del dispositivo.

Es posible que varios dispositivos tengan la misma dirección multicast de nodo solicitado. Si bien es poco común, esto puede suceder cuando los dispositivos tienen los mismos 24 bits que se encuentran más hacia la derecha en sus ID de interfaz. Esto no genera ningún problema, ya que el dispositivo aún procesa el mensaje encapsulado, el cual incluye la dirección IPv6 completa del dispositivo en cuestión.



Capítulo 8: Asignación de direcciones IP 8.3.1.1 Mensajes de ICMPv4 y ICMPv6

Si bien IP no es un protocolo confiable, la suite TCP/IP proporciona los mensajes que se deben enviar en caso de que se produzcan determinados errores. Estos mensajes se envían mediante los servicios de ICMP. El objetivo de estos mensajes es proporcionar respuestas acerca de temas relacionados con el procesamiento de paquetes IP bajo determinadas condiciones, no es hacer que el IP sea confiable. Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional. En este curso, el término ICMP se utilizará para referirse tanto a ICMPv4 como a ICMPv6.

Existen muchos tipos de mensajes de ICMP y muchos motivos por los cuales se envían estos mensajes. Analizaremos algunos de los mensajes más comunes.

Los mensajes ICMP comunes a ICMPv4 y a ICMPv6 incluyen lo siguiente:

- Confirmación de host
- Destino o servicio inaccesible
- Tiempo superado
- Redireccionamiento de ruta

Confirmación de host

Se puede utilizar un mensaje de eco de ICMP para determinar si un host está en funcionamiento. El host local envía una petición de eco de ICMP a un host. Si el host se encuentra disponible, el host de destino responde con una respuesta de eco. En la ilustración, haga clic en el botón Reproducir para ver una animación de la solicitud de eco o de la respuesta de eco de ICMP. Este uso de los mensajes de eco de ICMP es la base de la utilidad ping.

Destino o servicio inaccesible

Cuando un host o gateway recibe un paquete que no puede entregar, puede utilizar un mensaje de destino inalcanzable de ICMP para notificar al origen que el destino o el servicio es inalcanzable. El mensaje incluye un código que indica el motivo por el cual no se pudo entregar el paquete.

Algunos de los códigos de destino inalcanzable para ICMPv4 son los siguientes:

- 0: red inalcanzable
- 1: host inalcanzable
- 2: protocolo inalcanzable
- 3: puerto inalcanzable

Nota: los códigos de ICMPv6 para los mensajes de destino inalcanzable son similares, pero presentan algunas diferencias.

Tiempo superado

Los routers utilizan los mensajes de tiempo superado de ICMPv4 para indicar que un paquete no puede reenviarse debido a que el campo Tiempo de vida (TTL) del paquete se disminuyó a 0.

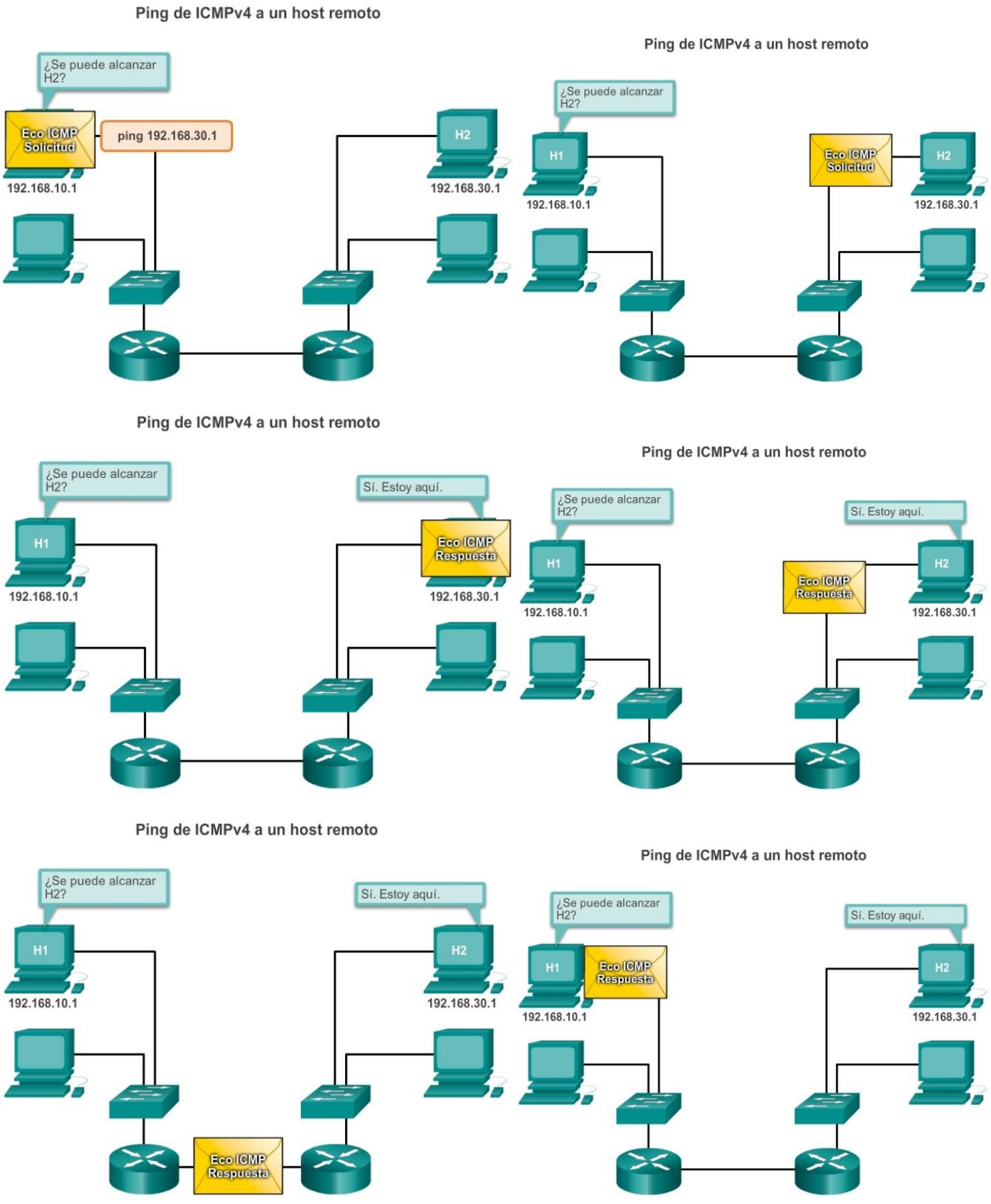
Si un router recibe un paquete y disminuye el campo TTL en el paquete IPV4 a cero, descarta el paquete y envía un mensaje de tiempo superado al host de origen.

ICMPv6 también envía un mensaje de tiempo superado si el router no puede reenviar un paquete IPv6 debido a que el paquete caducó. IPv6 no tiene un campo TTL, por lo que utiliza el campo de Límite de saltos para determinar si el paquete caducó.

Redireccionamiento de ruta

Un router puede usar un mensaje de redireccionamiento de ICMP para notificar a los hosts de una red acerca de una mejor ruta disponible para un destino en particular. Es posible que este mensaje sólo pueda usarse cuando el host de origen esté en la misma red física que ambos gateways.

Tanto ICMPv4 como ICMPv6 utilizan mensajes de redireccionamiento de ruta.



Capítulo 8: Asignación de direcciones IP 8.3.1.2 Mensajes de solicitud y de anuncio de router de ICMPv6

Los mensajes informativos y de error que se encuentran en ICMPv6 son muy similares a los mensajes de control y de error que implementa ICMPv4. Sin embargo, ICMPv6 tiene nuevas características y funcionalidad mejorada que no se encuentran en ICMPv4.

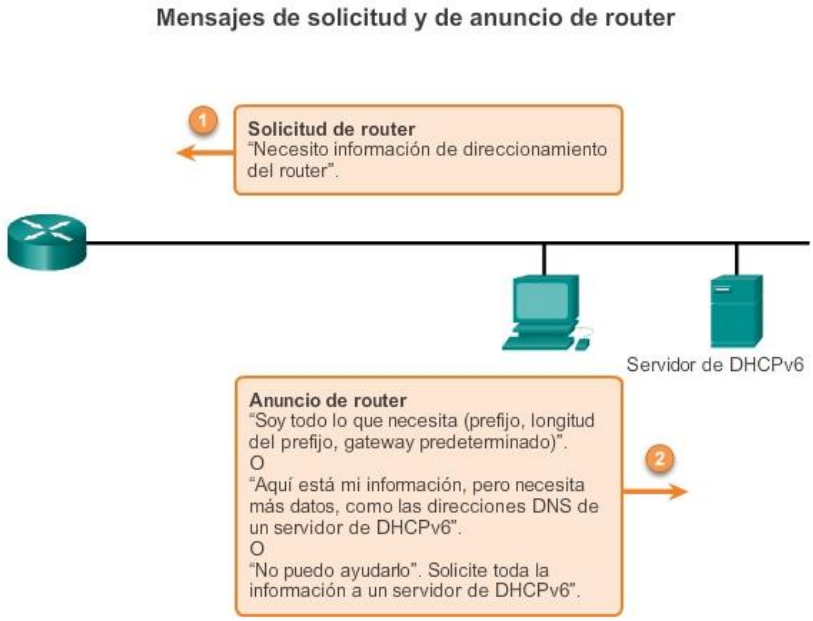
ICMPv6 incluye cuatro nuevos protocolos como parte del protocolo ND o NDP (Neighbor Discovery Protocol, protocolo de descubrimiento de vecinos):

- Mensaje de solicitud de router
- Mensaje de anuncio de router
- Mensaje de solicitud de vecino
- Mensaje de anuncio de vecino

Mensajes de solicitud y de anuncio de router

Los dispositivos con IPv6 habilitado pueden dividirse en dos categorías: routers y hosts. Los mensajes de solicitud de router y de anuncio de router se envían entre hosts y routers.

- Mensaje de solicitud de router (RS): cuando un host está configurado para obtener la información de direccionamiento de forma automática mediante la configuración automática de dirección sin estado (SLAAC), el host envía un mensaje de RS al router. El mensaje de RS se envía como un mensaje IPv6 multicast de todos los routers.
- Mensaje de anuncio de router (RA): los routers envían mensajes de RA para proporcionar información de direccionamiento a los hosts mediante SLAAC. El mensaje de RA puede incluir información de direccionamiento para el host, como el prefijo y la duración de prefijo. Los routers envían mensajes de RA de forma periódica o en respuesta a un mensaje de RS. De manera predeterminada, los routers Cisco envían mensajes de RA cada 200 segundos. Los mensajes de RA se envían a la dirección IPv6 multicast de todos los nodos. Los hosts que utilizan SLAAC establecen su gateway predeterminado en la dirección link-local del router que envió el mensaje de RA.



Capítulo 8: Asignación de direcciones IP 8.3.1.3 Mensajes de solicitud y de anuncio de vecino de ICMPv6

El protocolo de descubrimiento de vecinos de ICMPv6 incluye dos tipos de mensajes adicionales: mensaje de solicitud de vecino (NS) y mensaje de anuncio de vecino (NA).

Los mensajes de solicitud y de anuncio de vecino se utilizan para lo siguiente:

- Resolución de direcciones
- Detección de direcciones duplicadas (DAD)

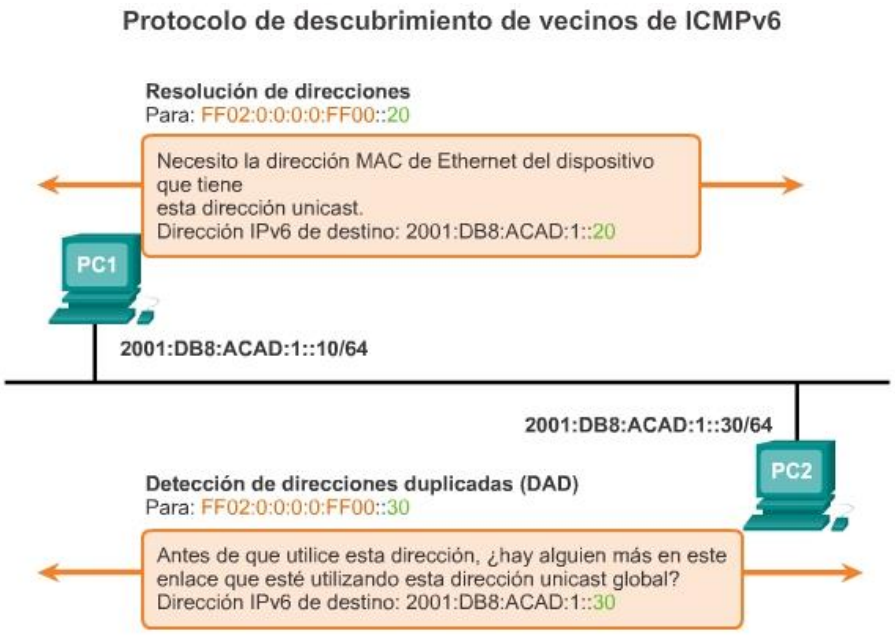
Resolución de direcciones

La resolución de direcciones se utiliza cuando un dispositivo en la LAN conoce la dirección IPv6 unicast de un destino, pero no conoce la dirección MAC de Ethernet. Para determinar la dirección MAC del destino, el dispositivo envía un mensaje de NS a la dirección de nodo solicitado. El mensaje incluye la dirección IPv6 conocida (objetivo). El dispositivo que tiene la dirección IPv6 objetivo responde con un mensaje de NA que contiene la dirección MAC de Ethernet.

Detección de direcciones duplicadas

Cuando se asigna una dirección unicast global o una dirección unicast link-local a un dispositivo, se recomienda llevar a cabo la detección de direcciones duplicadas (DAD) en la dirección para asegurarse de que sea única. Para revisar si una dirección es única, el dispositivo envía un mensaje de NS con su propia dirección IPv6 como la dirección IPv6 objetivo. Si otro dispositivo en la red tiene esta dirección, responde con un mensaje de NA. Este mensaje de NA notifica al dispositivo emisor que la dirección está en uso. Si no se devuelve un mensaje de NA correspondiente dentro de determinado período, la dirección unicast es única y su uso es aceptable.

Nota: la DAD no es obligatoria, pero en RFC 4861 se recomienda que se realice la DAD en direcciones unicast.



Capítulo 8: Asignación de direcciones IP 8.3.2.1 Ping para prueba del stack local

Ping es una utilidad de prueba que utiliza mensajes de solicitud y de respuesta de eco de ICMP para probar la conectividad entre hosts. Ping funciona tanto con IPv4 y con hosts IPv6.

Para probar la conectividad a otro host en una red, se envía una solicitud de eco a la dirección de host mediante el comando ping. Si el host en la dirección especificada recibe la solicitud de eco, responde con una respuesta de eco. A medida que se recibe cada respuesta de eco, ping proporciona comentarios acerca del tiempo transcurrido entre el envío de la solicitud y la recepción de la respuesta. Esta puede ser una medida del rendimiento de la red.

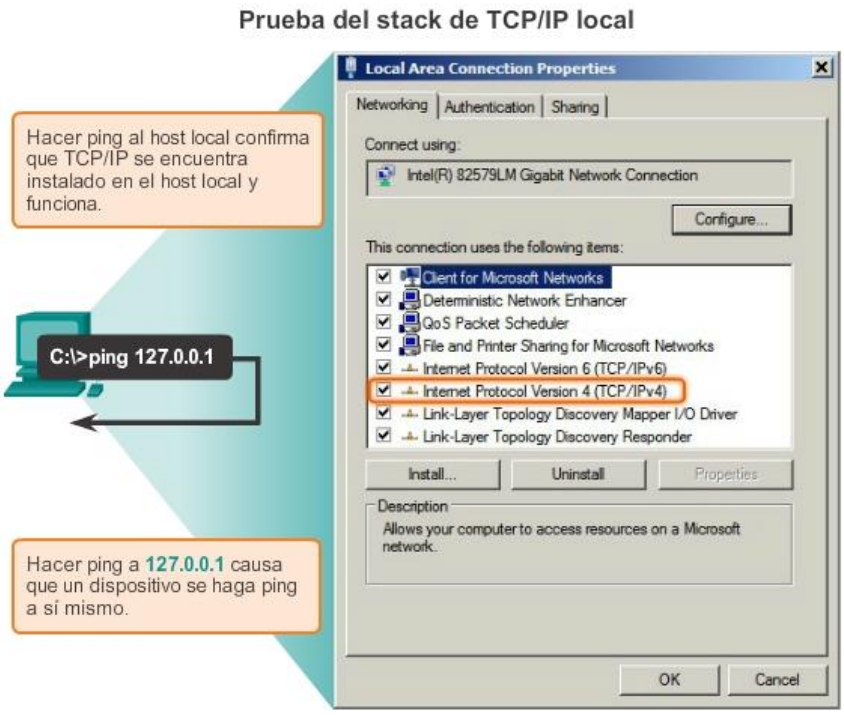
Ping posee un valor de tiempo de espera para la respuesta. Si no se recibe una respuesta dentro del tiempo de espera, ping proporciona un mensaje que indica que no se recibió una respuesta. Generalmente, esto indica que existe un problema, pero también podría indicar que se habilitaron características de seguridad que bloquean mensajes ping en la red.

Una vez que se envían todas las solicitudes, la utilidad ping proporciona un resumen que incluye la tasa de éxito y el tiempo promedio del recorrido de ida y vuelta al destino.

Ping del loopback local

Existen casos especiales de prueba y verificación para los cuales se puede usar el ping. Un caso es la prueba de la configuración interna de IPv4 o de IPv6 en el host local. Para realizar esta prueba, se debe hacer ping a la dirección de loopback de 127.0.0.1 para IPv4 (::1 para IPv6). En la ilustración, se muestra la prueba de la dirección IPv4 de loopback.

Una respuesta de 127.0.0.1 para IPv4 (o ::1 para IPv6) indica que IP está instalado correctamente en el host. Esta respuesta proviene de la capa de red. Sin embargo, esta respuesta no indica que las direcciones, máscaras o los gateways estén correctamente configurados. Tampoco indica nada acerca del estado de la capa inferior del stack de red. Sencillamente, prueba la IP en la capa de red del protocolo IP. Si se obtiene un mensaje de error, esto indica que el TCP/IP no funciona en el host.



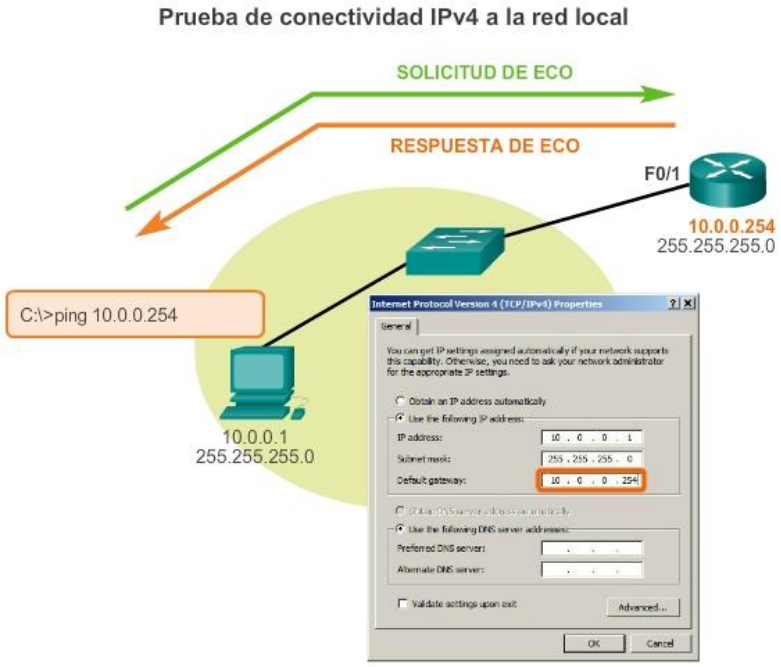
Capítulo 8: Asignación de direcciones IP 8.3.2.2 Ping para prueba de conectividad a la LAN local

También es posible utilizar ping para probar la capacidad de comunicación del host en la red local. Por lo general, esto se realiza haciendo ping a la dirección IP del gateway del host. Un ping al gateway indica que la interfaz del host y la interfaz del router que cumplen la función de gateway funcionan en la red local.

Para esta prueba, se usa la dirección de gateway con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la dirección de gateway no responde, se puede enviar un ping a la dirección IP de otro host en la red local que se sepa que funciona.

Si el gateway u otro host responden, los hosts locales pueden comunicarse correctamente a través de la red local. Si el gateway no responde pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como gateway.

Una posibilidad es que se haya configurado la dirección de gateway incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde a peticiones de ping.



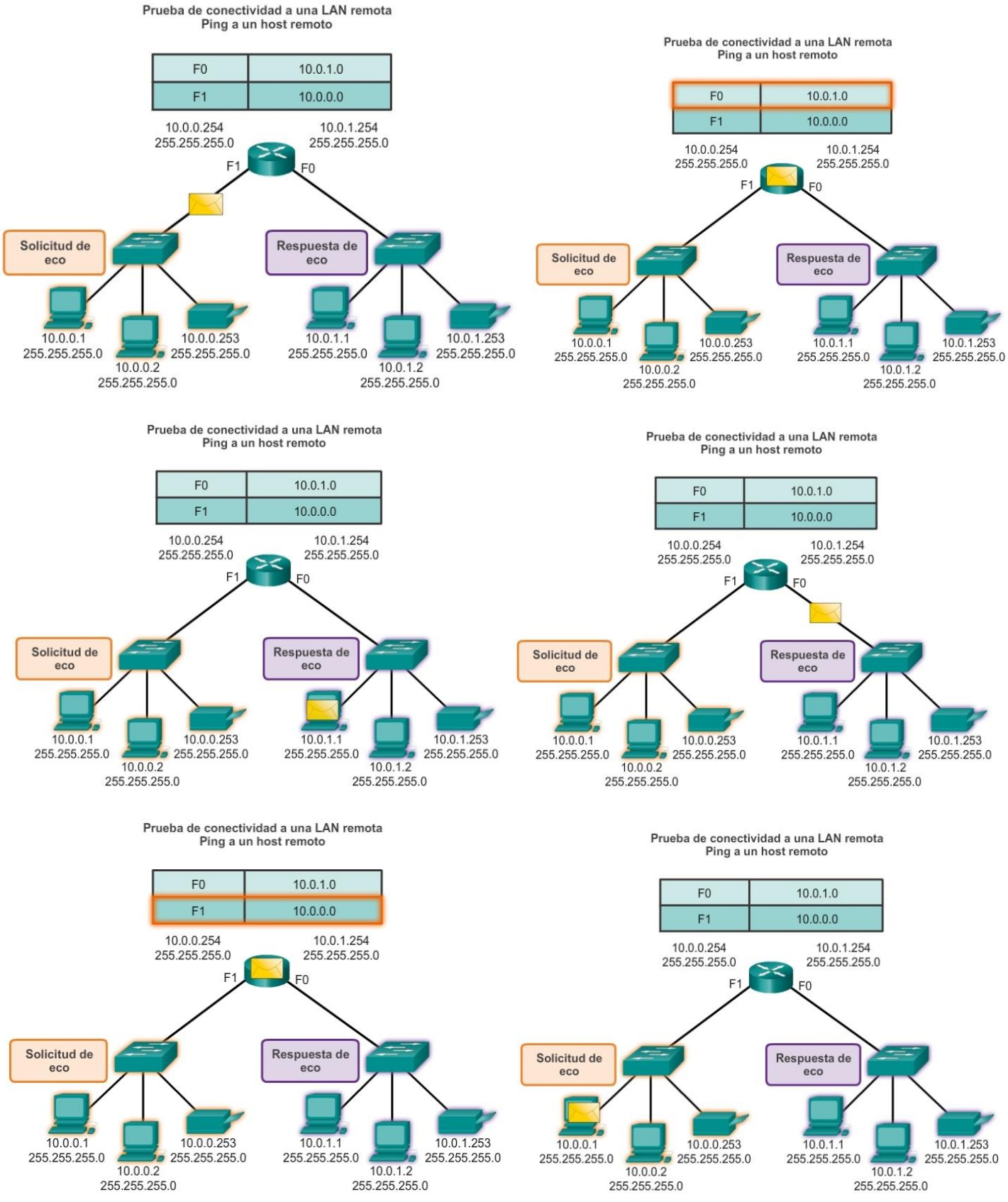
Capítulo 8: Asignación de direcciones IP 8.3.2.3 Ping para prueba de conectividad a dispositivo remoto

También se puede utilizar ping para probar la capacidad de un host local para comunicarse a través de una internetwork. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración.

Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la internetwork. Un ping correcto a través de la internetwork confirma la comunicación en la red local, el funcionamiento del router que funciona como gateway y el funcionamiento de todos los otros routers que podrían estar en la ruta entre la red local y la red del host remoto.

Además, es posible verificar la funcionalidad del host remoto. Si el host remoto no podía comunicarse fuera de la red local, no hubiera respondido.

Nota: muchos administradores de red limitan o prohíben la entrada de mensajes de ICMP a la red corporativa; motivo por el cual la ausencia de una respuesta de ping podría deberse a restricciones de seguridad.



Capítulo 8: Asignación de direcciones IP 8.3.2.4 Traceroute, prueba de la ruta

Ping se utiliza para probar la conectividad entre dos hosts, pero no proporciona información sobre los detalles de los dispositivos entre los hosts. Traceroute (tracert) es una utilidad que genera una lista de saltos que se

alcanzaron correctamente a lo largo de la ruta. Esta lista puede proporcionar información importante sobre la verificación y la resolución de problemas.

Si los datos llegan al destino, el rastreo indica la interfaz de cada router que aparece en la ruta entre los hosts. Si los datos fallan en algún salto a lo largo del camino, la dirección del último router que respondió al rastreo puede indicar dónde se encuentra el problema o las restricciones de seguridad.

Tiempo de ida y vuelta (RTT)

El uso de traceroute proporciona el tiempo de ida y vuelta para cada salto a lo largo de la ruta e indica si se produce una falla en la respuesta del salto. El tiempo de ida y vuelta es el tiempo que le lleva a un paquete llegar al host remoto y el tiempo que la respuesta del host demora en regresar. Se utiliza un asterisco (*) para indicar un paquete perdido o sin respuesta.

Esta información puede ser utilizada para ubicar un router problemático en el camino. Si en la pantalla se muestran tiempos de respuesta elevados o pérdidas de datos de un salto particular, esto constituye un indicio de que los recursos del router o sus conexiones pueden estar sobrecargados.

Tiempo de vida (TTL) de IPv4 y Límite de saltos de IPv6

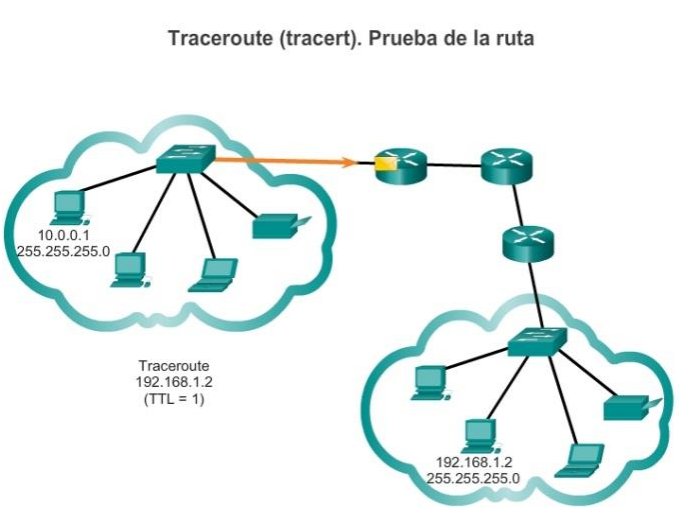
Traceroute utiliza una función del campo TTL en IPv4 y del campo Límite de saltos en IPv6 en los encabezados de capa 3, junto con el mensaje de tiempo superado de ICMP.

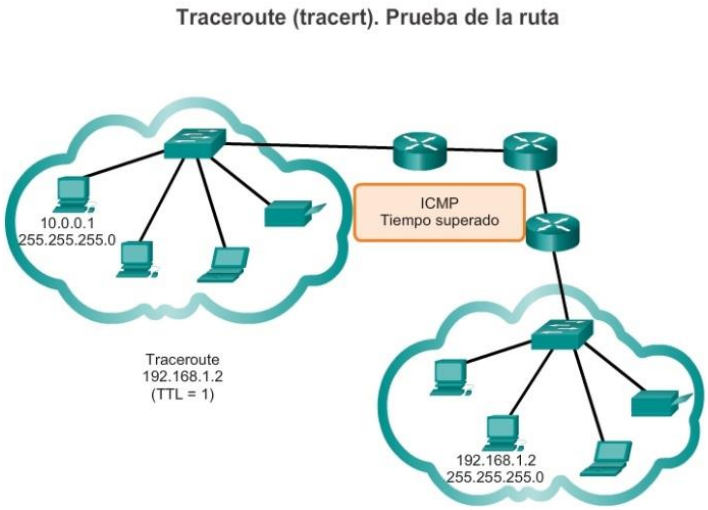
Reproduzca la animación en la figura para ver cómo Traceroute aprovecha el TTL.

La primera secuencia de mensajes enviados desde traceroute tiene un valor de 1 en el campo TTL. Esto hace que el TTL agote el tiempo de espera del paquete IPv4 en el primer router. Este router luego responde con un mensaje de ICMPv4. Traceroute ahora posee la dirección del primer salto.

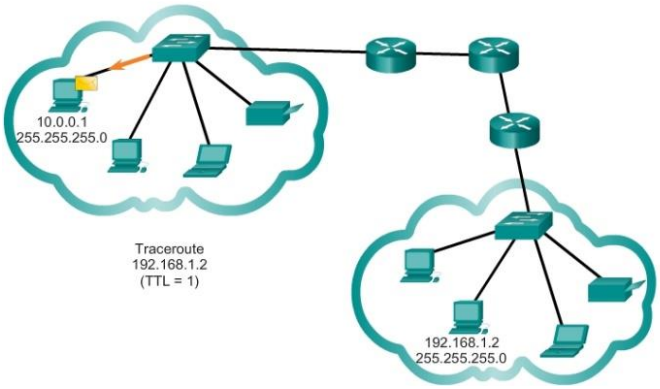
A continuación, Traceroute incrementa progresivamente el campo TTL (2, 3, 4...) para cada secuencia de mensajes. De esta manera se proporciona al rastreo la dirección de cada salto a medida que los paquetes expiran el límite de tiempo a lo largo del camino. El campo TTL continúa aumentando hasta que se llega a destino o hasta un máximo predefinido.

Una vez que se llega al destino final, el host responde con un mensaje de puerto inalcanzable de ICMP o un mensaje de respuesta de eco de ICMP, en lugar de hacerlo con un mensaje de tiempo superado de ICMP.

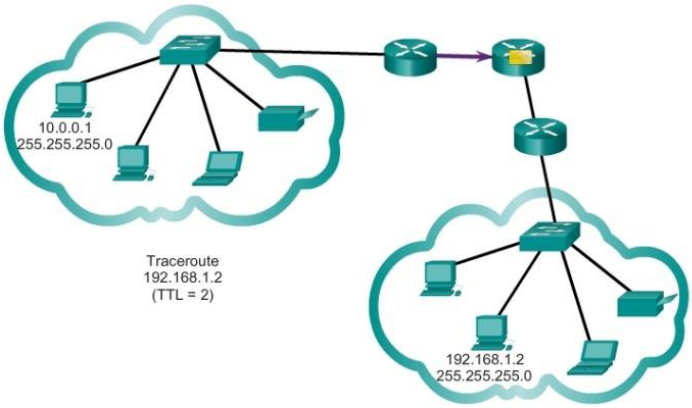




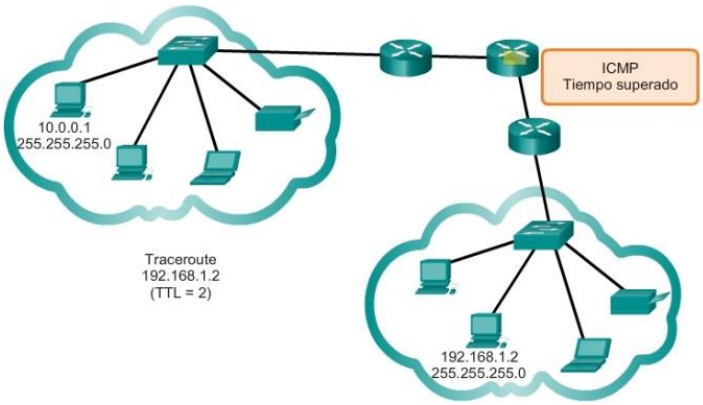
Traceroute (tracert). Prueba de la ruta



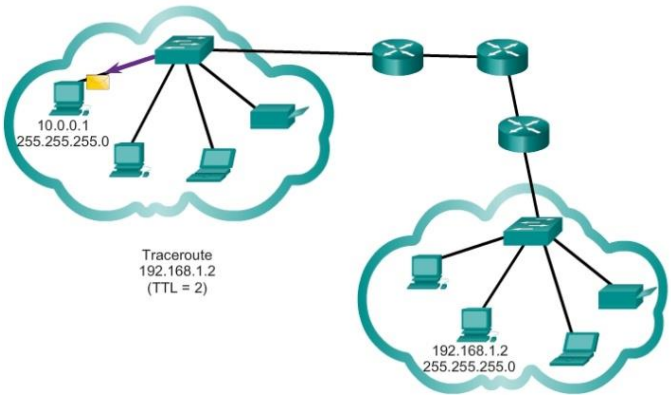
Traceroute (tracert). Prueba de la ruta



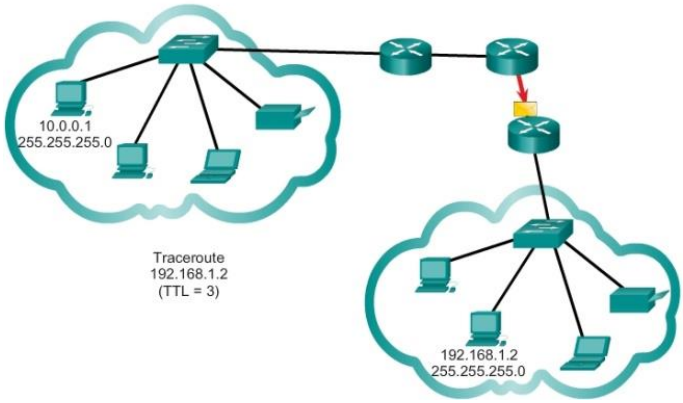
Traceroute (tracert). Prueba de la ruta



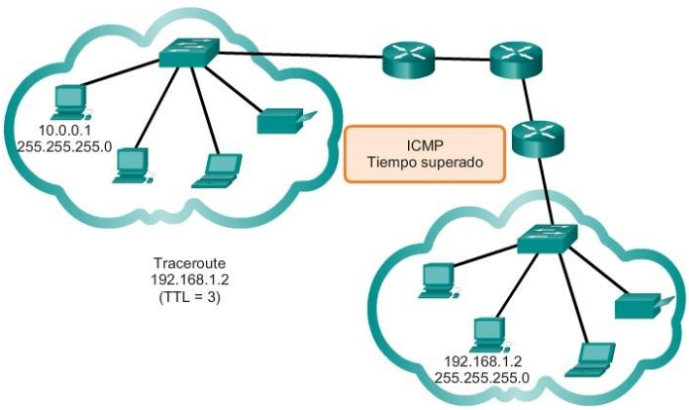
Traceroute (tracert). Prueba de la ruta

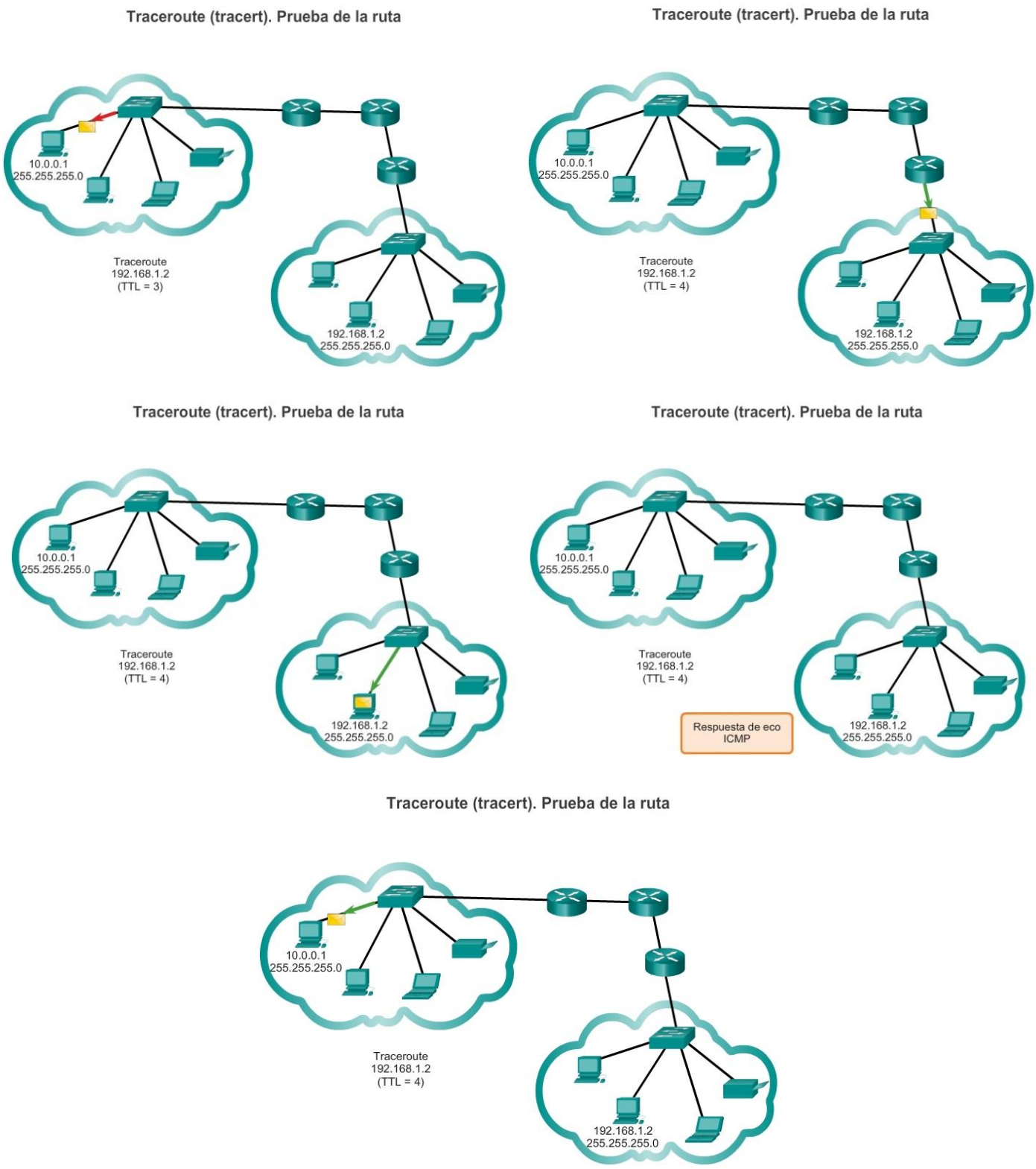


Traceroute (tracert). Prueba de la ruta



Traceroute (tracert). Prueba de la ruta





Capítulo 8: Asignación de direcciones IP 8.4.1.1 Actividad de clase: Internet de todo, por supuesto

Internet de todo, por supuesto

En este capítulo, obtuvo información sobre cómo las pequeñas y medianas empresas se conectan a redes en grupos. También se presentó Internet de todo en el inicio de la actividad de creación de modelos.

Para esta actividad, elija una de las siguientes opciones:

- Servicios bancarios en línea

- Noticias del mundo
- Pronóstico meteorológico/clima
- Condiciones del tráfico

Elabore un esquema de direccionamiento IPv6 para el área que eligió. En el esquema de direccionamiento, incluya la manera en que elaboraría planes para lo siguiente:

- División en subredes
- Transmisiones unicast
- Transmisiones multicast
- Broadcasts

Conserve una copia del esquema para compartir con la clase o la comunidad de aprendizaje. Esté preparado para explicar lo siguiente:

- Cómo se incorporarían la división en subredes y los procesos unicast, multicast y broadcast.
- Dónde podría utilizarse el esquema de direccionamiento.
- Cómo se verían afectadas las pequeñas y medianas empresas al utilizar el plan.

El diseño, la implementación y la administración de un plan eficaz de direccionamiento IP garantizan la eficacia de la red.

Capítulo 8: Asignación de direcciones IP 8.4.1.3 Resumen

Las direcciones IP son jerárquicas y tienen porciones de red, subred y host. Una dirección IP puede representar una red completa, un host específico o la dirección de broadcast de la red.

Es importante entender la notación binaria para determinar si dos hosts están en la misma red. Los bits dentro de la porción de red de la dirección IP deben ser idénticos para todos los dispositivos que residen en la misma red.

La máscara de subred o el prefijo se utilizan para determinar la porción de red de una dirección IP. Las direcciones IP pueden asignarse de manera estática o dinámica. El DHCP permite la asignación automática de información de direccionamiento, como una dirección IP, una máscara de subred, un gateway predeterminado y otra información de configuración.

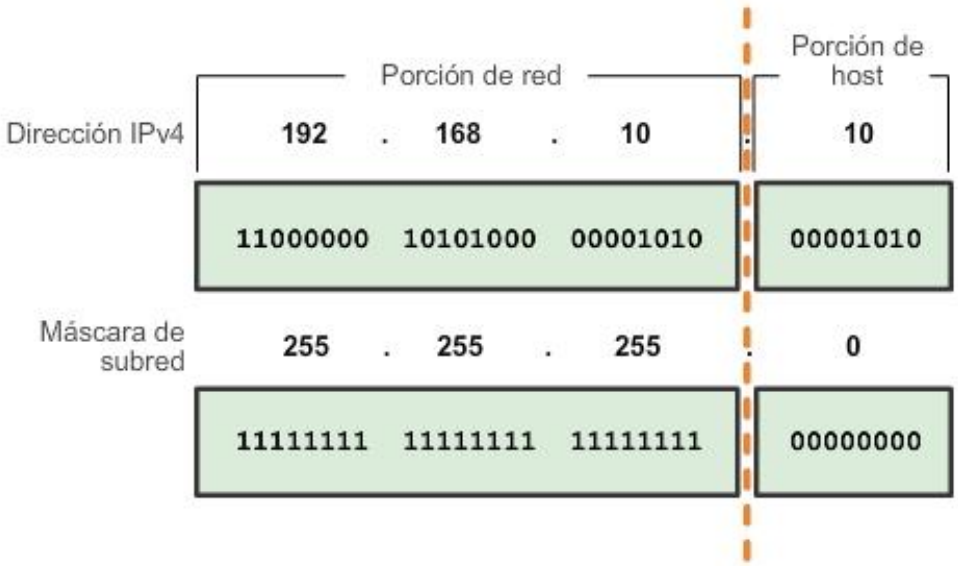
Los hosts IPv4 pueden comunicarse de una de tres maneras diferentes: por unicast, broadcast y multicast. Además, los bloques de direcciones que se utilizan en redes que requieren acceso limitado o inexistente a Internet se denominan “direcciones privadas”. Los bloques de direcciones IPv4 privadas son los siguientes: 10.0.0.0/8, 172.16.0.0/12 y 192.168.0.0/16.

La migración a IPv6 está motivada por el agotamiento del espacio de direcciones IPv4. Cada dirección IPv6 tiene 128 bits, en comparación con los 32 bits que poseen las direcciones IPv4. IPv6 no utiliza la notación decimal punteada de máscara de subred. La duración de prefijo se utiliza para indicar la porción de red de una dirección IPv6 mediante el siguiente formato: dirección IPv6/duración de prefijo.

Hay tres tipos de direcciones IPv6: unicast, multicast y anycast. 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. Las direcciones IPv6 link-local están en el rango de FE80::/10.

El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es ICMPv4. ICMPv6 proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional.

Una vez implementada, la red IP se debe probar para verificar la conectividad y el rendimiento operativo.



Capítulo 9: División de redes IP en subredes 9.0.1.1 Introducción

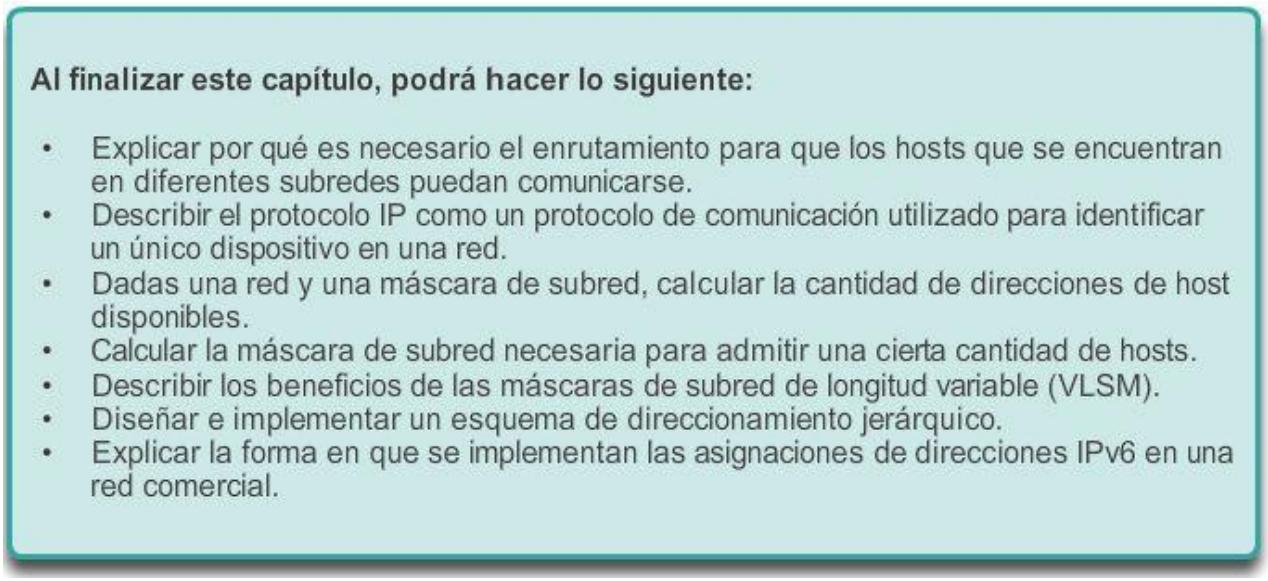
El diseño, la implementación y la administración de un plan de direccionamiento IP eficaz asegura que las redes puedan operar de manera eficaz y eficiente. Esto es así especialmente a medida que aumenta la cantidad de conexiones de host a una red. Comprender la estructura jerárquica de la dirección IP y cómo modificar esa jerarquía a fin de satisfacer con mayor eficacia los requisitos de enrutamiento constituye una parte importante de la planificación de un esquema de direccionamiento IP.

En la dirección IPv4 original, hay dos niveles de jerarquía: una red y un host. Estos dos niveles de direccionamiento permiten agrupaciones de red básicas que facilitan el enrutamiento de paquetes hacia una red de destino. El router reenvía paquetes sobre la base de la porción de red de una dirección IP. Una vez que se localiza la red, la porción de host de la dirección permite identificar el dispositivo de destino.

Sin embargo, a medida que las redes crecen y muchas organizaciones agregan cientos e incluso miles de hosts a su red, la jerarquía de dos niveles resulta insuficiente.

La subdivisión de redes agrega un nivel a la jerarquía de la red, lo cual básicamente crea tres niveles: una red, una subred y un host. La introducción de un nivel adicional a la jerarquía crea subgrupos adicionales dentro de una red IP, lo que facilita la entrega rápida de paquetes y proporciona un mayor filtrado al contribuir a minimizar el tráfico “local”.

En este capítulo, se analiza detalladamente la creación y la asignación de direcciones IP de red y de subred mediante el uso de la máscara de subred.



Capítulo 9: División de redes IP en subredes 9.0.1.2 Actividad: Llámame

Llámame

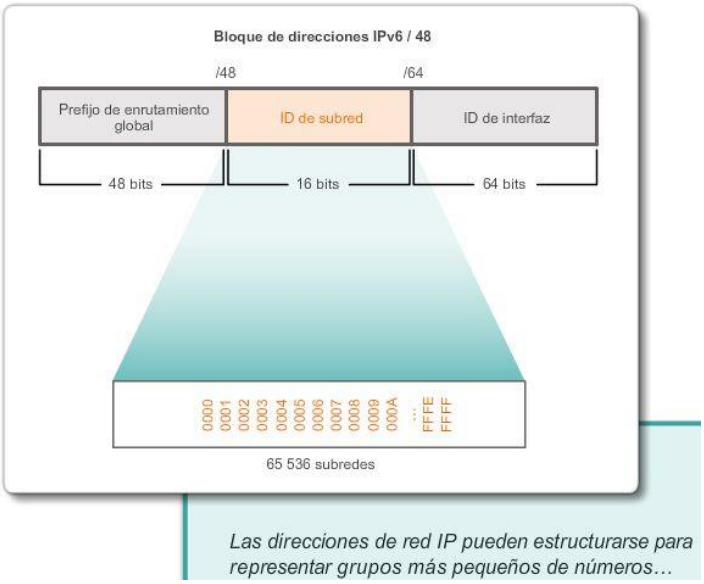
En este capítulo, aprenderá cómo se pueden agrupar los dispositivos de una red grande en subredes o grupos de redes más pequeños.

En esta actividad de creación de modelos, deberá pensar en un número que probablemente utilice a diario, como su número de teléfono. A medida que complete la actividad, piense en qué forma su número de teléfono es comparable con las estrategias que los administradores de red pueden utilizar para identificar hosts a fin de lograr una comunicación eficaz de datos.

Complete las dos preguntas que se indican a continuación y registre sus respuestas. Conserve una copia impresa o electrónica de las dos secciones para analizarlas más adelante en clase.

- Explique la forma en que su número de teléfono móvil o fijo se divide en grupos para su identificación. ¿Su número de teléfono posee código de área, identificador ISP o prefijo de ciudad, estado o país?

- ¿De qué manera la separación del número de teléfono en partes organizadas ayuda a contactarse y comunicarse con otras personas?



Capítulo 9: División de redes IP en subredes 9.1.1.1 Motivos para la división en subredes

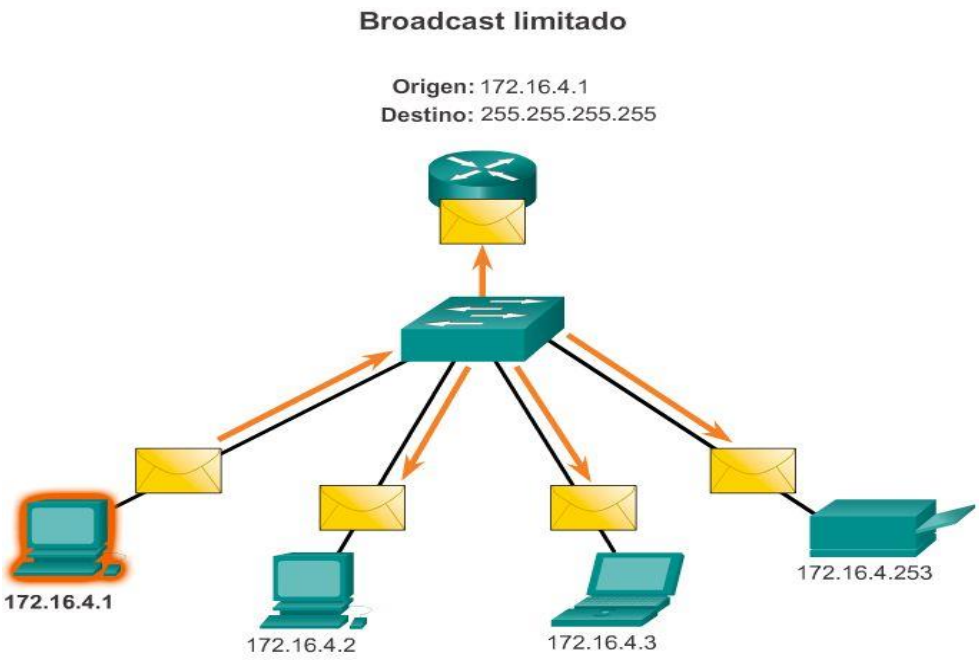
En las primeras implementaciones de red, era común que las organizaciones tuvieran todas las PC y otros dispositivos en red conectados a una única red IP. A todos los dispositivos de la organización se les asignaba una dirección IP con la correspondiente ID de la red. Este tipo de configuración se conoce como “diseño de red plana”. En una red pequeña, con una cantidad limitada de dispositivos, el diseño de red plana no presenta inconvenientes. Sin embargo, a medida que la red crece, este tipo de configuración puede generar problemas importantes.

Considere la forma en que, en una LAN Ethernet, los dispositivos utilizan broadcasts para localizar los servicios y dispositivos necesarios. Recuerde que, en las redes IP, se envía un broadcast a todos los hosts. El protocolo de configuración dinámica de host (DHCP) constituye un ejemplo de un servicio de red que depende de broadcasts. Los dispositivos envían broadcasts a través de la red para localizar el servidor de DHCP. En una red grande, esto podría generar una cantidad significativa de tráfico que retardaría las operaciones de red. Además, debido a que los broadcasts se dirigen a todos los dispositivos, todos ellos deben aceptar y procesar el tráfico, lo que da como resultado el aumento de los requisitos de procesamiento de los dispositivos. Si un dispositivo debe procesar una cantidad significativa de broadcasts, esto podría incluso llegar a disminuir la velocidad de las operaciones del dispositivo. Por motivos tales como los mencionados, las redes más grandes se deben segmentar en subredes más pequeñas, de modo que permanezcan localizadas en grupos más reducidos de dispositivos y servicios.

El proceso de segmentación de una red mediante su división en varios espacios de red más pequeños se denomina “división en subredes”.

Estas redes subordinadas se denominan “subredes”. Los administradores de red pueden agrupar dispositivos y servicios en subredes determinadas según la ubicación geográfica (por ejemplo, el tercer piso de un edificio), según la unidad organizativa (quizá el departamento de ventas), según el tipo de dispositivo (impresoras, servidores, WAN) o según cualquier otra división que tenga sentido para la red. La división en subredes puede reducir el tráfico general de la red y mejorar su rendimiento.

Nota: las subredes son equivalentes a las redes, y estos términos se pueden utilizar indistintamente. La mayoría de las redes son una subred de algún bloque de direcciones más grande.

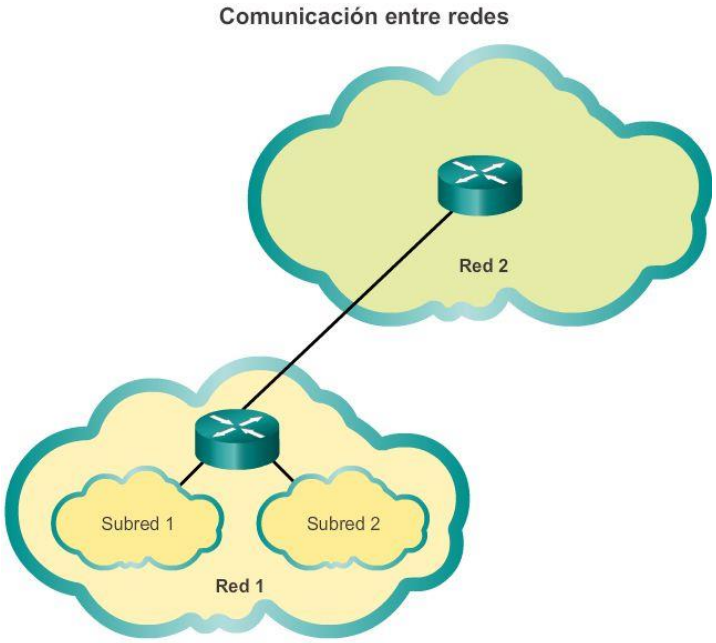


Capítulo 9: División de redes IP en subredes 9.1.1.2 Comunicación entre subredes

Se necesita un router para que dispositivos en redes distintas puedan comunicarse. Los dispositivos en una red utilizan la interfaz del router conectada a su LAN como gateway predeterminado. El router procesa el tráfico destinado a un dispositivo en una red remota y lo reenvía hacia el destino. Para determinar si el tráfico es local o remoto, el router utiliza la máscara de subred.

En un espacio de red dividido en subredes, esto funciona exactamente de la misma manera. Como se muestra en la ilustración, mediante la división en subredes se crean varias redes lógicas a partir de un único bloque de direcciones o una única dirección de red. Cada subred se considera un espacio de red independiente. Los dispositivos en la misma subred deben utilizar una dirección, una máscara de subred y un gateway predeterminado que se correspondan con la subred de la cual forman parte.

El tráfico no puede reenviarse entre subredes sin un router. Cada interfaz en el router debe tener una dirección de host IPv4 que pertenezca a la red o a la subred a la cual se conecta la interfaz del router.



Capítulo 9: División de redes IP en subredes 9.1.2.1 El plan

Como se muestra en la ilustración, la planificación de las subredes de la red requiere un análisis de las necesidades de uso de red por parte de la organización y de la forma en que se estructurarán las subredes. El punto de inicio consiste en llevar a cabo un estudio de los requisitos de la red. Esto significa analizar la totalidad de la red y determinar sus secciones principales y el modo en que se segmentarán. El plan de direcciones incluye la determinación de las necesidades de cada subred en cuanto a tamaño, cantidad de hosts por subred, forma en que se asignarán las direcciones de host, cuáles son los hosts que requerirán direcciones IP estáticas y cuáles pueden utilizar DHCP para obtener la información de direccionamiento.

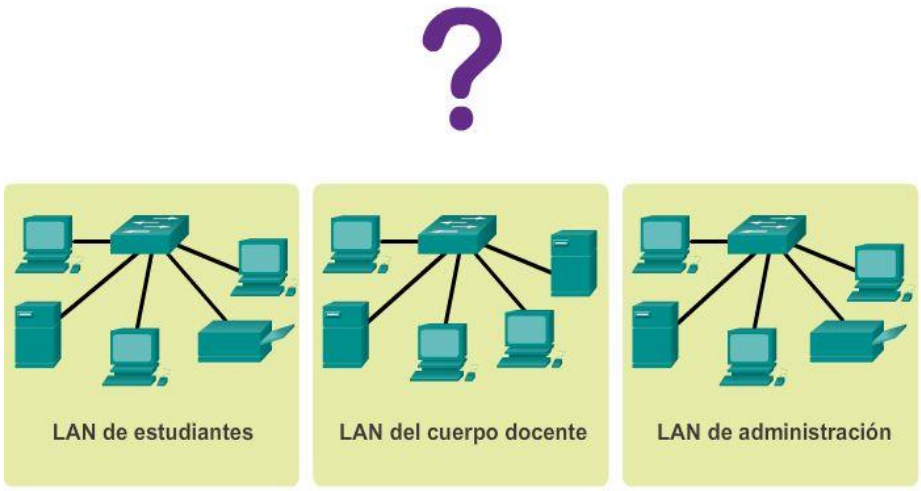
El tamaño de la subred implica planificar la cantidad de hosts que requerirán direcciones IP de host en cada subred de la red privada subdividida. Por ejemplo, en un diseño de red de campus, sería recomendable considerar cuántos hosts se necesitan en la LAN de la administración, cuántos en la LAN del cuerpo docente y cuántos en la LAN de los estudiantes. En una red doméstica, se podrían considerar la cantidad de hosts en la LAN principal de la casa y la cantidad de hosts en la LAN de la oficina doméstica.

Como ya se mencionó, el administrador de red decide el rango de direcciones IP privadas utilizado en una LAN y debe considerarlo cuidadosamente para asegurarse de que haya suficientes direcciones de host disponibles para los hosts conocidos hasta el momento y para futuras expansiones. Recuerde que los rangos de direcciones IP privadas son los siguientes:

- 10.0.0.0 con una máscara de subred de 255.0.0.0
- 172.16.0.0 con una máscara de subred de 255.240.0.0
- 192.168.0.0 con una máscara de subred de 255.255.0.0

Conocer los requisitos de dirección IP permite determinar el rango o los rangos de direcciones de host que se deben implementar. La división en subredes del espacio de direcciones IP privadas seleccionado proporciona direcciones de host para satisfacer las necesidades de la red.

Las direcciones públicas que se utilizan para conectarse a Internet las suele asignar un proveedor de servicios. Por lo tanto, si bien se aplicarían los mismos principios de la división en subredes, esto generalmente no es responsabilidad del administrador de red de la organización.



La planificación requiere decisiones sobre cada subred en lo que respecta al tamaño, la cantidad de hosts por subred y la forma de asignar las direcciones de host.

Capítulo 9: División de redes IP en subredes 9.1.2.2 El plan: asignación de direcciones

Cree estándares para la asignación de direcciones IP dentro de cada rango de subred. Por ejemplo:

- Se asignarán direcciones IP estáticas a las impresoras y los servidores.
- El usuario recibirá direcciones IP de los servidores de DHCP con subredes /24.
- A los routers se les asignan las primeras direcciones de host disponibles en el rango.

Dos factores muy importantes que conducen a la determinación de cuál es el bloque de direcciones privadas que se necesita son la cantidad de subredes requeridas y la cantidad máxima de hosts necesarios por subred. Cada uno de estos bloques de direcciones le permitirá asignar adecuadamente los hosts sobre la base del tamaño dado de una red y los hosts que requiere en la actualidad y los que requerirá en el futuro cercano. Los requisitos de espacio IP determinan el rango o los rangos de hosts que se deben implementar.

En los próximos ejemplos, verá una división en subredes basada en los bloques de direcciones que tienen máscaras de subred 255.0.0.0, 255.255.0.0 y 255.255.255.0.

Capítulo 9: División de redes IP en subredes 9.1.3.1 División básica en subredes

Cada dirección de red tiene un rango válido de direcciones de host. Todos los dispositivos conectados a la misma red tendrán una dirección de host IPv4 para esa red y una máscara de subred o un prefijo de red común.

El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

Las subredes IPv4 se crean utilizando uno o más de los bits de host como bits de red. Esto se hace ampliando la máscara para tomar prestado algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuantos más bits de host se tomen prestados, mayor será la cantidad de subredes que puedan definirse. Por cada bit que se toma prestado, se duplica la cantidad de subredes disponibles. Por ejemplo, si se toma prestado 1 bit, se pueden crear 2 subredes. Si se toman prestados 2 bits, se crean 4 subredes; si se toman prestados 3 bits, se crean 8 subredes, y así sucesivamente. Sin embargo, con cada bit que se toma prestado, se dispone de menos direcciones de host por subred.

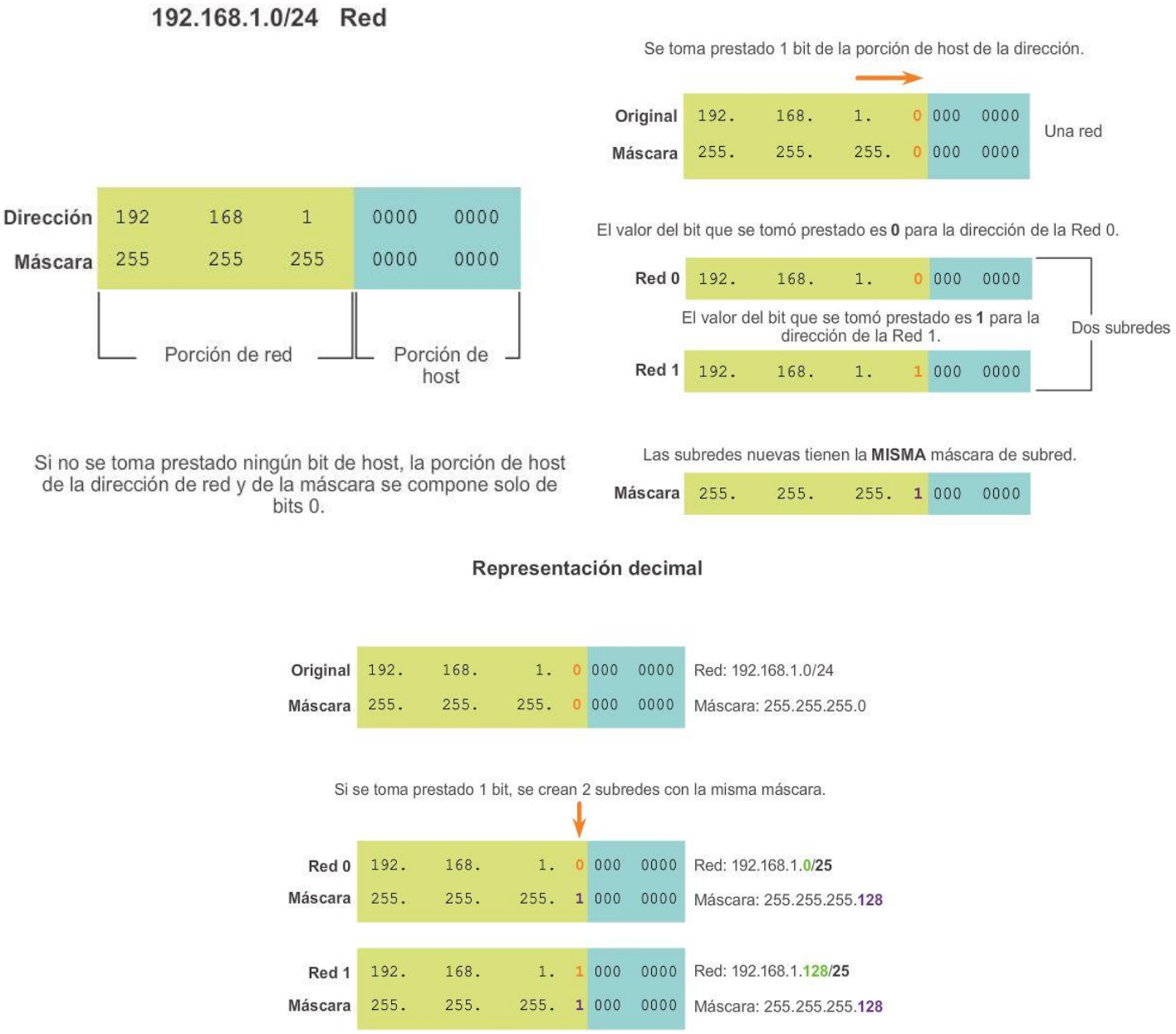
Los bits solo se pueden tomar prestados de la porción de host de la dirección. El proveedor de servicios determina la porción de red de la dirección, la que no puede modificarse.

Nota: en los ejemplos de las ilustraciones, solo se muestra el último octeto en formato binario debido a que únicamente se pueden tomar prestados bits de la porción de host.

Como se muestra en la figura 1, la red 192.168.1.0/24 tiene 24 bits en la porción de red y 8 bits en la porción de host, lo que se indica con la máscara de subred 255.255.255.0 o la notación /24. Sin división en subredes, esta red admite una única interfaz LAN. Si se necesitara otra LAN, sería necesario dividir la red en subredes.

En la figura 2, se toma prestado 1 bit del bit más significativo (el bit que se encuentra más a la izquierda) en la porción de host, lo que extiende la porción de red a 25 bits. Esto crea 2 subredes que se identifican mediante un 0 en el bit que se tomó prestado para la primera red y un 1 en el bit que se tomó prestado para la segunda red. La máscara de subred para ambas redes utiliza un 1 en la posición del bit que se tomó prestado para indicar que ahora este bit es parte de la porción de red.

Como se muestra en la figura 3, cuando convertimos el octeto binario al sistema decimal, advertimos que la dirección de la primera subred es 192.168.1.0 y la dirección de la segunda subred es 192.168.1.128. Dado que se tomó prestado un bit, la máscara de subred de cada subred es 255.255.255.128 o /25.



Capítulo 9: División de redes IP en subredes 9.1.3.2 Subredes en uso

En el ejemplo anterior, se dividió la red 192.168.1.0/24 para crear dos subredes:

192.168.1.0/25

192.168.1.128/25

En la figura 1, observe que el router R1 tiene dos segmentos LAN conectados a sus interfaces GigabitEthernet. Para los segmentos conectados a estas interfaces, se utilizarán subredes. Para cumplir la función de gateway para los dispositivos en la LAN, a cada una de las interfaces del router se le debe asignar una dirección IP dentro del rango de direcciones válidas para la subred asignada. Es habitual utilizar la primera o la última dirección disponible en un rango de red para la dirección de la interfaz del router.

La primera subred, 192.168.1.0/25, se utiliza para la red conectada a GigabitEthernet 0/0, y la segunda subred, 192.168.1.128/25, se utiliza para la red conectada a GigabitEthernet 0/1. Para asignar una dirección IP para cada una de estas interfaces, se debe determinar el rango de direcciones IP válidas para cada subred.

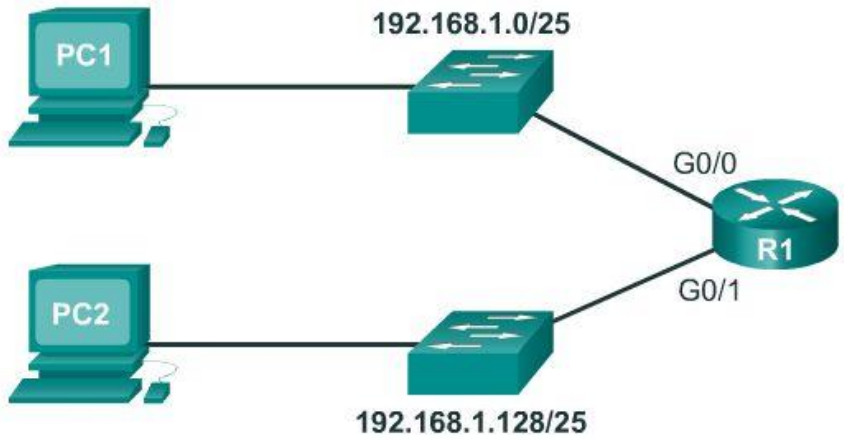
Las siguientes son pautas para cada una de las subredes:

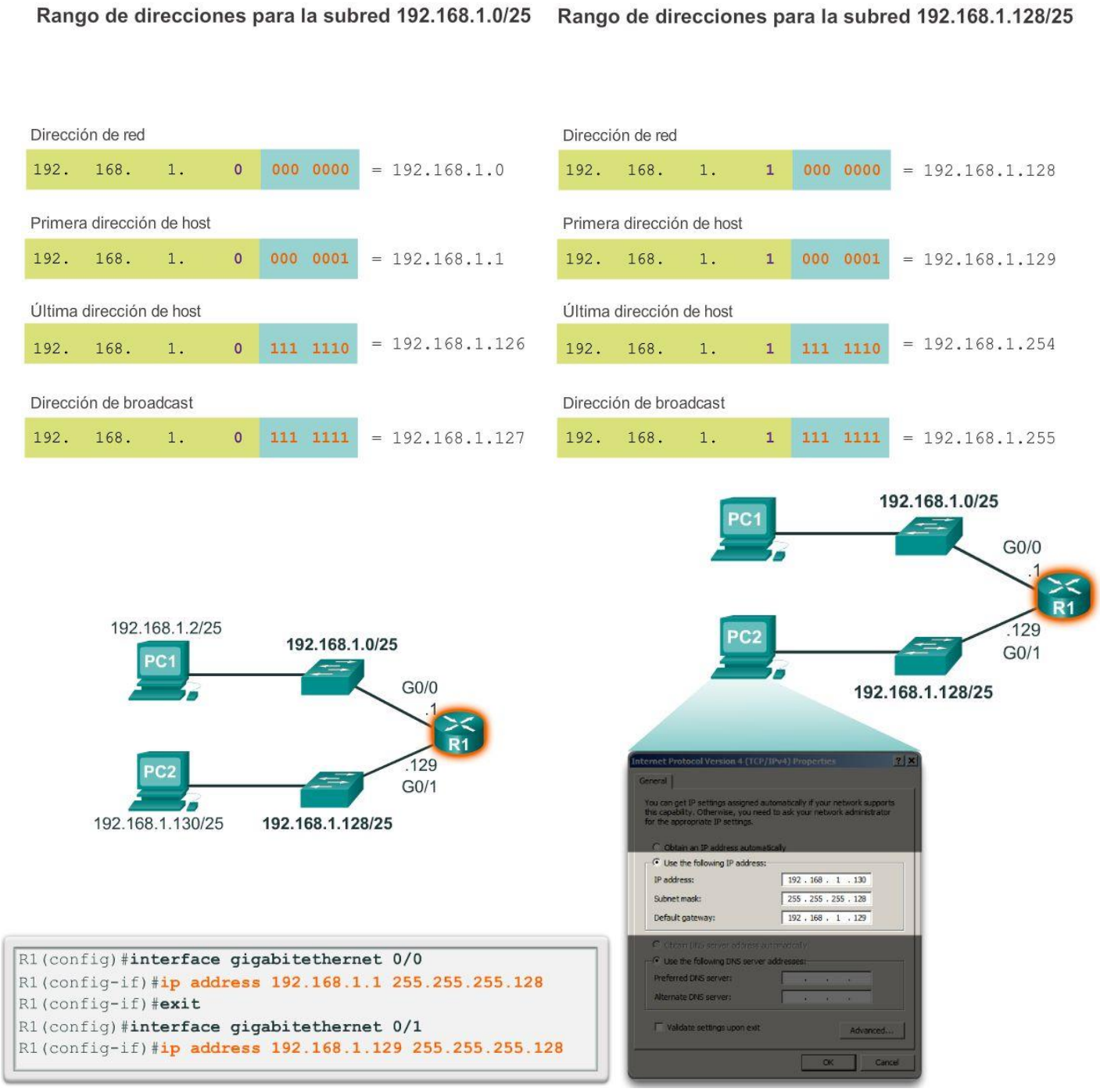
- Dirección de red: todos bits 0 en la porción de host de la dirección.
- Primera dirección de host: todos bits 0 más un bit 1 (en la máxima posición a la derecha) en la porción de host de la dirección.
- Última dirección de host: todos bits 1 más un bit 0 (en la máxima posición a la derecha) en la porción de host de la dirección.
- Dirección de broadcast: todos bits 1 en la porción de host de la dirección.

Como se muestra en la figura 2, la primera dirección de host para la red 192.168.1.0/25 es 192.168.1.1, y la última dirección de host es 192.168.1.126. En la figura 3, se muestra que la primera dirección de host para la red 192.168.1.128/25 es 192.168.1.129, y la última dirección de host es 192.168.1.254.

Para asignar la primera dirección de host en cada subred a la interfaz del router para esa subred, utilice el comando ip address en el modo de configuración de interfaz, como se muestra en la figura 4. Observe que cada subred utiliza la máscara de subred 255.255.255.128 para indicar que la porción de red de la dirección es 25 bits.

En la figura 5, se muestra una configuración de host para la red 192.168.1.128/25. Observe que la dirección IP del gateway es la dirección configurada en la interfaz G0/1 del R1, 192.168.1.129, y la máscara de subred es 255.255.255.128.





Capítulo 9: División de redes IP en subredes 9.1.3.3 Fórmulas de división en subredes

Cálculo de subredes

Use esta fórmula para calcular la cantidad de subredes:

2^n (donde “n” representa la cantidad de bits que se toman prestados)

Como se muestra en la figura 1, para el ejemplo 192.168.1.0/25, el cálculo es el siguiente:

2^1 = 2 subredes

Cálculo de hosts

Utilice la siguiente fórmula para calcular la cantidad de hosts por red:

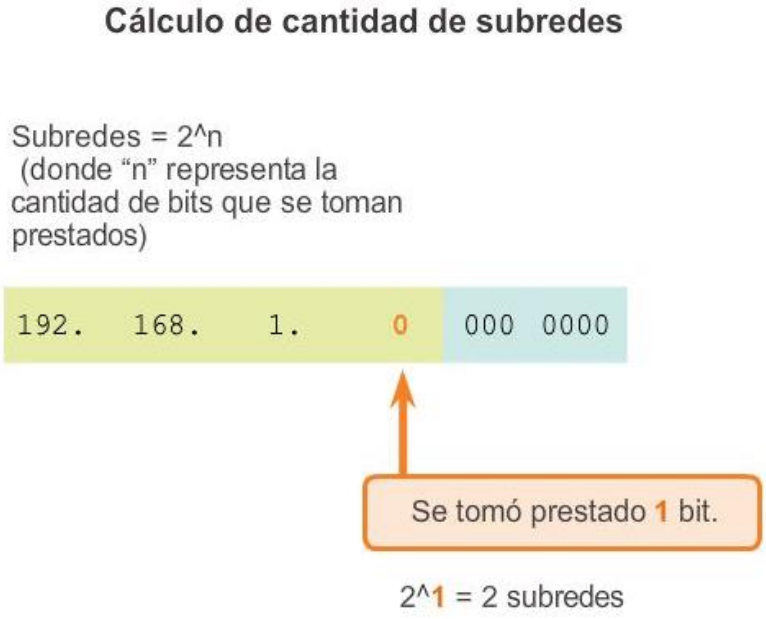
2^n (donde “n” representa la cantidad de bits restantes en el campo de host)

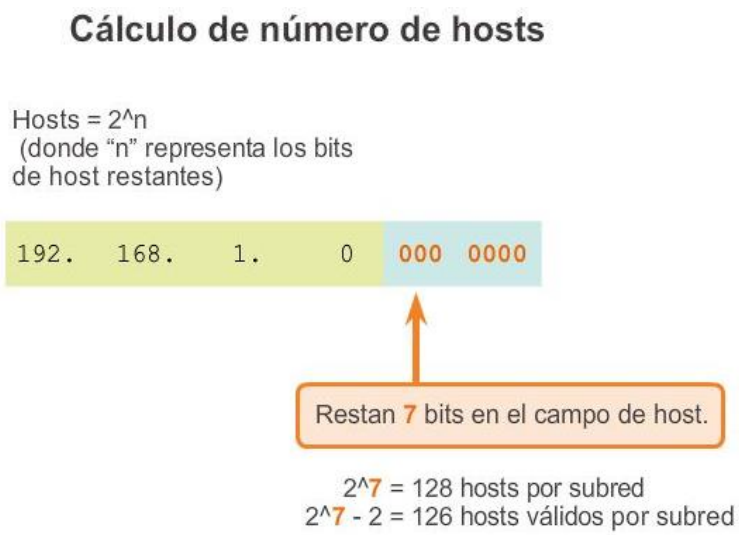
Como se muestra en la figura 2, para el ejemplo 192.168.1.0/25, el cálculo es el siguiente:

2^7 = 128

Debido a que los hosts no pueden utilizar la dirección de red o a la dirección de broadcast de una subred, dos de estas direcciones no son válidas para la asignación de hosts. Esto significa que cada una de las subredes tiene 126 (128-2) direcciones de host válidas.

Por lo tanto, en este ejemplo, si se toma prestado 1 bit de host para la red, se crean 2 subredes, y cada subred puede tener un total de 126 hosts asignados.





Capítulo 9: División de redes IP en subredes 9.1.3.4 Creación de cuatro subredes

Piense en una internetwork que requiere tres subredes.

Con el mismo bloque de direcciones 192.168.1.0/24, se deben tomar prestados bits de host para crear, al menos, tres subredes. Tomar prestado un único bit proporcionaría solo dos subredes. Para proporcionar más redes, se deben tomar prestados más bits de host. Calcule la cantidad de subredes que se crean si se toman prestados 2 bits mediante la fórmula 2^cantidad de bits que se toman prestados:

2^2 = 4 subredes

Si se toman prestados 2 bits, se crean 4 subredes, como se muestra en la figura 1.

Recuerde que la máscara de subred debe modificarse para que se muestren los bits prestados. En este ejemplo, cuando se toman prestados 2 bits, la máscara se extiende 2 bits en el último octeto. En formato decimal, la máscara se representa como 255.255.255.192, debido a que el último octeto es 1100 0000 en formato binario.

Cálculo de hosts

Para calcular la cantidad de hosts, examine el último octeto. Después de tomar prestados 2 bits para la subred, restan 6 bits de host.

Aplique la fórmula de cálculo de host que se muestra en la figura 2.

2^6 = 64

Sin embargo, recuerde que todos los bits 0 que se encuentran en la porción de host de la dirección forman la dirección de red, y que todos los bits 1 en la porción de host componen una dirección de broadcast. Por lo tanto, hay solo 62 direcciones de host realmente disponibles para cada subred.

Como se muestra en la figura 3, la primera dirección de host para la primera subred es 192.168.1.1, y la última dirección de host es 192.168.1.62. En la figura 4, se muestran los rangos para las subredes 0 a 2. Recuerde

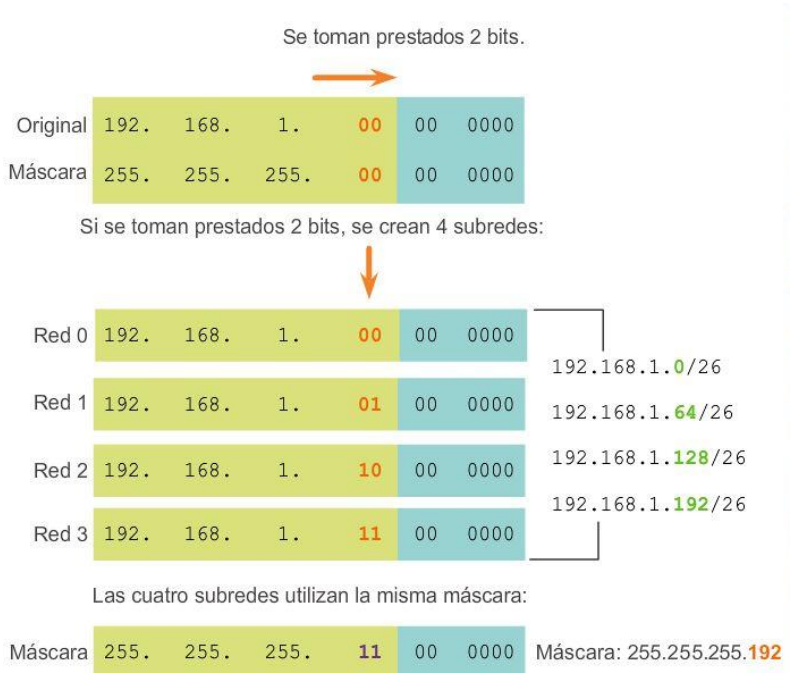
que cada host debe contener una dirección IP válida dentro del rango definido para ese segmento de red. La subred asignada a la interfaz del router determinará a qué segmento pertenece un host.

En la figura 5, se muestra un ejemplo de configuración. En esta configuración, la primera red se asigna a la interfaz GigabitEthernet 0/0, la segunda red se asigna a la interfaz GigabitEthernet 0/1, y la tercera red se asigna a la red Serial 0/0/0.

Una vez más, mediante un plan de direccionamiento común, se asigna la primera dirección de host en la subred a la interfaz del router. Los hosts de cada subred utilizarán la dirección de la interfaz del router como la dirección de gateway predeterminado.

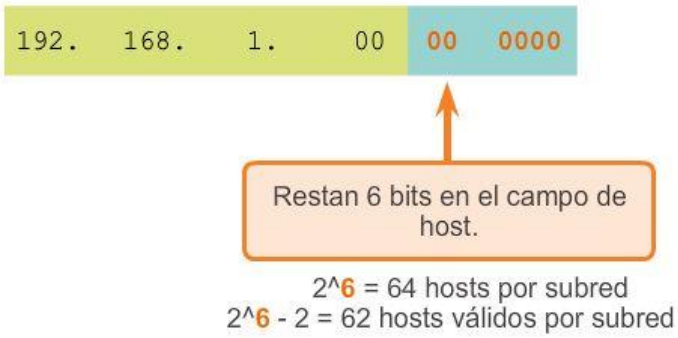
- La PC1 (192.168.1.2/26) utilizará 192.168.1.1 (dirección de la interfaz G0/0 del R1) como su dirección de gateway predeterminado.
- La PC2 (192.168.1.66/26) utilizará 192.168.1.65 (dirección de la interfaz G0/1 del R1) como su dirección de gateway predeterminado.

Nota: todos los dispositivos que se encuentran en la misma subred tendrán una dirección de host IPv4 del rango de direcciones de host y usarán la misma máscara de subred.



Cálculo de número de hosts

Hosts = 2^n
(donde “n” representa los bits de host restantes)



Rango de direcciones para la subred 192.168.1.0/26

Dirección de red

192. 168. 1. 00 00 0000 = 192.168.1.0

Primera dirección de host

192. 168. 1. 00 00 0001 = 192.168.1.1

Última dirección de host

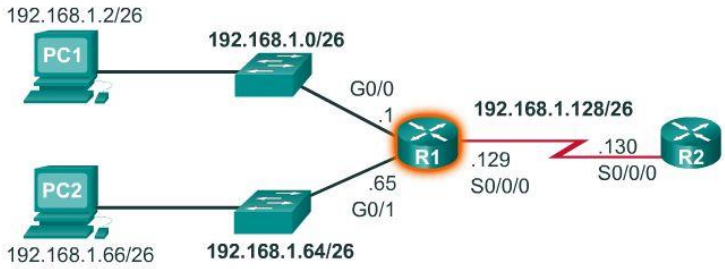
192. 168. 1. 00 11 1110 = 192.168.1.62

Dirección de broadcast

192. 168. 1. 00 11 1111 = 192.168.1.63

Rangos de direcciones para las redes 0 a 2

Red 0	Red	192.	168.	1.	00	00	0000	192.168.1.0
	Primero	192.	168.	1.	00	00	0001	192.168.1.1
	Última	192.	168.	1.	00	11	1110	192.168.1.62
	Broadcast	192.	168.	1.	00	11	1111	192.168.1.63
Red 1	Red	192.	168.	1.	01	00	0000	192.168.1.64
	Primero	192.	168.	1.	01	00	0001	192.168.1.65
	Última	192.	168.	1.	01	11	1110	192.168.1.126
	Broadcast	192.	168.	1.	01	11	1111	192.168.1.127
Red 2	Red	192.	168.	1.	10	00	0000	192.168.1.128
	Primero	192.	168.	1.	10	00	0001	192.168.1.129
	Última	192.	168.	1.	10	11	1110	192.168.1.190
	Broadcast	192.	168.	1.	10	11	1111	192.168.1.191




```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.192
R1(config-if)#exit
R1(config)#interface gigabitethernet 0/1
R1(config-if)#ip address 192.168.1.65 255.255.255.192
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.1.129 255.255.255.192
```

Capítulo 9: División de redes IP en subredes 9.1.3.5 Creación de ocho subredes

A continuación, imagine una internetwork que requiere cinco subredes, como se muestra en la figura 1.

Con el mismo bloque de direcciones 192.168.1.0/24, se deben tomar prestados bits de host para crear, al menos, cinco subredes. Tomar prestados 2 bits proporcionaría solo 4 subredes, como se muestra en el ejemplo anterior. Para proporcionar más redes, se deben tomar prestados más bits de host. Utilice la fórmula para calcular la cantidad de subredes que se crean si se toman prestados 3 bits:

2^3 = 8 subredes

Como se muestra en las figuras 2 y 3, si se toman prestados 3 bits, se crean 8 subredes. Cuando se toman prestados 3 bits, la máscara de subred se extiende 3 bits en el último octeto (/27), lo que da como resultado la máscara de subred 255.255.255.224. Todos los dispositivos en estas subredes utilizarán la máscara de la máscara de subred 255.255.255.224 (/27).

Cálculo de hosts

Para calcular la cantidad de hosts, examine el último octeto. Después de tomar prestados 3 bits para la subred, restan 5 bits de host.

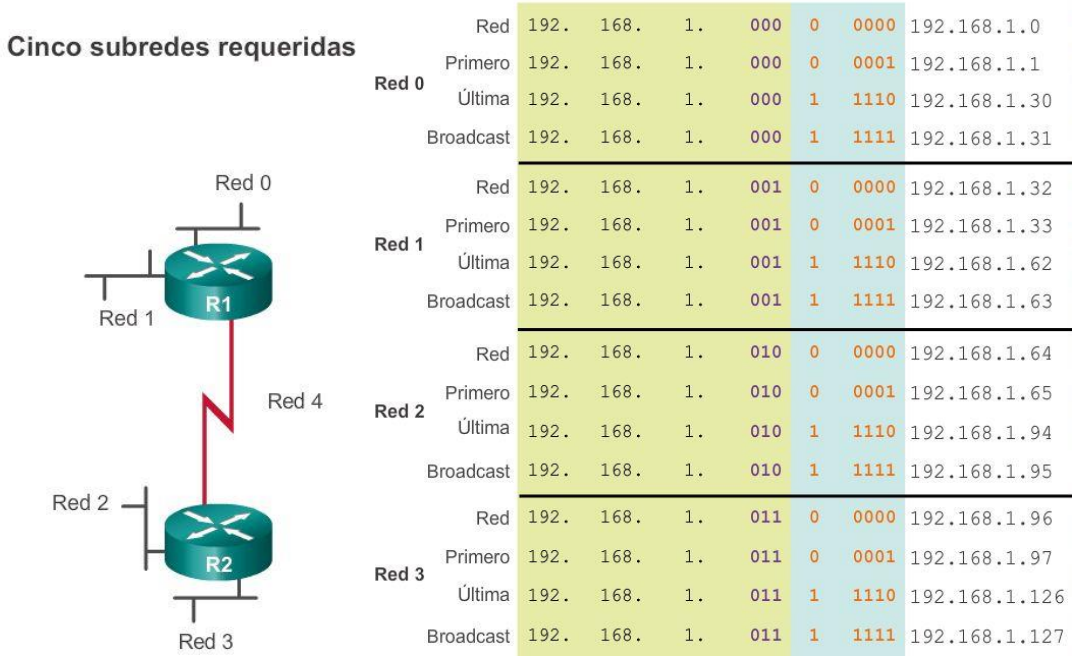
Aplique la fórmula de cálculo de host:

2^5 = 32, pero reste 2 por todos los 0 en la porción de host (dirección de red) y todos los 1 en la porción de host (dirección de broadcast).

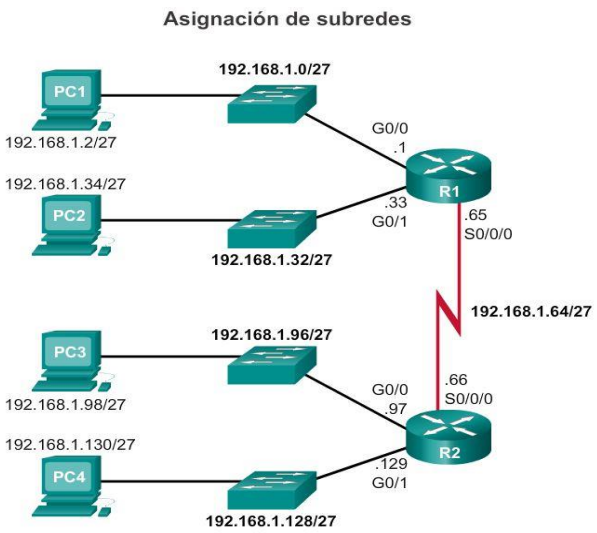
Las subredes se asignan a los segmentos de red necesarios para la topología, como se muestra en la figura 4.

Una vez más, mediante un plan de direccionamiento común, se asigna la primera dirección de host en la subred a la interfaz del router, como se muestra en la figura 5. Los hosts de cada subred utilizarán la dirección de la interfaz del router como la dirección de gateway predeterminado.

- La PC1 (192.168.1.2/27) utilizará la dirección 192.168.1.1 como la dirección de gateway predeterminado.
- La PC2 (192.168.1.34/27) utilizará la dirección 192.168.1.33 como la dirección de gateway predeterminado.
- La PC3 (192.168.1.98/27) utilizará la dirección 192.168.1.97 como la dirección de gateway predeterminado.
- La PC4 (192.168.1.130/27) utilizará la dirección 192.168.1.129 como la dirección de gateway predeterminado.



Red 0	Red	192.	168.	1.	000	0	0000	192.168.1.0
	Primero	192.	168.	1.	000	0	0001	192.168.1.1
	Última	192.	168.	1.	000	1	1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1	1111	192.168.1.31
Red 1	Red	192.	168.	1.	001	0	0000	192.168.1.32
	Primero	192.	168.	1.	001	0	0001	192.168.1.33
	Última	192.	168.	1.	001	1	1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1	1111	192.168.1.63
Red 2	Red	192.	168.	1.	010	0	0000	192.168.1.64
	Primero	192.	168.	1.	010	0	0001	192.168.1.65
	Última	192.	168.	1.	010	1	1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1	1111	192.168.1.95
Red 3	Red	192.	168.	1.	011	0	0000	192.168.1.96
	Primero	192.	168.	1.	011	0	0001	192.168.1.97
	Última	192.	168.	1.	011	1	1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1	1111	192.168.1.127



Red 4	Red	192.	168.	1.	100	0	0000	192.168.1.128
	Primero	192.	168.	1.	100	0	0001	192.168.1.129
	Última	192.	168.	1.	100	1	1110	192.168.1.158
	Broadcast	192.	168.	1.	100	1	1111	192.168.1.159
Red 5	Red	192.	168.	1.	101	0	0000	192.168.1.160
	Primero	192.	168.	1.	101	0	0001	192.168.1.161
	Última	192.	168.	1.	101	1	1110	192.168.1.190
	Broadcast	192.	168.	1.	101	1	1111	192.168.1.191
Red 6	Red	192.	168.	1.	110	0	0000	192.168.1.192
	Primero	192.	168.	1.	110	0	0001	192.168.1.193
	Última	192.	168.	1.	110	1	1110	192.168.1.222
	Broadcast	192.	168.	1.	110	1	1111	192.168.1.223
Red 7	Red	192.	168.	1.	111	0	0000	192.168.1.224
	Primero	192.	168.	1.	111	0	0001	192.168.1.225
	Última	192.	168.	1.	111	1	1110	192.168.1.254
	Broadcast	192.	168.	1.	111	1	1111	192.168.1.255

Capítulo 9: División de redes IP en subredes 9.1.3.10 Creación de 100 subredes con un prefijo /16

En los ejemplos anteriores, utilizamos una internetwork que requería tres subredes y una que requería cinco subredes. Para alcanzar el objetivo de crear cuatro subredes, tomamos prestados 2 bits de los 8 bits de host disponibles con una dirección IP que tiene la máscara predeterminada 255.255.255.0 o el prefijo /24. La máscara de subred resultante fue 255.255.255.192, y se crearon 4 subredes posibles en total. Con la fórmula de cálculo de hosts 2^6-2, determinamos que en cada una de dichas 4 subredes, podíamos tener 62 direcciones de host para asignar a los nodos.

Para adquirir 5 subredes, tomamos prestados 3 bits de los 8 bits de host disponibles con una dirección IP que tiene la máscara predeterminada 255.255.255.0 o el prefijo /24.

Al tomar prestados esos 3 bits de la porción de host de la dirección, quedaron 5 bits de host. La máscara de subred resultante fue 255.255.255.224, con un total de 8 subredes creadas y 30 direcciones de host por subred.

Piense en grandes organizaciones o campus con una internetwork que requiere 100 subredes. Al igual que en los ejemplos anteriores, para lograr el objetivo de crear 100 subredes, debemos tomar prestados bits de la porción de host de la dirección IP de la internetwork existente. Del mismo modo que antes, para calcular la cantidad de subredes debemos observar la cantidad de bits de host disponibles y utilizar la fórmula de cálculo de subredes 2^cantidad de bits que se toman prestados menos 2. Con la dirección IP del último ejemplo, 192.168.10.0/24, tenemos 8 bits de host. Para crear 100 subredes, debemos tomar prestados 7 bits.

Calcule la cantidad de subredes si se toman prestados 7 bits: 2^7=128 subredes.

Sin embargo, si se toman prestados 7 bits, restará solo un bit de host, y si aplicamos la fórmula de cálculo de hosts, el resultado sería que no hay hosts en estas subredes. Calcule la cantidad de hosts si resta un bit: 2^1=2. A continuación, reste 2 para la dirección de red y para la dirección de broadcast. El resultado es 0 hosts (2^1-2=0).

En una situación en la que se necesita una mayor cantidad de subredes, se requiere una red IP con más bits de host para tomar prestados, como una dirección IP con la máscara de subred predeterminada /16 o 255.255.0.0. Las direcciones que tienen un rango de 128 a 191 en el primer octeto tienen la máscara predeterminada 255.255.0.0 o /16. Las direcciones de este rango tienen 16 bits en la porción de red y 16 bits en la porción de host. Estos 16 bits son los bits disponibles para tomar prestados para la creación de subredes.

Con una nueva dirección IP del bloque de direcciones 172.16.0.0/16, se deben tomar prestados bits de host para crear, al menos, 100 subredes. Comenzaremos de izquierda a derecha con el primer bit de host disponible y tomaremos prestado un único bit por vez hasta alcanzar la cantidad de bits necesarios para crear 100 subredes. Si tomamos prestado 1 bit, crearíamos 2 subredes; si tomamos prestados 2 bits, crearíamos 4 subredes; con 3 bits crearíamos 8 subredes, y así sucesivamente. Calcule la cantidad de subredes que se crean si se toman prestados 7 bits mediante la fórmula 2^cantidad de bits que se toman prestados:

2^7 = 128 subredes

Si se toman prestados 7 bits, se crean 128 subredes, como se muestra en la ilustración.

Recuerde que la máscara de subred debe modificarse para que se muestren los bits prestados. En este ejemplo, cuando se toman prestados 7 bits, la máscara se extiende 7 bits en el tercer octeto. En formato decimal, la máscara se representa como 255.255.254.0 o el prefijo /23, debido a que, en formato binario, el tercer octeto es 11111110 y el cuarto octeto es 00000000. La división en subredes se realizará en el tercer octeto, con los bits de host del tercero y el cuarto octeto.

Capítulo 9: División de redes IP en subredes 9.1.3.11 Cálculo de hosts

Cálculo de hosts

Para calcular el número de hosts, observe el tercer y cuarto octeto. Después de tomar prestados 7 bits para la subred, resta un bit de host en el tercer octeto y 8 bits de host en el cuarto octeto.

Aplique la fórmula de cálculo de hosts como se muestra en la figura 1.

2^9 = 512

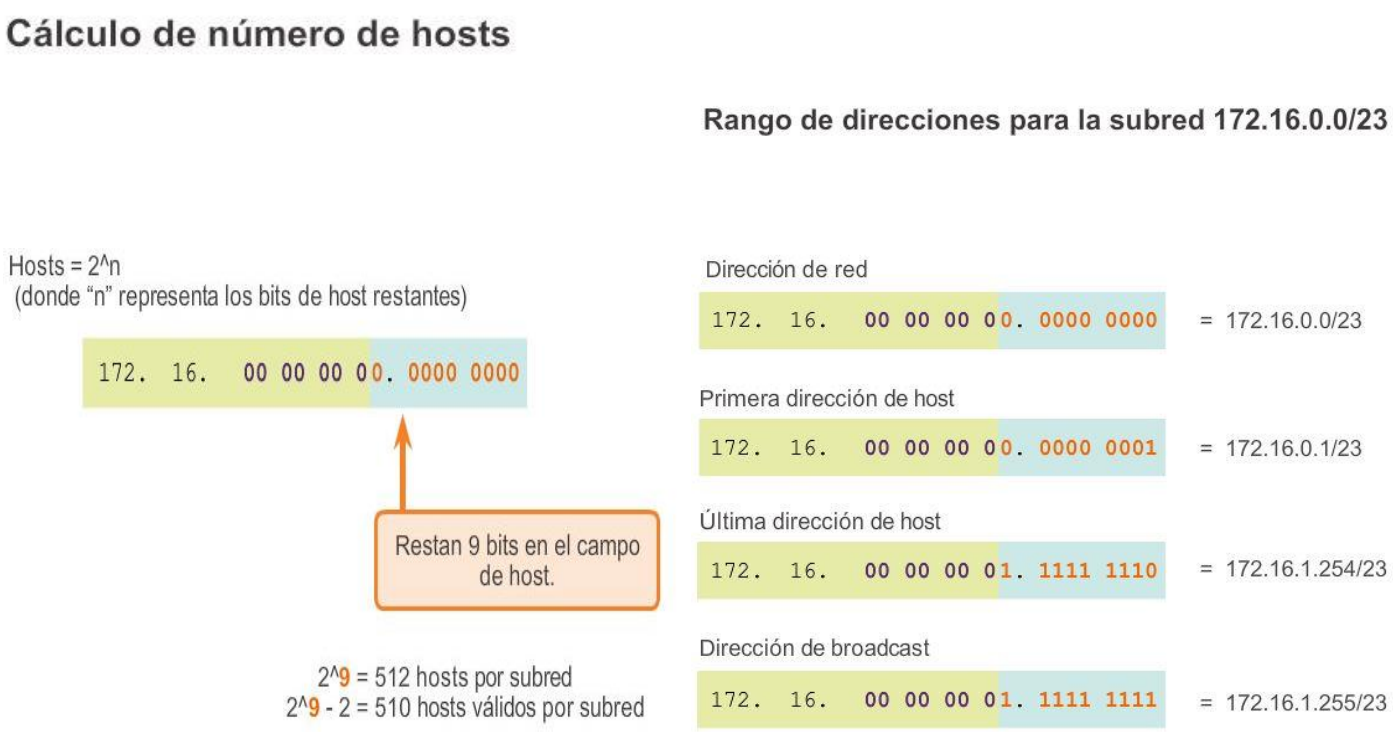
Sin embargo, recuerde que todos los bits 0 que se encuentran en la porción de host de la dirección forman la dirección de red, y que todos los bits 1 en la porción de host componen una dirección de broadcast. Por lo tanto, hay solo 510 direcciones de host realmente disponibles para cada subred.

Como se muestra en la figura 2, la primera dirección de host para la primera subred es 172.16.0.1, y la última dirección de host es 172.16.1.254.

Recuerde que cada host debe contener una dirección IP válida dentro del rango definido para ese segmento de red. La subred asignada a la interfaz del router determinará a qué segmento pertenece un host.

Recordatorio:

Los bits solo se pueden tomar prestados de la porción de host de la dirección. El proveedor de servicios determina la porción de red de la dirección, la que no puede modificarse. Por lo tanto, las organizaciones que requieren una cantidad significativa de subredes deben comunicar esta necesidad a su ISP de modo que este les asigne un bloque de direcciones IP con una máscara predeterminada con suficientes bits para crear las subredes necesarias.



Capítulo 9: División de redes IP en subredes 9.1.3.12 Cálculo de hosts

Existen algunas organizaciones, como los pequeños proveedores de servicios, que posiblemente necesiten incluso más de 100 subredes. Piense, por ejemplo, en una organización que requiere 1000 subredes. Como siempre, para crear subredes debemos tomar prestados bits de la porción de host de la dirección IP de la internetwork existente. Al igual que sucedió anteriormente, para calcular la cantidad de subredes es necesario analizar la cantidad de bits de host disponibles. En una situación como esta, es necesario que la dirección IP asignada por el ISP tenga suficientes bits de host disponibles para calcular 1000 subredes. Las direcciones IP que tienen el rango de 1 a 126 en el primer octeto tienen la máscara predeterminada 255.0.0.0 o /8. Esto significa que hay 8 bits en la porción de red y 24 bits de host disponibles para tomar prestados para realizar la división en subredes.

Con el bloque de direcciones 10.0.0.0/8, se deben tomar prestados bits de host para crear, al menos, 1000 subredes. Comenzaremos de izquierda a derecha con el primer bit de host disponible y tomaremos prestado un único bit por vez hasta alcanzar la cantidad de bits necesarios para crear 1000 subredes. Calcule la cantidad de subredes que se crean si se toman prestados 10 bits mediante la fórmula 2^cantidad de bits que se toman prestados:

2^10 = 1024 subredes

Si se toman prestados 10 bits, se crean 1024 subredes, como se muestra en la figura 1.

Recuerde que la máscara de subred debe modificarse para que se muestren los bits prestados. En este ejemplo, cuando se toman prestados 10 bits, la máscara se extiende 10 bits en el tercer octeto. En formato decimal, la máscara se representa como 255.255.192.0 o el prefijo /18, debido a que, en formato binario, el tercer octeto de la máscara de subred es 11000000 y el cuarto octeto es 00000000. La división en subredes se realizará en el tercer octeto, pero no olvide los bits de host del tercero y el cuarto octeto.

Cálculo de hosts

Para calcular el número de hosts, observe el tercer y cuarto octeto. Después de tomar prestados 10 bits para la subred, restan 6 bits de host en el tercer octeto y 8 bits de host en el cuarto octeto. En total, restan 14 bits de host.

Aplique la fórmula de cálculo de host que se muestra en la figura 2.

2^14 - 2 = 16382

La primera dirección de host para la primera subred es 10.0.0.1, y la última dirección de host es 10.0.63.254. Recuerde que cada host debe contener una dirección IP válida dentro del rango definido para ese segmento de red. La subred asignada a la interfaz del router determinará a qué segmento pertenece un host.

Nota: todos los dispositivos que se encuentran en la misma subred tendrán una dirección de host IPv4 del rango de direcciones de host y usarán la misma máscara de subred.

Rango de direcciones para la subred 10.0.0.0/18

Capítulo 9: División de redes IP en subredes 9.1.4.1 Requisitos de la división en subredes basada en hosts

La decisión sobre cuántos bits de host se deben tomar prestados para crear subredes constituye una decisión de planificación importante. Al planificar las subredes, deben considerarse dos aspectos: la cantidad de direcciones de host que se requieren para cada red y la cantidad de subredes individuales que se necesitan. En la animación, se muestran las posibilidades de subredes para la red 192.168.1.0.

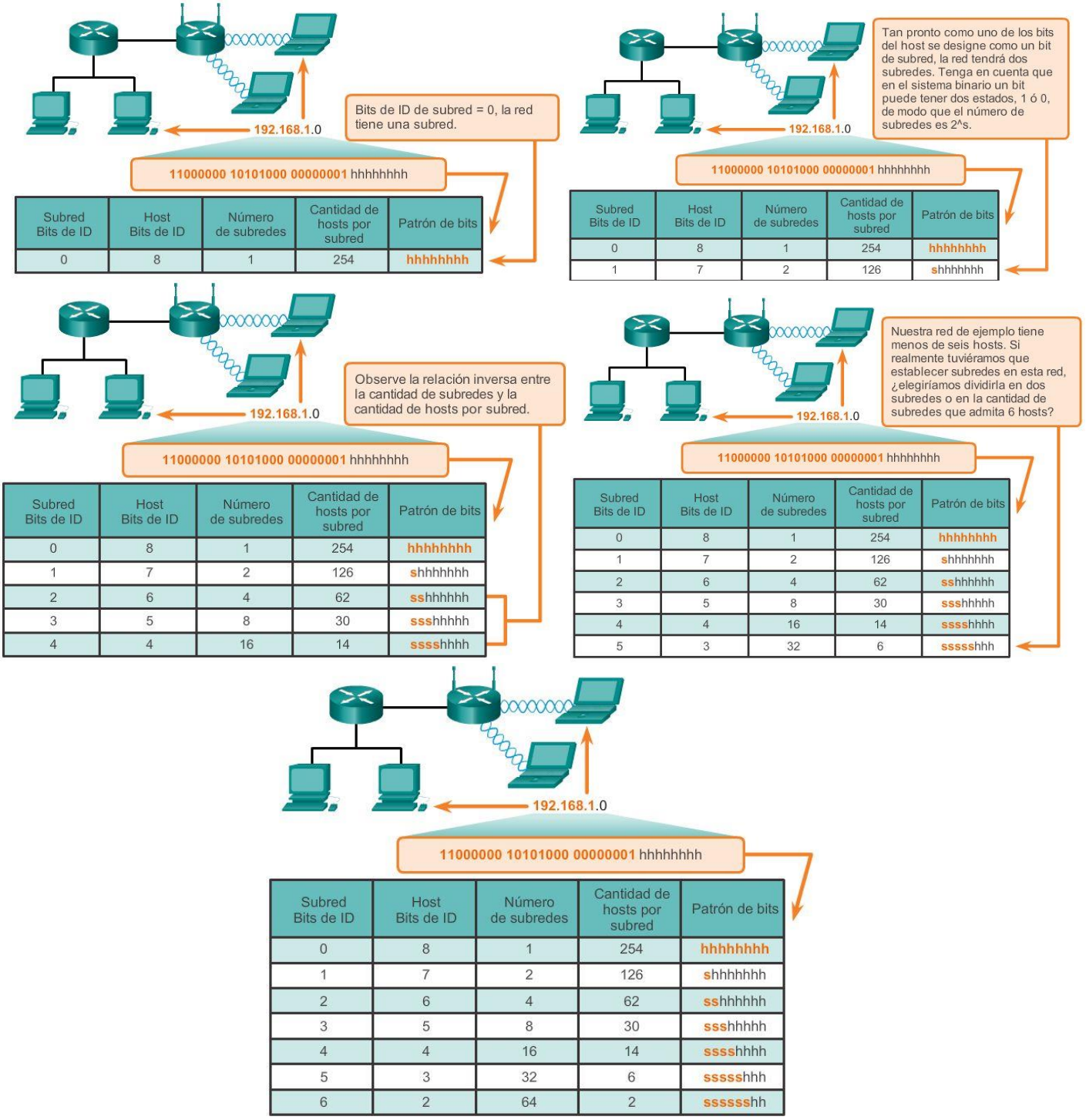
La selección de una cantidad de bits para la ID de subred afecta tanto la cantidad de subredes posibles como la cantidad de direcciones de host en cada subred.

Observe que existe una relación inversa entre la cantidad de subredes y la cantidad de hosts: cuantos más bits se toman prestados para crear subredes, menor es la cantidad de bits de host disponibles, lo que tiene

como resultado menos hosts por subred. Si se necesitan más direcciones de host, se requieren más bits de host, lo que tiene como resultado menos subredes.

Cantidad de hosts

Al tomar prestados bits para crear varias subredes, se deben dejar suficientes bits de host para la subred más grande. La cantidad de direcciones de host que se requieren en la subred más grande determina cuántos bits se deben dejar en la porción de host. La fórmula 2^n (donde “n” representa la cantidad de bits de host restantes) se utiliza para calcular cuántas direcciones disponibles habrá en cada subred. Recuerde que dos de las direcciones no se pueden utilizar, de modo que la cantidad utilizable de direcciones puede calcularse mediante la fórmula 2^n-2.



Subred Bits de ID	Host Bits de ID	Número de subredes	Cantidad de hosts por subred	Patrón de bits
0	8	1	254	hhhhhhhh
1	7	2	126	shhhhhhh
2	6	4	62	sshhhhhh
3	5	8	30	ssshhhhh
4	4	16	14	sssshhhh
5	3	32	6	ssssshh
6	2	64	2	ssssssh

Capítulo 9: División de redes IP en subredes 9.1.4.2 Requisitos de la división en subredes basada en redes

En ocasiones, se requiere una cantidad determinada de subredes, con menor énfasis en la cantidad de direcciones de host por subred. Esto puede suceder en el caso de una organización que decide separar el tráfico de la red sobre la base de la estructura interna o la organización de los departamentos. Por ejemplo, una organización puede elegir colocar todos los dispositivos host que utilizan los empleados del departamento de ingeniería en una red, y todos los dispositivos host que utiliza la gerencia en una red diferente. En este caso, la cantidad de subredes es el factor más importante para determinar cuántos bits se deben tomar prestados.

Recuerde que se puede calcular la cantidad de subredes que se crean cuando se toman bits prestados mediante la fórmula 2^n (donde “n” representa la cantidad de bits que se toman prestados). No hay necesidad de restar ninguna de las subredes resultantes, ya que todas son utilizables.

La clave es lograr un equilibrio entre la cantidad de subredes necesarias y la cantidad de hosts que se requieren para la subred más grande. Cuantos más bits se toman prestados para crear subredes adicionales, menor es la cantidad de hosts disponibles por subred.

Capítulo 9: División de redes IP en subredes 9.1.4.3 División en subredes para cumplir con los requisitos de la red

Toda red dentro de una organización está diseñada para admitir una cantidad finita de hosts. La división en subredes básica requiere que haya suficientes subredes para admitir las redes y, al mismo tiempo, que se proporcionen suficientes direcciones de host por subred.

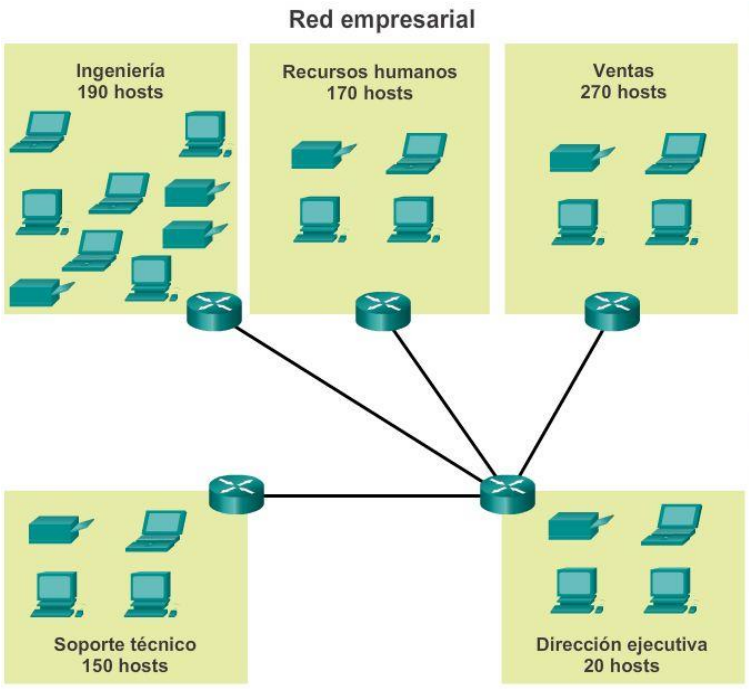
Algunas redes, como los enlaces WAN punto a punto, solo requieren dos hosts. Otras redes, como una LAN de usuario en un edificio o departamento grande, pueden necesitar la inclusión de cientos de hosts. Es necesario que los administradores de red diseñen el esquema de direccionamiento de la internetwork para admitir la cantidad máxima de hosts en cada red. La cantidad de hosts en cada división debe permitir el crecimiento de la cantidad de hosts.

Determine la cantidad total de hosts

Primero, considere la cantidad total de hosts que necesita toda la internetwork corporativa.

Se debe utilizar un bloque de direcciones lo suficientemente grande para admitir todos los dispositivos en todas las redes corporativas. Entre estos dispositivos se incluyen los dispositivos para usuarios finales, los servidores, los dispositivos intermediarios y las interfaces del router.

Considere el ejemplo de una internetwork corporativa que debe admitir un total de 123 hosts en sus cinco ubicaciones (consulte la figura 1). En este ejemplo, el proveedor de servicios asignó la dirección de red 172.20.0.0/21 (11 bits de host). Como se muestra en la figura 2, esto proporcionará 2046 direcciones de host, lo cual es más que suficiente para admitir las necesidades de direccionamiento de esta internetwork.



Capítulo 9: División de redes IP en subredes 9.1.4.4 División en subredes para cumplir con los requisitos de la red (cont.)

Determine la cantidad y el tamaño de las redes

A continuación, considere la cantidad de subredes que se requieren y la cantidad de direcciones de host que se necesitan en cada subred. Según la topología de la red que consta de 5 segmentos LAN y 4 conexiones de internetwork entre los routers, se requieren 9 subredes. La subred más grande requiere 40 hosts. Al diseñar un esquema de direccionamiento, debe prever el crecimiento en términos de cantidad de subredes y cantidad de hosts por subred.

La dirección de red 172.16.0.0/22 tiene 10 bits de host. Debido a que la subred más grande requiere 40 hosts, se debe tomar prestado un mínimo de 6 bits de host para proporcionar el direccionamiento de los 40 hosts. Esto se determina mediante la siguiente fórmula: 2^6 – 2 = 62 hosts.

Los primeros 4 bits de host pueden utilizarse para asignar subredes. Mediante la fórmula para determinar subredes, esto da como resultado 16 subredes: 2^4 = 16. Dado que la internetwork que se utilizó como ejemplo requiere 9 subredes, esto cumple con el requisito y permite cierto crecimiento adicional.

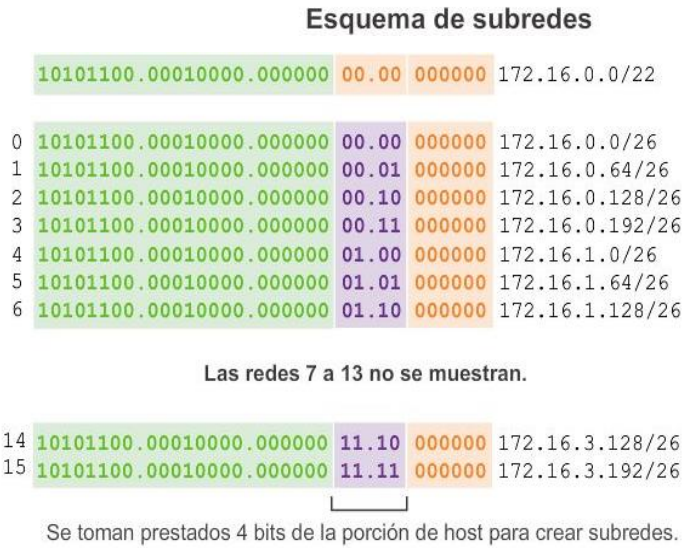
Cuando se toman prestados 4 bits, la nueva duración de prefijo es /26, con la máscara de subred 255.255.255.192.

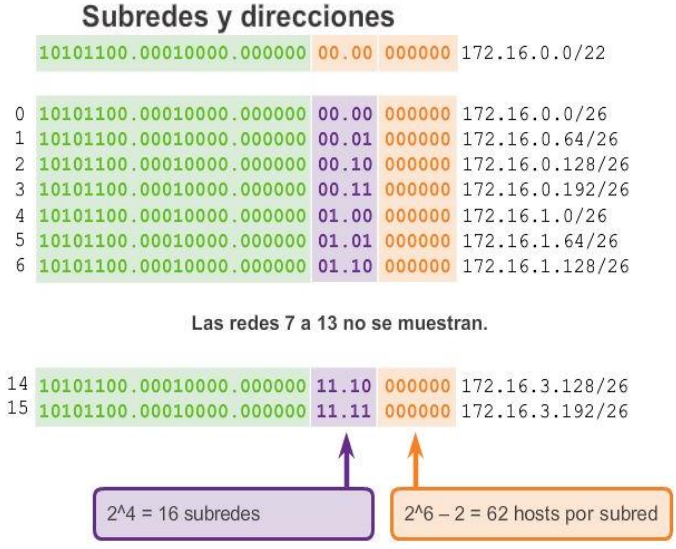
Como se muestra en la figura 1, mediante la duración de prefijo /26, se pueden determinar las 16 direcciones de subred. Solo aumenta la porción de subred de la dirección. Los 22 bits originales de la dirección de red no pueden cambiar, y la porción de host contendrá todos bits 0.

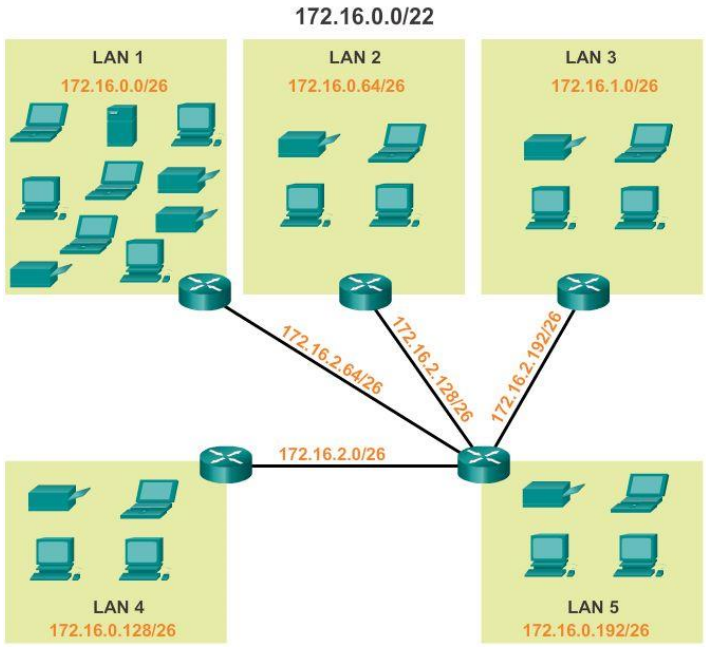
Nota: tenga en cuenta que, dado que la porción de subred está en el tercero y el cuarto octeto, uno o ambos de estos valores variarán en las direcciones de subred.

Como se muestra en la figura 2, la red 172.16.0.0/22 original era una única red con 10 bits de host que proporcionaban 1022 direcciones utilizables para asignar a los hosts. Al tomar prestados 4 bits de host, se pueden crear 16 subredes (0000 hasta 1111). Cada subred tiene 6 bits de host o 62 direcciones de host utilizables.

Como se muestra en la figura 3, las subredes se pueden asignar a los segmentos LAN y a conexiones de router a router.







Capítulo 9: División de redes IP en subredes 9.1.5.1 Desperdicio de direcciones de la división en subredes tradicional

Mediante la división en subredes tradicional, 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 eficaces. Sin embargo, esto no es lo que suele suceder.

Por ejemplo, la topología que se muestra en la figura 1 requiere siete subredes, una para cada una de las cuatro LAN y una para cada una de las tres conexiones WAN entre los routers. Si se utiliza la división en subredes tradicional con la dirección dada 192.168.20.0/24, se pueden tomar prestados 3 bits de la porción de host en el último octeto para cumplir el requisito de siete subredes. Como se muestra en la figura 2, si se toman prestados 3 bits, se crean 8 subredes y quedan 5 bits de host con 30 hosts utilizables por subred. Mediante este esquema, se crean las subredes necesarias y se cumplen los requisitos de host de la LAN más grande.

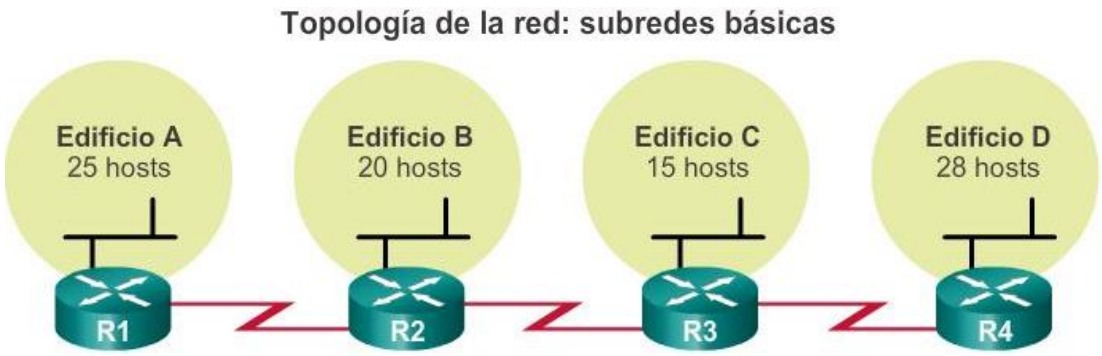
Si bien la división en subredes tradicional satisface las necesidades de la LAN más grande y divide el espacio de direcciones en una cantidad adecuada de subredes, da como resultado un desperdicio significativo de direcciones sin utilizar.

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 (28x3).

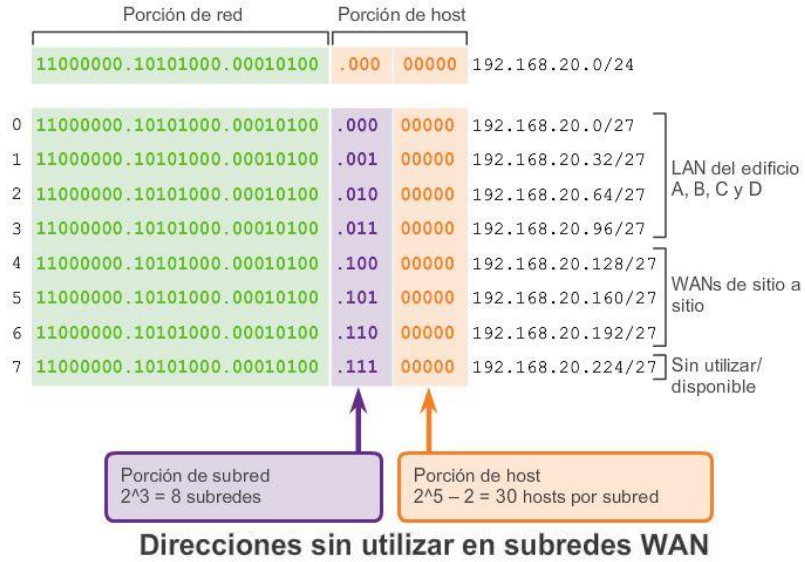
Además, de esta forma se limita el crecimiento futuro al reducir el número total de subredes disponibles. Este uso ineficiente de las direcciones es característico de la división en subredes tradicional de redes con clase.

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 buen modelo para mostrar cómo puede utilizarse la subdivisión de subredes para maximizar el uso de la dirección.

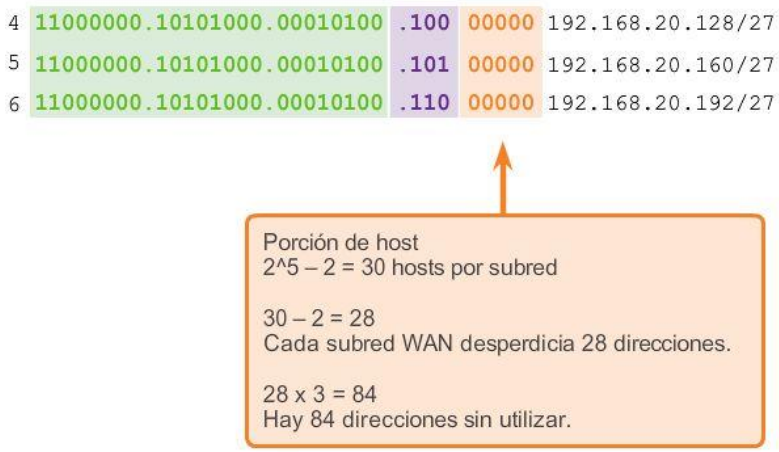
La subdivisión de subredes, o el uso de una máscara de subred de longitud variable (VLSM), se diseñó para evitar que se desperdicien direcciones.



Esquema de subredes básico



Direcciones sin utilizar en subredes WAN



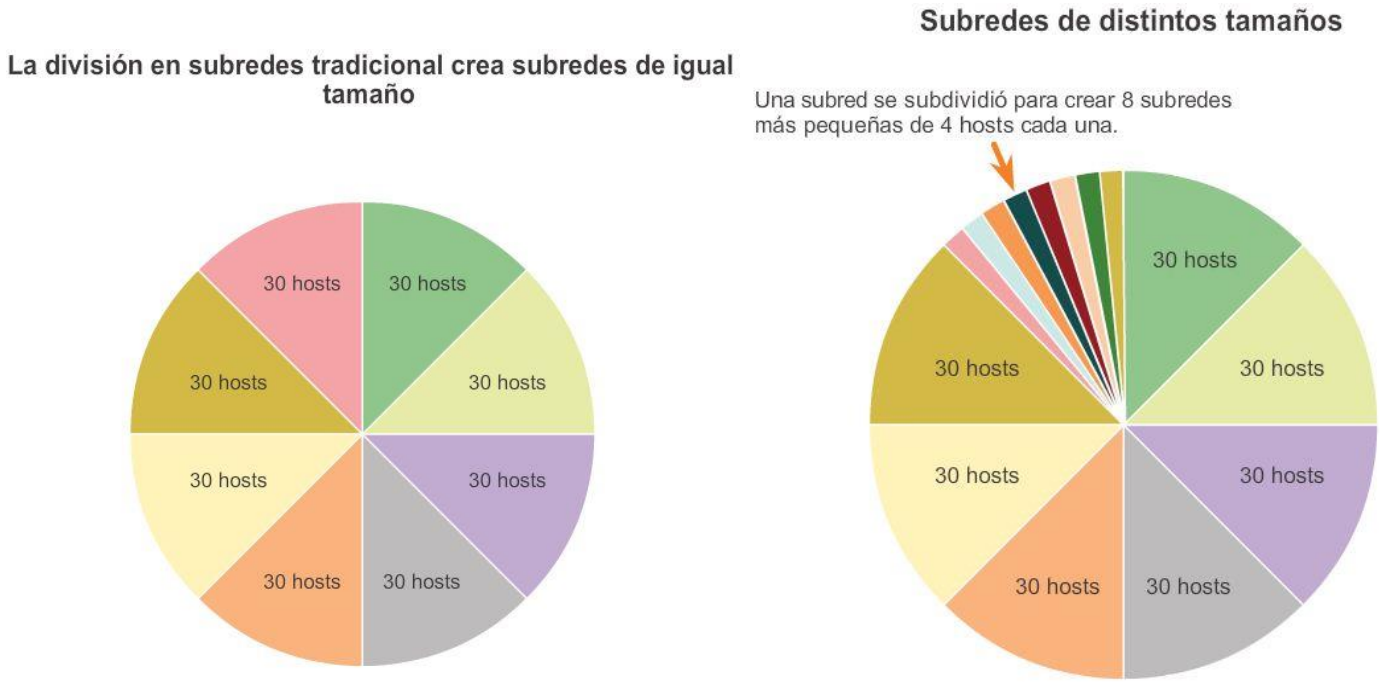
Capítulo 9: División de redes IP en subredes 9.1.5.2 Máscaras de subred de longitud variable (VLSM)

Observe que, en todos los ejemplos de división en subredes anteriores, se aplicó 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. Como se muestra en la figura 2, VLSM permite dividir un espacio de red en partes desiguales. Con VLSM, 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 VLSM.

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.



Capítulo 9: División de redes IP en subredes 9.1.5.3 VLSM básico

Para comprender mejor el proceso de VLSM, vuelva al ejemplo anterior.

En el ejemplo anterior, que se muestra en la figura 1, la red 192.168.20.0/24 se dividió en ocho subredes de igual tamaño, de las cuales se asignaron siete. Cuatro subredes se utilizaron para las LAN, y tres subredes se utilizaron para las conexiones WAN entre los routers.

Recuerde que el espacio de direcciones desperdiciado estaba en las subredes utilizadas para las conexiones WAN, dado que esas subredes requerían solo dos direcciones utilizables: una para cada interfaz del router. Para evitar este desperdicio, se puede utilizar VLSM para crear subredes más pequeñas para las conexiones WAN.

Para crear subredes más pequeñas para los enlaces WAN, se divide una de las subredes. En la figura 2, la última subred, 192.168.20.224/27, se vuelve a dividir en subredes.

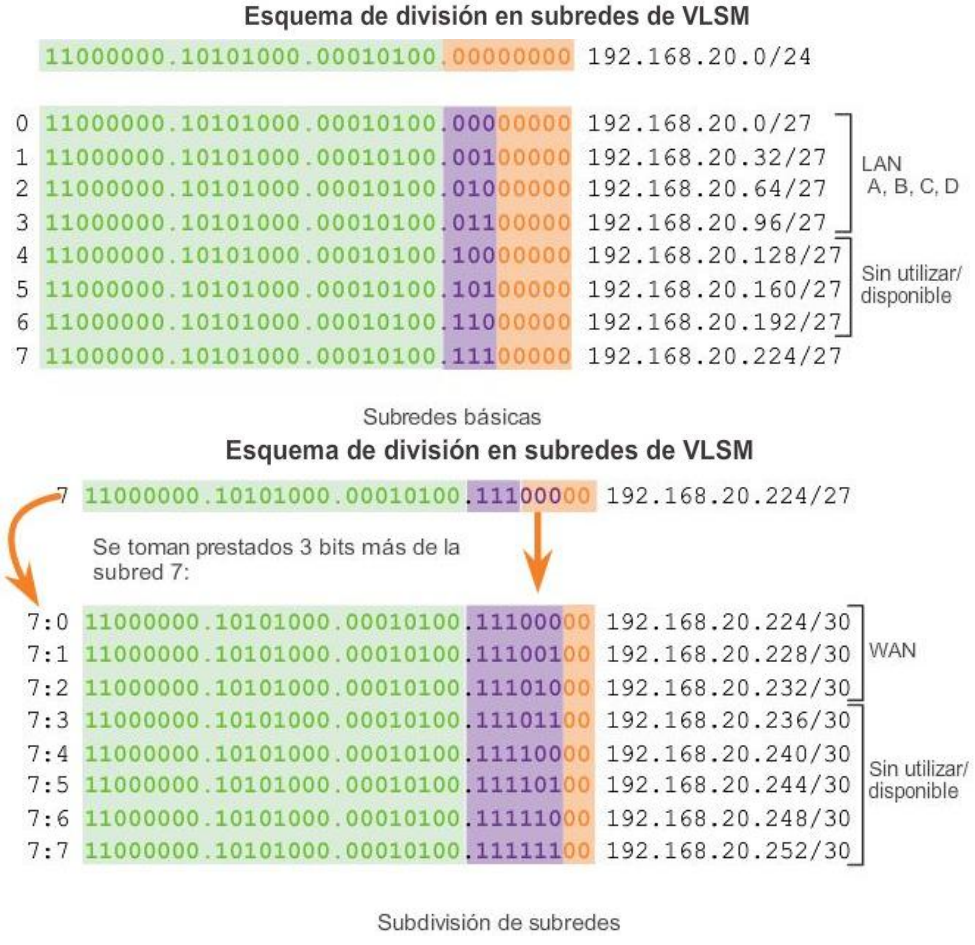
Recuerde que cuando se conoce la cantidad de direcciones de host necesarias, puede utilizarse la fórmula 2^n-2 (donde “n” es igual a la cantidad de bits de host restantes). Para proporcionar dos direcciones utilizables, se deben dejar 2 bits de host en la porción de host.

2^2 - 2 = 2

Debido a que hay 5 bits de host en el espacio de direcciones 192.168.20.224/27, se pueden tomar prestados 3 bits y dejar 2 bits en la porción de host.

Los cálculos que se realizan llegado este punto son exactamente los mismos que se utilizan para la división en subredes tradicional: se toman prestados los bits y se determinan los rangos de subred.

Como se muestra en la figura 2, este esquema de división en subredes VLSM reduce el número de direcciones por subred a un tamaño apropiado para las WAN. La subdivisión de la subred 7 para las WAN permite que las subredes 4, 5, y 6 estén disponibles para redes futuras y que haya varias subredes más disponibles para las WAN.



Capítulo 9: División de redes IP en subredes 9.1.5.4 VLSM en la práctica

Si se utilizan subredes VLSM, se pueden direccionar los segmentos LAN y WAN sin desperdicios innecesarios.

A los hosts en cada una de las LAN se les asignan una dirección de host con el rango para esa subred y una máscara /27 válidas. Cada uno de los cuatro routers tendrá una interfaz LAN con una subred /27 y una o más interfaces seriales con una subred /30.

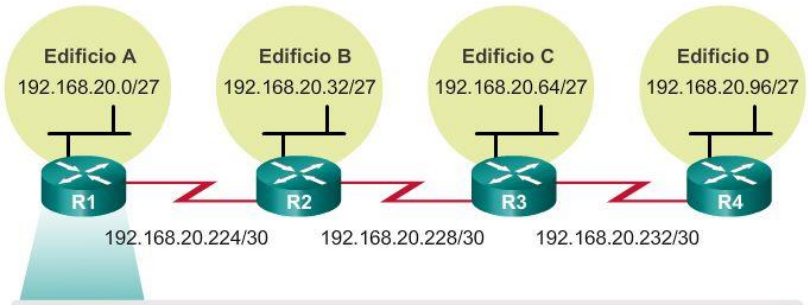
Mediante un esquema de direccionamiento común, la primera dirección IPv4 de host para cada subred se asigna a la interfaz LAN del router. A las interfaces WAN de los routers se les asignan las direcciones IP y la máscara para las subredes /30.

En las figuras 1 a 4, se muestra la configuración de interfaz para cada uno de los routers.

Los hosts en cada subred tendrán una dirección IPv4 de host del rango de direcciones de host para esa subred y una máscara adecuada. Los hosts utilizarán la dirección de la interfaz LAN del router conectada como dirección de gateway predeterminado.

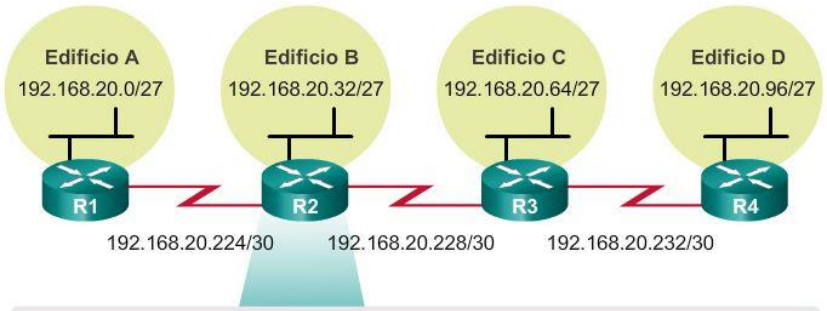
- Los hosts del edificio A (192.168.20.0/27) utilizarán la dirección del router 192.168.20.1 como dirección de gateway predeterminado.
- Los hosts del edificio B (192.168.20.32/27) utilizarán la dirección del router 192.168.20.33 como dirección de gateway predeterminado.
- Los hosts del edificio C (192.168.20.64/27) utilizarán la dirección del router 192.168.20.65 como dirección de gateway predeterminado.
- Los hosts del edificio D (192.168.20.96/27) utilizarán la dirección del router 192.168.20.97 como dirección de gateway predeterminado.

Topología de la red: subredes VLSM



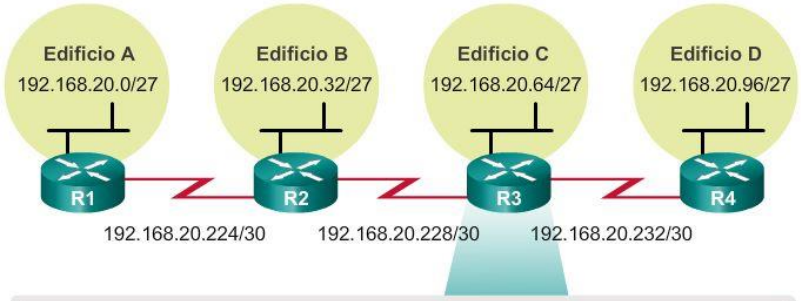

```
R1(config)#interface gigabitethernet 0/0
R1(config-if)#ip address 192.168.20.1 255.255.255.224
R1(config-if)#exit
R1(config)#interface serial 0/0/0
R1(config-if)#ip address 192.168.20.225 255.255.255.252
R1(config-if)#end
R1#
```

Topología de la red: subredes VLSM

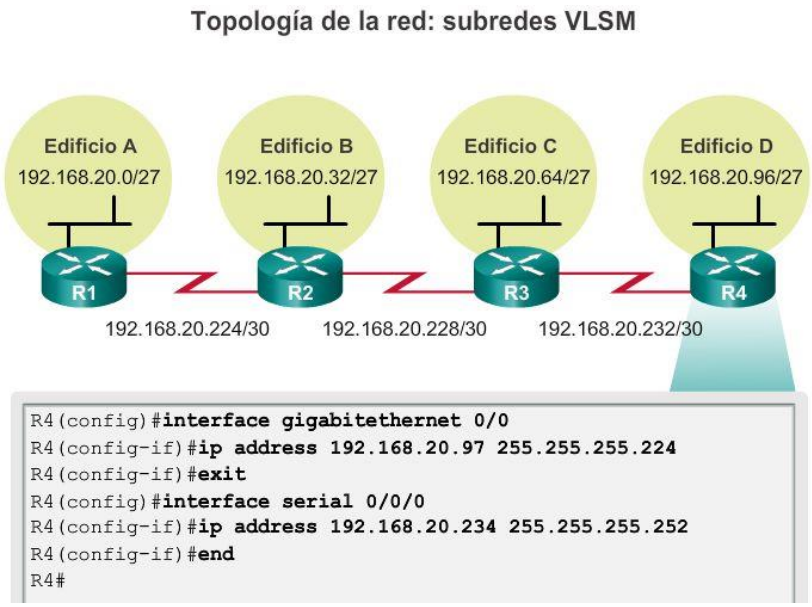



```
R2(config)#interface gigabitethernet 0/0
R2(config-if)#ip address 192.168.20.33 255.255.255.224
R2(config-if)#exit
R2(config)#interface serial 0/0/0
R2(config-if)#ip address 192.168.20.226 255.255.255.252
R2(config-if)#exit
R2(config)#interface serial 0/0/1
R2(config)#ip address 192.168.20.229 255.255.255.252
R2(config-if)#end
R2#
```

Topología de la red: subredes VLSM




```
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#
```



Capítulo 9: División de redes IP en subredes 9.1.5.5 Cuadro de VLSM

También se puede realizar la planificación de direcciones utilizando diversas herramientas. Un método es utilizar un cuadro de VLSM para identificar los bloques de direcciones disponibles para su uso y los que ya están asignados. Este método ayuda a evitar la asignación de direcciones que ya han sido asignadas. Con la red del ejemplo anterior, se puede utilizar el cuadro de VLSM para planificar la asignación de direcciones.

Análisis de las subredes /27

Como se muestra en la figura 1, al utilizar la división en subredes tradicional, los primeros siete bloques de direcciones se asignaron a las LAN y WAN. Recuerde que este esquema dio como resultado 8 subredes con 30 direcciones utilizables cada una (/27). Si bien este esquema funcionó para los segmentos LAN, se desperdiciaron muchas direcciones en los segmentos WAN.

Al diseñar el 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.

Asignación de bloques de direcciones VLSM

Como se muestra en la figura 2, 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 volvió a dividir en subredes para crear subredes /30. Las primeras 3 subredes se asignaron a enlaces WAN.

- .224 /30, rango de direcciones de host 225 a 226: enlace WAN entre R1 y R2
- .228 /30, rango de direcciones de host 229 a 230: enlace WAN entre R2 y R3
- .232 /30, rango de direcciones de host 233 a 234: enlace WAN entre R3 y R4
- .236 /30, rango de direcciones de host 237 a 238: disponible para utilizar
- .240 /30, rango de direcciones de host 241 a 242: disponible para utilizar
- .244 /30, rango de direcciones de host 245 a 246: disponible para utilizar
- .248 /30, rango de direcciones de host 249 a 250: disponible para utilizar
- .252 /30, rango de direcciones de host 253 a 254: disponible para utilizar

Si se diseña el esquema de direccionamiento de esta manera, quedan 3 subredes /27 y 5 subredes /30 sin utilizar.

División básica en subredes de 192.168.20.0/24

	Red/27	Hosts
Edificio A	.0	.1-.30
Edificio B	.32	.33-.62
Edificio C	.64	.65-.94
EdificioD	.96	.97-.126
WAN R1 – R2	.128	.129-.158
WAN R2 – R3	.160	.161-.190
WAN R3 – R4	.192	.193-.222
Sin utilizar	.224	.225-.254

División en subredes VLSM de 192.168.20.0/24

	Red/27	Hosts
Edificio A	.0	.1-.30
Edificio B	.32	.33-.62
Edificio C	.64	.65-.94
Edificio D	.96	.97-.126
Sin utilizar	.128	.129-.158
Sin utilizar	.160	.161-.190
Sin utilizar	.192	.193-.222
	.224	.225-.254

	Red /30	Hosts
WAN R1–R2	.224	.225 - .226
WAN R2–R3	.228	.229 - .230
WAN R3–R4	.232	.233 - .234
Sin utilizar	.236	.237 - .238
Sin utilizar	.240	.241 - .242
Sin utilizar	.244	.245 - .246
Sin utilizar	.248	.249 - .250
Sin utilizar	.252	.253 - .254

Capítulo 9: División de redes IP en subredes 9.2.1.1 Planificación del direccionamiento de la red

Como se muestra en la ilustración, es necesario que la asignación del espacio de direcciones de la capa de red dentro de la red corporativa esté bien diseñada. La asignación de direcciones no debe ser aleatoria. Al planificar la asignación de direcciones, se deben tener en cuenta tres aspectos principales:

- Evitar la duplicación de direcciones: cada host en una internetwork debe tener una dirección única. Sin la planificación y el registro adecuados, se podría asignar una dirección a más de un host, lo que ocasiona problemas de acceso para ambos hosts.

- Proporcionar y controlar el acceso: algunos hosts, como los servidores, proporcionan recursos tanto a hosts internos como a hosts externos. La dirección de capa 3 asignada a un servidor puede utilizarse

para controlar el acceso a ese servidor. Sin embargo, si la dirección se asigna de manera aleatoria y no está bien registrada, es más difícil controlar el acceso.

- Controlar la seguridad y el rendimiento: de manera similar, se deben controlar la seguridad y el rendimiento de los hosts de la red y de la red en su totalidad. Como parte del proceso de control, se examina el tráfico de la red para detectar direcciones que generan o reciben demasiados paquetes. Si se planifica y registra de forma correcta el direccionamiento de la red, es posible encontrar fácilmente los dispositivos de red problemáticos.

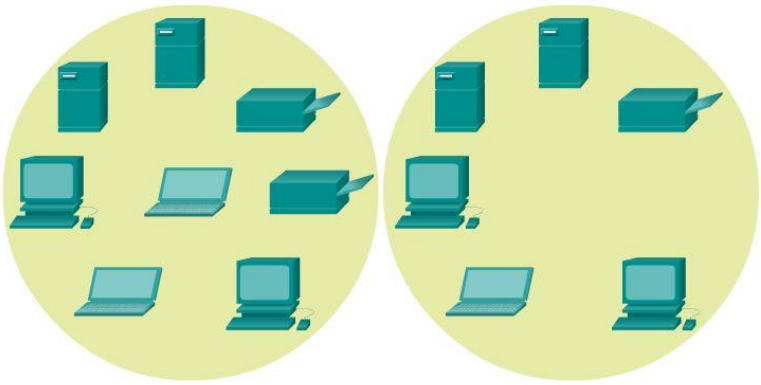
Asignación de direcciones dentro de una red

Dentro de una red, existen distintos tipos de dispositivos, incluidos los siguientes:

- Clientes de usuarios finales
- Servidores y periféricos
- Hosts a los que se accede desde Internet
- Dispositivos intermediarios
- Gateway

Al desarrollar un esquema de direccionamiento IP, por lo general se recomienda tener un patrón establecido de la forma en que se asignan las direcciones a cada tipo de dispositivo. Esto beneficia a los administradores cuando agregan y quitan dispositivos, ya que filtra el tráfico basado en IP y también simplifica el registro.

Planificación y asignación de direcciones IPv4



El direccionamiento de red debe basarse en la segmentación de red.

Capítulo 9: División de redes IP en subredes 9.2.1.2 Asignación de direcciones a dispositivos

Un plan de direccionamiento de red puede incluir el uso de un rango de direcciones distinto dentro de cada subred, para cada tipo de dispositivo.

Direcciones para clientes

Debido a los desafíos asociados con la administración de direcciones estáticas, los dispositivos para usuarios finales a menudo poseen direcciones asignadas en forma dinámica mediante el protocolo de configuración dinámica de host (DHCP). DHCP es generalmente el método preferido para asignar direcciones IP a los hosts

de grandes redes, dado que reduce la carga para al personal de soporte de la red y prácticamente elimina los errores de entrada.

Otro de los beneficios del DHCP es que las direcciones no se asignan permanentemente a un host, sino que son arrendadas durante un período. Si necesitamos cambiar el esquema de división en subredes de nuestra red, no es necesario volver a asignar estáticamente las direcciones de host individuales. Con DHCP, solo debemos volver a configurar el servidor de DHCP con la nueva información de subred. Después de realizar esto, los hosts solo deben renovar automáticamente las direcciones IP.

Direcciones para servidores y periféricos

Cualquier recurso de red, como un servidor o una impresora, debe tener una dirección IP estática, como se muestra en la ilustración. Los hosts clientes acceden a estos recursos utilizando las direcciones IP de estos dispositivos. Por lo tanto, se necesitan direcciones predecibles para cada uno de estos servidores y periféricos.

Los servidores y periféricos son un punto de concentración para el tráfico de red. Se envían muchos paquetes desde las direcciones IPv4 de estos dispositivos y hacia éstas. Al monitorear el tráfico de red con una herramienta como Wireshark, un administrador de red debe poder identificar rápidamente estos dispositivos. Utilizar un sistema de numeración consistente para estos dispositivos facilita la identificación.

Direcciones para hosts accesibles desde Internet

En la mayoría de las internetworks, los hosts fuera de la empresa pueden acceder sólo a unos pocos dispositivos. En la mayoría de los casos, estos dispositivos son normalmente algún tipo de servidor. Al igual que todos los dispositivos en una red que proporciona recursos de red, las direcciones IP para estos dispositivos deben ser estáticas.

En el caso de los servidores a los que se puede acceder desde Internet, cada uno debe tener una dirección de espacio público asociada. Además, las variaciones en la dirección de uno de estos dispositivos hará que no se pueda acceder a éste desde Internet. En muchos casos, estos dispositivos se encuentran en una red numerada mediante direcciones privadas. Esto significa que el router o el firewall del perímetro de la red debe estar configurado para traducir la dirección interna del servidor en una dirección pública. Debido a esta configuración adicional del dispositivo que actúa como intermediario del perímetro, resulta aun más importante que estos dispositivos tengan una dirección predecible.

Direcciones para dispositivos intermediarios

Los dispositivos intermediarios también son un punto de concentración para el tráfico de la red. Casi todo el tráfico dentro redes o entre ellas pasa por alguna forma de dispositivo intermediario. Por lo tanto, estos dispositivos de red ofrecen una ubicación oportuna para la administración, el monitoreo y la seguridad de red.

A la mayoría de los dispositivos intermediarios se les asignan direcciones de capa 3, ya sea para la administración del dispositivo o para su funcionamiento. Los dispositivos como hubs, switches y puntos de acceso inalámbrico no requieren direcciones IPv4 para funcionar como dispositivos intermediarios. Sin embargo, si es necesario acceder a estos dispositivos como hosts para configurar o controlar la red, o resolver problemas de funcionamiento de esta, estos dispositivos deben tener direcciones asignadas.

Debido a que es necesario saber cómo comunicarse con dispositivos intermediarios, estos deben tener direcciones predecibles. Por lo tanto, típicamente, las direcciones se asignan manualmente. Además, las

direcciones de estos dispositivos deben estar en un rango diferente dentro del bloque de red que las direcciones de dispositivos de usuario.

Dirección para el gateway (routers y firewalls)

A diferencia de otros dispositivos intermediarios mencionados, se asigna a los dispositivos de router y firewall un dirección IP para cada interfaz. Cada interfaz se encuentra en una red diferente y funciona como gateway para los hosts de esa red. Normalmente, la interfaz del router utiliza la dirección más baja o más alta de la red. Esta asignación debe ser uniforme en todas las redes de la empresa, de manera que el personal de red siempre conozca la gateway de la red, independientemente de cuál sea la red en la que están trabajando.

Las interfaces de router y firewall son el punto de concentración del tráfico que entra y sale de la red. Debido a que los hosts de cada red usan una interfaz de dispositivo router o firewall como gateway para salir de la red, existe un flujo abundante de paquetes en estas interfaces. Por lo tanto, estos dispositivos pueden cumplir una función importante en la seguridad de red al filtrar los paquetes según las direcciones IP de origen y destino. Agrupar los diferentes tipos de dispositivos en grupos de direccionamiento lógicos hace que la asignación y el funcionamiento del filtrado de paquetes sea más eficiente.

Rangos de direcciones IP

Red: 192.168.1.0/24

Uso	Primero	Última
Dispositivos host	.1	.229
Servidores	.230	.239
Impresoras	.240	.249
Dispositivos intermediarios	.250	.253
Gateway (interfaz LAN del router)	.254	

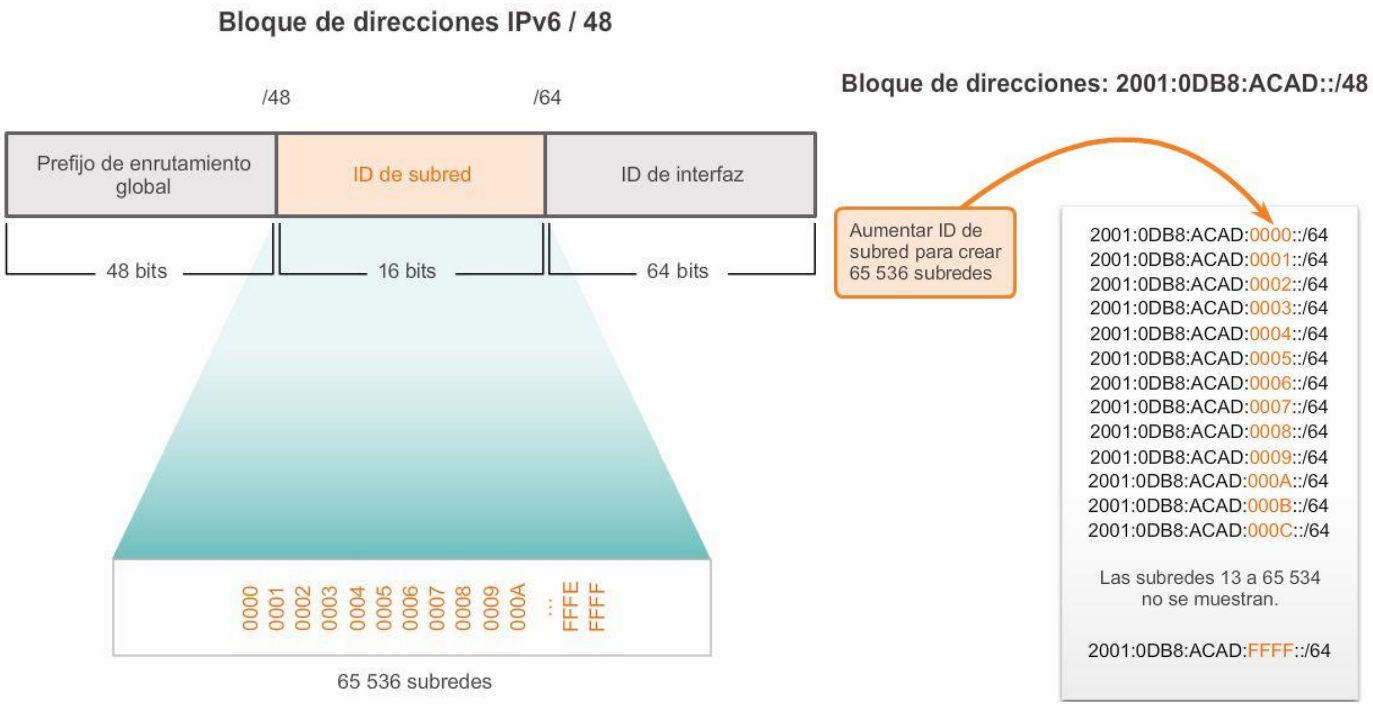
Capítulo 9: División de redes IP en subredes 9.3.1.1 División en subredes mediante la ID de subred

La división en subredes IPv6 requiere un enfoque diferente que la división en subredes IPv4. El motivo principal es que con IPv6 hay tantas direcciones que la división en subredes se realiza por razones completamente distintas. Los espacios de direcciones IPv6 no se dividen en subredes para conservar direcciones, sino para admitir el diseño lógico jerárquico de la red. Mientras que la división en subredes IPv4 tiene que ver con administrar la escasez de direcciones, la división en subredes IPv6 se relaciona con armar una jerarquía de direccionamiento basada en la cantidad de routers y las redes que estos admiten.

Recuerde que un bloque de direcciones IPv6 con el prefijo /48 tiene 16 bits para la ID de subred, como se muestra en la figura 1. La división en subredes mediante la ID de subred de 16 bits produce un total de 65 536 subredes /64 posible y no requiere tomar prestados bits de la ID de interfaz ni de la porción de host de la dirección. Cada subred /64 IPv6 contiene alrededor de 18 trillones de direcciones, obviamente más de lo que jamás se necesitará en un segmento de red IP.

Las subredes creadas a partir de la ID de subred son fáciles de representar, ya que no es necesaria la conversión al sistema binario. Para determinar la siguiente subred disponible, simplemente sume valores hexadecimales. Como se muestra en la figura 2, esto significa aumentar el valor hexadecimal en la porción de ID de subred.

El prefijo de enrutamiento global es igual para todas las subredes. Solo se incrementa el cuarteto de la ID de subred para cada subred.



Capítulo 9: División de redes IP en subredes 9.3.1.2 Asignación de subred IPv6

Con la posibilidad de elegir entre más de 65 000 subredes, la tarea del administrador de red se convierte en una tarea de diseño de un esquema lógico para direccionar la red.

Como se muestra en la figura 1, la topología que se utiliza de ejemplo requerirá subredes para cada LAN así como para el enlace WAN entre el R1 y el R2. A diferencia del ejemplo para IPv4, con IPv6 la subred del enlace WAN no se vuelve a dividir en subredes. Aunque esto puede provocar el “desperdicio” de direcciones, eso no constituye un motivo de preocupación al utilizar IPv6.

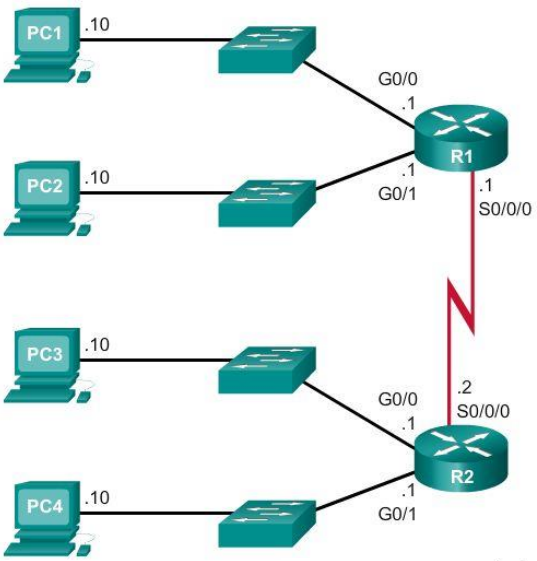
Como se muestra en la figura 2, en este ejemplo se utilizará la asignación de 5 subredes IPv6, con el campo de ID de subred 0001 a 0005. Cada subred /64 proporcionará más direcciones de las que jamás se necesitarán.

Como se muestra en la figura 3, se asigna una subred /64 a cada segmento LAN y al enlace WAN.

De manera similar a la configuración de IPv4, en la figura 4 se muestra que cada una de las interfaces del router se configuró para estar en una subred IPv6 distinta.

División en subredes IPv6

Topología de ejemplo

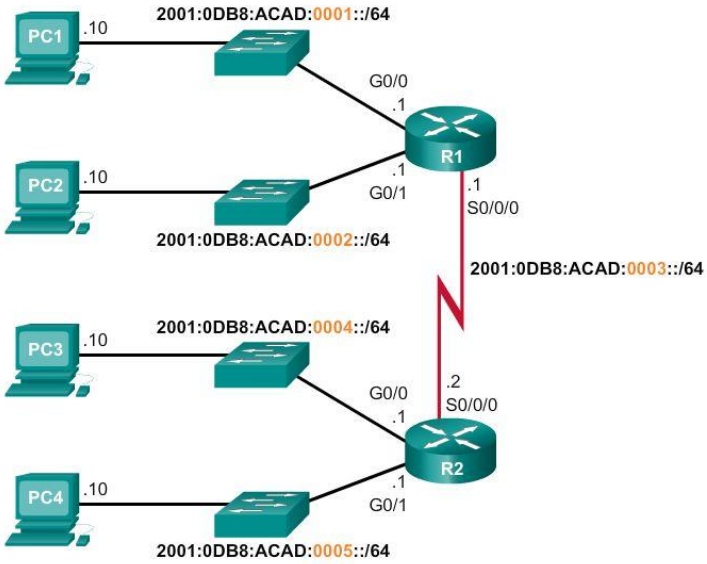


Bloque de direcciones: 2001:0DB8:ACAD::/48

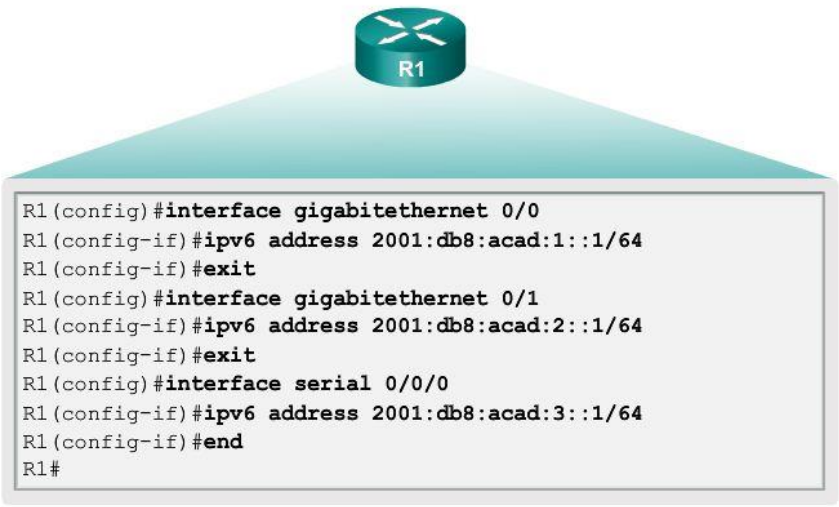
Cinco subredes asignadas de 65 536 subredes disponibles

```
2001:0DB8:ACAD:0000::/64
2001:0DB8:ACAD:0001::/64
2001:0DB8:ACAD:0002::/64
2001:0DB8:ACAD:0003::/64
2001:0DB8:ACAD:0004::/64
2001:0DB8:ACAD:0005::/64
2001:0DB8:ACAD:0006::/64
2001:0DB8:ACAD:0007::/64
2001:0DB8:ACAD:0008::/64
                :
2001:0DB8:ACAD:FFFF::/64
```

Asignación de subred IPv6



Configuración de direcciones IPv6



Capítulo 9: División de redes IP en subredes 9.3.1.3 División en subredes en la ID de interfaz

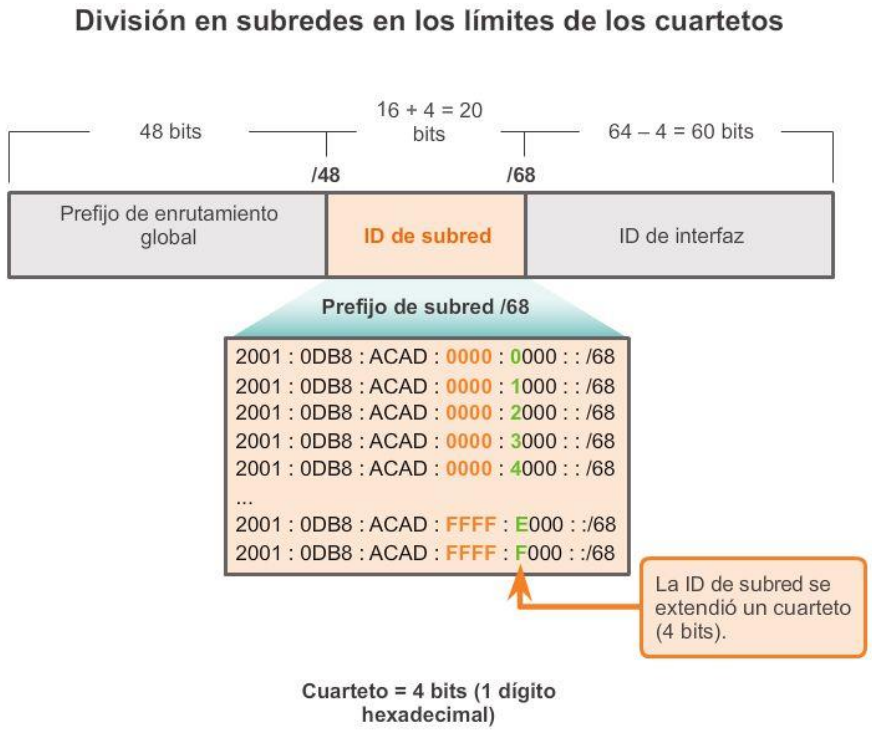
De manera similar a cuando se toman bits prestados de la porción de host de una dirección IPv4, con IPv6 se pueden tomar prestados bits de la ID de interfaz para crear subredes IPv6 adicionales. Por lo general, esto se realiza por motivos de seguridad para crear menos hosts por subred, y no necesariamente para crear subredes adicionales.

Cuando se extiende la ID de subred al tomar prestados bits de la ID de interfaz, la práctica recomendada es realizar la división en subredes en el límite de un cuarteto. Un cuarteto equivale a 4 bits o un dígito hexadecimal. Como se muestra en la ilustración, el prefijo de subred /64 se extiende 4 bits o 1 cuarteto a /68. Esto reduce el tamaño de la ID de interfaz en 4 bits, es decir, de 64 a 60 bits.

La división en subredes en los límites de los cuartetos significa que solo se utilizan máscaras de subred alineadas en cuartetos. Comenzando en /64, las máscaras de subred alineadas en cuartetos son /68, /72, /76, /80, etcétera.

Mediante la división en subredes en los límites de los cuartetos, se crean subredes utilizando el valor hexadecimal adicional. En el ejemplo, la nueva ID de subred consta de los 5 valores hexadecimales que van desde 00000 hasta FFFFF.

Si bien es posible realizar la división en subredes dentro del límite de un cuarteto —dentro de un dígito hexadecimal—, no se recomienda hacerlo y ni siquiera es necesario. Realizar la división en subredes dentro de un cuarteto elimina la ventaja de determinar fácilmente el prefijo a partir de la ID de interfaz. Por ejemplo, si se utiliza la duración de prefijo /66, los dos primeros bits serían parte de la ID de subred, y el segundo conjunto de dos bits sería parte de la ID de interfaz.



Capítulo 9: División de redes IP en subredes 9.4.1.1 Actividad: ¿Puedes llamarme ahora?

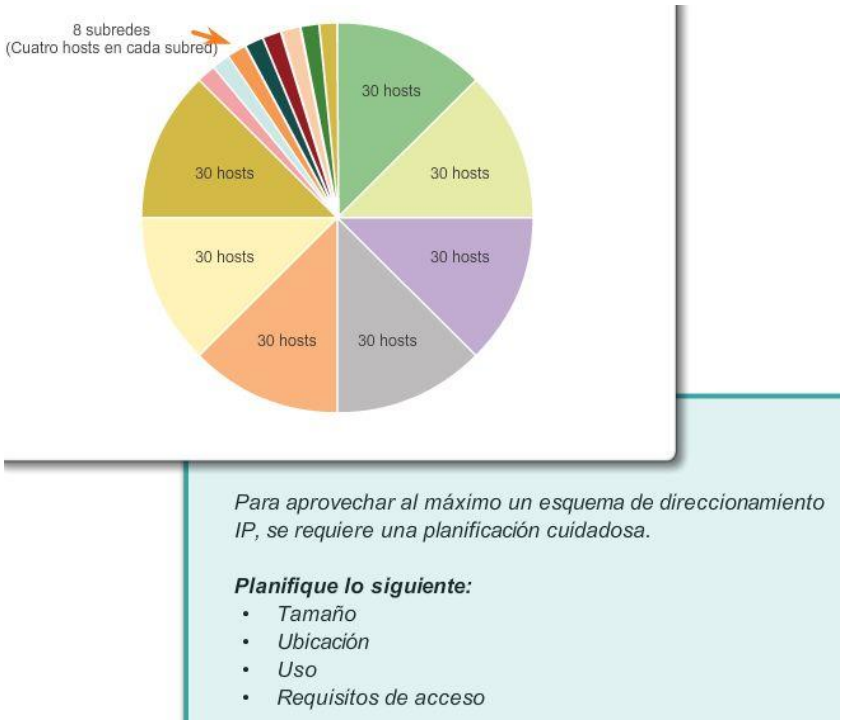
¿Puedes llamarme ahora?

Nota: esta actividad se puede realizar de forma individual o en grupos pequeños o grandes utilizando el software Packet Tracer.

Está configurando un esquema dedicado de direccionamiento de PC para las habitaciones de un hospital. El switch estará ubicado de manera central en la enfermería, ya que cada una de las cinco habitaciones estará conectada por cable de modo que los pacientes simplemente puedan conectarse a un puerto RJ-45 incorporado en la pared de su habitación. Diseñe una topología física y lógica para solo uno de los seis pisos con los siguientes requisitos para el esquema de direccionamiento:

- Hay seis pisos con cinco habitaciones de pacientes en cada piso, lo que da un total de 30 conexiones. Cada habitación necesita una conexión de red.
- Debe incorporarse división en subredes al esquema.
- Utilice un router, un switch y cinco estaciones host para fines de direccionamiento.
- Verifique que todas las PC puedan conectarse a los servicios internos del hospital.

Conserve una copia del esquema para compartirlo más adelante con la clase o la comunidad de aprendizaje. Esté preparado para explicar la forma en que se incorporarían la división en subredes y las transmisiones unicast, multicast y broadcasts, y dónde podría utilizarse su esquema de direccionamiento.



Capítulo 9: División de redes IP en subredes 9.4.1.3 Resumen

Como se muestra en la ilustración, el proceso de segmentación de una red mediante su división en varios espacios de red más pequeños se denomina “división en subredes”.

Cada dirección de red tiene un rango válido de direcciones de host. Todos los dispositivos conectados a la misma red tendrán una dirección de host IPv4 para esa red y una máscara de subred o un prefijo de red común. Es posible reenviar el tráfico entre hosts directamente, siempre que estén en la misma subred. El tráfico no puede reenviarse entre subredes sin un router. Para determinar si el tráfico es local o remoto, el router utiliza la máscara de subred. El prefijo y la máscara de subred son diferentes formas de representar lo mismo, la porción de red de una dirección.

Las subredes IPv4 se crean utilizando uno o más de los bits de host como bits de red. Dos factores muy importantes que conducen a la determinación del bloque de direcciones IP con la máscara de subred son la cantidad de subredes requeridas y la cantidad máxima de hosts necesarios por subred.

Existe una relación inversa entre la cantidad de subredes y la cantidad de hosts: cuantos más bits se toman prestados para crear subredes, menor es la cantidad de bits de host disponibles, lo que tiene como resultado menos hosts por subred.

La fórmula 2^n (donde “n” representa la cantidad de bits de host restantes) se utiliza para calcular cuántas direcciones disponibles habrá en cada subred. Sin embargo, la dirección de red y la dirección de broadcast dentro de un rango no son utilizables, por lo que es necesario realizar el cálculo 2^n-2 para determinar la cantidad utilizable de direcciones.

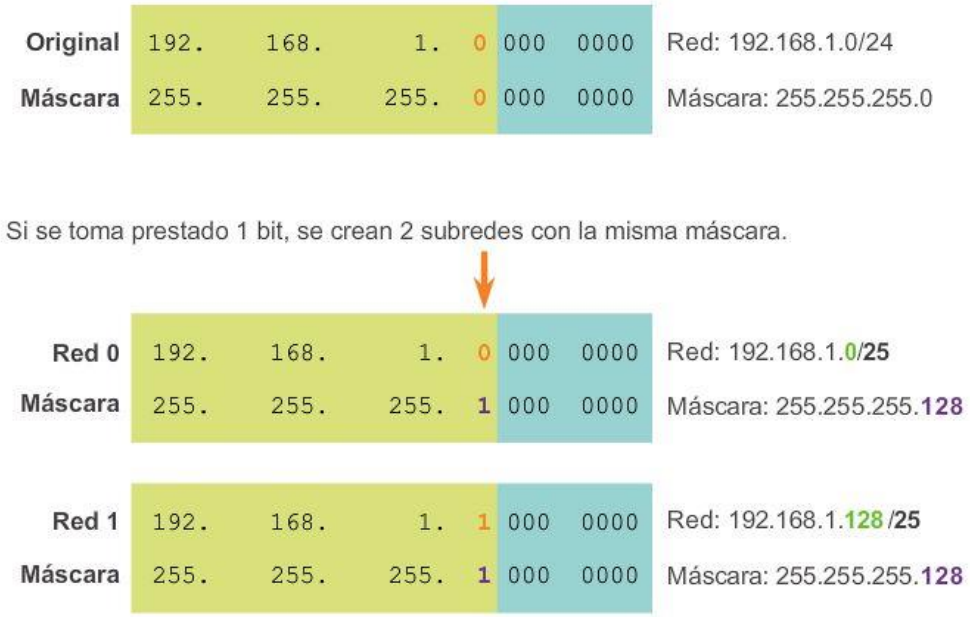
La subdivisión de subredes, o el uso de una máscara de subred de longitud variable (VLSM), se diseñó para evitar que se desperdicien direcciones.

La división en subredes IPv6 requiere un enfoque diferente que la división en subredes IPv4. Los espacios de direcciones IPv6 no se dividen en subredes para conservar direcciones, sino para admitir el diseño lógico jerárquico de la red. Por lo tanto, mientras que la división en subredes IPv4 tiene que ver con administrar la

escasez de direcciones, la división en subredes IPv6 se relaciona con armar una jerarquía de direccionamiento basada en la cantidad de routers y las redes que estos admiten.

Se requiere una planificación cuidadosa para hacer buen uso del espacio de direcciones disponible. Los requisitos de tamaño, ubicación, uso y acceso son consideraciones que se deben tener en cuenta en el proceso de planificación de direcciones.

Una vez implementada, la red IP se debe probar para verificar la conectividad y el rendimiento operativo.



Capítulo 10: Capa de aplicación 10.0.1.1 Introducción

Vivimos la experiencia de Internet a través de la World Wide Web cuando transmitimos videos, jugamos juegos en línea, chateamos con amigos y les enviamos correos electrónicos, y buscamos ofertas en sitios Web. Las aplicaciones, como las que se utilizan para proporcionar los servicios mencionados, brindan la interfaz humana a la red subyacente. Estas aplicaciones nos permiten enviar y recibir datos de forma relativamente fácil. En general, podemos acceder a estas aplicaciones y utilizarlas sin saber cómo funcionan. Sin embargo, para los profesionales de la red, es importante saber cómo una aplicación puede formatear, transmitir e interpretar mensajes que se envían y se reciben a través de la red.

La visualización de los mecanismos que permiten la comunicación a través de la red se hace más fácil si utilizamos el esquema en capas del modelo OSI.

En este capítulo, analizaremos la función de la capa de aplicación y la manera en que las aplicaciones, los servicios y los protocolos que están dentro de la capa de aplicación hacen posible una comunicación sólida a través de las redes de datos.

Al finalizar este capítulo, podrá hacer lo siguiente:

- Explicar la forma en que las funciones de la capa de aplicación, de la capa de sesión y de la capa de presentación operan conjuntamente para proporcionar servicios de red a las aplicaciones de usuario final.
- Describir la forma en que los protocolos de capa de aplicación comunes interactúan con las aplicaciones de usuario final.
- Describir los protocolos de capa de aplicación comunes que proporcionan servicios de Internet a usuarios finales, incluidos los servicios WWW y el correo electrónico, en un nivel elevado.
- Describir los protocolos de capa de aplicación que proporcionan servicios de direccionamiento IP, incluso: DNS y DHCP.
- Describir las características y el funcionamiento de los protocolos de capa de aplicación conocidos que permiten los servicios de intercambio de archivos, entre los que se encuentran FTP, servicios de uso compartido de archivos, protocolo SMB.
- Explicar la forma en que los datos se transfieren a través de la red, desde que se abre una aplicación hasta que se reciben los datos.

Capítulo 10: Capa de aplicación 10.0.1.2 Actividad: Investigación de aplicaciones

Qué sucedería si…

Su empleador decidió instalar teléfonos IP en el lugar de trabajo, lo que provocó que la red se encuentre fuera de servicio hasta la semana próxima.

Sin embargo, usted debe continuar con su trabajo. Tiene correos electrónicos que enviar y cotizaciones que preparar para obtener la aprobación del gerente. Debido a posibles problemas de seguridad, no tiene permitido finalizar el trabajo de la compañía utilizando sistemas informáticos o equipos de computación personales o externos, o equipos y sistemas que se encuentren en otra ubicación.

El instructor puede solicitarle que complete las preguntas de las dos situaciones que se presentan a continuación o que elija una de ellas (A. Correos electrónicos, o B. Cotización para obtener la aprobación del gerente). Responda las preguntas para las situaciones de forma completa. Esté preparado para comentar sus respuestas en clase.

A. Correos electrónicos

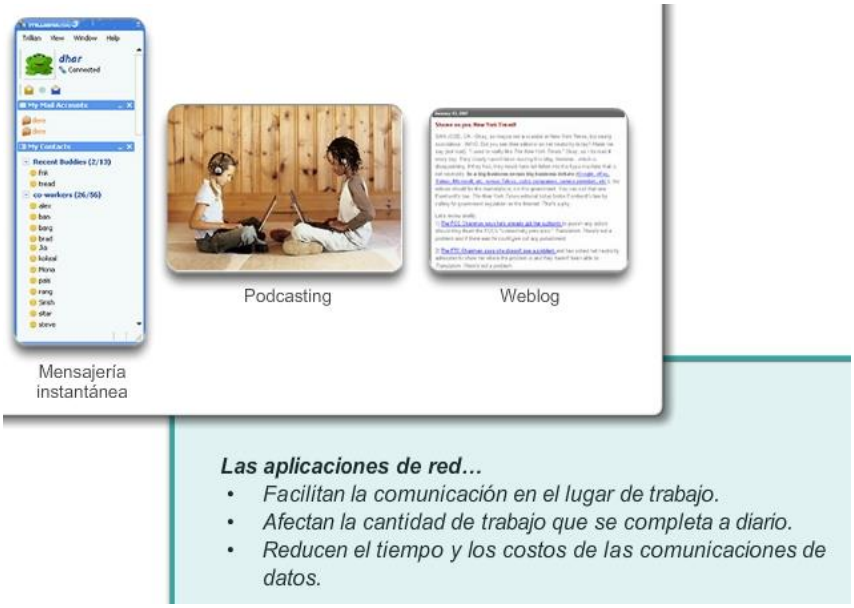
- ¿Qué métodos puede utilizar para enviar comunicaciones por correo electrónico?
- ¿Cómo puede enviar el mismo correo electrónico a varios destinatarios?
- ¿Cómo enviaría un archivo adjunto grande a varios destinatarios, en caso de ser necesario?
- ¿Estos métodos son rentables para la compañía?
- ¿Infringen alguna política de seguridad de la compañía?

B. Cotización para obtener la aprobación del gerente.

- Tiene un paquete de software de aplicaciones de escritorio instalado en su PC. ¿Será relativamente fácil generar la cotización que su gerente necesita para el nuevo contrato, que tiene una fecha límite a finales de la semana? ¿Qué limitaciones experimentará al intentar finalizar la cotización?

- ¿Cómo presentará la cotización al gerente para obtener su aprobación? ¿Cómo cree que el gerente enviará la cotización al cliente para que la apruebe?

- ¿Estos métodos son rentables para la compañía? Justifique su respuesta.



Capítulo 10: Capa de aplicación 10.1.1.1 Modelos OSI y TCP/IP: nuevo análisis

Como se muestra en la ilustración, los profesionales de redes utilizan los modelos OSI y TCP/IP para comunicarse tanto verbalmente como mediante documentación técnica escrita. Como tales, los profesionales de redes pueden utilizar estos modelos para describir el comportamiento de protocolos y aplicaciones.

En el modelo OSI, la información pasa de una capa a otra: de la capa de aplicación en el host de transmisión pasa por la jerarquía hacia la capa física y luego por el canal de comunicaciones hacia el host de destino, donde la información vuelve a la jerarquía y termina en la capa de aplicación.

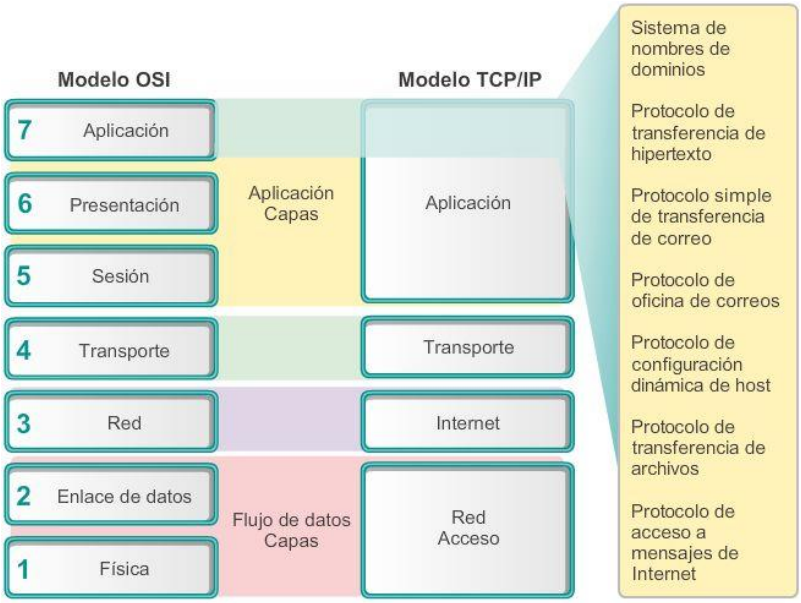
La capa de aplicación es la capa superior de los modelos OSI y TCP/IP. La capa de aplicación de TCP/IP incluye un número de protocolos que proporciona funcionalidad específica a una variedad de aplicaciones de usuario final. La funcionalidad de los protocolos de capa de aplicación de TCP/IP se adapta aproximadamente al esquema de las tres capas superiores del modelo OSI: la de aplicación, la de presentación y la de sesión. Las capas 5, 6 y 7 del modelo OSI se utilizan como referencias para proveedores y desarrolladores de software de aplicación para fabricar productos, como exploradores Web, que necesitan acceder a las redes.

Las semejanzas clave están en la capa de red y en la capa de transporte.

Capítulo 10: Capa de aplicación 10.1.1.2 Capa de aplicación

Capa de aplicación

La capa de aplicación es la más cercana al usuario final. Como se muestra en la ilustración, es la capa que proporciona la interfaz entre las aplicaciones que utilizamos para comunicarnos y la red subyacente en la cual se transmiten los mensajes. Los protocolos de capa de aplicación se utilizan para intercambiar los datos entre los programas que se ejecutan en los hosts de origen y destino. Existen muchos protocolos de capa de aplicación, y están en constante desarrollo. Algunos de los protocolos de capa de aplicación más conocidos incluyen el protocolo de transferencia de hipertexto (HTTP), el protocolo de transferencia de archivos (FTP), el protocolo trivial de transferencia de archivos (TFTP), el protocolo de acceso a mensajes de Internet (IMAP) y el protocolo del Sistema de nombres de dominios (DNS).



Capítulo 10: Capa de aplicación 10.1.1.3 Capas de presentación y sesión

Capa de presentación

La capa de presentación tiene tres funciones principales:

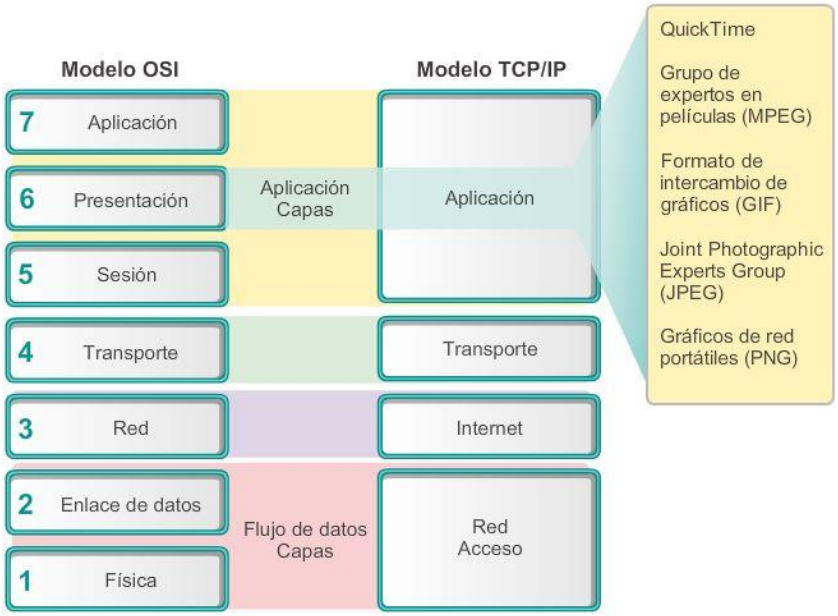
- Dar formato a los datos del dispositivo de origen, o presentarlos, en una forma compatible para que lo reciba el dispositivo de destino.
- Comprimir los datos de forma tal que los pueda descomprimir el dispositivo de destino.
- Encriptar los datos para su transmisión y posterior descifrado al llegar al dispositivo de destino.

Como se muestra en la ilustración, la capa de presentación da formato a los datos para la capa de aplicación y establece estándares para los formatos de archivo. Dentro de los estándares más conocidos para video encontramos QuickTime y el Grupo de expertos en películas (MPEG). QuickTime es una especificación de PC de Apple para audio y video, y MPEG es un estándar para la codificación y compresión de audio y video.

Entre los formatos gráficos de imagen conocidos que se utilizan en redes, se incluyen los siguientes: formato de intercambio de gráficos (GIF), formato del Joint Photographic Experts Group (JPEG) y formato de gráficos de red portátiles (PNG). Los formatos GIF y JPEG son estándares de compresión y codificación de imágenes gráficas. El formato PNG se diseñó para abordar algunas de las limitaciones del formato GIF y para reemplazar este último.

Capa de sesión

Como su nombre lo indica, las funciones de la capa de sesión crean y mantienen diálogos entre las aplicaciones de origen y destino. La capa de sesión maneja el intercambio de información para iniciar los diálogos y mantenerlos activos y para reiniciar sesiones que se interrumpieron o que estuvieron inactivas durante un período prolongado.



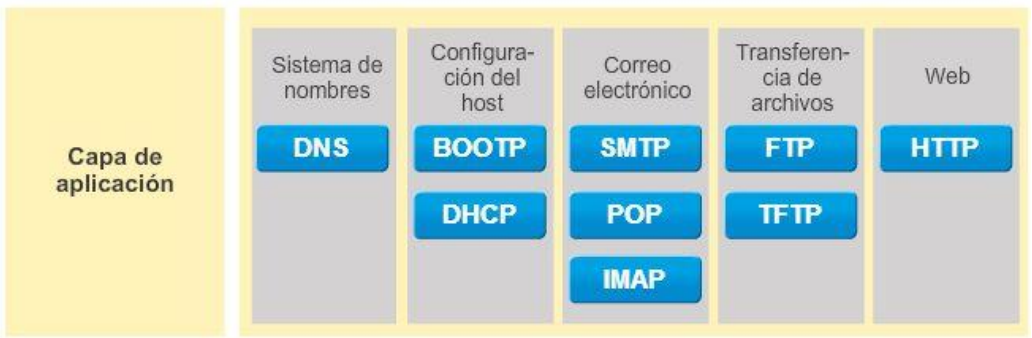
Capítulo 10: Capa de aplicación 10.1.1.4 Protocolos de capa de aplicación de TCP/IP

Si bien el modelo OSI separa las funciones individuales de las capas de aplicación, presentación y sesión, las aplicaciones de TCP/IP más conocidas e implementadas incorporan la funcionalidad de las tres capas.

Los protocolos de aplicación de TCP/IP especifican el formato y la información de control necesarios para muchas funciones de comunicación comunes de Internet. Algunos de los protocolos TCP/IP son:

- Sistema de nombres de dominios (DNS): este protocolo resuelve nombres de Internet en direcciones IP.
- Telnet: se utiliza para proporcionar acceso remoto a servidores y dispositivos de red.
- Protocolo simple de transferencia de correo (SMTP): este protocolo transfiere mensajes y archivos adjuntos de correo electrónico.
- Protocolo de configuración dinámica de host (DHCP): se utiliza para asignar una dirección IP y direcciones de máscara de subred, de gateway predeterminado y de servidor DNS a un host.
- Protocolo de transferencia de hipertexto (HTTP): este protocolo transfiere archivos que conforman las páginas Web de la World Wide Web.
- Protocolo de transferencia de archivos (FTP): se utiliza para la transferencia de archivos interactiva entre sistemas.
- Protocolo trivial de transferencia de archivos (TFTP): se utiliza para la transferencia de archivos activa sin conexión.
- Protocolo bootstrap (BOOTP): este protocolo es un precursor del protocolo DHCP. BOOTP es un protocolo de red que se utiliza para obtener información de la dirección IP durante el arranque.
- Protocolo de oficina de correos (POP): es un protocolo que utilizan los clientes de correo electrónico para recuperar el correo electrónico de un servidor remoto.
- Protocolo de acceso a mensajes de Internet (IMAP): este es otro protocolo que se utiliza para recuperar correo electrónico.

Los protocolos de capa de aplicación son utilizados tanto por los dispositivos de origen como de destino durante una sesión de comunicación. Para que las comunicaciones se lleven a cabo correctamente, los protocolos de capa de aplicación que se implementaron en los hosts de origen y de destino deben ser compatibles.



Capítulo 10: Capa de aplicación 10.1.2.1 Redes punto a punto

Cuando se accede a la información en un dispositivo de red, ya sea una PC, una computadora portátil, una tablet PC, un smartphone o algún otro dispositivo conectado a una red, los datos no se pueden almacenar físicamente en el dispositivo.

En este caso, se debe solicitar permiso al dispositivo que contiene los datos para acceder a esa información.

En el modelo de red punto a punto (P2P), se accede a los datos de un dispositivo punto sin utilizar un servidor dedicado.

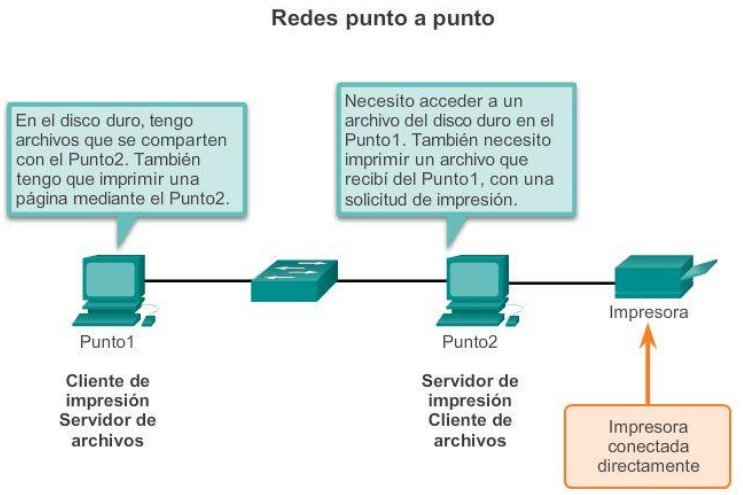
El modelo de red P2P consta de dos partes: las redes P2P y las aplicaciones P2P. Ambas partes tienen características similares, pero en la práctica son muy diferentes.

P2P Networks

En una red P2P, hay dos o más PC que están conectadas por medio de una red y pueden compartir recursos (como impresoras y archivos) sin tener un servidor dedicado. Todo dispositivo final conectado (conocido como “punto”) puede funcionar como servidor y como cliente. Una computadora puede asumir la función de servidor para una transacción mientras funciona en forma simultánea como cliente para otra transacción. Las funciones de cliente y servidor se establecen por solicitud.

Un ejemplo de esto es una red doméstica simple con dos PC, como se muestra en la ilustración. En este ejemplo, el Punto2 tiene una impresora conectada a él directamente por USB y está configurado para compartir la impresora en la red de modo que el Punto1 pueda imprimir con esta. El Punto1 está configurado para compartir una unidad o una carpeta en la red. Esto permite que el Punto2 acceda a los archivos de la carpeta compartida y los guarde. Además de compartir archivos, una red como esta permitiría que los usuarios habiliten juegos en red o compartan una conexión a Internet.

Las redes P2P descentralizan los recursos en una red. En lugar de ubicar datos para compartir en los servidores dedicados, los datos se pueden colocar en cualquier parte y en cualquier dispositivo conectado. La mayoría de los sistemas operativos actuales admiten compartir archivos e impresoras sin requerir software del servidor adicional. Sin embargo, las redes P2P no utilizan cuentas de usuario centralizadas ni acceden a servidores para mantener permisos. Por lo tanto, es difícil aplicar políticas de seguridad y de acceso en redes que contienen varias PC. Se deben establecer cuentas de usuario y derechos de acceso en forma individual para cada dispositivo.



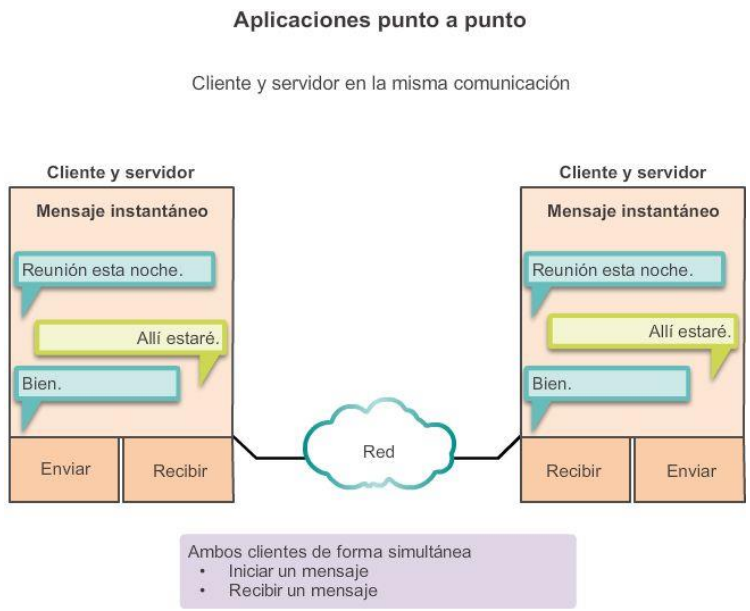
En un intercambio punto a punto, ambos dispositivos se consideran iguales en el proceso de comunicación.

Capítulo 10: Capa de aplicación 10.1.2.2 Aplicaciones punto a punto

Una aplicación punto a punto (P2P) permite que un dispositivo funcione como cliente y como servidor dentro de la misma comunicación, como se muestra en la ilustración. En este modelo, cada cliente es un servidor y cada servidor es un cliente. Ambos pueden iniciar una comunicación y se consideran iguales en el proceso de comunicación. Sin embargo, las aplicaciones P2P requieren que cada dispositivo final proporcione una interfaz de usuario y ejecute un servicio en segundo plano. Cuando inicia una aplicación P2P específica, se cargan los servicios en segundo plano y la interfaz de usuario requeridos; a continuación, los dispositivos se pueden comunicar directamente.

Algunas aplicaciones P2P utilizan un sistema híbrido donde se descentraliza el intercambio de recursos, pero los índices que apuntan a las ubicaciones de los recursos están almacenados en un directorio centralizado. En un sistema híbrido, cada punto accede a un servidor de índice para alcanzar la ubicación de un recurso almacenado en otro punto. El servidor de índice también puede ayudar a conectar dos puntos, pero una vez conectados, la comunicación se lleva a cabo entre los dos puntos sin comunicación adicional con el servidor de índice.

Las aplicaciones P2P se pueden utilizar en redes P2P, en redes cliente/servidor y a través de Internet.



Capítulo 10: Capa de aplicación 10.1.2.3 Aplicaciones P2P comunes

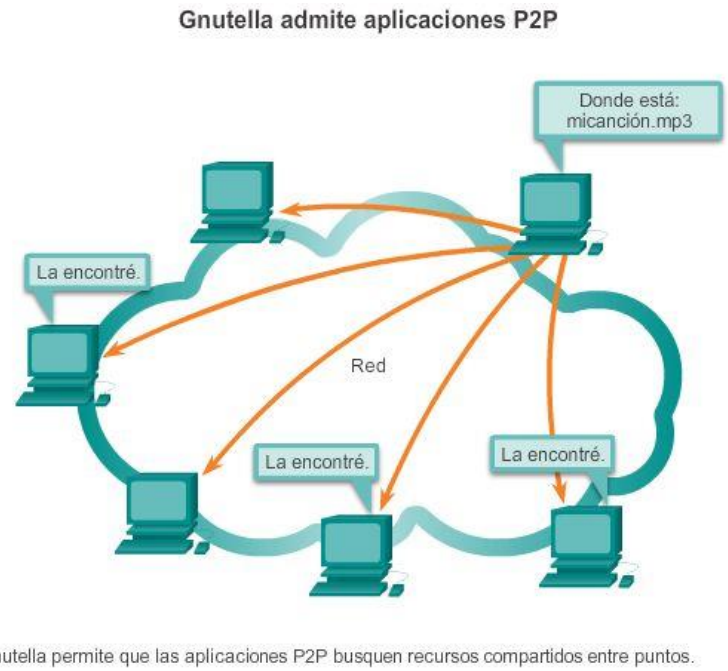
Con las aplicaciones P2P, cada PC de la red que ejecuta la aplicación puede funcionar como cliente o como servidor para las otras PC en la red que ejecutan la aplicación. Las aplicaciones P2P comunes incluyen las siguientes:

- eDonkey
- eMule
- Shareaza
- BitTorrent
- Bitcoin
- LionShare

Algunas aplicaciones P2P se basan en el protocolo Gnutella. Estas aplicaciones permiten compartir archivos en discos duros con otras personas. Como se muestra en la ilustración, el software de cliente compatible con Gnutella permite a los usuarios conectarse a los servicios Gnutella a través de Internet, además de ubicar los recursos compartidos por otros puntos Gnutella y acceder a dichos recursos. Hay muchas aplicaciones cliente disponibles para acceder a la red Gnutella tales como BearShare, Gnucleus, LimeWire, Morpheus, WinMX y XoloX.

Mientras que el foro de desarrolladores de Gnutella mantiene el protocolo básico, los proveedores de aplicaciones suelen desarrollar extensiones para lograr que el protocolo funcione mejor con dichas aplicaciones.

Muchas de las aplicaciones P2P no utilizan una base de datos central para registrar todos los archivos disponibles en los puntos. Por el contrario, los dispositivos en la red se indican mutuamente qué archivos están disponibles cuando hay una consulta, y utilizan el protocolo y los servicios de intercambio de archivos para dar soporte a la búsqueda de recursos.



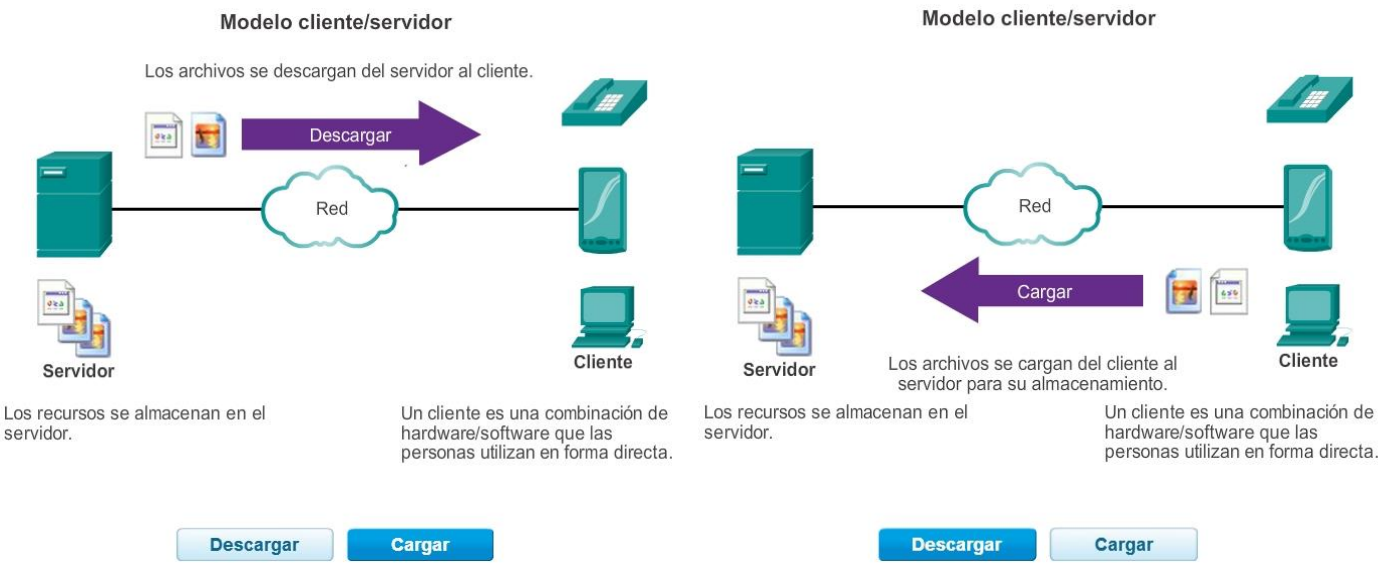
Gnutella permite que las aplicaciones P2P busquen recursos compartidos entre puntos.

Capítulo 10: Capa de aplicación 10.1.2.5 Modelo Cliente-Servidor

En el modelo cliente-servidor, el dispositivo que solicita información se denomina “cliente”, y el dispositivo que responde a la solicitud se denomina “servidor”. Los procesos de cliente y servidor se consideran parte de la capa de aplicación. El cliente comienza el intercambio solicitando los datos al servidor, quien responde enviando uno o más streams de datos al cliente. Los protocolos de la capa de aplicación describen el formato de las solicitudes y respuestas entre clientes y servidores. Además de la transferencia real de datos, este intercambio también puede requerir la autenticación del usuario y la identificación de un archivo de datos que se vaya a transferir.

Un ejemplo de una red cliente-servidor es el uso del servicio de correo electrónico de un ISP para enviar, recibir y almacenar correo electrónico. El cliente de correo electrónico en una PC doméstica emite una solicitud al servidor de correo electrónico del ISP para que se le envíe todo correo no leído. El servidor responde enviando al cliente el correo electrónico solicitado.

Aunque los datos se describen generalmente como el flujo del servidor al cliente, algunos datos fluyen siempre del cliente al servidor. El flujo de datos puede ser el mismo en ambas direcciones, o inclusive puede ser mayor en la dirección que va del cliente al servidor. Por ejemplo, un cliente puede transferir un archivo al servidor con fines de almacenamiento. Como se muestra en la ilustración, la transferencia de datos de un cliente a un servidor se conoce como “subida” y la transferencia de datos de un servidor a un cliente se conoce como “descarga”.



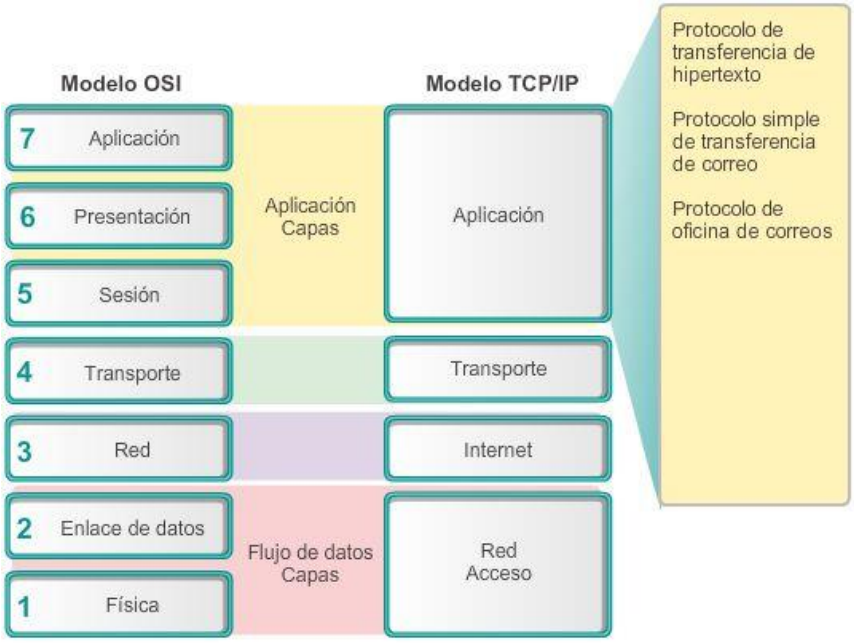
Capítulo 10: Capa de aplicación 10.2.1.1 Repaso de los protocolos de capa de aplicación

Existen muchos protocolos de capa de aplicación, pero en un día típico probablemente utiliza solo cinco o seis. Los siguientes son tres protocolos de capa de aplicación que forman parte del trabajo o los juegos cotidianos:

- Protocolo de transferencia de hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Protocolo de oficina de correos (POP)

Estos protocolos de capa de aplicación permiten explorar la Web y enviar y recibir correo electrónico. HTTP se utiliza para que los usuarios puedan conectarse a sitios Web a través de Internet. SMTP permite que los usuarios puedan enviar correo electrónico. POP permite que los usuarios puedan recibir correo electrónico.

En las próximas páginas, se hará hincapié en estos tres protocolos de capa de aplicación.



Capítulo 10: Capa de aplicación 10.2.1.2 Protocolo de transferencia de hipertexto y lenguaje de marcado de hipertexto

Cuando se escribe una dirección Web o un localizador uniforme de recursos (URL) en un explorador Web, el explorador establece una conexión con el servicio Web que se ejecuta en el servidor mediante el protocolo HTTP. Los nombres que la mayoría de las personas asocia con las direcciones Web son URL e identificador uniforme de recursos (URI).

El URL http://www.cisco.com/index.html es un ejemplo de un URL que se refiere a un recurso específico: una página Web llamada index.html en un servidor identificado como cisco.com. Haga clic en cada ilustración para ver los pasos que utiliza HTTP.

Los exploradores Web son el tipo de aplicación cliente que utiliza una PC para conectarse a la World Wide Web y acceder a recursos almacenados en un servidor Web. Al igual que con la mayoría de los procesos de servidores, el servidor Web funciona como un servicio básico y genera diferentes tipos de archivos disponibles.

Para acceder al contenido, los clientes Web establecen conexiones al servidor y solicitan los recursos deseados. El servidor responde con el recurso y, al recibirlo, el explorador interpreta los datos y los presenta al usuario.

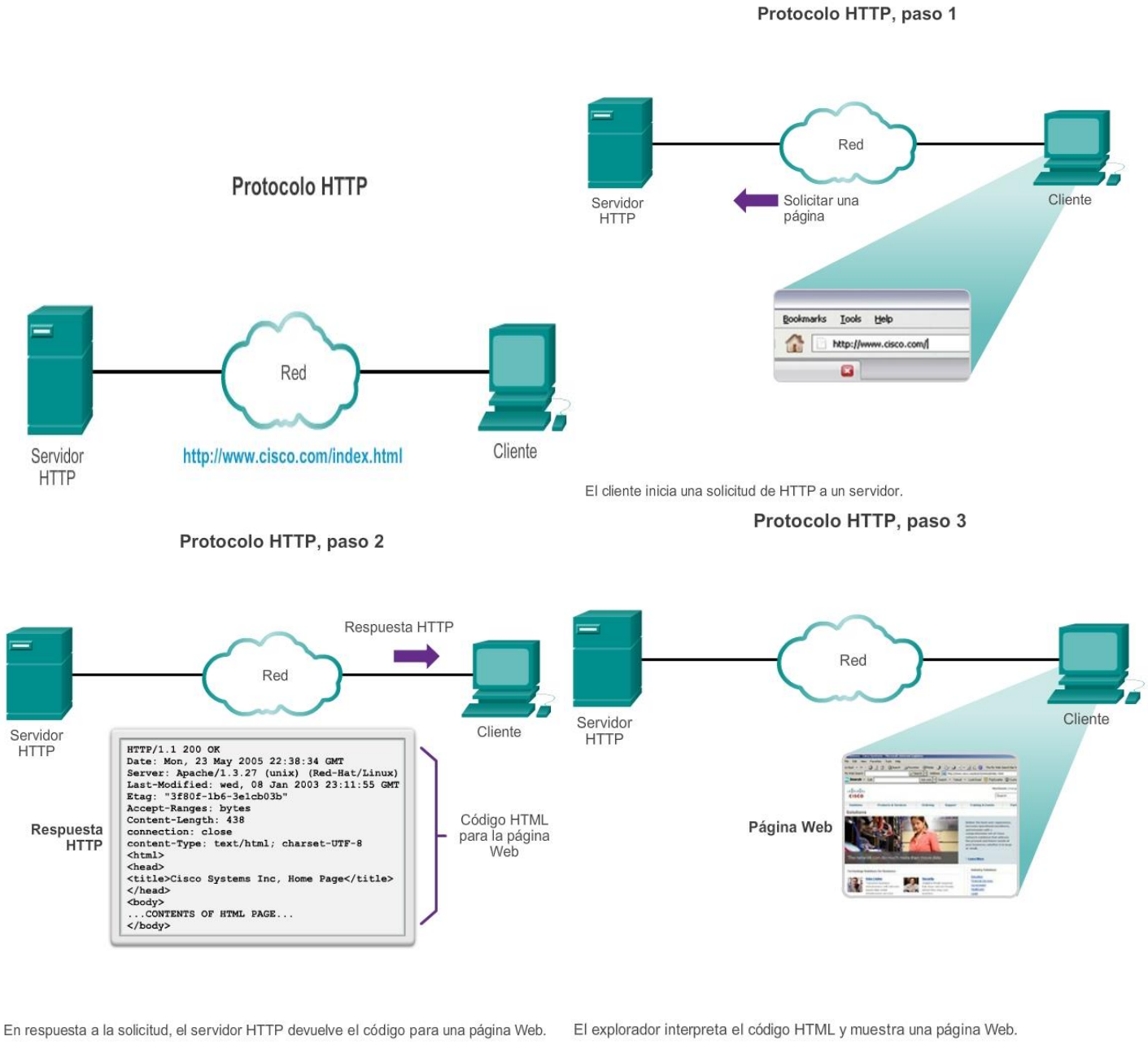
Los exploradores pueden interpretar y presentar muchos tipos de datos (como texto no cifrado o lenguaje de marcado de hipertexto, que es el lenguaje que se utiliza para construir páginas Web). Otros tipos de datos, sin embargo, requieren de otro servicio o programa. Generalmente se les conoce como plug-ins o complementos. Para ayudar al explorador a determinar qué tipo de archivo está recibiendo, el servidor especifica qué clase de datos contiene el archivo.

Para comprender mejor cómo interactúan el explorador Web con el cliente Web, podemos analizar cómo se abre una página Web en un explorador. Para este ejemplo, utilice el URL http://www.cisco.com/index.html.

Primero, el explorador interpreta las tres partes del URL, como se muestra en la figura 1:

1. http (el protocolo o esquema)
2. www.cisco.com (el nombre del servidor)
3. index.html (el nombre de archivo específico solicitado)

A continuación, el explorador verifica con un servidor de nombre para convertir a www.cisco.com en una dirección numérica que utiliza para conectarse al servidor, como se muestra en la figura 2. Mediante los requisitos de HTTP, el explorador envía una solicitud GET al servidor y solicita el archivo index.html. El servidor envía el código HTML para esta página Web al explorador, como se muestra en la figura 3. Finalmente, el explorador descifra el código HTML y da formato a la página para que se pueda visualizar en la ventana del explorador, como se muestra en la figura 4.



Capítulo 10: Capa de aplicación 10.2.1.3 HTTP y HTTPS

HTTP se utiliza a través de la World Wide Web para transferencia de datos y es uno de los protocolos de aplicación más utilizados hoy en día. Originalmente, este protocolo se desarrolló solo para publicar y recuperar páginas HTML. Sin embargo, la flexibilidad de HTTP lo convirtió en una aplicación fundamental de los sistemas de información distribuidos y cooperativos.

HTTP es un protocolo de solicitud/respuesta. Cuando un cliente, por lo general un explorador Web, envía una solicitud a un servidor Web, HTTP especifica los tipos de mensaje que se utilizan para esa comunicación. Los tres tipos de mensajes comunes son GET, POST y PUT (consulte la ilustración).

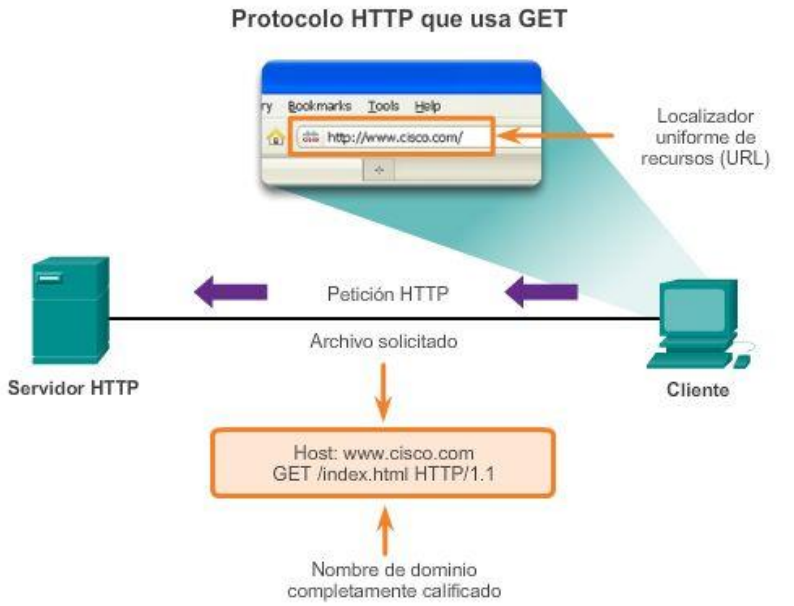
GET es una solicitud de datos por parte del cliente. Un cliente (explorador Web) envía el mensaje GET al servidor Web para solicitar las páginas HTML. Cuando el servidor recibe la solicitud GET, este responde con una línea de estado, como HTTP/1.1 200 OK, y un mensaje propio. El mensaje del servidor puede incluir el archivo HTML solicitado, si está disponible, o puede contener un mensaje de error o de información, como “Se modificó la ubicación del archivo solicitado”.

Los mensajes POST y PUT se utilizan para subir datos al servidor Web. Por ejemplo, cuando el usuario introduce datos en un formulario que está integrado en una página Web (p. ej., cuando se completa una solicitud de pedido), el mensaje POST se envía al servidor Web. En el mensaje POST, se incluyen los datos que el usuario introdujo en el formulario.

PUT carga los recursos o el contenido en el servidor Web. Por ejemplo, si un usuario intenta subir un archivo o una imagen a un sitio Web, el cliente envía un mensaje PUT al servidor con la imagen o el archivo adjunto.

Aunque HTTP es sumamente flexible, no es un protocolo seguro. Los mensajes de solicitud envían información al servidor en un texto sin formato que puede ser interceptado y leído. De forma similar, las respuestas del servidor, generalmente páginas HTML, también se descifran.

Para una comunicación segura a través de Internet, se utiliza el protocolo HTTP seguro (HTTPS) para acceder o subir información al servidor Web. El HTTPS puede utilizar autenticación y encriptación para asegurar los datos mientras viajan entre el cliente y el servidor. HTTPS especifica reglas adicionales para pasar datos entre la capa de aplicación y la capa de transporte. El protocolo HTTPS utiliza el mismo proceso de solicitud del cliente-respuesta del servidor que HTTP, pero el stream de datos se encripta con capa de sockets seguros (SSL) antes de transportarse a través de la red. El HTTPS crea una carga y un tiempo de procesamiento adicionales en el servidor debido a la encriptación y el descifrado de tráfico.



Al escribir "http://www.cisco.com" en la barra de dirección de un explorador Web, se genera el mensaje HTTP "GET".

Capítulo 10: Capa de aplicación 10.2.1.4 SMTP, POP e IMAP

Uno de los principales servicios que un ISP ofrece es hosting de correo electrónico. El correo electrónico revolucionó la forma en que las personas se comunican gracias a su sencillez y velocidad. No obstante, para ejecutar el correo electrónico en una PC o en otro dispositivo final, este requiere varios servicios y aplicaciones.

El correo electrónico es un método para almacenar y enviar que se utiliza para enviar, almacenar y recuperar mensajes electrónicos a través de una red. Los mensajes de correo electrónico se guardan en bases de datos

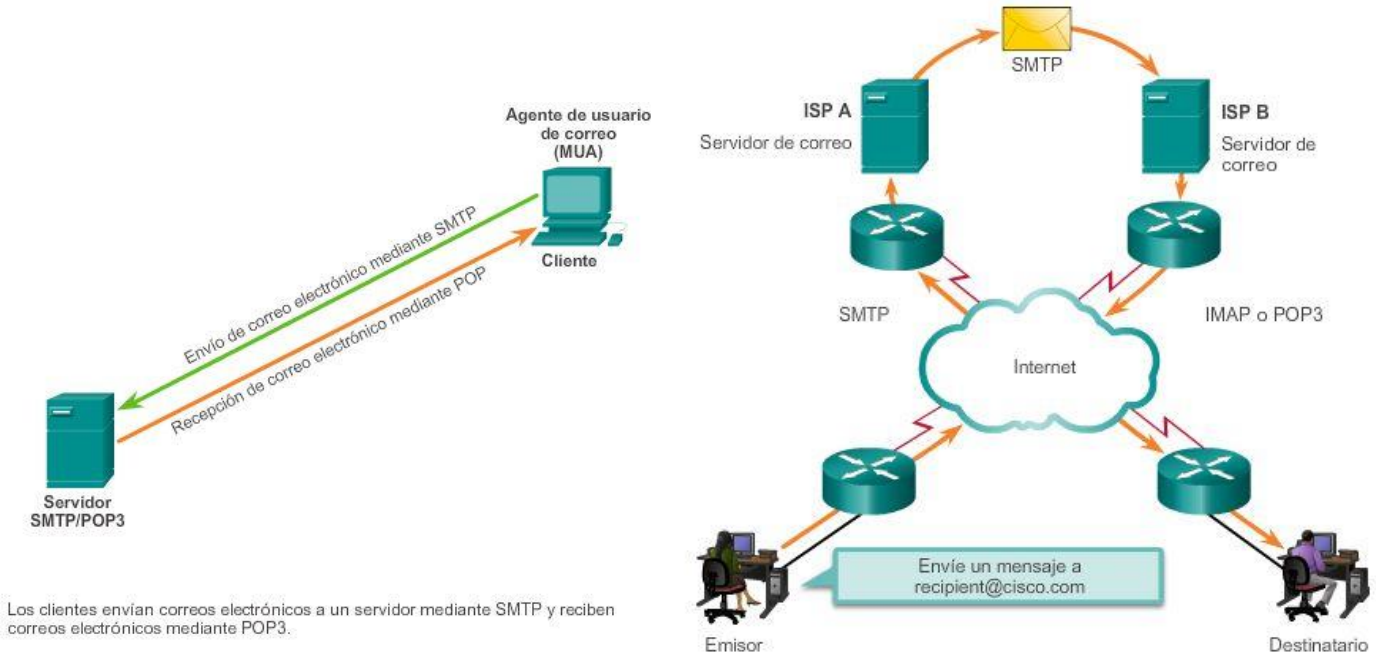
en servidores de correo. A menudo, los ISP mantienen servidores de correo que admiten varias cuentas de clientes diferentes.

Los clientes de correo electrónico se comunican con servidores de correo para enviar y recibir mensajes de correo electrónico. Los servidores de correo se comunican con otros servidores de correo para transportar mensajes desde un dominio a otro. Un cliente de correo electrónico no se comunica directamente con otro cliente de correo electrónico cuando envía un mensaje. Más bien, ambos clientes dependen del servidor de correo para el transporte de los mensajes. Esto sucede incluso cuando ambos usuarios se encuentran en el mismo dominio.

Los clientes de correo electrónico envían mensajes al servidor de correo electrónico determinado en las configuraciones de aplicaciones. Cuando el servidor recibe el mensaje, verifica si el dominio receptor se encuentra en su base de datos local. De no ser así, envía una solicitud de DNS para determinar la dirección IP del servidor de correo electrónico para el dominio de destino. A continuación, el correo electrónico se reenvía al servidor correspondiente.

El correo electrónico admite tres protocolos diferentes para su funcionamiento: el protocolo simple de transferencia de correo (SMTP), el protocolo de oficina de correos (POP) y el protocolo de acceso a mensajes de Internet (IMAP). El proceso de capa de aplicación que envía correo utiliza SMTP. Esto sucede cuando se envía correo de un cliente a un servidor y cuando se envía correo de un servidor a otro.

Sin embargo, un cliente recupera el correo electrónico mediante uno de dos protocolos de capa de aplicación: POP o IMAP.



Capítulo 10: Capa de aplicación 10.2.1.5 SMTP, POP y IMAP (cont.)

El protocolo simple de transferencia de correo (SMTP) transfiere correo electrónico con confianza y eficacia. Para que las aplicaciones del SMTP funcionen bien, se debe formatear correctamente el mensaje de correo electrónico y los procesos SMTP deben estar en ejecución en el cliente y en el servidor.

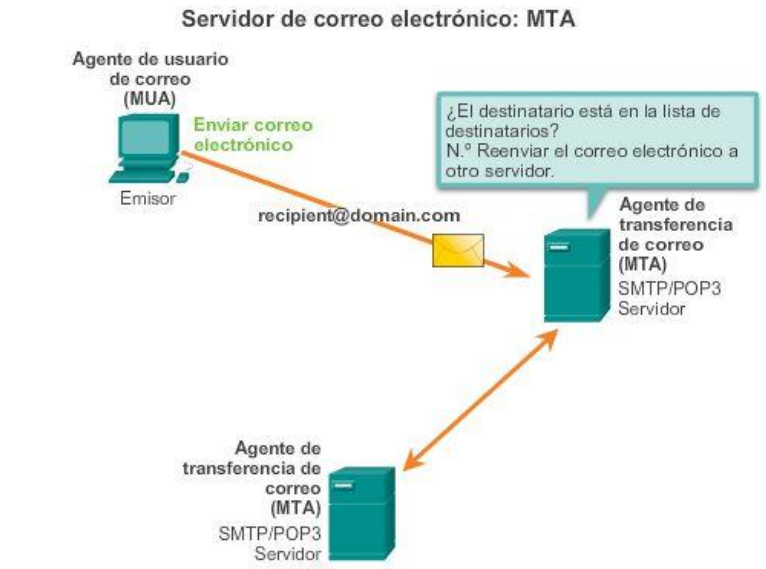
Los formatos de mensajes SMTP necesitan un encabezado y un cuerpo de mensaje. Mientras que el cuerpo del mensaje puede contener la cantidad de texto que se desee, el encabezado debe contar con una dirección

de correo electrónico de destinatario correctamente formateada y una dirección de emisor. Toda otra información de encabezado es opcional.

Cuando un cliente envía correo electrónico, el proceso SMTP del cliente se conecta a un proceso SMTP del servidor en el puerto bien conocido 25.

Después de que se establece la conexión, el cliente intenta enviar el correo electrónico al servidor a través de esta. Una vez que el servidor recibe el mensaje, lo ubica en una cuenta local (si el destinatario es local) o lo reenvía mediante el mismo proceso de conexión SMTP a otro servidor de correo para su entrega.

El servidor de correo electrónico de destino puede no estar en línea, o muy ocupado, cuando se envían los mensajes. Por lo tanto, el SMTP pone los mensajes en cola para enviarlos posteriormente. El servidor verifica periódicamente la cola en busca de mensajes e intenta enviarlos nuevamente. Si el mensaje aún no se ha entregado después de un tiempo predeterminado de expiración, se devolverá al emisor como imposible de entregar.



El proceso de agente de transferencia de correo rige el envío de correo electrónico entre los servidores y los clientes.

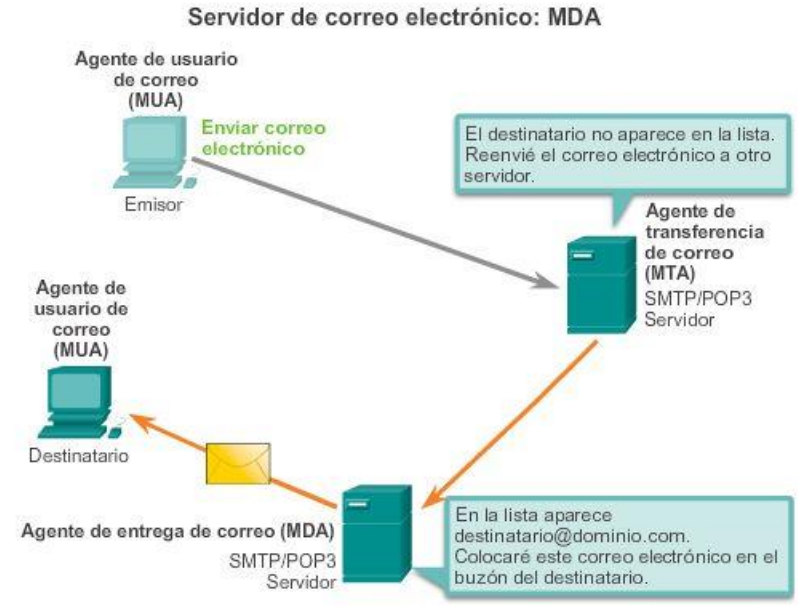
Capítulo 10: Capa de aplicación 10.2.1.6 SMTP, POP y IMAP (cont.)

El protocolo de oficina de correos (POP) permite que una estación de trabajo pueda recuperar correos de un servidor de correo. Con POP, el correo se descarga desde el servidor al cliente y después se elimina en el servidor.

El servidor comienza el servicio POP escuchando de manera pasiva en el puerto TCP 110 las solicitudes de conexión del cliente. Cuando un cliente desea utilizar el servicio, envía una solicitud para establecer una conexión TCP con el servidor. Una vez establecida la conexión, el servidor POP envía un saludo. A continuación, el cliente y el servidor POP intercambian comandos y respuestas hasta que la conexión se cierra o cancela.

Dado que estos mensajes de correo electrónico se descargan para el cliente y se eliminan del servidor, esto significa que no existe una ubicación centralizada donde se conserven los mensajes de correo electrónico. Como el POP no almacena mensajes, no es una opción adecuada para una pequeña empresa que necesita una solución de respaldo centralizada.

El POP3 es deseable para los ISP, ya que aligera su responsabilidad de manejar grandes cantidades de almacenamiento para sus servidores de correo electrónico.



El proceso de agente de entrega de correo rige la entrega de correo electrónico entre los servidores y los clientes.

Capítulo 10: Capa de aplicación 10.2.1.7 SMTP, POP y IMAP (cont.)

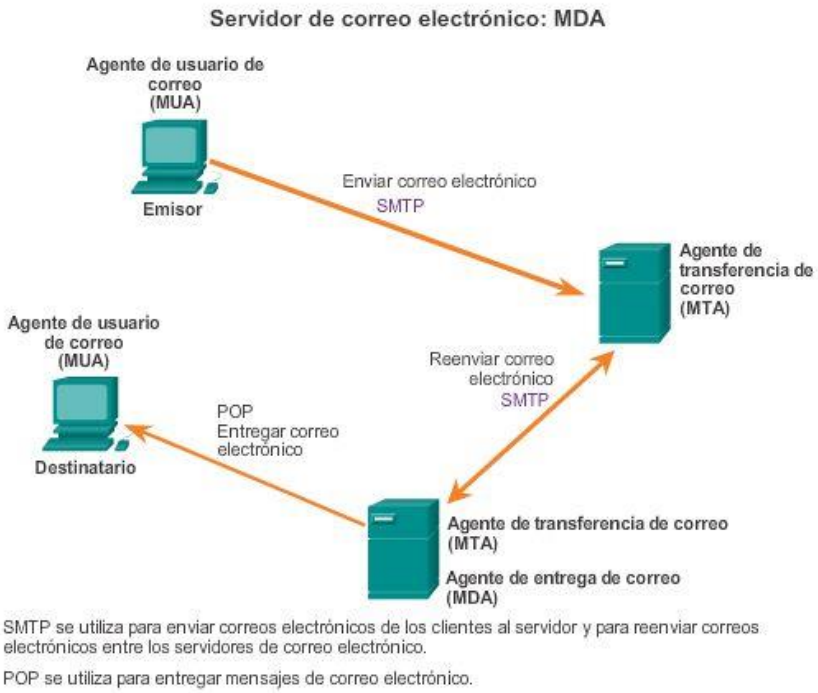
El Protocolo de acceso a mensajes de Internet (IMAP, Internet Message Access Protocol) es otro protocolo que describe un método para recuperar mensajes de correo electrónico. Sin embargo, a diferencia del POP, cuando el usuario se conecta a un servidor para IMAP, se descargan copias de los mensajes a la aplicación del cliente.

Los mensajes originales se mantienen en el servidor hasta que se eliminen manualmente. Los usuarios ven copias de los mensajes en su software de cliente de correo electrónico.

Los usuarios pueden crear una jerarquía de archivos en el servidor para organizar y guardar el correo. Dicha estructura de archivos se duplica también en el cliente de correo electrónico. Cuando un usuario decide eliminar un mensaje, el servidor sincroniza esa acción y elimina el mensaje del servidor.

Para pequeñas o medianas empresas, son muchas las ventajas al utilizar el protocolo IMAP. El IMAP puede realizar un almacenamiento a largo plazo de mensajes de correo electrónico en servidores de correo y permitir el respaldo centralizado. También les permite a los empleados acceder a mensajes de correo electrónico desde distintas ubicaciones, utilizando dispositivos o software de cliente diferentes. La estructura de carpetas del buzón que un usuario espera ver se encuentra disponible para visualizarla, independientemente del modo en que el usuario obtenga acceso al buzón.

Para un ISP, el IMAP puede no ser el protocolo elegido. El espacio de disco para admitir la gran cantidad de mensajes de correo electrónico almacenados puede ser costoso de comprar y mantener. Además, si los clientes esperan que se realicen copias de respaldo a sus buzones periódicamente, esto puede aumentar aún más los costos para el ISP.



Capítulo 10: Capa de aplicación 10.2.2.1 Servicio de nombres de dominios

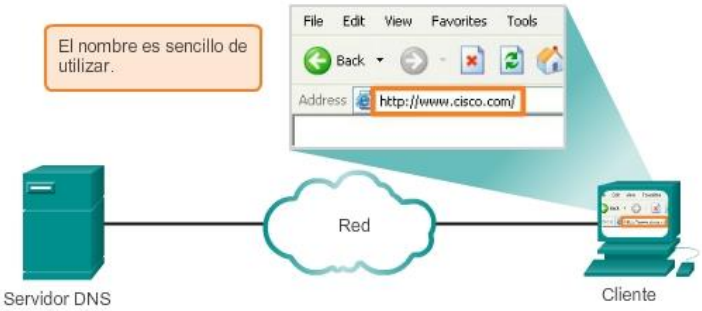
En las redes de datos, los dispositivos se etiquetan con direcciones IP numéricas para enviar y recibir datos a través de las redes. La mayoría de las personas no puede recordar estas direcciones numéricas. Los nombres de dominio se crearon para convertir las direcciones numéricas en un nombre sencillo y reconocible.

En Internet, estos nombres de dominio, como http://www.cisco.com, son mucho más fáciles de recordar que algo como 198.133.219.25, que es la dirección numérica real de ese servidor. Si Cisco decide cambiar la dirección numérica www.cisco.com, es claro para el usuario, porque el nombre de dominio se mantiene. Simplemente se une la nueva dirección al nombre de dominio existente y se mantiene la conectividad. Cuando las redes eran pequeñas, resultaba fácil mantener la asignación entre los nombres de dominios y las direcciones que representaban. A medida que el tamaño de las redes y la cantidad de dispositivos aumentaron, este sistema manual se volvió inviable.

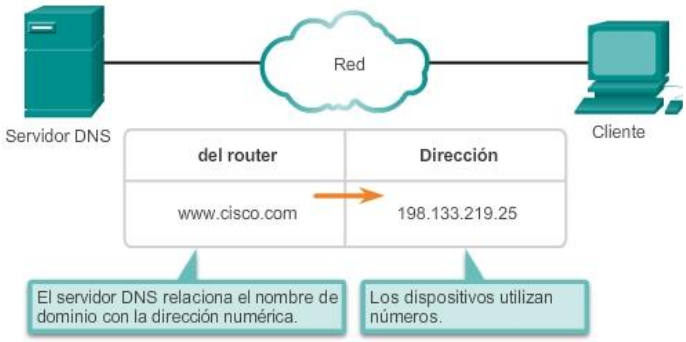
El Sistema de nombres de dominio (DNS) se creó para que el nombre del dominio busque soluciones para estas redes. DNS utiliza un conjunto distribuido de servidores para resolver los nombres asociados con estas direcciones numéricas. Haga clic en los botones de la ilustración para conocer los pasos para resolver direcciones de DNS.

El protocolo DNS define un servicio automatizado que coincide con nombres de recursos que tienen la dirección de red numérica solicitada. Incluye el formato de consultas, respuestas y datos. Las comunicaciones del protocolo DNS utilizan un único formato llamado “mensaje”. Este formato de mensaje se utiliza para todos los tipos de solicitudes de clientes y respuestas del servidor, mensajes de error y para la transferencia de información de registro de recursos entre servidores.

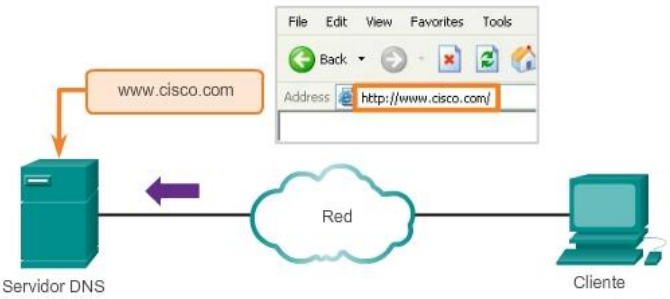
Resolución de direcciones DNS, paso 1



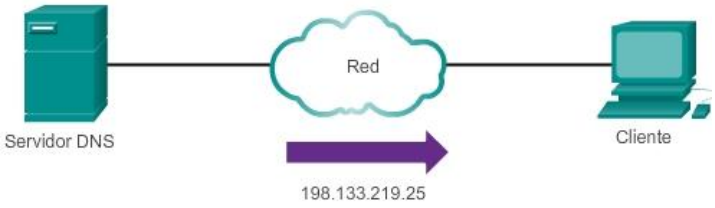
Resolución de direcciones DNS, paso 2



Resolución de direcciones DNS, paso 3



Resolución de direcciones DNS, paso 4



El número se envía de regreso al cliente para utilizarlo en la realización de solicitudes de servidor.

Resolución de direcciones DNS, paso 5

El protocolo DNS resuelve el nombre de dominio para la dirección numérica de dispositivo de red.

En las figuras 1 a 5, se muestran los pasos relacionados con la resolución DNS.

Capítulo 10: Capa de aplicación 10.2.2.2 Formato del mensaje DNS

Un servidor DNS proporciona la resolución de nombres mediante *Berkeley Internet Domain Name* (BIND), o el demonio de nombres, que a menudo se denomina “named” (pronunciado “neimdi”). BIND fue desarrollado originalmente por cuatro estudiantes de la Universidad de California en Berkeley a principios de la década de los ochenta. Como se muestra en la ilustración, el formato del mensaje DNS que utiliza BIND es el formato DNS más utilizado en Internet.

El servidor DNS almacena diferentes tipos de registros de recursos utilizados para resolver nombres. Estos registros contienen el nombre, la dirección y el tipo de registro.

Algunos de estos tipos de registros son:

- A: una dirección de dispositivo final
- NS: un servidor de nombre autoritativo
- CNAME: el nombre canónico (o el nombre de dominio completamente calificado) para un alias; se utiliza cuando varios servicios tienen una dirección de red única, pero cada servicio tiene su propia entrada en el DNS.
- MX: registro de intercambio de correos; asigna un nombre de dominio a una lista de servidores de intercambio de correo para ese dominio.

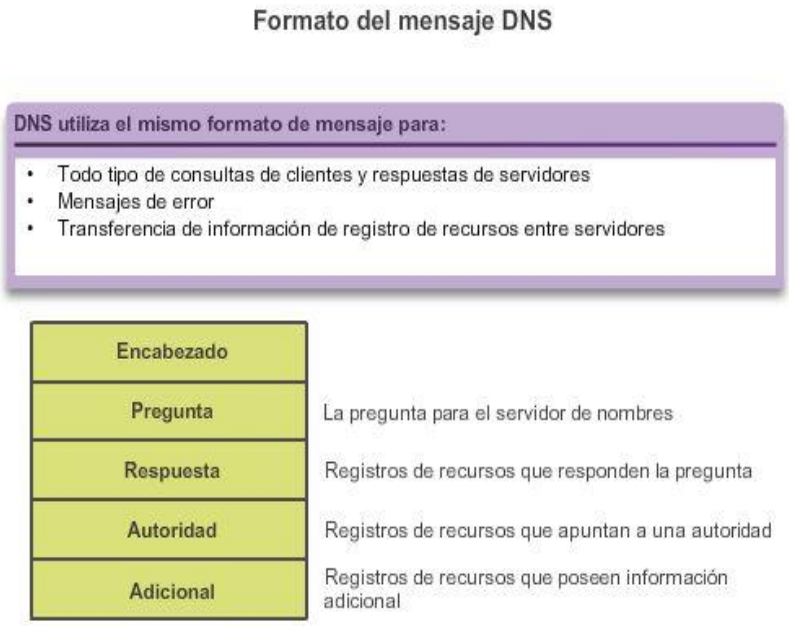
Cuando un cliente realiza una consulta, el proceso BIND del servidor observa primero sus propios registros para resolver el nombre. Si no puede resolverlo con los registros almacenados, contacta a otros servidores para hacerlo.

La solicitud puede pasar a lo largo de cierta cantidad de servidores, lo cual puede tomar más tiempo y consumir banda ancha. Una vez que se encuentra una coincidencia y se la devuelve al servidor solicitante original, este almacena temporalmente en la memoria caché la dirección numerada que coincide con el nombre.

Si vuelve a solicitarse ese mismo nombre, el primer servidor puede regresar la dirección utilizando el valor almacenado en el caché de nombres.

El almacenamiento en caché reduce el tráfico de la red de datos de consultas DNS y las cargas de trabajo de los servidores más altos de la jerarquía.

El servicio del cliente DNS en los equipos Windows optimiza el rendimiento de la resolución de nombres DNS al almacenar también los nombres resueltos previamente en la memoria. El comando ipconfig /displaydns muestra todas las entradas DNS en caché en un sistema de computación Windows.



Capítulo 10: Capa de aplicación 10.2.2.3 Jerarquía DNS

El protocolo DNS utiliza un sistema jerárquico para crear una base de datos que proporcione la resolución de nombres. La jerarquía es similar a un árbol invertido con la raíz en la parte superior y las ramas por debajo (consulte la ilustración). DNS utiliza nombres de domino para formar la jerarquía.

La estructura de denominación se divide en zonas pequeñas y manejables. Cada servidor DNS mantiene un archivo de base de datos específico y sólo es responsable de administrar las asignaciones de nombre a IP para esa pequeña porción de toda la estructura DNS.

Cuando un servidor DNS recibe una solicitud para una traducción de nombre que no se encuentra dentro de esa zona DNS, el servidor DNS reenvía la solicitud a otro servidor DNS dentro de la zona adecuada para su traducción.

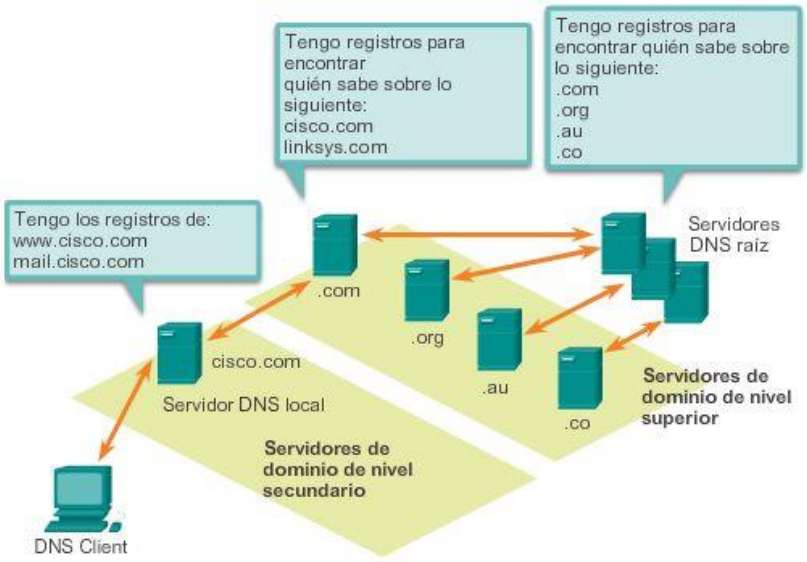
Nota: DNS es escalable, porque la resolución de los nombres de hosts se distribuye entre varios servidores.

Los diferentes dominios de primer nivel representan el tipo de organización o el país de origen. Entre los ejemplos de dominios del nivel superior se encuentran:

- .au: Australia
- .co: Colombia
- .com: una empresa o industria
- .jp: Japón
- .org: una organización sin fines de lucro

Después de los dominios del nivel superior, se encuentran los nombres de los dominios de segundo nivel y debajo de estos hay otros dominios de nivel inferior. Cada nombre de dominio es una ruta hacia este árbol invertido que comienza de la raíz. Por ejemplo, como se muestra en la ilustración, es posible que el servidor DNS raíz no sepa exactamente dónde se encuentra el registro del servidor de correo electrónico, mail.cisco.com, pero conserva un registro del dominio .com dentro del dominio de nivel superior. Asimismo, es posible que los servidores dentro del dominio .com no tengan un registro de mail.cisco.com, pero sí tienen un registro del dominio. Los servidores dentro del dominio cisco.com tienen un registro (un registro MX para ser precisos) para mail.cisco.com.

El DNS depende de esta jerarquía de servidores descentralizados para almacenar y mantener estos registros de recursos. Los registros de recursos enumeran nombres de dominios que el servidor puede resolver y servidores alternativos que también pueden procesar solicitudes. Si un servidor dado tiene registros de recursos que corresponden a su nivel en la jerarquía de dominios, se dice que es autoritativo para dichos registros. Por ejemplo, un servidor de nombre en el dominio cisco.netacad.net no sería autoritativo para el registro de mail.cisco.com, porque dicho registro se mantiene en un servidor de nivel de dominio superior, específicamente el servidor de nombre en el dominio cisco.com.



Una jerarquía de servidores DNS contiene los registros de recursos que relacionan los nombres con las direcciones.

Capítulo 10: Capa de aplicación 10.2.2.4 nslookup

DNS es un servicio cliente/servidor. Sin embargo, difiere de los otros servicios cliente/servidor. Mientras otros servicios utilizan un cliente que es una aplicación (como un explorador Web o un cliente de correo electrónico), el cliente DNS ejecuta un servicio por sí mismo. El cliente DNS, a veces denominado “resolución DNS”, admite la resolución de nombres para otras aplicaciones de red y otros servicios que lo necesiten.

Al configurar un dispositivo de red, generalmente proporcionamos una o más direcciones del servidor DNS que el cliente DNS puede utilizar para la resolución de nombres. En general, el proveedor de servicios de Internet (ISP) suministra las direcciones para utilizar con los servidores DNS. Cuando la aplicación del usuario pide conectarse a un dispositivo remoto por nombre, el cliente DNS solicitante consulta a uno de estos servidores de nombres para resolver el nombre para una dirección numérica.

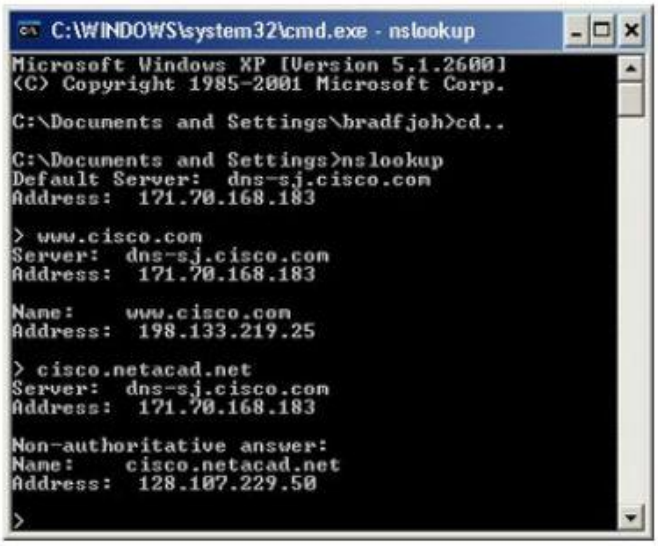
Los sistemas operativos de las PC también cuentan con una utilidad llamada “nslookup” que permite que el usuario consulte los servidores de nombres de forma manual para resolver un nombre de host determinado. Esta utilidad también puede utilizarse para solucionar los problemas de resolución de nombres y verificar el estado actual de los servidores de nombres.

En la ilustración, cuando se ejecuta el comando nslookup, se muestra el servidor DNS predeterminado configurado para su host. En este ejemplo, el servidor DNS es dns-sj.cisco.com, que tiene la dirección 171.70.168.183.

El nombre de un host o de un dominio se puede introducir en la petición de entrada de nslookup. En la primera consulta de la ilustración, se hace una consulta para www.cisco.com. El servidor de nombre que responde proporciona la dirección 198.133.219.25.

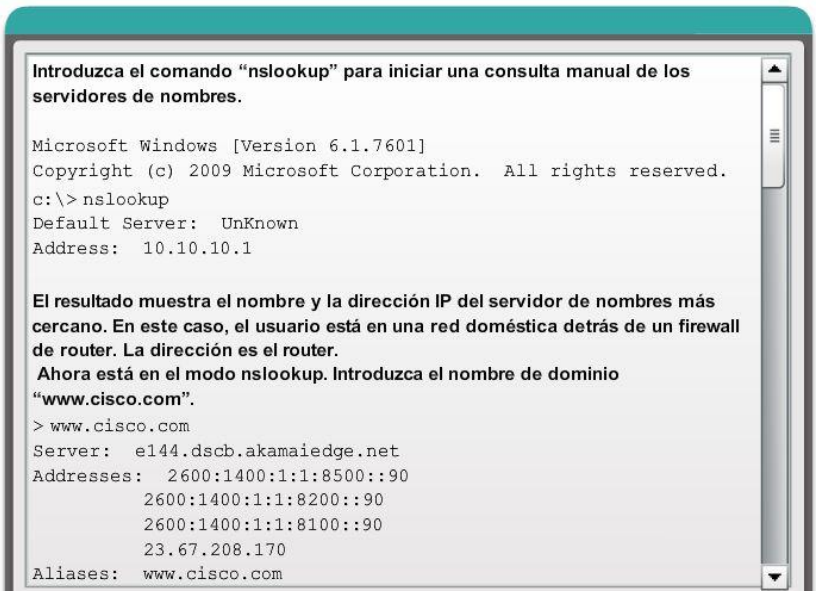
Las consultas mostradas en la figura son sólo pruebas simples. La utilidad nslookup tiene muchas opciones disponibles para realizar una prueba y una verificación exhaustivas del proceso DNS. Al finalizar, escriba exitpara salir de la utilidad nslookup.

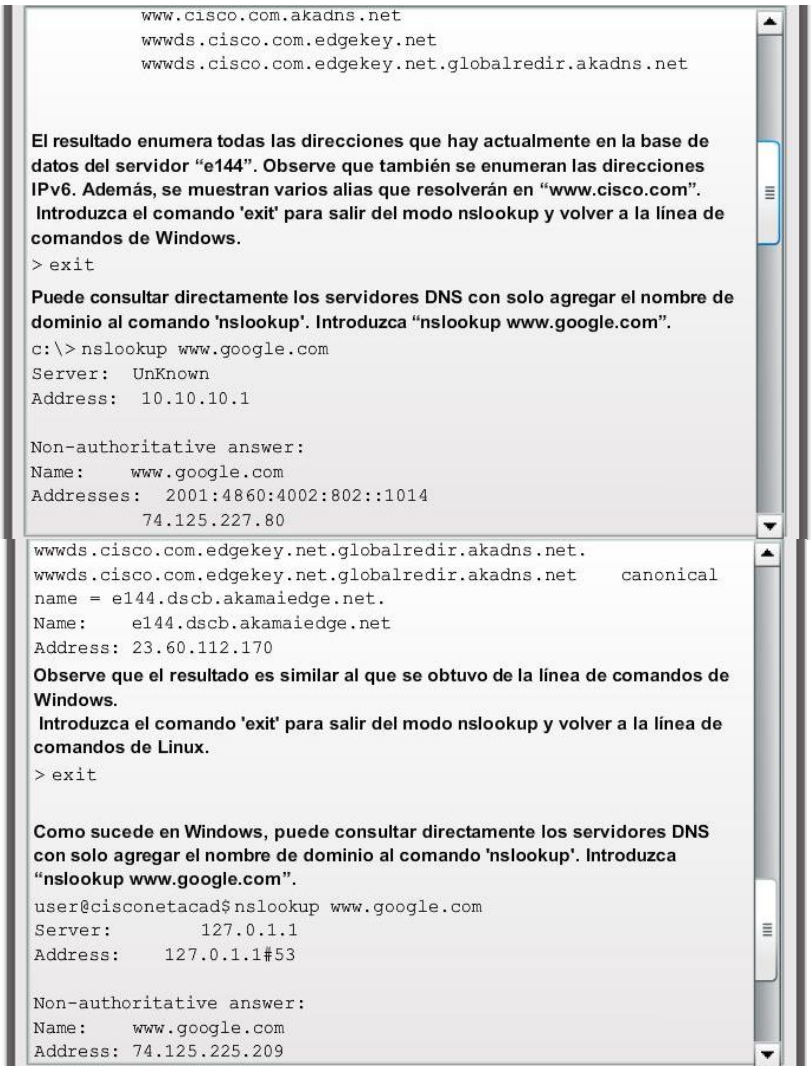
Uso de nslookup



Capítulo 10: Capa de aplicación 10.2.2.5 Verificador de sintaxis: Comandos de CLI DNS en Windows y UNIX

Uso del comando nslookup `nslookup`





```
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

El resultado enumera todas las direcciones que hay actualmente en la base de datos del servidor "e144". Observe que también se enumeran las direcciones IPv6. Además, se muestran varios alias que resolverán en "www.cisco.com".
Introduzca el comando 'exit' para salir del modo nslookup y volver a la línea de comandos de Windows.

```
> exit
```

Puede consultar directamente los servidores DNS con solo agregar el nombre de dominio al comando 'nslookup'. Introduzca "nslookup www.google.com".

```
c:\> nslookup www.google.com
Server:  UnKnown
Address:  10.10.10.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2001:4860:4002:802::1014
          74.125.227.80
```

```
wwwds.cisco.com.edgekey.net.globalredir.akadns.net.
wwwds.cisco.com.edgekey.net.globalredir.akadns.net    canonical
name = e144.dscb.akamaiedge.net.
Name:    e144.dscb.akamaiedge.net
Address: 23.60.112.170
```

Observe que el resultado es similar al que se obtuvo de la línea de comandos de Windows.
Introduzca el comando 'exit' para salir del modo nslookup y volver a la línea de comandos de Linux.

```
> exit
```

Como sucede en Windows, puede consultar directamente los servidores DNS con solo agregar el nombre de dominio al comando 'nslookup'. Introduzca "nslookup www.google.com".

```
user@cisconetacad$ nslookup www.google.com
Server:        127.0.1.1
Address:    127.0.1.1#53

Non-authoritative answer:
Name:    www.google.com
Address: 74.125.225.209
```

Capítulo 10: Capa de aplicación 10.2.2.6 Protocolo de configuración dinámica de host

El servicio Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol) permite a los dispositivos de una red obtener direcciones IP y demás información de un servidor DHCP. Este servicio automatiza la asignación de direcciones IP, máscaras de subred, gateway y otros parámetros de redes IP. Esto se denomina "direccionamiento dinámico". La alternativa al direccionamiento dinámico es el direccionamiento estático. Al utilizar el direccionamiento estático, el administrador de red introduce manualmente la información de la dirección IP en los hosts de red.

DHCP permite a un host obtener una dirección IP de forma dinámica cuando se conecta a la red. Se realiza el contacto con el servidor de DHCP y se solicita una dirección. El servidor de DHCP elige una dirección de un rango de direcciones configurado llamado "pool" y la asigna (concede) al host por un período establecido.

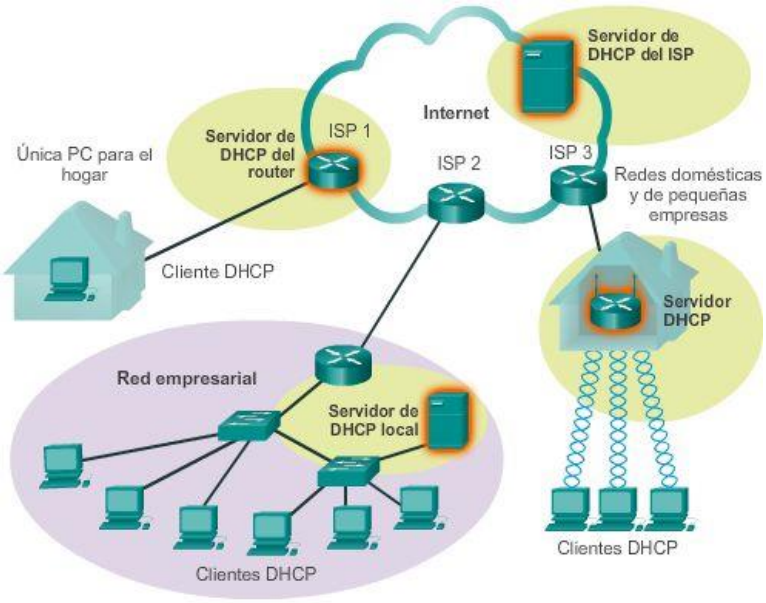
En redes locales más grandes, o donde los usuarios cambian con frecuencia, se prefiere asignar direcciones con DHCP. Es posible que los nuevos usuarios tengan computadoras portátiles y necesiten una conexión; otros pueden tener estaciones de trabajo nuevas que deben estar conectadas. En lugar de que el administrador de red asigne direcciones IP para cada estación de trabajo, es más eficaz que las direcciones IP se asignen automáticamente mediante el DHCP.

Las direcciones distribuidas por DHCP no se asignan de forma permanente a los hosts, sino que solo se conceden por un cierto período. Si el host se apaga o se desconecta de la red, la dirección regresa al pool para volver a utilizarse. Esto es especialmente útil en el caso de los usuarios móviles que entran en una red y salen de ella. Los usuarios pueden moverse libremente desde una ubicación a otra y volver a establecer las conexiones de red. El host puede obtener una dirección IP una vez que se conecta el hardware, ya sea por cable o por LAN inalámbrica.

DHCP permite el acceso a Internet por medio de zonas de cobertura inalámbrica en aeropuertos o cafeterías. Cuando un dispositivo inalámbrico ingresa a una zona de cobertura, el cliente DHCP del dispositivo entra en contacto con el servidor de DHCP local mediante una conexión inalámbrica, y el servidor de DHCP asigna una dirección IP al dispositivo.

Como lo muestra la figura, varios tipos de dispositivos pueden ser servidores de DHCP cuando ejecutan software de servicio de DHCP. En la mayoría de las redes medianas a grandes, el servidor de DHCP suele ser un servidor local dedicado con base en una PC. En las redes domésticas, el servidor de DHCP suele estar ubicado en el router local que conecta la red doméstica al ISP. Los hosts locales reciben la información de la dirección IP directamente del router local. El router local recibe una dirección IP del servidor de DHCP en el ISP.

DHCP puede representar un riesgo a la seguridad porque cualquier dispositivo conectado a la red puede recibir una dirección. Este riesgo hace que la seguridad física sea un factor determinante para el uso del direccionamiento dinámico o manual. Tanto el direccionamiento dinámico como el estático tienen un lugar en el diseño de red. Muchas redes utilizan tanto el direccionamiento estático como el DHCP. DHCP se utiliza para hosts de uso general, como los dispositivos para usuarios finales, mientras que el direccionamiento estático se utiliza para dispositivos de red, como gateways, switches, servidores e impresoras.



Capítulo 10: Capa de aplicación 10.2.2.7 Funcionamiento de DHCP

Sin DHCP los usuarios tienen que introducir manualmente la dirección IP, la máscara de subred y otros parámetros de red para poder unirse a esta. El servidor de DHCP mantiene un pool de las direcciones IP y alquila una dirección a cualquier cliente habilitado por DHCP cuando el cliente está activado. Debido a que las direcciones IP son dinámicas (concedidas) en lugar de estáticas (asignadas en forma permanente), las direcciones en desuso regresan automáticamente al pool para que se vuelvan a asignar. Como se muestra en la ilustración, cuando un dispositivo configurado con DHCP se inicia o se conecta a la red, el cliente transmite un mensaje de descubrimiento de DHCP (DHCPDISCOVER) para identificar cualquier servidor de DHCP disponible en la red. Un servidor de DHCP responde con un mensaje de oferta de DHCP (DHCPOFFER), que ofrece una concesión al cliente. El mensaje de oferta contiene la dirección IP y la máscara de subred que se

deben asignar, la dirección IP del servidor DNS y la dirección IP del gateway predeterminado. La oferta de concesión también incluye la duración de esta.

El cliente puede recibir varios mensajes DHCPOFFER si hay más de un servidor de DHCP en la red local; por lo tanto, debe elegir entre ellos y enviar un mensaje de solicitud de DHCP (DHCPREQUEST) que identifique el servidor explícito y la oferta de concesión que el cliente acepta. Un cliente también puede optar por solicitar una dirección previamente asignada por el servidor.

Suponiendo que la dirección IP solicitada por el cliente, u ofrecida por el servidor, aún está disponible, el servidor devuelve un mensaje de acuse de recibo de DHCP (DHCPACK) que le informa al cliente que finalizó la concesión. Si la oferta ya no es válida, quizá debido a que hubo un tiempo de espera o a que otro cliente tomó la concesión, entonces el servidor seleccionado responde con un mensaje de acuse de recibo negativo de DHCP (DHCPNAK). Si se devuelve un mensaje DHCPNAK, entonces el proceso de selección debe volver a comenzar con la transmisión de un nuevo mensaje DHCPDISCOVER. Una vez que el cliente tiene la concesión, se debe renovar mediante otro mensaje DHCPREQUEST antes de que expire.

El servidor de DHCP asegura que todas las direcciones IP sean únicas (no se puede asignar la misma dirección IP a dos dispositivos de red diferentes de forma simultánea). Usar DHCP permite a los administradores de red volver a configurar fácilmente las direcciones IP del cliente sin tener que realizar cambios a los clientes en forma manual. La mayoría de los proveedores de Internet utilizan DHCP para asignar direcciones a los clientes que no necesitan una dirección estática.

Capítulo 10: Capa de aplicación 10.2.3.1 Protocolo de transferencia de archivos

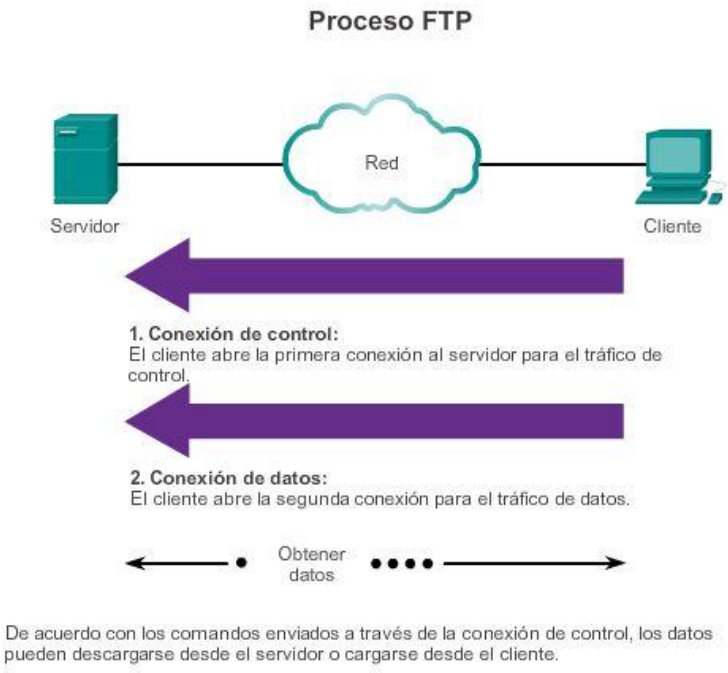
El protocolo de transferencia de archivos (FTP) es otro protocolo de capa de aplicación que se utiliza comúnmente. El protocolo FTP se desarrolló para permitir las transferencias de datos entre un cliente y un servidor. Un cliente FTP es una aplicación que se ejecuta en una PC y que se utiliza para insertar y extraer datos en un servidor que ejecuta un demonio FTP (FTPd).

Como se muestra en la ilustración, para transferir datos correctamente, FTP requiere dos conexiones entre el cliente y el servidor, una para los comandos y las respuestas y la otra para la transferencia de archivos propiamente dicha:

- El cliente establece la primera conexión al servidor para el tráfico de control, que está constituido por comandos del cliente y respuestas del servidor.

- El cliente establece la segunda conexión al servidor para la transferencia de datos propiamente dicha. Esta conexión se crea cada vez que hay datos para transferir.

La transferencia de datos se puede producir en ambas direcciones. El cliente puede descargar (extraer) datos del servidor o subir datos a él (insertarlos).



Capítulo 10: Capa de aplicación 10.2.3.4 Bloque de mensajes del servidor

El bloque de mensajes del servidor (SMB) es un protocolo de intercambio de archivos cliente/servidor que desarrolló IBM a fines de la década de los ochenta para describir la estructura de los recursos de red compartidos, como archivos, directorios, impresoras y puertos serie. Es un protocolo de solicitud-respuesta.

El protocolo SMB describe el acceso al sistema de archivos y la manera en que los clientes hacen solicitudes de archivos. Además describe la comunicación entre procesos del protocolo SMB. Todos los mensajes SMB comparten un mismo formato. Este formato utiliza un encabezado de tamaño fijo seguido de un parámetro de tamaño variable y un componente de datos.

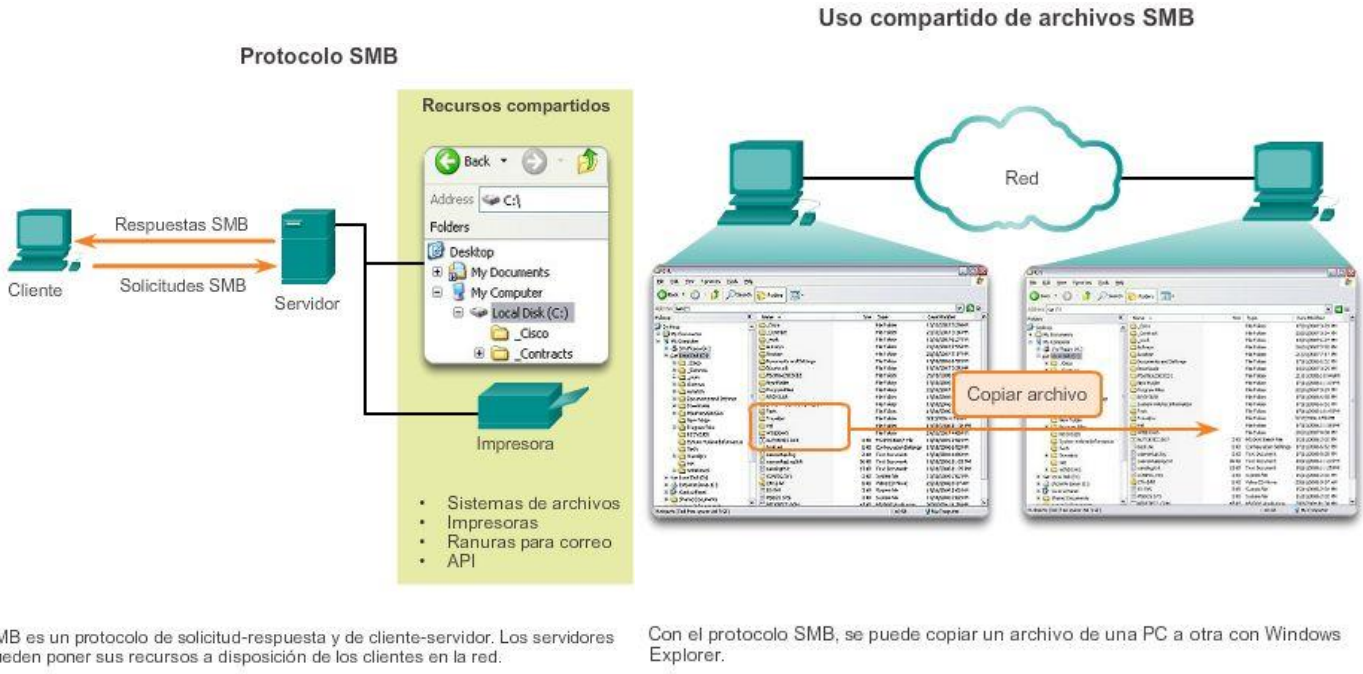
Los mensajes de SMB pueden:

- Iniciar, autenticar y terminar sesiones
- Controlar el acceso a los archivos y a la impresora
- Autorizar una aplicación para enviar o recibir mensajes para o de otro dispositivo

Los servicios de impresión y el SMB para compartir archivos se han transformado en el pilar de las redes de Microsoft. Con la presentación de la serie de software Windows 2000, Microsoft cambió la estructura subyacente para el uso del SMB. En versiones anteriores de los productos de Microsoft, los servicios de SMB utilizaron un protocolo que no es TCP/IP para implementar la resolución de nombres.
A partir de Windows 2000, todos los productos subsiguientes de Microsoft utilizan la convención de nomenclatura DNS, que permite que los protocolos TCP/IP admitan directamente el uso compartido de recursos de SMB, como se muestra en la figura 1. El proceso de intercambio de archivos de SMB entre equipos Windows se muestra en la figura 2.

A diferencia del uso compartido de archivos que admite el protocolo de transferencia de archivos (FTP), los clientes establecen una conexión a largo plazo con los servidores. Una vez establecida la conexión, el usuario del cliente puede acceder a los recursos en el servidor como si el recurso fuera local para el host del cliente.

Los sistemas operativos LINUX y UNIX también proporcionan un método de intercambio de recursos con redes de Microsoft mediante una versión del SMB llamado SAMBA. Los sistemas operativos Macintosh de Apple también admiten recursos compartidos utilizando el protocolo SMB.



SMB es un protocolo de solicitud-respuesta y de cliente-servidor. Los servidores pueden poner sus recursos a disposición de los clientes en la red.

Con el protocolo SMB, se puede copiar un archivo de una PC a otra con Windows Explorer.

Capítulo 10: Capa de aplicación 10.3.1.1 Internet de las cosas

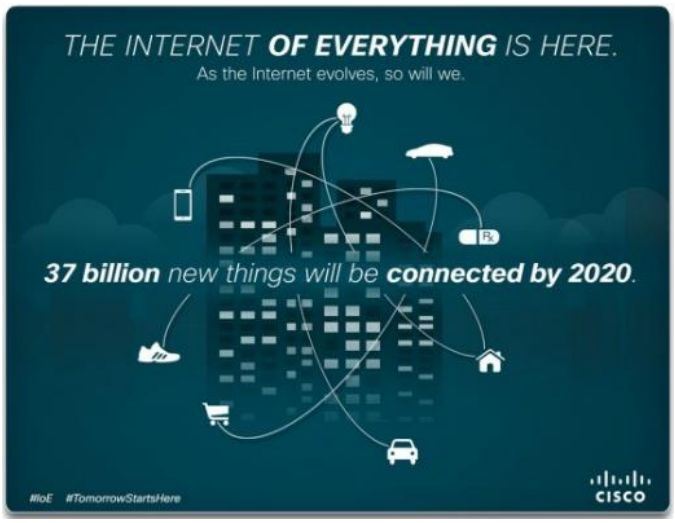
La capa de aplicación es responsable del acceso directo a los procesos subyacentes que administran y transmiten la comunicación a través de la red. Esta capa funciona como origen y destino de las comunicaciones a través de las redes de datos, independientemente del tipo de red de datos que se utilice. De hecho, los avances en la forma en que nos conectamos mediante redes tienen un impacto directo en el tipo de aplicaciones que están en desarrollo.

Las tendencias como Traiga su propio dispositivo (BYOD), el acceso desde cualquier lugar, la virtualización y las conexiones de máquina a máquina (m2m) abrieron el camino hacia una nueva generación de aplicaciones. Se estima que para el año 2020 habrá aproximadamente 50 000 millones de dispositivos conectados. Solo en 2010 se desarrollaron más de 350 000 aplicaciones, de las que se realizaron más de tres millones de descargas. Todo esto conduce a un mundo de conexiones intuitivas entre personas, procesos, datos y los elementos que están en la red.

Mediante el uso de etiquetas inteligentes y de la conectividad avanzada para digitalizar productos que no son de tecnología inteligente (desde bicicletas y botellas hasta refrigeradores y automóviles) y para conectarlos a Internet, las personas y las compañías podrán interactuar en formas nuevas e inimaginables. Los objetos podrán recopilar, recibir y enviar información a usuarios y a otros objetos conectados. Como se muestra en la ilustración, esta nueva ola de desarrollo de Internet se conoce como Internet de las cosas.

En la actualidad, existen más de 100 millones de máquinas expendedoras, vehículos, detectores de humo y otros dispositivos que ya comparten información automáticamente, una cifra que los analistas de mercado de Berg Insight esperan que suba a 360 millones para el año 2016. Actualmente, las fotocopiadoras que

cuentan con un módulo M2M pueden pedir tóner y papel nuevos en forma automática, o avisar a los técnicos sobre una falla; incluso pueden indicarles qué piezas deben traer.



Capítulo 10: Capa de aplicación 10.3.1.2 El mensaje viaja a través de una red

La explosión masiva de aplicaciones se debe, en gran medida, al genio del enfoque en capas para el procesamiento de datos a través de una red. Concretamente, si se mantiene la funcionalidad de la capa de aplicación separada de la funcionalidad del transporte de datos, los protocolos de capa de aplicación se pueden modificar, y se pueden desarrollar nuevas aplicaciones, sin que el desarrollador deba preocuparse por el procedimiento de obtención de datos a través de la red. Esa es la funcionalidad de otras capas y, por lo tanto, de otros desarrolladores.

Como se muestra en la ilustración, cuando una aplicación envía una solicitud a una aplicación de servidor, la capa de aplicación construye el mensaje, pero después se pasa por las diversas funcionalidades de la capa en el cliente para entregarse. Mientras se traslada por el stack, cada capa inferior encapsula los datos con un encabezado que contiene los protocolos de comunicación para esa capa. Estos protocolos, que se implementan en los hosts emisores y receptores, interactúan para proporcionar una entrega extremo a extremo de las aplicaciones a través de la red.

Por ejemplo, los protocolos como el HTTP, admiten el envío de páginas Web a dispositivos finales. Ahora que conocemos todas las diversas capas y sus funcionalidades, podemos seguir la solicitud de una página Web de un cliente desde el servidor Web para ver cómo funciona cada una de estas funcionalidades individuales en forma completa y conjunta.

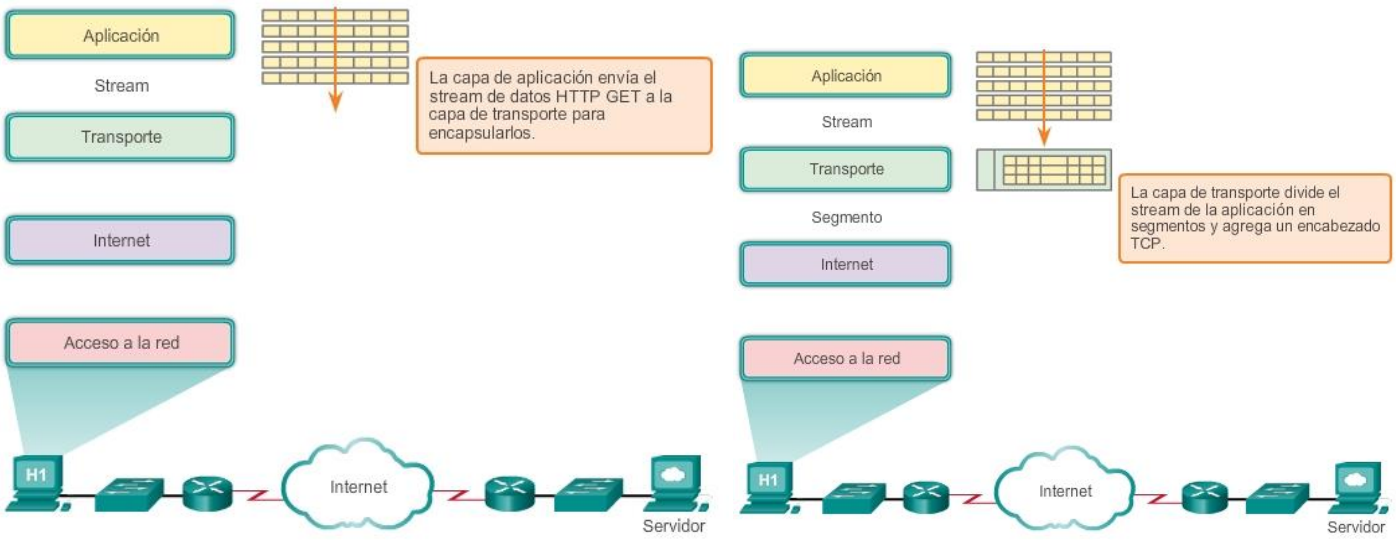
Si se utiliza el modelo TCP/IP, un proceso completo de comunicación incluye los siguientes seis pasos:

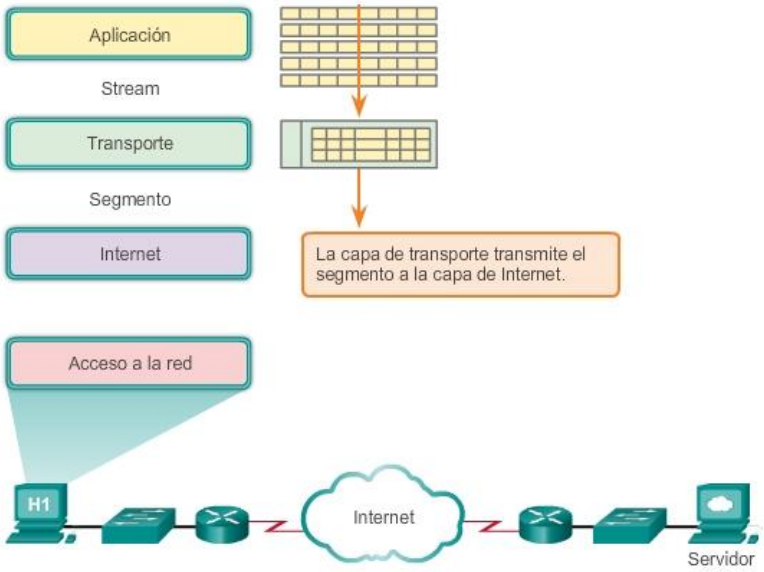
Creación de los datos

El primer paso es la creación de datos en la capa de aplicación del dispositivo final de origen que inicia la comunicación. En este caso, después de crear la solicitud del cliente Web, conocida como HTTP GET, esos datos se codifican, comprimen y encriptan, si es necesario. De esto se encarga el protocolo de capa de aplicación del modelo TCP/IP, pero incluye la funcionalidad descrita por las capas de aplicación, presentación y sesión del modelo OSI. La capa de aplicación envía estos datos como un stream a la capa de transporte.

Segmentación y encapsulación inicial

El siguiente paso es la segmentación y la encapsulación de los datos a medida que pasan por el stack de protocolos. En la capa de transporte, el mensaje HTTP GET se divide en partes más pequeñas y fáciles de manejar. A cada parte del mensaje se le agrega un encabezado de capa de transporte. Dentro del encabezado de la capa de transporte, hay indicadores que establecen cómo reconstruir el mensaje. También se incluye un identificador, el número de puerto 80. Este se utiliza para avisar al servidor de destino que se quiere enviar el mensaje a su aplicación de servidor Web. También se agrega un puerto de origen generado aleatoriamente para asegurarse de que el cliente pueda seguir la comunicación de retorno y reenviarla a la aplicación cliente correcta.





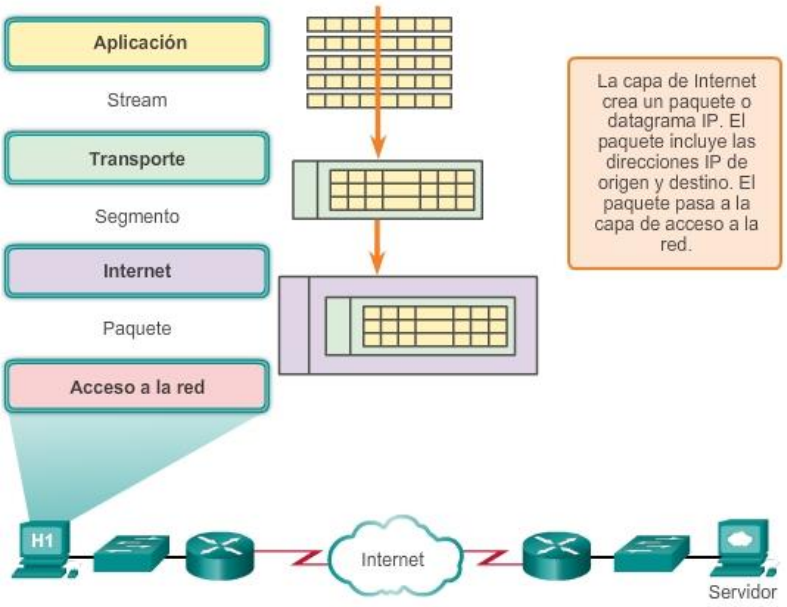
Capítulo 10: Capa de aplicación 10.3.1.3 Envío de datos al dispositivo final

Direccionamiento

A continuación, se agregan los identificadores de dirección a los segmentos, como se muestra en la ilustración. Así como hay capas múltiples de protocolos que preparan los datos para la transmisión a su destino, hay capas múltiples de direccionamiento para asegurar su entrega. La función de la capa de red es agregar el direccionamiento que permite la transferencia de los datos desde el host que los origina hasta el host que los utiliza. La capa de red logra esto mediante el encapsulamiento de cada segmento en el

encabezado del paquete IP. El encabezado del paquete IP contiene las direcciones IP del dispositivo de origen y de destino. (La dirección IP del dispositivo de destino se determina generalmente mediante un proceso de aplicación anterior conocido como “servicio de nombre de dominio”).

La combinación de la dirección IP de origen y de destino con el número de puerto de origen y de destino se conoce como “socket”. El socket se utiliza para identificar el servidor y el servicio que solicita el cliente.



Capítulo 10: Capa de aplicación 10.3.1.4 Transporte de datos a través de internetwork

Preparación para el transporte

Después de agregar el direccionamiento IP, el paquete se traslada a la capa de acceso a la red para generar datos en los medios, como se muestra en la ilustración. Para que esto ocurra, la capa de acceso a la red primero debe preparar el paquete para la transmisión; para eso, lo coloca en una trama con un encabezado y un tráiler. Esta trama incluye la dirección física del host de origen y la dirección física del salto siguiente en la ruta al destino final. Esto equivale a la funcionalidad de la capa 2, o la capa de enlace de datos, del modelo OSI. La Capa 2 está relacionada con la entrega de los mensajes en una red local única. La dirección de la Capa 2 es exclusiva en la red local y representa la dirección del dispositivo final en el medio físico. En una LAN que utiliza Ethernet, esta dirección se denomina dirección de Control de acceso a los medios (MAC). Una vez que la capa de acceso a la red preparó la trama con las direcciones de origen y de destino, codifica la trama en bits y luego en impulsos eléctricos o en destellos de luz que se envían a través de los medios de red.

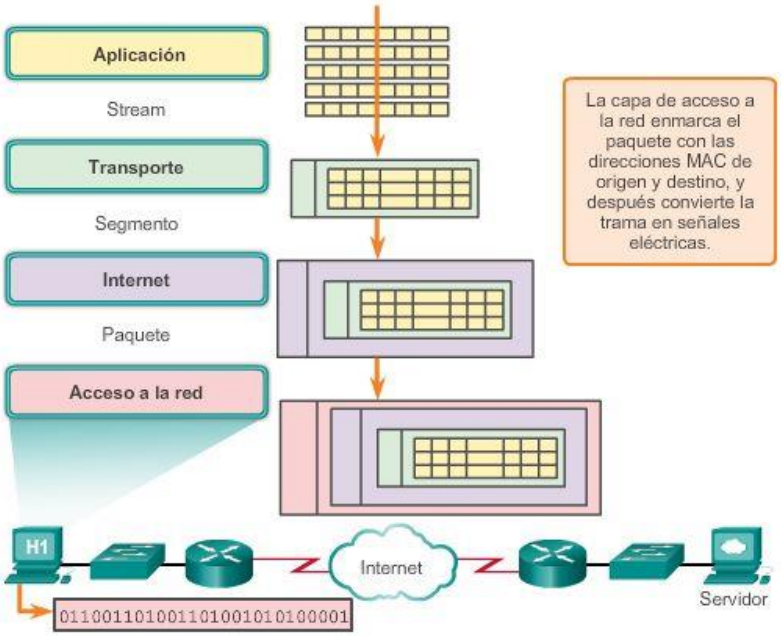
Transporte de datos

Los datos se transportan mediante la internetwork, que está compuesta por medios y por cualquier dispositivo intermedio. Como el mensaje encapsulado se transmite a través de la red, puede viajar a través de diferentes medios y tipos de red. La capa de acceso a la red especifica las técnicas para colocar la trama en los medios y quitarla de ellos, lo que se conoce también como “método de control de acceso al medio”.

Si el host de destino está en la misma red que el host de origen, el paquete se envía entre dos hosts en el medio local sin la necesidad de un router. Sin embargo, si el host de destino y el host de origen no están en la

misma red, el paquete se puede transportar a través de muchas redes, en muchos tipos diferentes de medios y a través de muchos routers. Cuando pasa por la red, la información contenida en la trama no se modifica.

En los límites de cada red local, un dispositivo de red intermedio, por lo general, un router, desencapsula la trama para leer la dirección de host de destino incluida en el encabezado del paquete. Los routers utilizan la porción del identificador de red de esta dirección para determinar qué ruta utilizar para llegar al host de destino. Una vez que se determina la ruta, el router encapsula el paquete en una nueva trama y lo envía al siguiente salto del trayecto hacia el dispositivo final de destino.



Capítulo 10: Capa de aplicación 10.3.1.5 Envío de datos a la aplicación correcta

Entrega de datos a la aplicación de destino correcta

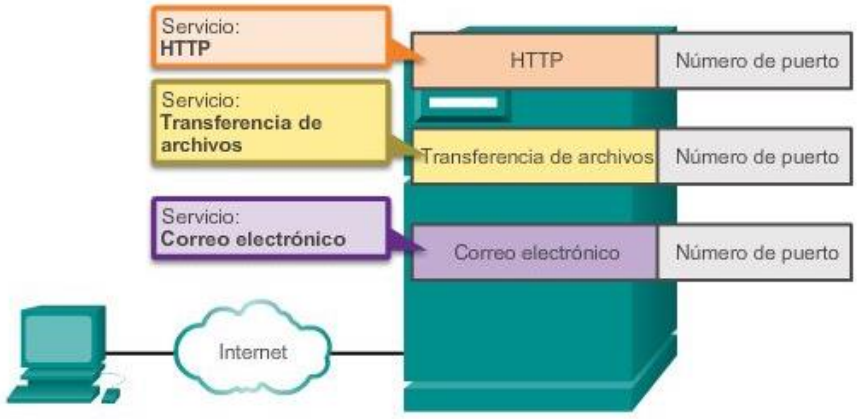
Por último, se recibe la trama en el dispositivo final de destino. Cuando los datos pasan por el stack en el dispositivo de destino, estos se desencapsulan y se vuelven a armar. Los datos pasan continuamente por las capas, de la capa de acceso a la red a la capa de red y a la capa de transporte, hasta que llegan a la capa de aplicación para ser procesados. Pero ¿cómo puede estar seguro el dispositivo de que se identifique el proceso de aplicación correcto?

Como se muestra en la ilustración, recuerde que en la capa de transporte, la información que contiene el encabezado PDU identifica el proceso o el servicio específico que se ejecuta en el dispositivo del host de destino que funcionará con los datos. Los hosts, sean clientes o servidores en Internet, pueden ejecutar múltiples aplicaciones de red simultáneamente. Las personas que utilizan PC suelen tener un cliente de correo electrónico que se ejecuta al mismo tiempo que el explorador Web, un programa de mensajería instantánea, algún streaming media y, tal vez, incluso algún juego. Todos estos programas ejecutándose en forma separada son ejemplos de procesos individuales.

Ver una página Web invoca al menos un proceso de red. Hacer clic en un hipervínculo hace que un explorador Web se comunique con un servidor Web. Al mismo tiempo, en segundo plano, es posible que un cliente de correo electrónico envíe o reciba un correo y un colega o amigo envíe un mensaje instantáneo.

Piense en una computadora que tiene sólo una interfaz de red. Todos los streams de datos que crean las aplicaciones que se ejecutan en la PC entran y salen a través de esa interfaz; no obstante, los mensajes instantáneos no aparecen de repente en medio de documentos del procesador de textos y los correos electrónicos no aparecen en la interfaz de un juego.

Esto es porque los procesos induviduales que se ejecutan en los hosts de origen y destino se comunican unos con otros. Cada aplicación o servicio se representa por un número de puerto en la Capa 4. Un diálogo único entre dispositivos se identifica con un par de números de puerto de origen y de destino de Capa 4 que son representativos de las dos aplicaciones de comunicación. Cuando los datos se reciben en el host, se examina el número de puerto para determinar qué aplicación o proceso es el destino correcto de los datos.



En el dispositivo final, el número de puerto de servicio dirige los datos a la conversación correcta.

Capítulo 10: Capa de aplicación 10.3.1.6 Guerreros de la red

Un recurso de entretenimiento para ayudar a visualizar los conceptos de red es la película animada “Warriors of the Net” (Guerreros de la red), de TNG Media Lab. Antes de ver el video, se debe tener en cuenta lo siguiente: Primero, en cuanto a los conceptos que ha aprendido en este capítulo, piense en qué momento del video está en la LAN, en la WAN, en intranet o en Internet, y cuáles son los dispositivos finales vs. los dispositivos intermedios, cómo se aplican los modelos OSI y TCP/IP y qué protocolos están involucrados.

En segundo lugar, si bien se hace referencia a los números de puerto 21, 23, 25, 53 y 80 de forma explícita en el video, se hace referencia a las direcciones IP solo de forma implícita, ¿puede ver dónde? ¿Dónde se pudieron involucrar las direcciones MAC en el video?

Finalmente, aunque todas las animaciones con frecuencia tienen simplificaciones en ellas, hay un error categórico en el video. Aproximadamente a los cinco minutos se afirma lo siguiente: “Lo que el Sr. IP hace cuando no recibe un acuse de recibo es enviar un paquete de reemplazo.” Esta no es una función del protocolo de Internet de capa 3, que es “poco confiable”, y de entrega de máximo esfuerzo, sino que es una función del protocolo TCP de la capa de transporte.

Descargue la película de http://www.warriorsofthe.net.

Capítulo 10: Capa de aplicación 10.4.1.1 Actividad de creación de modelos: Hágalo realidad

Hágalo realidad

Consulte la actividad de creación de modelos que se encuentra al comienzo de este capítulo como base para esta actividad. Los teléfonos IP se instalaron en media jornada, en lugar de tomar una semana completa como se previó inicialmente. Se restauró la capacidad total de la red, y las aplicaciones de red están disponibles para que las utilice. Tiene los mismos correos electrónicos que enviar y cotizaciones que preparar para obtener la aprobación del gerente.

Utilice la misma situación que completó en la actividad de creación de modelos introductoria para responder las siguientes preguntas:

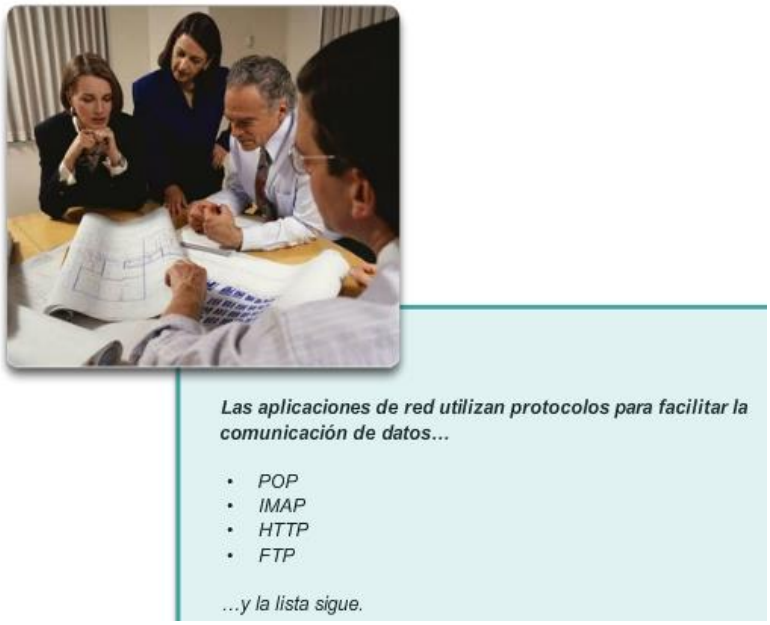
A. Correos electrónicos

- ¿Qué métodos puede utilizar para enviar correspondencia electrónica ahora que la red funciona?
- ¿En qué formato se enviarán sus correos electrónicos a través de la red?
- ¿Cómo puede enviar el mismo mensaje a varios destinatarios ahora?
- ¿Cómo puede enviar los adjuntos grandes a varios destinatarios usando aplicaciones de red?
- ¿El uso de aplicaciones de red resultaría un método de comunicación rentable para la compañía?

B. Cotización para obtener la aprobación del gerente.

- Dado que tiene programas de aplicaciones de escritorio instalados en su PC, ¿será relativamente fácil generar la cotización que su gerente necesita para el nuevo contrato, que tiene una fecha límite a finales de la semana? Justifique su respuesta.
- Cuando termine de redactar la cotización, ¿cómo la presentará al gerente para obtener su aprobación? ¿Cómo enviará el gerente la cotización al cliente para que la apruebe?
- ¿El uso de aplicaciones de red constituye un modo rentable de realizar transacciones comerciales? Justifique su respuesta.

Conserve una copia impresa o una copia electrónica de sus respuestas. Esté preparado para comentar sus respuestas en clase.



Capítulo 10: Capa de aplicación 10.4.1.4 Resumen

La capa de aplicación es responsable del acceso directo a los procesos subyacentes que administran y transmiten la comunicación a través de la red humana. Esta capa sirve como origen y destino de las comunicaciones a través de las redes de datos. Las aplicaciones, los protocolos y los servicios de la capa de aplicación permiten a los usuarios interactuar con la red de datos de manera significativa y eficaz.

- Las aplicaciones son programas informáticos con los que el usuario interactúa y que inician el proceso de transferencia de datos a solicitud del usuario.

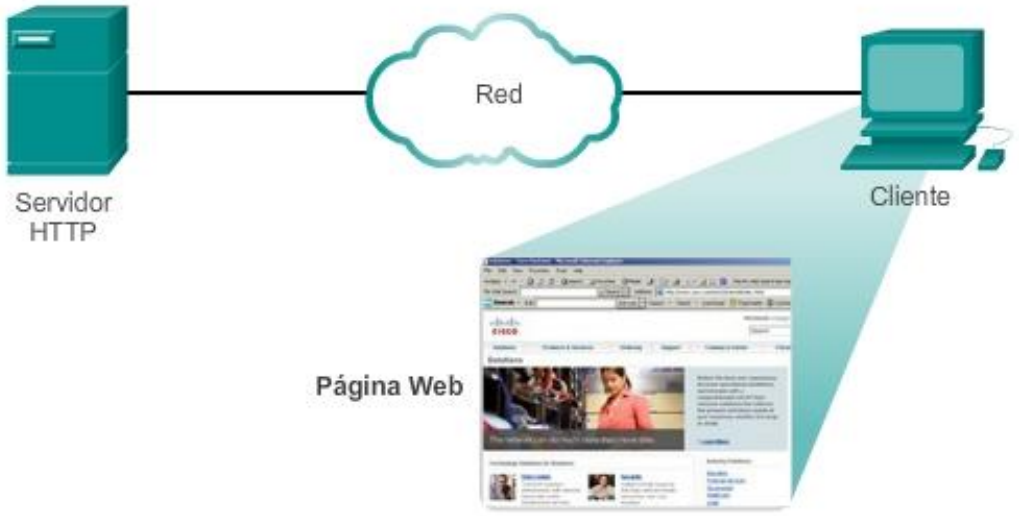
- Los servicios son programas en segundo plano que proporcionan conexión entre la capa de aplicación y las capas inferiores del modelo de red.

- Los protocolos proporcionan una estructura de reglas y procesos acordados que garantizan que los servicios que se ejecutan en un dispositivo particular puedan enviar y recibir datos de una variedad de dispositivos de red diferentes.

Un cliente puede solicitar a un servidor la entrega de datos por la red, o se puede solicitar entre dispositivos que funcionan en una disposición P2P, donde la relación cliente/servidor se establece según el dispositivo de origen y de destino en ese momento. Los mensajes se intercambian entre los servicios de la capa de aplicación en cada dispositivo final de acuerdo con las especificaciones del protocolo para establecer y utilizar estas relaciones.

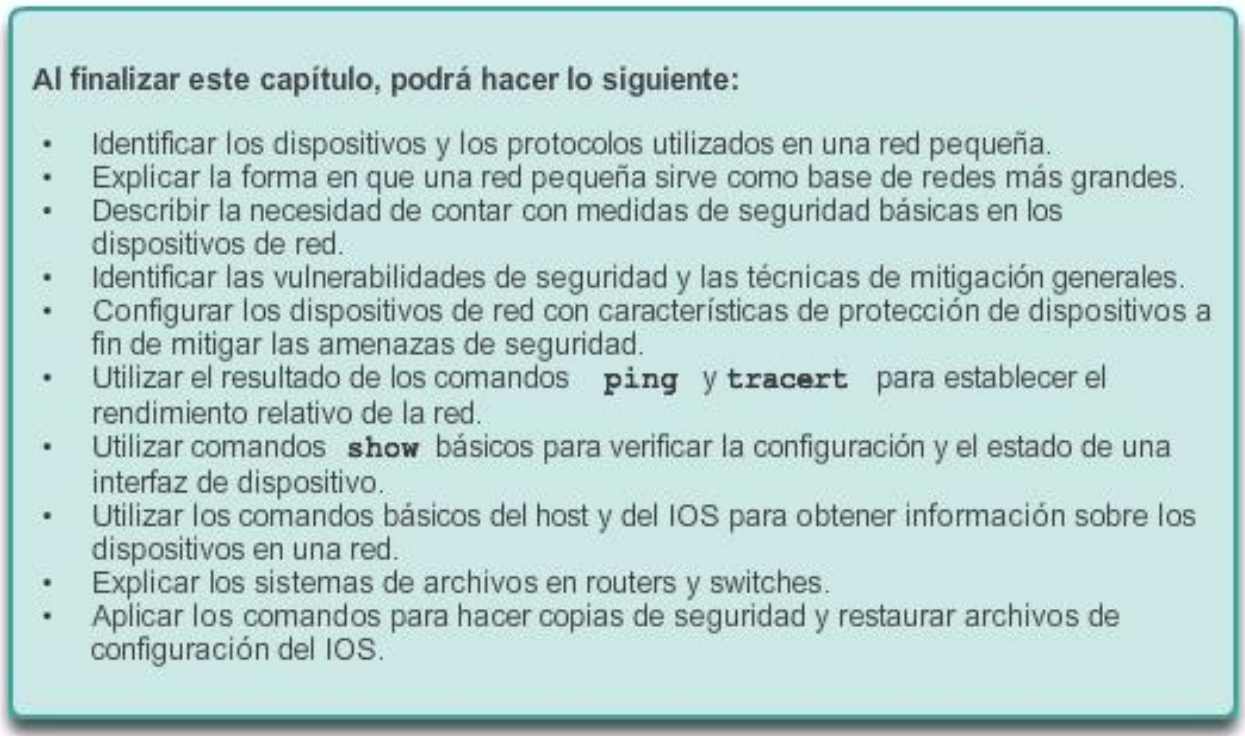
Por ejemplo, los protocolos como el HTTP, admiten el envío de páginas Web a dispositivos finales. SMTP y POP admiten el envío y la recepción de correo electrónico. SMB y FTP permiten compartir archivos a los usuarios. Las aplicaciones P2P facilitan a los consumidores la tarea de compartir medios sin inconvenientes de una manera distribuida. DNS resuelve los nombres utilizados para referirse a los recursos de red en direcciones numéricas utilizables por la red. Las nubes son ubicaciones ascendentes remotas que almacenan datos y aplicaciones host, de modo que los usuarios no requieran tantos recursos locales y para que puedan acceder al contenido sin inconvenientes desde distintos dispositivos en cualquier ubicación.

Todos estos elementos funcionan conjuntamente, en la capa de aplicación. La capa de aplicación permite que los usuarios trabajen y jueguen a través de Internet.



Capítulo 11: Es una red 11.0.1.1 Introducción

Hasta este punto en el curso, hemos considerado los servicios que una red de datos puede proporcionar a la red humana, hemos examinado las características de cada capa del modelo OSI y las operaciones de los protocolos TCP/IP y observamos en detalle Ethernet, una tecnología LAN universal. El siguiente paso consiste en aprender cómo reunir estos elementos para formar una red que funcione y se pueda mantener.



Capítulo 11: Es una red 11.0.1.2 Actividad: ¿Se dio cuenta?

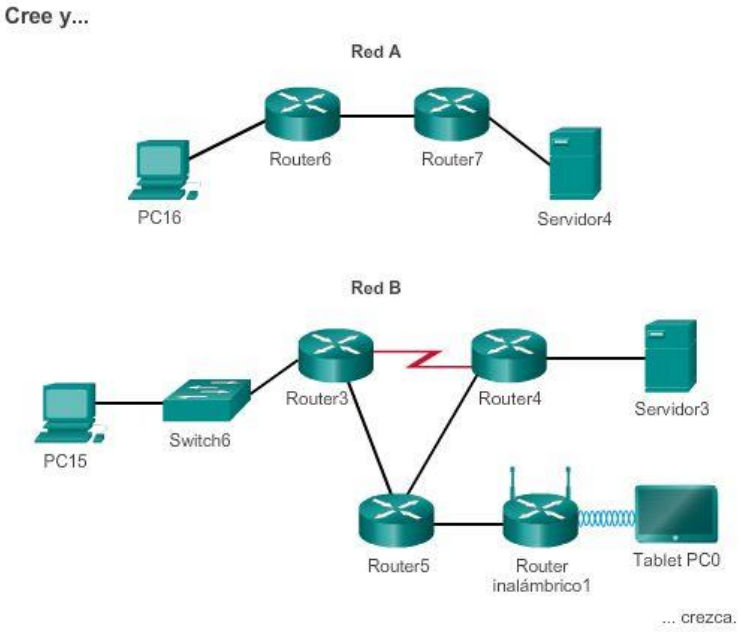
¿Se dio cuenta?

Nota: los estudiantes pueden trabajar de forma individual, de a dos o todos juntos para completar esta actividad.

Observe las dos redes en el diagrama. Compare y contraste visualmente las dos redes. Tome nota de los dispositivos utilizados en cada diseño de red. Dado que los dispositivos están rotulados, ya sabe qué tipos de dispositivos finales e intermediarios hay en cada red.

Pero ¿en qué se diferencian las dos redes? ¿Son distintas simplemente en que hay más dispositivos en la red B que en la red A?

Seleccione la red que utilizaría si fuera dueño de una pequeña o mediana empresa. Debe poder justificar su elección sobre la base del costo, la velocidad, los puertos, las posibilidades de expansión y la facilidad de administración.



Capítulo 11: Es una red 11.1.1.1 Topologías de redes pequeñas

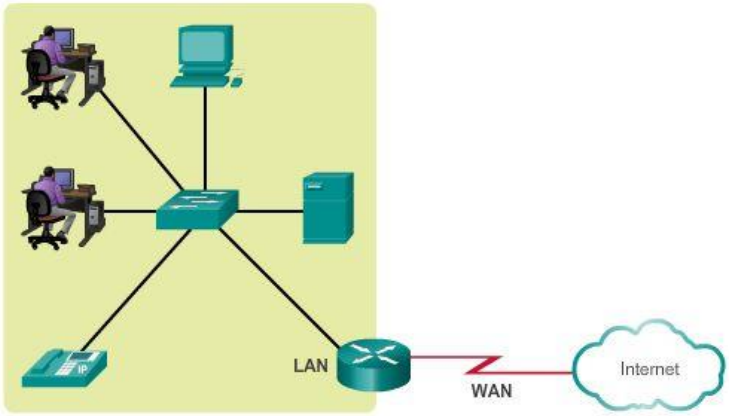
La mayoría de las empresas son pequeñas empresas. Por lo tanto, es de esperarse que la mayoría de las redes sean redes pequeñas.

En las redes pequeñas, el diseño de la red suele ser simple. La cantidad y el tipo de dispositivos en la red se reducen considerablemente en comparación con una red más grande. En general, las topologías de red para las redes pequeñas constan de un único router y uno o más switches. Las redes pequeñas también pueden tener puntos de acceso inalámbrico (posiblemente incorporados al router) y teléfonos IP. En cuanto a la conexión a Internet, las redes pequeñas normalmente tienen una única conexión WAN proporcionada por una conexión DSL, por cable o Ethernet.

La administración de una red pequeña requiere muchas de las mismas habilidades necesarias para administrar redes más grandes. La mayor parte del trabajo se centra en el mantenimiento y la resolución de problemas de equipos existentes, así como en la protección de los dispositivos y de la información de la red. La administración de las redes pequeñas está a cargo de un empleado de la compañía o de una persona contratada por esta, según el tamaño de la empresa y el tipo de actividad que realice.

En la ilustración, se muestra la típica red de una pequeña empresa.

Red típica de una pequeña empresa



Capítulo 11: Es una red 11.1.1.2 Selección de dispositivos para redes pequeñas

Para cumplir con los requisitos de los usuarios, incluso las redes pequeñas requieren planificación y diseño. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación.

Una de las primeras consideraciones de diseño al implementar una red pequeña es el tipo de dispositivos intermediarios que se utilizarán para dar soporte a la red. Al elegir el tipo de dispositivos intermediarios, se deben tener en cuenta varios factores, como se muestra en la ilustración.

Costo

Generalmente, el costo es uno de los factores más importantes al seleccionar equipos para la red de una pequeña empresa. El costo de un switch o un router se determina sobre la base de sus capacidades y características. La capacidad del dispositivo incluye la cantidad y los tipos de puertos disponibles, además de la velocidad de backplane.

Otros factores que afectan el costo son las capacidades de administración de red, las tecnologías de seguridad incorporadas y las tecnologías de conmutación avanzadas optativas. También se debe tener en cuenta el costo del tendido de cable necesario para conectar cada dispositivo de la red. Otro elemento clave que afecta la consideración del costo es la cantidad de redundancia que se debe incorporar a la red; esto incluye los dispositivos, los puertos por dispositivo y el cableado de cobre o fibra óptica.

Velocidad y tipos de puertos e interfaces

Elegir la cantidad y el tipo de puertos en un router o un switch es una decisión fundamental. Las preguntas que se deben hacer incluyen las siguientes: “¿Pedimos los puertos suficientes para satisfacer las necesidades actuales o tenemos en cuenta los requisitos de crecimiento?”, “¿necesitamos una mezcla de velocidades UTP?” y “¿necesitamos puertos UTP y de fibra?”.

Las PC más modernas tienen NIC de 1 Gbps incorporadas. Algunos servidores y estaciones de trabajo ya vienen con puertos de 10 Gbps incorporados. Si bien es más costoso, elegir dispositivos de capa 2 que puedan admitir velocidades mayores permite que la red evolucione sin reemplazar los dispositivos centrales.

Capacidad de expansión

Los dispositivos de red incluyen configuraciones físicas modulares y fijas. Las configuraciones fijas tienen un tipo y una cantidad específica de puertos o interfaces. Los dispositivos modulares tienen ranuras de expansión que proporcionan la flexibilidad necesaria para agregar nuevos módulos a medida que aumentan los requisitos. La mayoría de estos dispositivos incluyen una cantidad básica de puertos fijos además de ranuras de expansión. Existen switches con puertos adicionales especiales para uplinks de alta velocidad optativos. Asimismo, se debe tener el cuidado de seleccionar las interfaces y los módulos adecuados para los medios específicos, ya que los routers pueden utilizarse para conectar diferentes cantidades y tipos de redes. Las preguntas que se deben tener en cuenta incluyen las siguientes: “¿Pedimos dispositivos con módulos que se puedan actualizar?” y “¿qué tipos de interfaces WAN se requieren en los routers (si son necesarias)?”.

Características y servicios de los sistemas operativos

Según la versión del sistema operativo, los dispositivos de red pueden admitir determinados servicios y características, por ejemplo:

- Seguridad
- QoS
- VoIP
- Conmutación de Capa 3
- NAT
- DHCP

Los routers pueden ser costosos según las interfaces y las características necesarias. Los módulos adicionales, como la fibra óptica, aumentan el costo de los dispositivos de red.

Factores que se deben considerar al elegir un dispositivo

Capítulo 11: Es una red 11.1.1.3 Direccionamiento IP para redes pequeñas

Al implementar una red pequeña, es necesario planificar el espacio de direccionamiento IP. Todos los hosts dentro de una internetwork deben tener una dirección exclusiva. Incluso en una red pequeña, la asignación de direcciones dentro de la red no debe ser aleatoria.

En lugar de esto, se debe planificar, registrar y mantener un esquema de direccionamiento IP basado en el tipo de dispositivo que recibe la dirección.

Los siguientes son ejemplos de diferentes tipos de dispositivos que afectan el diseño de IP:

- Dispositivos finales para usuarios
- Servidores y periféricos
- Hosts a los que se accede desde Internet
- Dispositivos intermediaries

La planificación y el registro del esquema de direccionamiento IP ayudan al administrador a realizar un seguimiento de los tipos de dispositivos. Por ejemplo, si se asigna una dirección de host entre los rangos 50 y 100 a todos los servidores, resulta fácil identificar el tráfico de servidores por dirección IP. Esto puede resultar muy útil al llevar a cabo la resolución de problemas de tráfico de la red mediante un analizador de protocolos.

Además, los administradores pueden controlar mejor el acceso a los recursos de la red sobre la base de las direcciones IP cuando se utiliza un esquema de direccionamiento IP determinista. Esto puede ser especialmente importante para los hosts que proporcionan recursos a la red interna y la red externa.

Los servidores Web o los servidores de e-commerce cumplen dicha función. Si las direcciones para estos recursos no son planificadas y documentadas, no es posible controlar fácilmente la seguridad y accesibilidad de los dispositivos. Si se asigna una dirección aleatoria a un servidor, resulta difícil bloquear el acceso a esta dirección, y es posible que los clientes no puedan localizar ese recurso.

Cada uno de estos diferentes tipos de dispositivos debería asignarse a un bloque lógico de direcciones dentro del rango de direcciones de la red.

Planificación y asignación de direcciones IPv4

Capítulo 11: Es una red 11.1.1.4 Redundancia en redes pequeñas

Otra parte importante del diseño de red es la confiabilidad. Incluso las pequeñas empresas con frecuencia dependen en gran medida de la red para su operación. Una falla en la red puede tener consecuencias muy costosas. Para mantener un alto grado de confiabilidad, se requiere redundancia en el diseño de red. La redundancia ayuda a eliminar puntos de error únicos. Existen muchas formas de obtener redundancia en una red. La redundancia se puede obtener mediante la instalación de equipos duplicados, pero también se puede obtener al suministrar enlaces de red duplicados en áreas fundamentales, como se muestra en la ilustración.

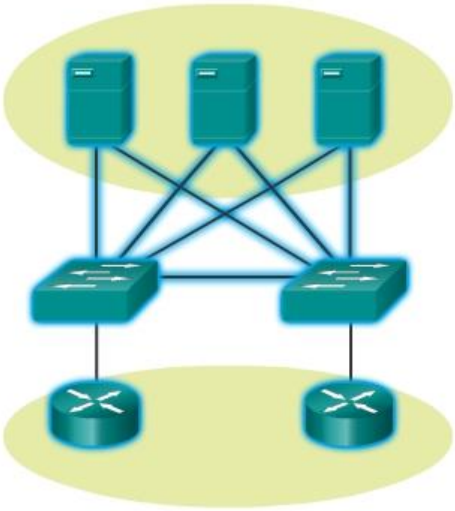
Cuanto más pequeña es la red, menor es la posibilidad de que la redundancia de los equipos sea accesible. Por lo tanto, un método frecuente para incorporar redundancia consiste en el uso de conexiones de switch redundantes entre varios switches en la red, y entre switches y routers.

Además, los servidores suelen tener varios puertos de NIC que habilitan conexiones redundantes a uno o más switches. En las redes pequeñas, los servidores generalmente se implementan como servidores Web, servidores de archivos o servidores de correo electrónico.

Por lo general, las redes pequeñas proporcionan un único punto de salida a Internet a través de uno o más gateways predeterminados.

Con un router en la topología, la única redundancia en términos de rutas de capa 3 se obtiene utilizando más de una interfaz Ethernet interna en el router. Sin embargo, si el router falla, toda la red pierde la conectividad a Internet. Por este motivo, puede ser recomendable para las pequeñas empresas contratar una cuenta con una opción de menor costo a un segundo proveedor de servicios a modo de respaldo.

Redundancia a una granja de servidores



Haga clic en los dispositivos y las conexiones resaltados en azul para obtener más información.

Capítulo 11: Es una red 11.1.1.5 Consideraciones de diseño para una red pequeña

Los usuarios esperan un acceso inmediato a sus correos electrónicos y a los archivos que están compartiendo o actualizando. Para contribuir al aseguramiento de esta disponibilidad, el diseñador de la red debe llevar a cabo los siguientes pasos:

Paso 1. Aportar seguridad a los servidores de archivos y de correo en una ubicación centralizada.
Paso 2. Proteger la ubicación contra el acceso no autorizado mediante la implementación de medidas de seguridad lógica y física.
Paso 3. Crear redundancia en la granja de servidores para asegurar que no se pierdan los archivos si falla un dispositivo.
Paso 4. Configurar rutas redundantes a los servidores.

Además, en las redes modernas suelen utilizarse alguna forma de video o voz sobre IP para comunicarse con los clientes y los socios comerciales. Este tipo de red convergente se implementa como solución integrada o como forma adicional de datos sin procesar superpuestos en la red IP. El administrador de red debe tener en

cuenta los diversos tipos de tráfico y su tratamiento en el diseño de la red. Los routers y switches en una red pequeña se deben configurar para admitir el tráfico en tiempo real, como voz y video, de forma independiente del tráfico de otros datos. De hecho, un buen diseño de red clasifica el tráfico cuidadosamente según la prioridad, como se muestra en la ilustración. Las clases de tráfico pueden ser tan específicas como las siguientes:

- Transferencia de archivos
- Correo electrónico
- Voz
- Video
- Mensajería
- Transaccional

En definitiva, el objetivo de un buen diseño de red, incluso para una red pequeña, es aumentar la productividad de los empleados y reducir el tiempo de inactividad de la red.

La puesta en cola según prioridad se compone de cuatro colas. La cola de prioridad alta siempre se vacía primero.

Capítulo 11: Es una red 11.1.2.1 Aplicaciones comunes en redes pequeñas

La utilidad de las redes depende de las aplicaciones que se encuentren en ellas. Como se muestra en la ilustración, dentro de la capa de aplicación hay dos formas de procesos o programas de software que proporcionan acceso a la red: las aplicaciones de red y los servicios de la capa de aplicación.

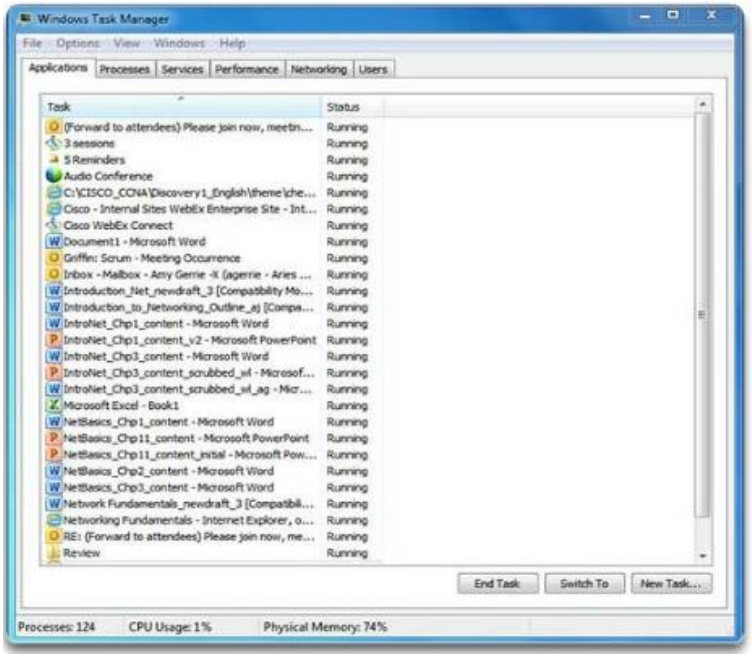
Aplicaciones de red

Las aplicaciones son los programas de software que se utilizan para comunicarse a través de la red. Algunas aplicaciones de usuario final reconocen la red, lo que significa que implementan los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los exploradores Web son ejemplos de este tipo de aplicaciones.

Servicios de la capa de aplicación

Otros programas pueden necesitar la asistencia de los servicios de la capa de aplicación para utilizar recursos de red, como la transferencia de archivos o la administración de las colas de impresión en la red. Si bien el empleado no se da cuenta, estos servicios son los programas que interactúan con la red y preparan los datos para la transferencia. Los distintos tipos de datos, ya sean de texto, gráficos o video, requieren distintos servicios de red para asegurar que estén correctamente preparados para que los procesen las funciones que se encuentran en las capas inferiores del modelo OSI.

Cada servicio de red o aplicación utiliza protocolos que definen los estándares y los formatos de datos que se deben utilizar. Sin protocolos, la red de datos no tendría una manera común de formatear y direccionar los datos. Es necesario familiarizarse con los protocolos subyacentes que rigen la operación de los diferentes servicios de red para entender su función.



Capítulo 11: Es una red 11.1.2.2 Protocolos comunes de una red pequeña

La mayor parte del trabajo de un técnico, ya sea en una red pequeña o una red grande, está relacionada de alguna manera con los protocolos de red.

Los protocolos de red admiten los servicios y aplicaciones que usan los empleados en una red pequeña. Los protocolos de red comunes incluyen los siguientes:

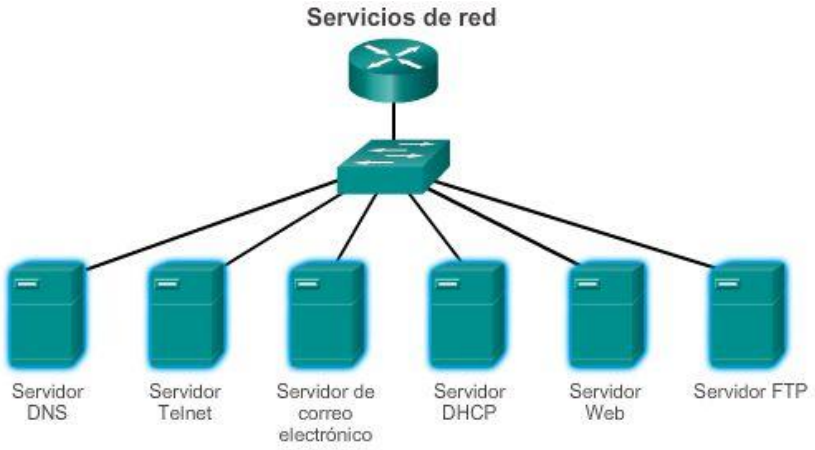
- DNS
- Telnet
- IMAP, SMTP, POP (correo electrónico)
- DHCP
- HTTP
- FTP

Haga clic en los servidores de la ilustración para ver una descripción breve de los servicios de red que proporciona cada uno.

Estos protocolos de red conforman el conjunto de herramientas fundamental de los profesionales de red. Cada uno de estos protocolos de red define lo siguiente:

- Procesos en cualquier extremo de una sesión de comunicación.
- Tipos de mensajes.
- Sintaxis de los mensajes.
- Significado de los campos informativos.
- Cómo se envían los mensajes y la respuesta esperada.
- Interacción con la capa inferior siguiente.

Muchas compañías establecieron una política de utilización de versiones seguras de estos protocolos, siempre que sea posible. Estos protocolos son HTTPS, SFTP y SSH.



Capítulo 11: Es una red 11.1.2.3 Aplicaciones en tiempo real para redes pequeñas

Además de los protocolos de red comunes que se describieron anteriormente, las empresas modernas, incluso las pequeñas, suelen utilizar aplicaciones en tiempo real para comunicarse con los clientes y los socios. Si bien es posible que una compañía pequeña no pueda justificar el costo de una solución Cisco Telepresence para empresas, existen otras aplicaciones en tiempo real, como se muestra en la figura 1, que son accesibles y justificables para las pequeñas empresas. En comparación con otros tipos de datos, las aplicaciones en tiempo real requieren más planificación y servicios dedicados para asegurar la entrega prioritaria del tráfico de voz y de video.

Esto significa que el administrador de red debe asegurarse de que se instalen los equipos adecuados en la red y que se configuren los dispositivos de red para asegurar la entrega según las prioridades. En la figura 2, se muestran elementos de una red pequeña que admiten aplicaciones en tiempo real.

Infraestructura

Para admitir las aplicaciones en tiempo real propuestas y existentes, la infraestructura debe adaptarse a las características de cada tipo de tráfico. El diseñador de red debe determinar si los switches y el cableado existentes pueden admitir el tráfico que se agregará a la red. El cableado que puede admitir transmisiones en gigabits debe ser capaz de transportar el tráfico generado sin necesitar ningún cambio en la infraestructura. Los switches más antiguos quizás no admitan alimentación por Ethernet (PoE). El cableado obsoleto quizás no admita los requisitos de ancho de banda. Los switches y el cableado necesitarán ser actualizados para admitir estas aplicaciones.

VoIP

VoIP se implementa en organizaciones que todavía utilizan teléfonos tradicionales. VoIP utiliza routers con capacidades de voz. Estos routers convierten la voz analógica de señales telefónicas tradicionales en paquetes IP. Una vez que las señales se convierten en paquetes IP, el router envía dichos paquetes entre las ubicaciones correspondientes. VoIP es mucho más económico que una solución de telefonía IP integrada, pero la calidad de las comunicaciones no cumple con los mismos estándares. Las soluciones de video y voz sobre IP para pequeñas empresas pueden consistir, por ejemplo, en Skype y en las versiones no empresariales de Cisco WebEx.

Telefonía IP

En la telefonía IP, el teléfono IP propiamente dicho realiza la conversión de voz a IP. En las redes con solución de telefonía IP integrada, no se requieren routers con capacidades de voz. Los teléfonos IP utilizan un servidor dedicado para el control y la señalización de llamadas. En la actualidad, existen numerosos proveedores que ofrecen soluciones de telefonía IP dedicada para redes pequeñas.

Aplicaciones en tiempo real

Para transportar streaming media de manera eficaz, la red debe ser capaz de admitir aplicaciones que requieran entrega dependiente del factor tiempo. El Protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol) y el Protocolo de control de transporte en tiempo real (RTCP, Real-Time Transport Control Protocol) admiten este requisito. RTP y RTCP habilitan el control y la escalabilidad de los recursos de red al permitir la incorporación de mecanismos de calidad de servicio (QoS). Estos mecanismos de QoS proporcionan herramientas valiosas para minimizar problemas de latencia en aplicaciones de streaming en tiempo real.

Capítulo 11: Es una red 11.1.3.1 Escalamiento de redes pequeñas

El crecimiento es un proceso natural para muchas pequeñas empresas, y sus redes deben crecer en consecuencia. El administrador de una red pequeña trabajará de forma reactiva o proactiva, según la mentalidad de los directores de la compañía, que a menudo incluyen al administrador de red. En forma ideal, el administrador de red tiene un plazo suficiente para tomar decisiones inteligentes acerca del crecimiento de la red con relación al crecimiento de la compañía.

Para escalar una red, se requieren varios elementos:

- Documentación de la red: topología física y lógica.
- Inventario de dispositivos: lista de dispositivos que utilizan o conforman la red.
- Presupuesto: presupuesto de TI detallado, incluido el presupuesto de adquisición de equipos para el año fiscal.
- Análisis de tráfico: se deben registrar los protocolos, las aplicaciones, los servicios y sus respectivos requisitos de tráfico.

Estos elementos se utilizan para fundamentar la toma de decisiones que acompaña el escalamiento de una red pequeña.

Capítulo 11: Es una red 11.1.3.2 Análisis de protocolos de redes pequeñas

Para admitir y ampliar una red pequeña, se necesita estar familiarizado con los protocolos y las aplicaciones de red que se ejecutan en ella. Si bien en entornos de redes pequeñas los administradores tienen más tiempo para analizar individualmente el uso de la red por parte de cada dispositivo, se recomienda un enfoque más integral con algún tipo de analizador de protocolos basado en software o hardware.

Como se muestra en la ilustración, los analizadores de protocolos permiten que los profesionales de red recopilen información estadística sobre los flujos de tráfico en una red rápidamente.

Al intentar determinar cómo administrar el tráfico de la red, en especial a medida que esta crece, es importante comprender el tipo de tráfico que atraviesa la red y el flujo de tráfico actual. Si se desconocen los tipos de tráfico, el analizador de protocolos ayuda a identificar el tráfico y su origen.

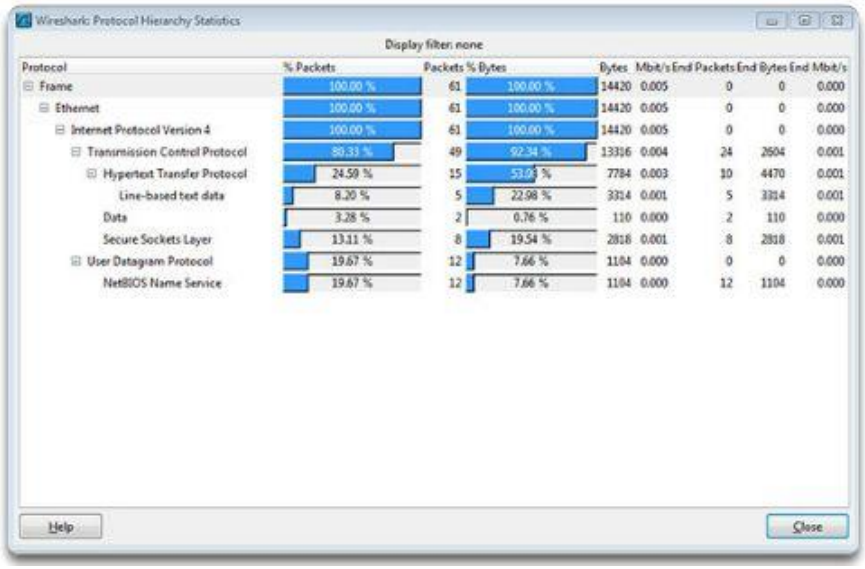
Para determinar patrones de flujo de tráfico, es importante:

- Capturar tráfico en horas de uso pico para obtener una buena representación de los diferentes tipos de tráfico.

- Realizar la captura en diferentes segmentos de la red porque parte del tráfico es local en un segmento en particular.

La información recopilada por el analizador de protocolos se analiza de acuerdo con el origen y el destino del tráfico, y con el tipo de tráfico que se envía. Este análisis puede utilizarse para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente. Para hacerlo, se pueden reducir los flujos de tráfico innecesarios o modificar completamente los patrones de flujo mediante el traslado de un servidor, por ejemplo.

En ocasiones, simplemente reubicar un servidor o un servicio en otro segmento de red mejora el rendimiento de la red y permite adaptarse a las necesidades del tráfico creciente. Otras veces, la optimización del rendimiento de la red requiere el rediseño y la intervención de la red principal.



Capítulo 11: Es una red 11.1.3.3 Evolución de los requisitos de los protocolos

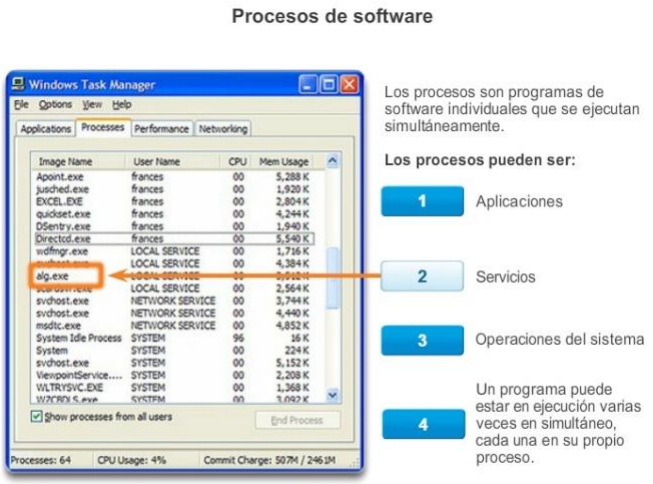
Además de comprender las tendencias cambiantes del tráfico, los administradores de red también deben ser conscientes de cómo cambia el uso de la red. Como se muestra en la ilustración, los administradores de redes pequeñas tienen la capacidad de obtener “instantáneas” de TI en persona del uso de aplicaciones por parte de los empleados para una porción considerable de la fuerza laboral a través del tiempo. Generalmente, estas instantáneas incluyen la siguiente información:

- OS y versión del OS
- Aplicaciones Non-Network
- Aplicaciones de red
- Uso de CPU
- Utilización de unidades
- Utilización de RAM

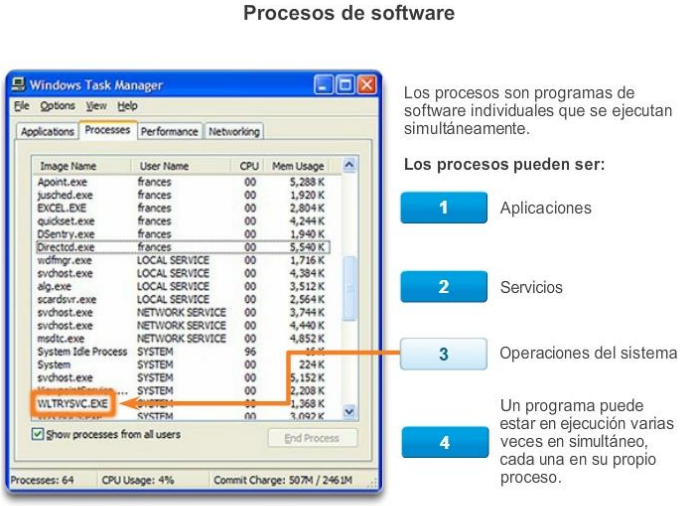
El registro de instantáneas de los empleados en una red pequeña durante un período determinado resulta muy útil para informar al administrador de red sobre la evolución de los requisitos de los protocolos y los flujos de tráfico relacionados. Por ejemplo, es posible que algunos empleados utilicen recursos externos, como los medios sociales, para posicionar mejor una compañía en términos de marketing. Cuando estos empleados comenzaron a trabajar para la compañía, es posible que no le hayan dado tanta importancia a la publicidad basada en Internet. Este cambio en la utilización de recursos puede requerir que el administrador de red cambie la asignación de los recursos de red en consecuencia.

Es responsabilidad del administrador de red realizar un seguimiento de los requisitos de utilización y de flujo de tráfico de la red, e implementar modificaciones en la red para optimizar la productividad de los empleados a medida que la red y la empresa crecen.

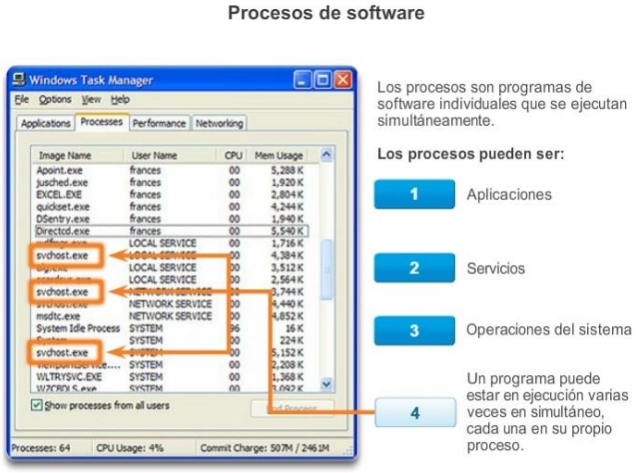
Ejemplos de procesos en ejecución en el sistema operativo Windows



Ejemplos de procesos en ejecución en el sistema operativo Windows



Ejemplos de procesos en ejecución en el sistema operativo Windows



Ejemplos de procesos en ejecución en el sistema operativo Windows

Capítulo 11: Es una red 11.2.1.1 Categorías de amenazas a la seguridad de red

Ya sean redes conectadas por cable o inalámbricas, las redes de computadoras son cada vez más fundamentales para las actividades cotidianas. Tanto las personas como las organizaciones dependen de las PC y las redes. Las intrusiones de personas no autorizadas pueden causar interrupciones costosas en la red y pérdidas de trabajo. Los ataques a una red pueden ser devastadores y pueden causar pérdida de tiempo y de dinero debido a los daños o robos de información o de activos importantes.

Los intrusos pueden acceder a una red a través de vulnerabilidades de software, ataques de hardware o descifrando el nombre de usuario y la contraseña de alguien. Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software se los denomina piratas informáticos.

Una vez que un pirata informático obtiene acceso a la red, pueden surgir cuatro tipos de amenazas:

- Robo de información
- Robo de identidad
- Pérdida o manipulación de datos
- Interrupción del servicio

Incluso en las redes pequeñas, se deben tener en cuenta las amenazas y vulnerabilidades de seguridad al planificar una implementación de red.

Robo de información

Ingreso no autorizado en una computadora para obtener información confidencial. La información puede utilizarse o venderse con diferentes fines. Por ejemplo, el robo de información exclusiva de propiedad de una organización, como información de investigación y desarrollo.

Pérdida y manipulación de datos

Ingreso no autorizado en una computadora para destruir o alterar registros de datos. Ejemplos de pérdida de datos: el envío de un virus que cambia el formato del disco duro de una PC. Ejemplo de manipulación de datos: ingreso no autorizado a un sistema de registros para modificar información, como el precio de un artículo.

Robo de identidad

Forma de robo de información en la que se roba información personal con el fin de usurpar la identidad de otra persona. Al utilizar esta información, una persona puede obtener documentos legales, solicitar créditos y hacer compras no autorizadas en línea. El robo de identidad es un problema creciente que cuesta miles de millones de dólares al año.

Interrupción del servicio

Evitar que los usuarios legítimos accedan a servicios a los que deberían poder acceder. Ejemplos: ataques por denegación de servicio (DoS) en los servidores, los dispositivos de red o los enlaces de comunicaciones de red.

Capítulo 11: Es una red 11.2.1.2 Seguridad física

Cuando se piensa en seguridad de red, o incluso en seguridad informática, es posible que se piense en atacantes que explotan las vulnerabilidades de software. Una vulnerabilidad igualmente importante es la

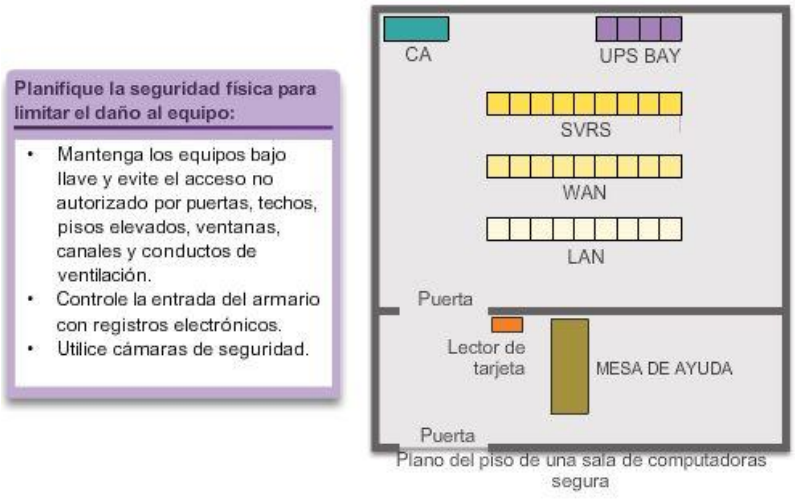
seguridad física de los dispositivos, como se muestra en la ilustración. Si los recursos de red están expuestos a riesgos físicos, un atacante puede denegar el uso de dichos recursos.

Las cuatro clases de amenazas físicas son las siguientes:

- Amenazas de hardware: daño físico a servidores, routers, switches, planta de cableado y estaciones de trabajo
- Amenazas ambientales: extremos de temperatura (demasiado calor o demasiado frío) o extremos de humedad (demasiado húmedo o demasiado seco)
- Amenazas eléctricas: picos de voltaje, suministro de voltaje insuficiente (apagones parciales), alimentación sin acondicionamiento (ruido) y caída total de la alimentación
- Amenazas de mantenimiento: manejo deficiente de componentes eléctricos clave (descarga electrostática), falta de repuestos críticos, cableado y etiquetado deficientes

Algunos de estos problemas se deben abordar en las políticas de la organización. Algunos de ellos dependen de una buena dirección y administración de la organización.

Plan de seguridad física



Capítulo 11: Es una red 11.2.1.3 Tipos de vulnerabilidades de seguridad

Tres factores de seguridad de red son la vulnerabilidad, las amenazas y los ataques.

La vulnerabilidad es el grado de debilidad inherente a cada red y dispositivo. Esto incluye routers, switches, computadoras de escritorio, servidores e, incluso, dispositivos de seguridad.

Las amenazas incluyen a las personas interesadas en aprovechar cada debilidad de seguridad y capacitadas para hacerlo. Es de esperarse que estas personas busquen continuamente nuevas vulnerabilidades y debilidades de seguridad.

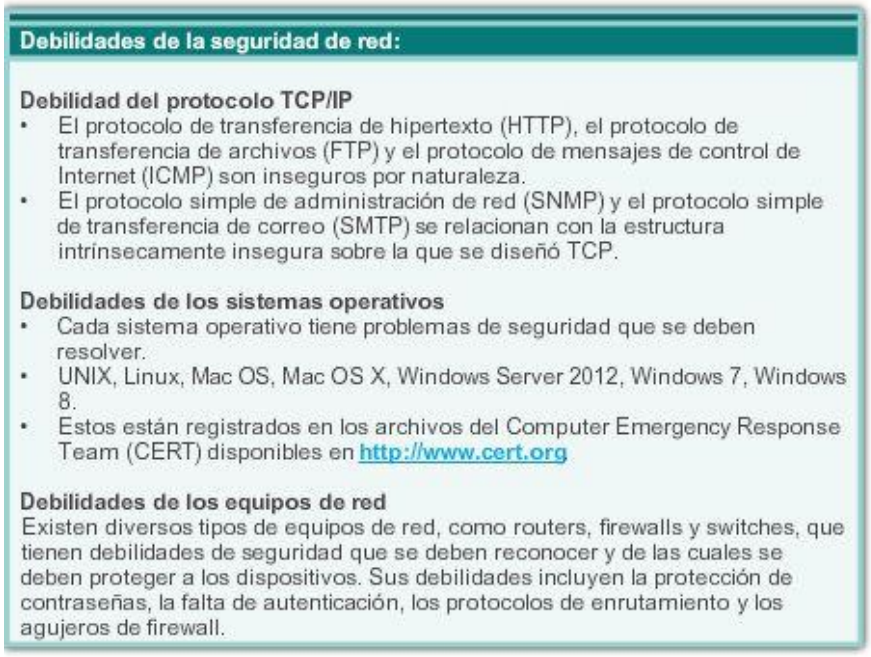
Las amenazas se llevan a cabo con una variedad de herramientas, secuencias de comandos y programas para iniciar ataques contra las redes y los dispositivos de red. Por lo general, los dispositivos de red que sufren ataques son las terminales, como los servidores y las computadoras de escritorio.

Existen tres vulnerabilidades o debilidades principales:

- Tecnológicas, como las que se muestran en la figura 1.
- De configuración, como las que se muestran en la figura 2.
- De política de seguridad, como las que se muestran en la figura 3.

Todas estas vulnerabilidades o debilidades pueden dar origen a diversos ataques, incluidos los ataques de código malintencionado y los ataques de red.

Vulnerabilidades: tecnología



Vulnerabilidades: configuración

Debilidad en la configuración	Cómo se aprovecha la debilidad
Cuentas de usuario no seguras	La información de cuenta de usuario se puede transmitir de manera insegura a través de la red. Esto expone nombres de usuario y contraseñas a los curiosos.
Cuentas del sistema con contraseñas fáciles de adivinar	Este problema común se debe a la elección de contraseñas de usuario deficientes y fáciles de adivinar.
Servicios de Internet mal configurados	Un problema común es activar JavaScript en los exploradores Web, lo que permite ataques mediante scripts hostiles cuando se accede a sitios no confiables. IIS, FTP, y los servicios terminales también constituyen problemas.
Configuraciones predeterminadas no seguras dentro de productos	Muchos productos tienen configuraciones predeterminadas que habilitan los agujeros de seguridad.
Equipos de red mal configurados	Las malas configuraciones del propio equipo pueden causar problemas de seguridad importantes. Por ejemplo, las listas de acceso mal configuradas, los protocolos de enrutamiento o las cadenas comunitarias SNMP pueden abrir enormes agujeros de seguridad.

Vulnerabilidades: política

Debilidad en las políticas	Cómo se aprovecha la debilidad
Falta de políticas de seguridad por escrito	Una política no escrita no se puede aplicar sistemáticamente ni se puede hacer cumplir.
Política	Las batallas políticas y las luchas territoriales pueden dificultar la implementación de una política de seguridad sistemática.
Falta de continuidad de autenticación	Las contraseñas mal elegidas, fáciles de decodificar o las contraseñas predeterminadas pueden permitir accesos no autorizados a la red.
Controles de acceso lógico no aplicados	El monitoreo y la auditoría inadecuados permiten que los ataques y el uso no autorizado continúen. Esto hace que la empresa desperdicie recursos. Esto puede dar origen a acciones legales o despidos de los técnicos de TI, de la administración de TI o, incluso, de los directores de la compañía, que permiten que se continúe trabajando en condiciones poco seguras.
La instalación de software y hardware y los cambios no respetan la política	Los cambios no autorizados que se realizan en la topología de la red o en la instalación de aplicaciones no aprobadas crean agujeros de seguridad.
No existe plan de recuperación de desastres	La falta del plan de recuperación de desastres produce caos, pánico y confusión cuando alguien ataca la empresa.

Capítulo 11: Es una red 11.2.2.1 Virus, gusanos y caballos de Troya

Los ataques de código malintencionado incluyen diversos tipos de programas de PC que se crearon con la intención de causar pérdida de datos o daños a estos. Los tres tipos principales de ataques de código malintencionado son los virus, los caballos de Troya y los gusanos.

Un virus es un tipo de software malintencionado que se asocia a otro programa para ejecutar una función no deseada específica en una estación de trabajo. Un ejemplo es un programa que se asocia a command.com (el intérprete principal para los sistemas Windows), elimina determinados archivos e infecta cualquier otra versión de command.com que pueda encontrar.

Un caballo de Troya solo se diferencia en que toda la aplicación se creó con el fin de que aparente ser otra cosa, cuando en realidad es una herramienta de ataque. Un ejemplo de un caballo de Troya es una aplicación de software que ejecuta un juego simple en una estación de trabajo. Mientras el usuario se entretiene con el juego, el caballo de Troya envía una copia de sí mismo por correo electrónico a cada dirección de la libreta de direcciones del usuario. Los demás usuarios reciben el juego y lo utilizan, por lo que el caballo de Troya se propaga a las direcciones de cada libreta de direcciones.

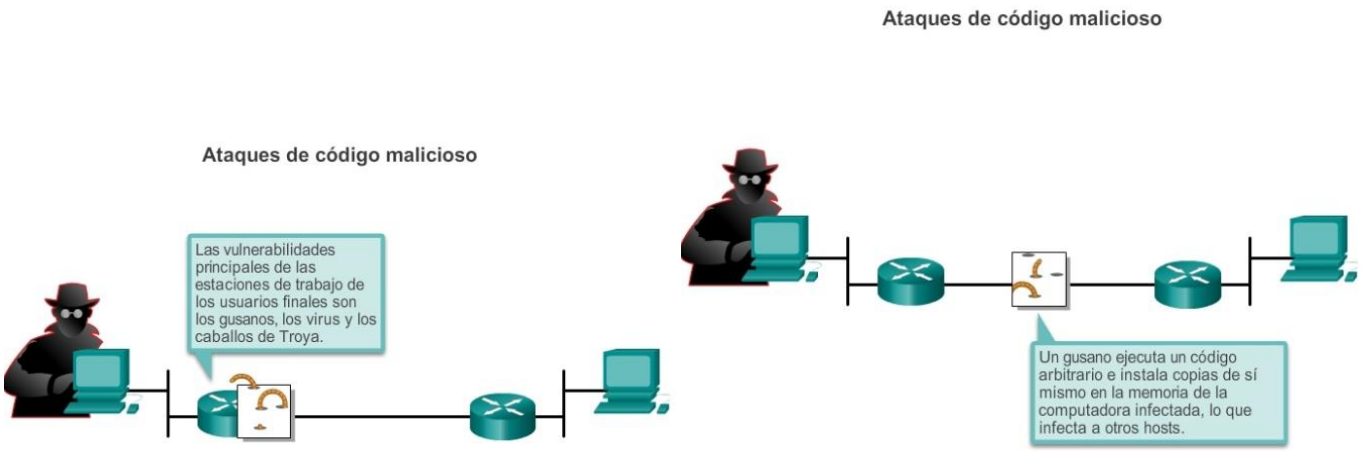
En general, los virus requieren un mecanismo de entrega, un vector, como un archivo zip o algún otro archivo ejecutable adjunto a un correo electrónico, para transportar el código del virus de un sistema a otro. El elemento clave que distingue a un gusano de PC de un virus de computadora es que se requiere interacción humana para facilitar la propagación de un virus.

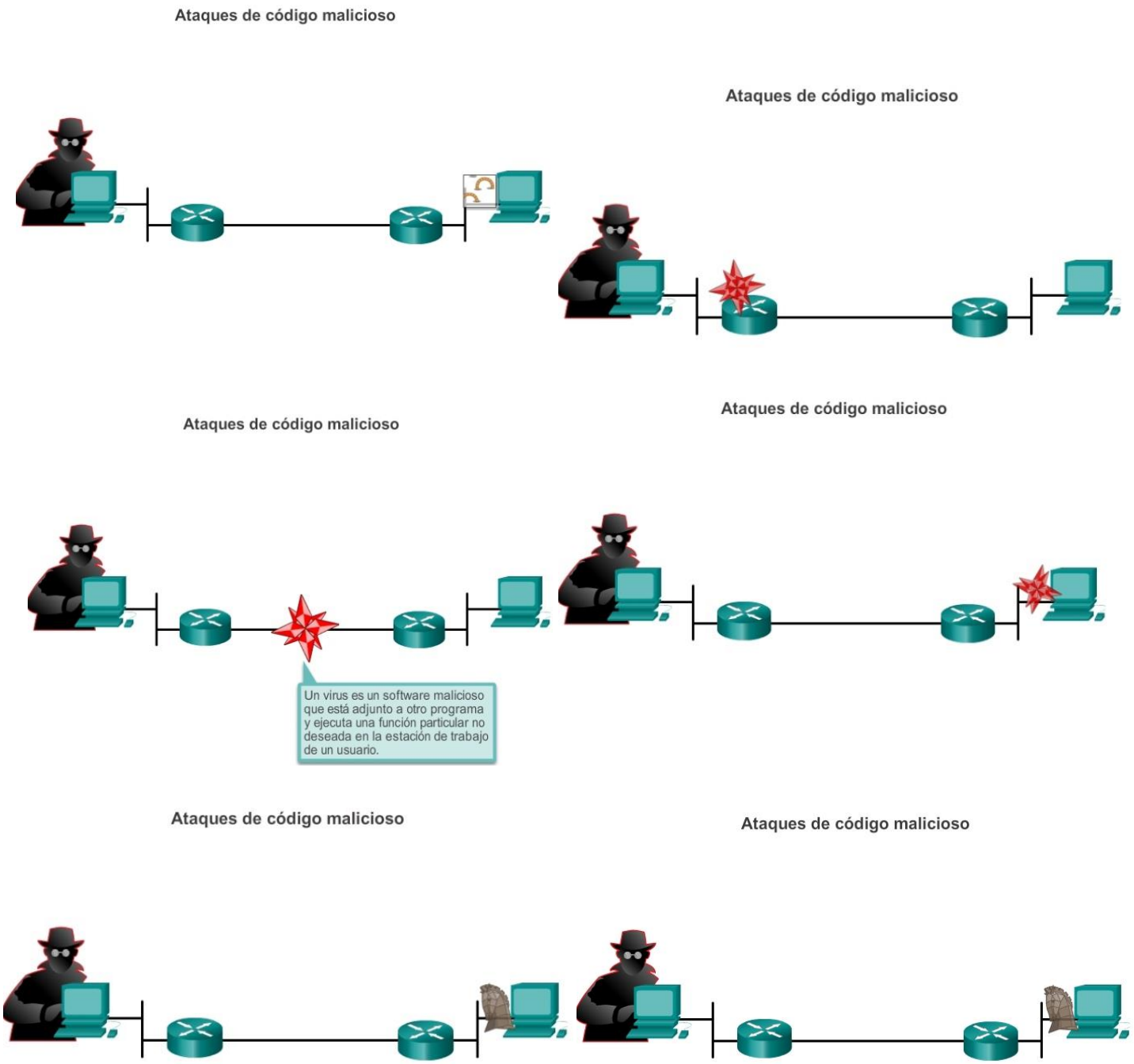
Los gusanos son programas autónomos que atacan un sistema e intentan explotar una vulnerabilidad específica del objetivo. Una vez que logra explotar dicha vulnerabilidad, el gusano copia su programa del host atacante al sistema atacado recientemente para volver a iniciar el ciclo. La anatomía de un ataque de gusano es la siguiente:

- Vulnerabilidad habilitadora: el gusano se instala mediante la explotación de las vulnerabilidades conocidas de los sistemas, como usuarios finales ingenuos que abren archivos adjuntos ejecutables sin verificar en los correos electrónicos.

- Mecanismo de propagación: después de obtener acceso a un host, el gusano se copia a dicho host y luego selecciona nuevos objetivos.

- Contenido: una vez que se infectó un host con el gusano, el atacante tiene acceso al host, a menudo como usuario privilegiado. Los atacantes pueden utilizar una vulnerabilidad local para elevar su nivel de privilegio al de administrador.





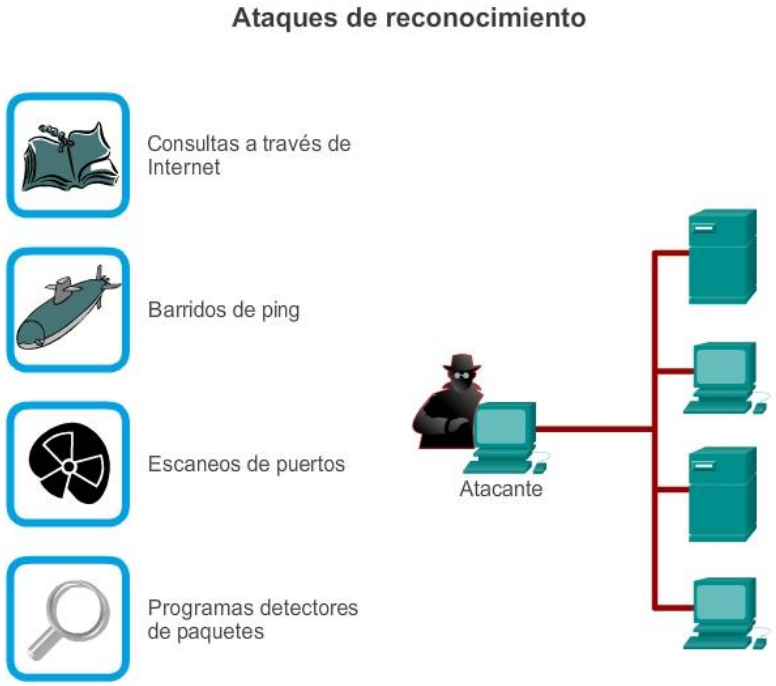
Capítulo 11: Es una red 11.2.2.2 Ataques de reconocimiento

Además de los ataques de código malintencionado, es posible que las redes sean presa de diversos ataques de red. Los ataques de red pueden clasificarse en tres categorías principales:

- Ataques de reconocimiento: detección y esquematización no autorizadas de sistemas, servicios o vulnerabilidades.
- Ataques de acceso: manipulación no autorizada de datos, de accesos al sistema o de privilegios de usuario.
- Denegación de servicio: consisten en desactivar o dañar redes, sistemas o servicios.

Ataques de reconocimiento

Los atacantes externos pueden utilizar herramientas de Internet, como las utilidades nslookup y whois, para determinar fácilmente el espacio de direcciones IP asignado a una empresa o a una entidad determinada. Una vez que se determina el espacio de direcciones IP, un atacante puede hacer ping a las direcciones IP públicamente disponibles para identificar las direcciones que están activas. Para contribuir a la automatización de este paso, un atacante puede utilizar una herramienta de barrido de ping, como fping o gping, que hace ping sistemáticamente a todas las direcciones de red en un rango o una subred determinados. Esto es similar a revisar una sección de una guía telefónica y llamar a cada número para ver quién atiende.



Capítulo 11: Es una red 11.2.2.3 Ataques con acceso

Ataques con acceso

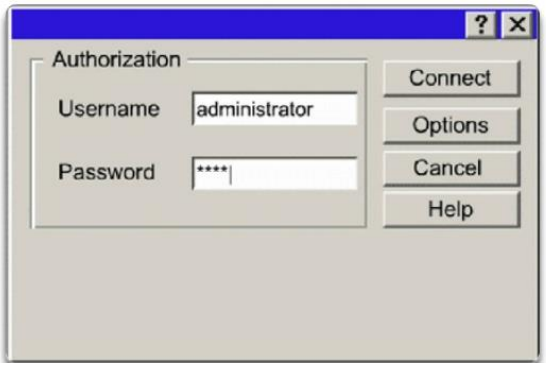
Los ataques de acceso explotan las vulnerabilidades conocidas de los servicios de autenticación, los servicios FTP y los servicios Web para obtener acceso a las cuentas Web, a las bases de datos confidenciales y demás información confidencial. Un ataque de acceso permite que una persona obtenga acceso no autorizado a información que no tiene derecho a ver. Los ataques de acceso pueden clasificarse en cuatro tipos. Uno de los tipos de ataques de acceso más comunes es el ataque a contraseñas. Los ataques a contraseñas se pueden implementar con programas detectores de paquetes para obtener cuentas de usuario y contraseñas que se transmiten como texto no cifrado. Los ataques a contraseñas también pueden referirse a los intentos repetidos de inicio de sesión en un recurso compartido, como un servidor o un router, para identificar una cuenta de usuario, una contraseña o ambas. Estos intentos repetidos se denominan “ataques por diccionario” o “ataques de fuerza bruta”.

Haga clic en los botones de la ilustración para ver ejemplos de ataques de acceso.

Ataque a la contraseña

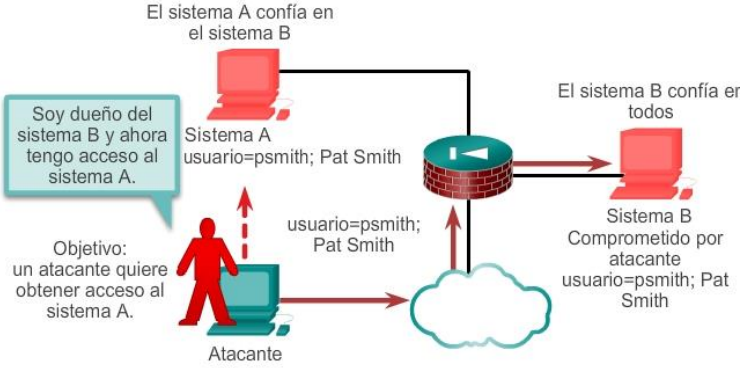
Los atacantes pueden implementar ataques a contraseñas mediante diversos métodos:

- Ataques por fuerza bruta
- Programas de caballos de Troya
- Programas detectores de paquetes



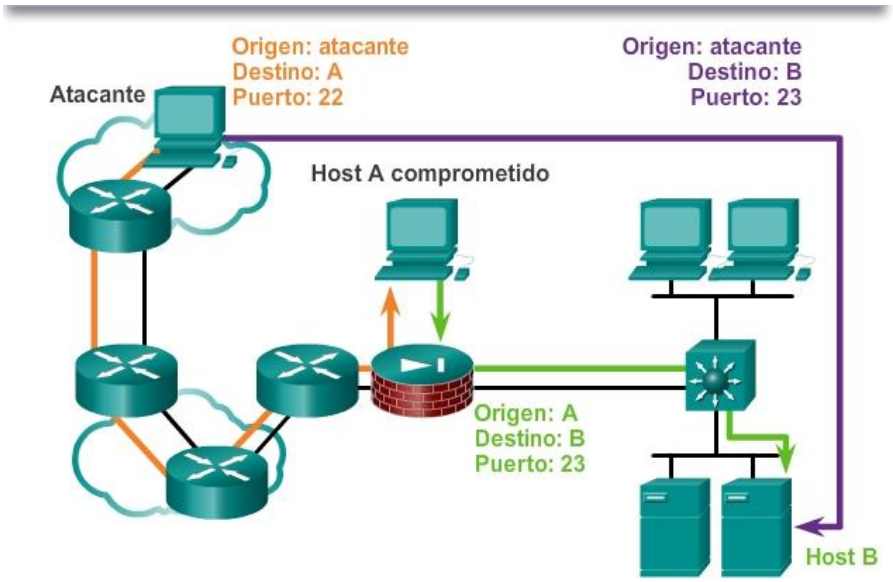
Explotación de confianza

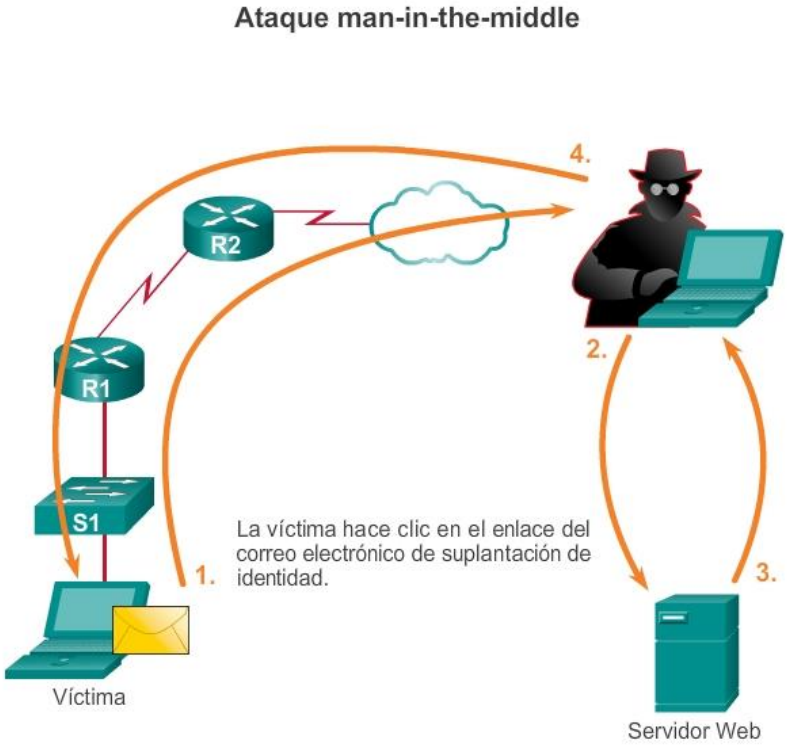
SO de la red	Modelos de confianza
Windows	Dominios Active Directory (AD)
Linux y UNIX	Sistema de archivos de red (NFS, Network File System) Servicio de información de red Plus (NIS+, Network Information Service Plus)



Redirección de puertos

La redirección de puertos es un tipo de ataque de explotación de confianza que utiliza un host comprometido para pasar tráfico que de otra manera se descartaría a través un firewall. Se mitiga principalmente con el uso de modelos de confianza adecuados. Los softwares antivirus y los IDS basados en host pueden ayudar a detectar si un atacante instala utilidades de redirección de puertos en el host y a evitar que esto suceda.





Capítulo 11: Es una red 11.2.2.4 Ataques en DoS

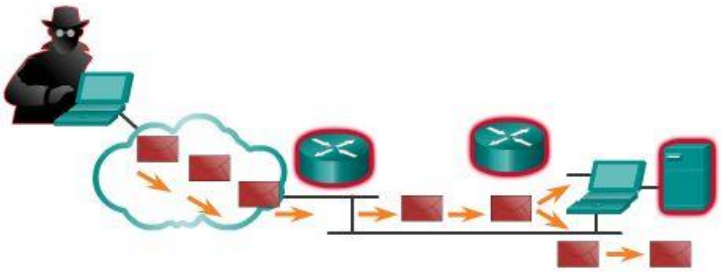
Denegación de servicio

Los ataques DoS son la forma de ataque más conocida y también están entre los más difíciles de eliminar. Incluso dentro de la comunidad de atacantes, los ataques DoS se consideran triviales y están mal vistos, ya que requieren muy poco esfuerzo de ejecución. Sin embargo, debido a la facilidad de implementación y a los daños potencialmente considerables, los administradores de seguridad deben prestar especial atención a los ataques DoS.

Los ataques DoS tienen muchas formas. Fundamentalmente, evitan que las personas autorizadas utilicen un servicio mediante el consumo de recursos del sistema.

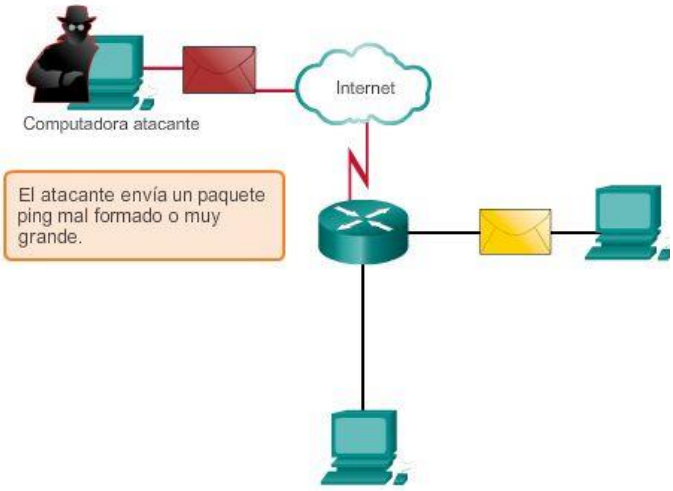
Ataque de DoS

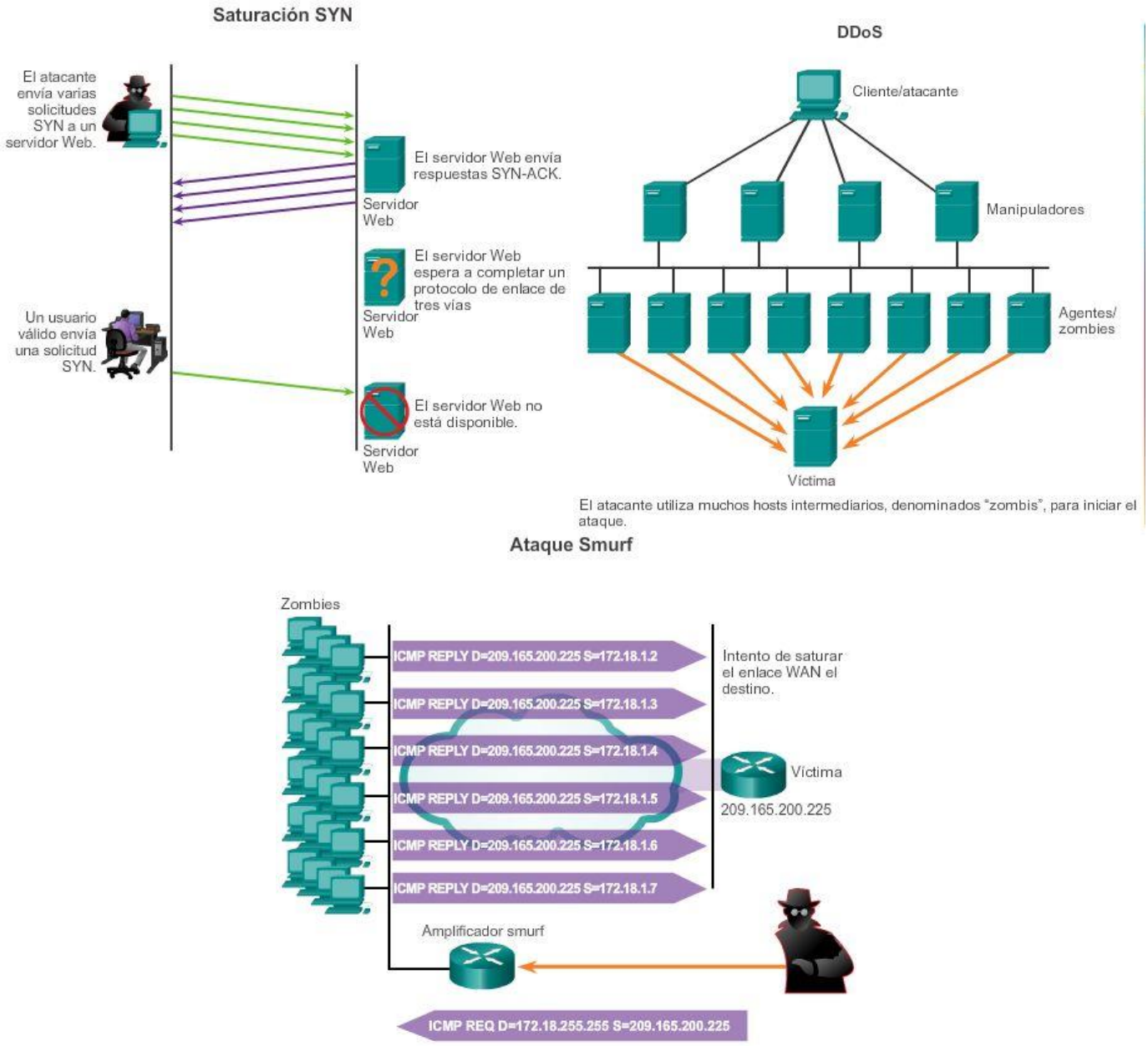
Sobrecargas de recursos	Datos mal formados
Espacio en disco, ancho de banda, búferes	Paquetes de tamaños excesivos como el ping de la muerte
Saturación de ping como el smurf	Paquete superpuesto como el winuke
Tormentas de paquetes como las bombas UDP y fraggle	Datos no gestionados como el teardrop



Los ataques de DoS evitan que el personal autorizado use un servicio mediante la utilización de los recursos del sistema.

Ping de la muerte





Capítulo 11: Es una red 11.2.3.1 Copias de seguridad, actualizaciones y parches

Los softwares antivirus pueden detectar la mayoría de los virus y muchas aplicaciones de caballo de Troya, y evitar que se propaguen en la red. Los softwares antivirus se pueden implementar en el nivel de usuario y en el nivel de red.

Mantenerse actualizado con los últimos avances en estos tipos de ataques también puede contribuir a una defensa más eficaz contra ellos. A medida que se publican nuevas aplicaciones de virus y troyanos, las empresas deben mantenerse al día con actualizaciones a las versiones más recientes de los softwares antivirus.

La mitigación de ataques de gusanos requiere la diligencia del personal de administración de redes y sistemas. Los siguientes son los pasos recomendados para mitigar ataques de gusanos:

- Contención: contenga la propagación del gusano dentro de la red. Divida en secciones las partes no infectadas de la red.

- Inoculación: comience a aplicar parches a todos los sistemas y, si es posible, examine en busca de sistemas vulnerables.

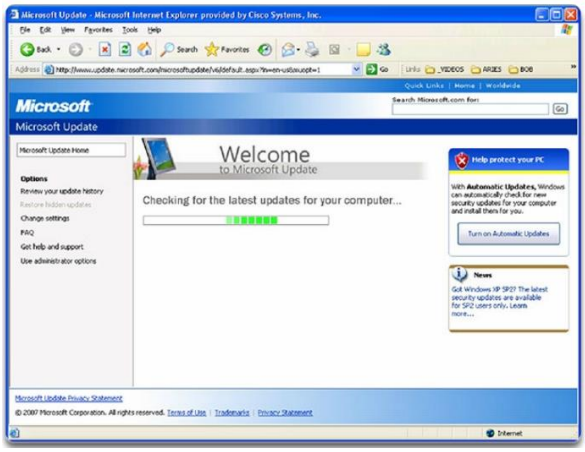
- Cuarentena: realice un seguimiento de todas las máquinas infectadas dentro de la red. Desconecte o quite las máquinas infectadas de la red o bloquéelas.

- Tratamiento: limpie todos los sistemas infectados y aplíqueles parches. Es posible que algunos gusanos requieran la reinstalación completa del sistema central para limpiar el sistema.

La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos los sistemas vulnerables. Esto resulta difícil con los sistemas de usuario no controlados en la red local. La administración de numerosos sistemas implica la creación de una imagen de software estándar (sistema operativo y aplicaciones acreditadas cuyo uso esté autorizado en los sistemas cliente) que se implementa en los sistemas nuevos o actualizados. Sin embargo, los requisitos de seguridad cambian, y es posible que se deban instalar parches de seguridad actualizados en los sistemas que ya están implementados.

Una solución para la administración de parches críticos de seguridad es crear un servidor central de parches con el que deban comunicarse todos los sistemas después de un período establecido, como el que se muestra en la ilustración. Todo parche que no esté aplicado en un host se descarga automáticamente del servidor de parches y se instala sin que intervenga el usuario.

Parches de SO



Capítulo 11: Es una red 11.2.3.2 Autenticación, autorización y contabilidad

Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA o “triple A”) proporcionan el marco principal para configurar el control de acceso en dispositivos de red. AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y observar las acciones que realizan mientras acceden a la red (contabilizar). AAA proporciona un mayor grado de escalabilidad que los comandos de autenticación de EXEC privilegiado, consola, puertos auxiliares y VTY.

Autenticación

Los usuarios y administradores deben probar que son quienes dicen ser. La autenticación se puede establecer utilizando combinaciones de nombre de usuario y contraseña, preguntas de desafío y respuesta, tarjetas token y otros métodos. Por ejemplo: “Soy el usuario ‘estudiante’. Conozco la contraseña para probar que soy el usuario ‘estudiante’”.

En redes pequeñas, se suele utilizar la autenticación local. Con la autenticación local, cada dispositivo mantiene su propia base de datos de combinaciones de nombre de usuario y contraseña.

Sin embargo, cuando hay más de unas pocas cuentas de usuario en la base de datos de un dispositivo local, administrar dichas cuentas puede resultar complejo. Además, a medida que la red crece y se le agregan más dispositivos, la autenticación local se hace difícil de mantener y no se puede escalar. Por ejemplo, si hay 100 dispositivos de red, se deben agregar todas las cuentas de usuario a los 100 dispositivos.

En el caso de redes más grandes, una solución más escalable es la autenticación externa. La autenticación externa permite autenticar a todos los usuarios a través de un servidor de red externo. Las dos opciones más populares para la autenticación externa de usuarios son RADIUS y TACACS+:

- RADIUS es un estándar abierto con poco uso de memoria y recursos de la CPU. Lo utilizan una variedad de dispositivos de red, como switches, routers y dispositivos inalámbricos.

- TACACS+ es un mecanismo de seguridad que habilita servicios modulares de autenticación, autorización y contabilidad. Utiliza un demonio TACACS+ que se ejecuta en un servidor de seguridad.

Autorización

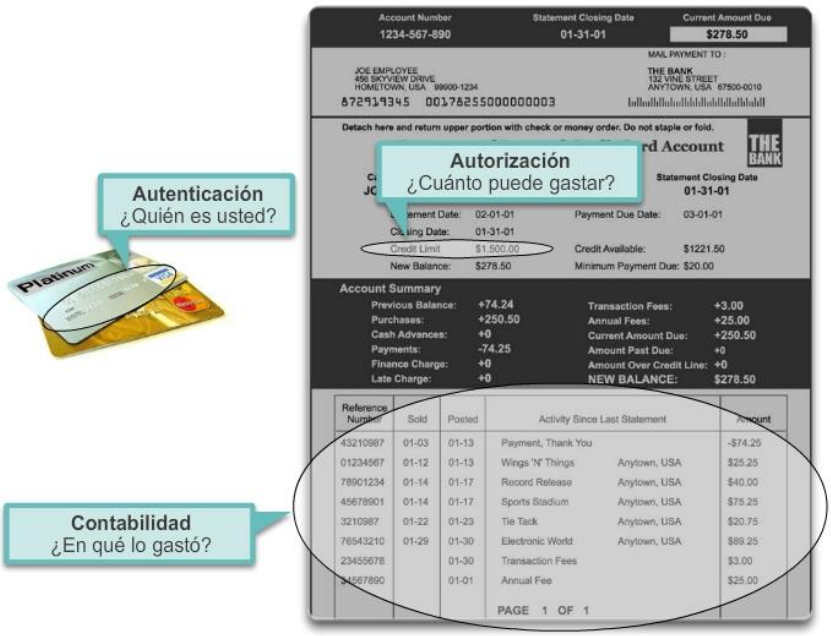
Una vez autenticado el usuario, los servicios de autorización determinan a qué recursos puede acceder el usuario y qué operaciones está habilitado para realizar. Un ejemplo es “El usuario ‘estudiante’ puede acceder al servidor host XYZ mediante Telnet únicamente”.

Contabilidad

La contabilidad registra lo que hace el usuario, incluidos los elementos a los que accede, la cantidad de tiempo que accede al recurso y todos los cambios que se realizaron. La contabilidad realiza un seguimiento de la forma en que se utilizan los recursos de red. Un ejemplo es “El usuario ‘estudiante" accedió al servidor host XYZ mediante Telnet durante 15 minutos”.

El concepto de AAA es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica quién la puede utilizar y cuánto puede gastar ese usuario, y lleva un registro de los elementos en los que el usuario gastó dinero, como se muestra en la ilustración.

El concepto de AAA es similar al uso de una tarjeta de crédito



Capítulo 11: Es una red 11.2.3.3 Firewalls

Además de proteger las computadoras y servidores individuales conectados a la red, es importante controlar el tráfico de entrada y de salida de la red.

El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios internos de la red contra amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas, además de evitar el acceso no autorizado. Los productos de firewall usan diferentes técnicas para determinar qué acceso permitir y qué acceso denegar en una red. Estas técnicas son las siguientes:

- Filtrado de paquetes: evita o permite el acceso según las direcciones IP o MAC.
- Filtrado de aplicaciones: evita o permite el acceso de tipos específicos de aplicaciones según los números de puerto.
- Filtrado de URL: evita o permite el acceso a sitios Web según palabras clave o URL específicos.
- Inspección de paquetes con estado (SPI): los paquetes entrantes deben constituir respuestas legítimas a solicitudes de los hosts internos. Los paquetes no solicitados son bloqueados, a menos que se permitan específicamente. La SPI también puede incluir la capacidad de reconocer y filtrar tipos específicos de ataques, como los ataques por denegación de servicio (DoS).

Los productos de firewall pueden admitir una o más de estas capacidades de filtrado. Además, los firewalls suelen llevar a cabo la traducción de direcciones de red (NAT). La NAT traduce una dirección o un grupo de direcciones IP internas a una dirección IP pública y externa que se envía a través de la red. Esto permite ocultar las direcciones IP internas de los usuarios externos.

Los productos de firewall vienen en distintos formatos, como se muestra en la ilustración.

- Firewalls basados en aplicaciones: un firewall basado en una aplicación es un firewall incorporado en un dispositivo de hardware dedicado, conocido como una aplicación de seguridad.

- Firewalls basados en servidor: un firewall basado en servidor consta de una aplicación de firewall que se ejecuta en un sistema operativo de red (NOS), como UNIX o Windows.

- Firewalls integrados: un firewall integrado se implementa mediante la adición de funcionalidades de firewall a un dispositivo existente, como un router.

- Firewalls personales: los firewalls personales residen en las computadoras host y no están diseñados para implementaciones LAN. Pueden estar disponibles de manera predeterminada en el OS o pueden provenir de un proveedor externo.

Aplicaciones de seguridad de Cisco

Firewall basado en servidor

Router inalámbrico Linksys con firewall integrado

Firewall personal

Aplicaciones de seguridad de Cisco

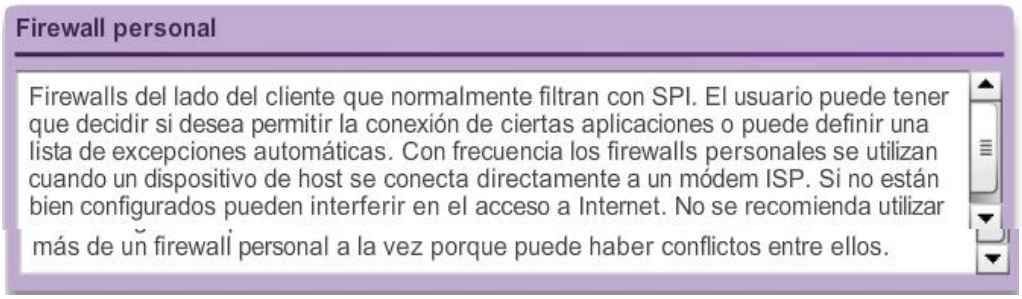
Los dispositivos de firewall dedicados son computadoras especializadas que no tienen periféricos ni discos duros. Los firewalls basados en aplicaciones pueden inspeccionar el tráfico con mayor rapidez y son menos propensos a sufrir fallos.

Firewall basado en servidor

Aplicaciones de firewall que generalmente proporcionan una solución que combina un firewall SPI y control de acceso basado en direcciones IP o aplicaciones. Los firewalls basados en servidor pueden ser menos seguros que los firewalls dedicados basados en dispositivos, debido a los puntos débiles de seguridad de los OS de uso general.

Router inalámbrico Linksys con firewall integrado

La mayoría de los routers integrados domésticos tienen incorporadas capacidades de firewall básicas que admiten el filtrado de paquetes, de aplicaciones y de sitios Web. Los routers más especializados que ejecutan sistemas operativos especiales como el Sistema Operativo de Internetwork de Cisco (IOS) también tienen capacidades de firewall



Capítulo 11: Es una red 11.2.3.4 Seguridad de terminales

Una red es apenas tan segura como su enlace más débil. Las amenazas destacadas que más se analizan en los medios de comunicación son las amenazas externas, como los gusanos de Internet y los ataques DoS. Pero la protección de la red interna es tan importante como la protección del perímetro de una red. La red interna consta de terminales de red, algunas de las cuales se muestran en la ilustración. Una terminal, o un host, es un sistema de computación o un dispositivo individual que actúa como cliente de red. Las terminales comunes son computadoras portátiles, computadoras de escritorio, servidores, smartphones y tablet PC. Si los usuarios no aplican seguridad a los dispositivos terminales, ninguna precaución de seguridad garantizará una red segura.

La seguridad de los dispositivos terminales es uno de los trabajos más desafiantes para un administrador de red, ya que incluye a la naturaleza humana. Las compañías deben aplicar políticas bien documentadas, y los empleados deben estar al tanto de estas reglas. Se debe capacitar a los empleados sobre el uso correcto de la red. En general, estas políticas incluyen el uso de software antivirus y la prevención de intrusión de hosts. Las soluciones más integrales de seguridad de terminales dependen del control de acceso a la red.

La seguridad de terminales también requiere la protección de los dispositivos de capa 2 en la infraestructura de la red, a fin de evitar ataques de capa 2, como los ataques de suplantación de direcciones MAC, los de desbordamiento de la tabla de direcciones MAC y los ataques de saturación de LAN. Esto se conoce como “mitigación de ataques”.

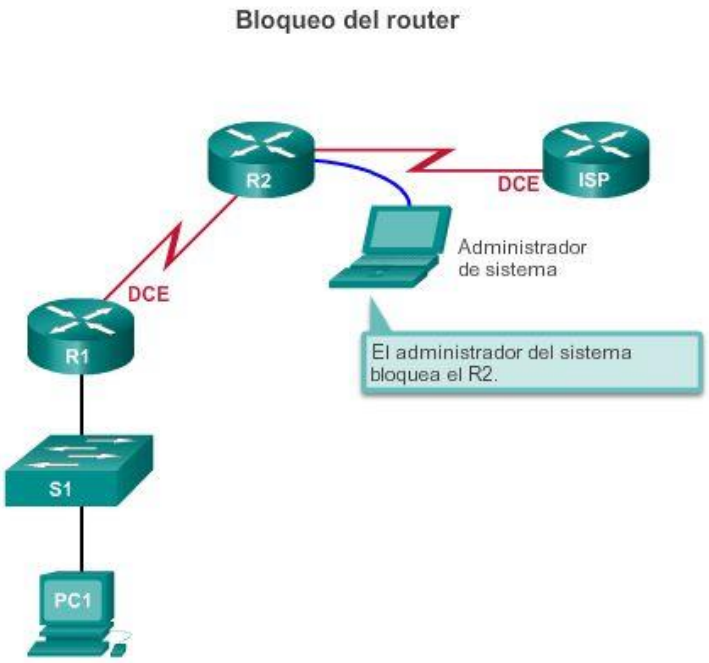
Capítulo 11: Es una red 11.2.4.1 Introducción a la protección de dispositivos

Una parte de la seguridad de la red consiste en proteger los dispositivos propiamente dichos, incluidos los dispositivos finales y los intermediarios, como los dispositivos de red.

Cuando se instala un nuevo sistema operativo en un dispositivo, la configuración de seguridad está establecida en los valores predeterminados. En la mayoría de los casos, ese nivel de seguridad es insuficiente. En los routers Cisco, se puede utilizar la característica Cisco AutoSecure para proteger el sistema, como se describe en la ilustración. Existen algunos pasos simples que se deben seguir y que se aplican a la mayoría de los sistemas operativos:

- Se deben cambiar de inmediato los nombres de usuario y las contraseñas predeterminados.
- Se debe restringir el acceso a los recursos del sistema solamente a las personas que están autorizadas a utilizar dichos recursos.
- Siempre que sea posible, se deben desactivar y desinstalar todos los servicios y las aplicaciones innecesarios.

Se deben actualizar todos los dispositivos con parches de seguridad a medida que estén disponibles. A menudo, los dispositivos enviados por el fabricante pasaron cierto tiempo en un depósito y no tienen los parches más actualizados instalados. Antes de la implementación, es importante actualizar cualquier software e instalar los parches de seguridad.



Capítulo 11: Es una red 11.2.4.2 Contraseñas

Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Las pautas estándar que se deben seguir son las siguientes:

- Utilice una longitud de contraseña de, al menos, ocho caracteres y preferentemente de diez caracteres o más. Cuanto más larga sea, mejor será la contraseña.

- Cree contraseñas complejas. Incluya una combinación de letras mayúsculas y minúsculas, números, símbolos y espacios, si están permitidos.

- Evite las contraseñas basadas en la repetición, las palabras comunes de diccionario, las secuencias de letras o números, los nombres de usuario, los nombres de parientes o mascotas, información biográfica (como fechas de nacimiento), números de identificación, nombres de antepasados u otra información fácilmente identificable.

- Escriba una contraseña con errores de ortografía a propósito. Por ejemplo, Smith = Smyth = 5mYth, o Seguridad = 5egur1dad.

- Cambie las contraseñas con frecuencia. Si se pone en riesgo una contraseña sin saberlo, se limitan las oportunidades para que el atacante la utilice.

- No anote las contraseñas ni las deje en lugares obvios, por ejemplo, en el escritorio o el monitor.

En la ilustración, se muestran ejemplos de contraseñas seguras y no seguras.

En los routers Cisco, se ignoran los espacios iniciales para las contraseñas, pero no se ignoran los espacios que le siguen al primer carácter. Por lo tanto, un método para crear una contraseña segura es utilizar la barra espaciadora en la contraseña y crear una frase compuesta de muchas palabras. Esto se denomina “frase de contraseña”. Una frase de contraseña suele ser más fácil de recordar que una contraseña simple. Además, es más larga y más difícil de descifrar.

Los administradores deben asegurarse de que se utilicen contraseñas seguras en toda la red. Una forma de lograr esto es utilizar las mismas herramientas de ataque por “fuerza bruta” que utilizan los atacantes como método para verificar la seguridad de la contraseña.

Contraseñas seguras y no seguras

Contraseña no segura	Por qué no es segura
secreto	Contraseña simple de diccionario
smith	Apellido de soltera de la madre
toyota	Marca de automóvil
bob1967	Nombre y cumpleaños de un usuario
Blueleaf23	Palabras y números simples

Contraseña segura	Por qué es segura
b67n42d39c	Combina caracteres alfanuméricos
12^h u4@1p7	Combina caracteres alfanuméricos, símbolos y además incluye un espacio

Capítulo 11: Es una red 11.2.4.3 Prácticas de seguridad básicas

Al implementar dispositivos, es importante seguir todas las pautas de seguridad establecidas por la organización. Esto incluye la denominación de dispositivos de tal manera que facilite las tareas de registro y seguimiento, pero que también mantenga algún tipo de seguridad. No se recomienda proporcionar demasiada

información sobre el uso del dispositivo en el nombre de host. Existen muchas otras medidas básicas de seguridad que se deben implementar.

Seguridad adicional de contraseñas

Las contraseñas seguras resultan útiles en la medida en que sean secretas. Se pueden tomar diversas medidas para asegurar que las contraseñas sigan siendo secretas. Mediante el comando de configuración global service password-encryption, se evita que las personas no autorizadas vean las contraseñas como texto no cifrado en el archivo de configuración, como se muestra en la ilustración. Este comando provoca la encriptación de todas las contraseñas sin encriptar.

Además, para asegurar que todas las contraseñas configuradas tengan una longitud mínima específica, utilice el comando security passwords min-length del modo de configuración global.

Otra forma en la que los piratas informáticos descubren las contraseñas es simplemente mediante ataques de fuerza bruta, es decir, probando varias contraseñas hasta que una funcione. Es posible evitar este tipo de ataques si se bloquean los intentos de inicio de sesión en el dispositivo cuando se produce una determinada cantidad de errores en un lapso específico.

Router(config)# login block-for 120 attempts 3 within 60

Este comando bloquea los intentos de inicio de sesión durante 120 segundos si hay tres intentos de inicio de sesión fallidos en 60 segundos.

Mensajes

Los mensajes de aviso son similares a los avisos de prohibición de entrada. Son importantes para poder demandar en un tribunal a cualquiera que acceda al sistema de forma inapropiada. Asegúrese de que los mensajes de aviso cumplan con las políticas de seguridad de la organización.

Router(config)# banner motd #message#

Exec Timeout

Otra recomendación es configurar tiempos de espera de ejecución.

Al configurar el tiempo de espera de ejecución, le ordena al dispositivo Cisco que desconecte automáticamente a los usuarios en una línea después de que hayan estado inactivos durante el valor de tiempo de espera de ejecución. Los tiempos de espera de ejecución se pueden configurar en los puertos de consola, vty y auxiliares.

Router(config)# line vty 0 4

Router(config-vty)# exec-timeout 10

Este comando desconecta a los usuarios después de 10 minutos.

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 exec-timeout 10
 login
```

Capítulo 11: Es una red 11.2.4.4 Activar SSH

Acceso remoto mediante SSH

El antiguo protocolo para administrar dispositivos de manera remota es Telnet. Telnet no es seguro. Los datos contenidos en un paquete Telnet se transmiten sin encriptar. Mediante una herramienta como Wireshark, es posible que alguien detecte una sesión de Telnet y obtenga información de contraseñas. Por este motivo, se recomienda especialmente habilitar SSH en los dispositivos para obtener un método de acceso remoto seguro. Es posible configurar un dispositivo Cisco para que admita SSH mediante cuatro pasos, como se muestra en la ilustración.

Paso 1. Asegúrese de que el router tenga un nombre de host exclusivo y configure el nombre de dominio IP de la red mediante el comando ip domain-name *nombre-de-dominio* en el modo de configuración global.

Paso 2. Se deben generar claves secretas unidireccionales para que un router encripte el tráfico SSH. La clave es precisamente lo que se utiliza para encriptar y descifrar datos. Para crear una clave de encriptación, utilice el comando crypto key generate rsa general-keys modulus *tamaño-del-módulo* en el modo de configuración global.

El significado específico de las distintas partes de este comando es complejo y excede el ámbito de este curso, pero de momento, simplemente tenga en cuenta que el módulo determina el tamaño de la clave y se puede configurar con un valor de 360 a 2048 bits. Cuanto más grande es el módulo, más segura es la clave, pero más se tarda en encriptar y descifrar la información. La longitud mínima de módulo recomendada es de 1024 bits.

Router(config)# crypto key generate rsa general-keys modulus 1024

Paso 3. Cree una entrada de nombre de usuario en la base de datos local mediante el comando username*nombre* secret *secreto* del modo de configuración global.

Paso 4. Habilite las sesiones SSH entrantes por vty mediante los comandos line vty login local ytransport input ssh.

Ahora se puede acceder al servicio SSH del router mediante un software de cliente SSH.


```
R1#conf t
R1(config)#ip domain-name span.com
R1(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#username Bob secret cisco
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

Paso 1. Configurar el nombre de dominio IP.
Paso 2. Generar claves secretas unidireccionales.
Paso 3. Verificar o crear una entrada de base de datos local.
Paso 4. Habilitar las sesiones SSH entrantes por VTY.

Capítulo 11: Es una red 11.3.1.1 Interpretación de los resultados de ping

Una vez que se implementa la red, el administrador debe poder probar la conectividad de red para asegurarse de que funcione correctamente. Además, se recomienda que el administrador de red realice un registro de la red.

El comando ping

El comando ping es una manera eficaz de probar la conectividad. Por lo general, a esta prueba se la conoce como “prueba del stack de protocolos”, porque el comando ping va desde la capa 3 del modelo OSI hasta la capa 2 y, luego, hasta la capa 1. Este comando utiliza el protocolo ICMP para verificar la conectividad.

El comando ping no siempre identifica la naturaleza de un problema, pero puede contribuir a identificar su origen, un primer paso importante en la resolución de problemas de una falla de red.

El comando ping proporciona un método para probar el stack de protocolos y la configuración de direcciones IPv4 en un host, así como para probar la conectividad a los hosts de destino local o remoto, como se muestra en la ilustración. Existen herramientas adicionales que pueden proporcionar más información que el ping, como Telnet o Trace, las cuales serán analizadas luego en mayor profundidad.

Indicadores de ping IOS

Un ping emitido desde el IOS tiene como resultado una de varias indicaciones para cada eco ICMP enviado. Los indicadores más comunes son:

- ! : indica la recepción de un mensaje de respuesta de eco ICMP.
- . : indica que se agotó el tiempo mientras se esperaba un mensaje de respuesta de eco ICMP.

- U: se recibió un mensaje ICMP inalcanzable.

El signo “!” (signo de exclamación) indica que el ping se completó correctamente y verifica la conectividad de capa 3.

El "." (punto) puede indicar problemas en la comunicación. Puede señalar que se produjo un problema de conectividad en alguna parte de la ruta. También puede indicar que un router de la ruta no contaba con una ruta hacia el destino y no envió un mensaje de ICMP de destino inalcanzable. También puede señalar que el ping fue bloqueado por la seguridad del dispositivo.

La “U” indica que un router de la ruta no contaba con una ruta hacia la dirección de destino o que se bloqueó la solicitud de ping y se respondió con un mensaje de ICMP de destino inalcanzable.

Prueba de loopback

El comando ping se utiliza para verificar la configuración IP interna en el host local. Recuerde que esta prueba se realiza utilizando el comando ping en una dirección reservada denominada “dirección de loopback” (127.0.0.1). Esto verifica que el stack de protocolos funcione correctamente desde la capa de red hasta la capa física y viceversa, sin colocar realmente una señal en los medios.

Los comandos ping se introducen en una línea de comandos.

Utilice la siguiente sintaxis para hacer ping a la dirección de loopback:

C:\> ping 127.0.0.1

La respuesta de este comando se parecería a ésta:

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Respuesta desde 127.0.0.1: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 127.0.0.1:

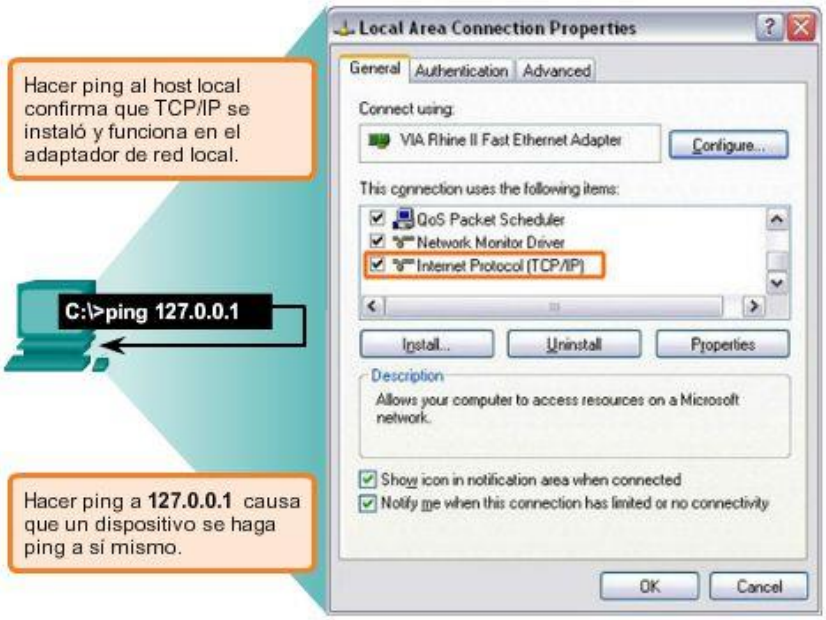
Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),

Tiempo aproximado de ida y vuelta en milisegundos:

Mínimo = 0ms, Máximo = 0ms, Media = 0ms

El resultado indica que se enviaron cuatro paquetes de prueba de 32 bytes desde el host 127.0.0.1 y se devolvieron a este en un tiempo de menos de 1 ms. TTL son las siglas de tiempo de vida, que define la cantidad de saltos que le restan al paquete ping antes de que se descarte.

Prueba del stack de TCP/IP local



Capítulo 11: Es una red 11.3.1.2 Ping extendido

Cisco IOS ofrece un modo “extendido” del comando ping. Se ingresa a este modo escribiendo “ping” (sin las comillas) en el modo EXEC privilegiado, sin una dirección IP de destino. Luego, se presenta una serie de peticiones de entrada, como se muestra en el siguiente ejemplo. Al presionar Intro se aceptan los valores predeterminados indicados.

El siguiente ejemplo muestra cómo forzar que la dirección de origen para un ping sea 10.1.1.1 (observe el R2 en la ilustración); la dirección de origen para un ping estándar sería 209.165.200.226. De esta manera, el administrador de red puede verificar de forma remota (desde el R2) que el R1 tenga la ruta 10.1.1.0/24 en su tabla de enrutamiento.

R2# ping

Protocol [ip]:

Target IP address: 192.168.10.1

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: y

Source address or interface: 10.1.1.1

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

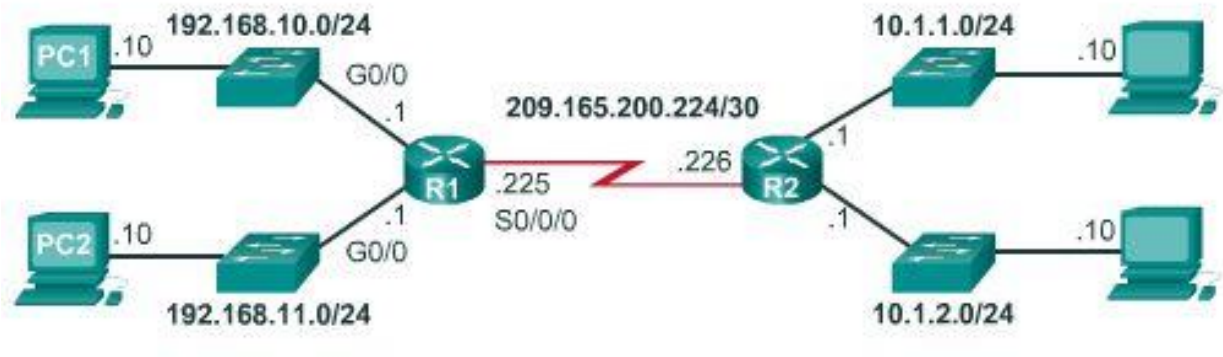
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/97/132 ms

Al ingresar un período de tiempo de espera más prolongado que el predeterminado, se podrán detectar posibles problemas de latencia. Si la prueba de ping es exitosa con un valor superior, existe una conexión entre los hosts, pero es posible que haya un problema de latencia en la red.

Tenga en cuenta que introducir “y” en la petición de entrada “Extended commands” (Comandos extendidos) proporciona más opciones que resultar útiles para la resolución de problemas.



Capítulo 11: Es una red 11.3.1.3 Línea base de red

Una de las herramientas más efectivas para controlar y resolver problemas relacionados con el rendimiento de la red es establecer una línea de base de red. Una línea de base es un proceso para estudiar la red en intervalos regulares a fin de asegurar que la red funciona según su diseño.

Una línea de base de red es más que un simple informe que detalla el estado de la red en determinado momento. La creación de una línea de base efectiva del rendimiento de la red se logra con el tiempo. La medición del rendimiento en distintos momentos (figuras 1 y 2) y con distintas cargas ayuda a tener una idea más precisa del rendimiento general de la red.

El resultado que deriva de los comandos de la red puede aportar datos a la línea de base de red.

Un método para iniciar una línea de base es copiar y pegar en un archivo de texto los resultados de los comandos ping, trace u otro comando relevante. Estos archivos de texto pueden tener grabada la fecha y la hora y pueden guardarse en un archivo para su posterior recuperación.

Un uso eficaz de la información almacenada consiste en comparar los resultados en el transcurso del tiempo (figura 3). Entre los elementos que se deben considerar se encuentran los mensajes de error y los tiempos de respuesta de host a host. Si se observa un aumento considerable de los tiempos de respuesta, es posible que exista un problema de latencia para considerar.

No bastan las palabras para destacar la importancia de crear documentación. La verificación de la conectividad de host a host, los problemas de latencia y las resoluciones de problemas identificados puede ayudar a un administrador de red a mantener el funcionamiento más eficiente posible de la red.

Las redes corporativas deben tener líneas de base extensas; más extensas de lo que podemos describir en este curso.

Existen herramientas de software a nivel profesional para almacenar y mantener información de línea de base. En este curso, solo se abarcan algunas técnicas básicas y se analiza el propósito de las líneas de base.

Las prácticas recomendadas para los procesos de línea de base se pueden encontrar aquí.

La captura del resultado del comando ping también se puede completar desde la petición de entrada del IOS, como se muestra en la figura 4.

Ejecute la misma prueba

8 de febrero de 2013, 08:14:43

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

17 de marzo de 2013, 14:41:06

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

En diferentes momentos

8 de febrero de 2013, 08:14:43

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

17 de marzo de 2013, 14:41:06

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Compare valores

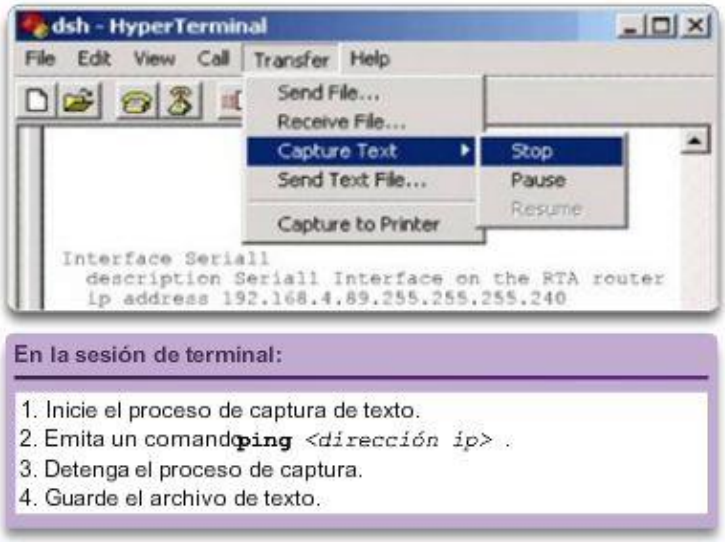
8 de febrero de 2013, 08:14:43

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

17 de marzo de 2013, 14:41:06

```
C:\>ping 10.66.254.159

Pinging 10.66.254.159 with 32 bytes of data:

Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128

Ping statistics for 10.66.254.159:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Cómo guardar una captura de ping del router en un archivo de texto



Capítulo 11: Es una red 11.3.2.1 Interpretación de mensajes de tracert

Un rastreo proporciona una lista de saltos cuando un paquete se enruta a través de una red. La forma del comando depende de dónde se emita el comando. Cuando lleve a cabo el rastreo desde un equipo Windows, utilice tracert. Cuando lleve a cabo el rastreo desde la CLI de un router, utilice traceroute, como se muestra en la figura 1.

Al igual que los comandos ping, los comandos trace se introducen en la línea de comandos y llevan una dirección IP como argumento.

Aquí, sobre la base de que el comando se emite desde un equipo Windows, se utiliza la forma tracert:

C:\> tracert 10.1.0.2

Traza a 10.1.0.2 sobre caminos de 30 saltos como máximo

1 2 ms 2 ms 2 ms 10.0.0.254

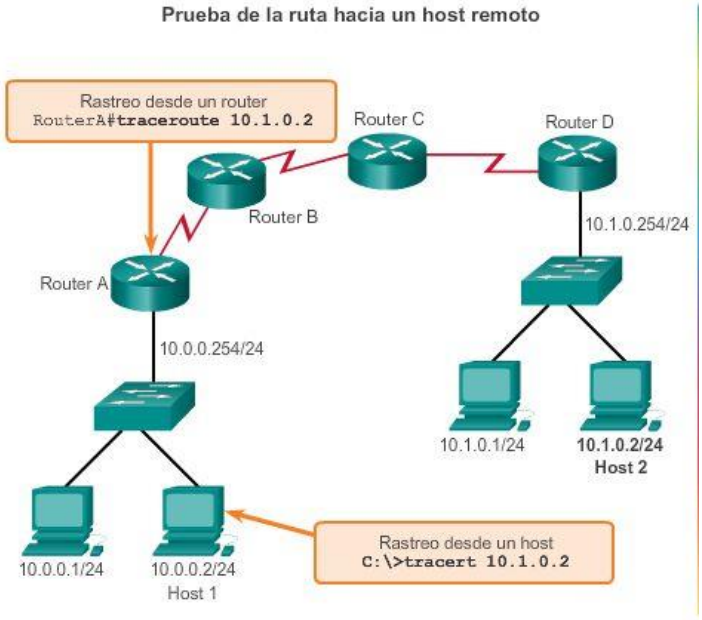
2 * * * Tiempo de espera agotado.

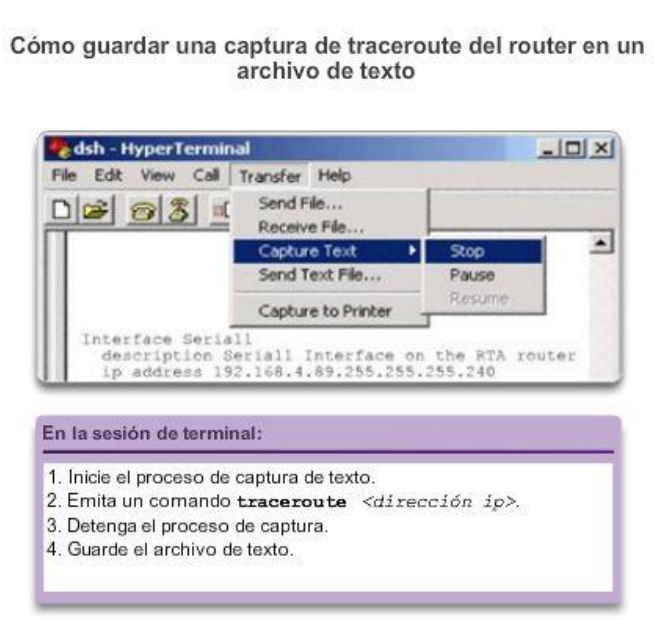
3 * * * Tiempo de espera agotado.

4 ^C

La única respuesta correcta fue la del gateway del router A. El tiempo de espera para las solicitudes de trace se agotó, lo que significa que el router de siguiente salto no respondió. Los resultados del comando trace indican que la falla entonces se encuentra en la internetwork más allá de la LAN.

La captura del resultado del comando traceroute también se puede realizar desde la petición de entrada del router, como se muestra en la figura 2.





Capítulo 11: Es una red 11.3.3.1 Repaso de comandos show comunes

Los comandos show de la CLI de Cisco IOS muestran información importante sobre la configuración y el funcionamiento del dispositivo.

Los técnicos de red utilizan los comandos show con frecuencia para ver los archivos de configuración, revisar el estado de los procesos y las interfaces del dispositivo, y verificar el estado de funcionamiento del dispositivo. Los comandos show están disponibles independientemente de si el dispositivo se configuró utilizando la CLI o Cisco Configuration Professional.

Se puede mostrar el estado de casi todos los procesos o funciones del router mediante un comando show. Algunos de los comandos show más conocidos son:

- show running-config (figura 1).
- show interfaces (figura 2).
- show arp (figura 3).
- show ip route (figura 4).
- show protocols (figura 5)
- show version (figura 6)

Show running-config

```
R1#show running-config
 <Resultado omitido>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
 description LAN 192.168.1.0 default gateway
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
```

Show interfaces

```
R1#show interfaces
 <Resultado omitido>
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e
  (bia 001b.5325.256e)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:17, output 00:00:01, 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
```

Show arp

```
R1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.17.0.1             -   001b.5325.256e  ARPA
FastEthernet0/0
Internet  172.17.0.2            12   000b.db04.a5cd  ARPA
FastEthernet0/0
```

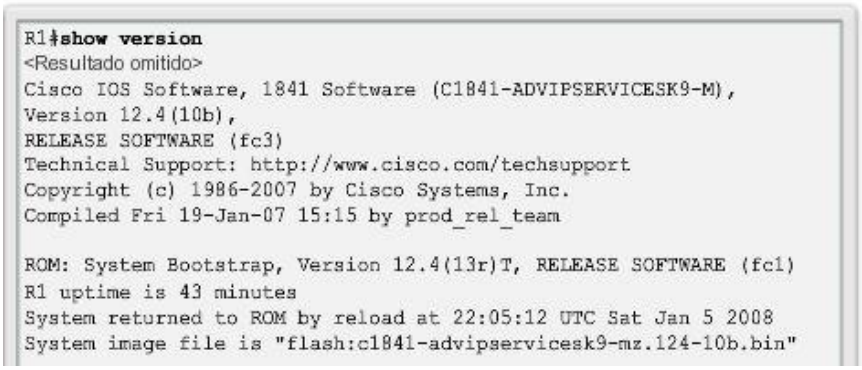
Show ip route

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

Gateway of last resort is not set
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
R    192.168.3.0/24 [120/1] via 192.168.2.2, 00:00:24, Serial0/0/0
```

Show protocols

```
R1#show protocols
Global values:
  Internet Protocol routing is enabled
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.1/24
FastEthernet0/1 is administratively down, line protocol is down
FastEthernet0/1/0 is up, line protocol is down
FastEthernet0/1/1 is up, line protocol is down
FastEthernet0/1/2 is up, line protocol is down
FastEthernet0/1/3 is up, line protocol is down
Serial0/0/0 is up, line protocol is up
  Internet address is 192.168.2.1/24
Serial0/0/1 is administratively down, line protocol is down
Vlan1 is up, line protocol is down
```

Show version



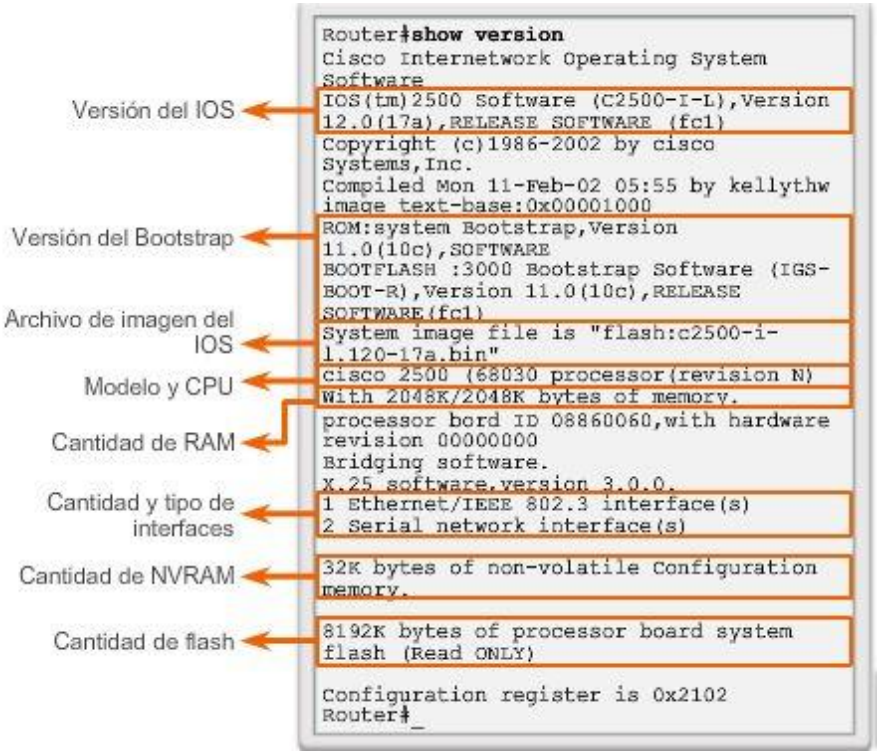
Capítulo 11: Es una red 11.3.3.2 Visualización de la configuración del router mediante el comando show versión

Una vez que se carga el archivo de configuración de inicio y el router arranca correctamente, se puede utilizar el comando show version para verificar y resolver los problemas de algunos de los componentes básicos de hardware y software que se utilizan durante el proceso de arranque. El resultado del comando show versionincluye lo siguiente:

- La versión del software Cisco IOS que se está utilizando.
- La versión del software bootstrap del sistema almacenado en la memoria ROM que se utilizó inicialmente para arrancar el router.
- El nombre de archivo completo de la imagen IOS de Cisco y dónde lo colocó el programa bootstrap.
- El tipo de CPU del router y la cantidad de RAM. Es posible que resulte necesario actualizar la cantidad de RAM cuando se actualice el software Cisco IOS.
- La cantidad y el tipo de las interfases físicas del router.
- La cantidad de NVRAM. La NVRAM se utiliza para almacenar el archivo startup-config.
- La cantidad de memoria flash del router. Es posible que resulte necesario actualizar la cantidad de flash cuando se actualice el software Cisco IOS.
- El valor configurado actualmente del registro de configuración del software en formato hexadecimal.

Haga clic en Reproducir en la ilustración para ver una animación sobre la manera de identificar estas características del resultado de show version.

El registro de configuración le dice al router cómo iniciarse. Por ejemplo, la configuración predeterminada de fábrica para el registro de configuración es 0x2102. Este valor indica que el router intenta cargar una imagen del software Cisco IOS desde la memoria flash y carga el archivo de configuración de inicio desde la NVRAM. Es posible cambiar el registro de configuración y, por ende, cambiar dónde busca el router la imagen IOS de Cisco y el archivo de configuración de inicio durante el proceso de arranque. Si hay un segundo valor entre paréntesis se implica el valor del registro de configuración que se debe utilizar durante la siguiente recarga del router.

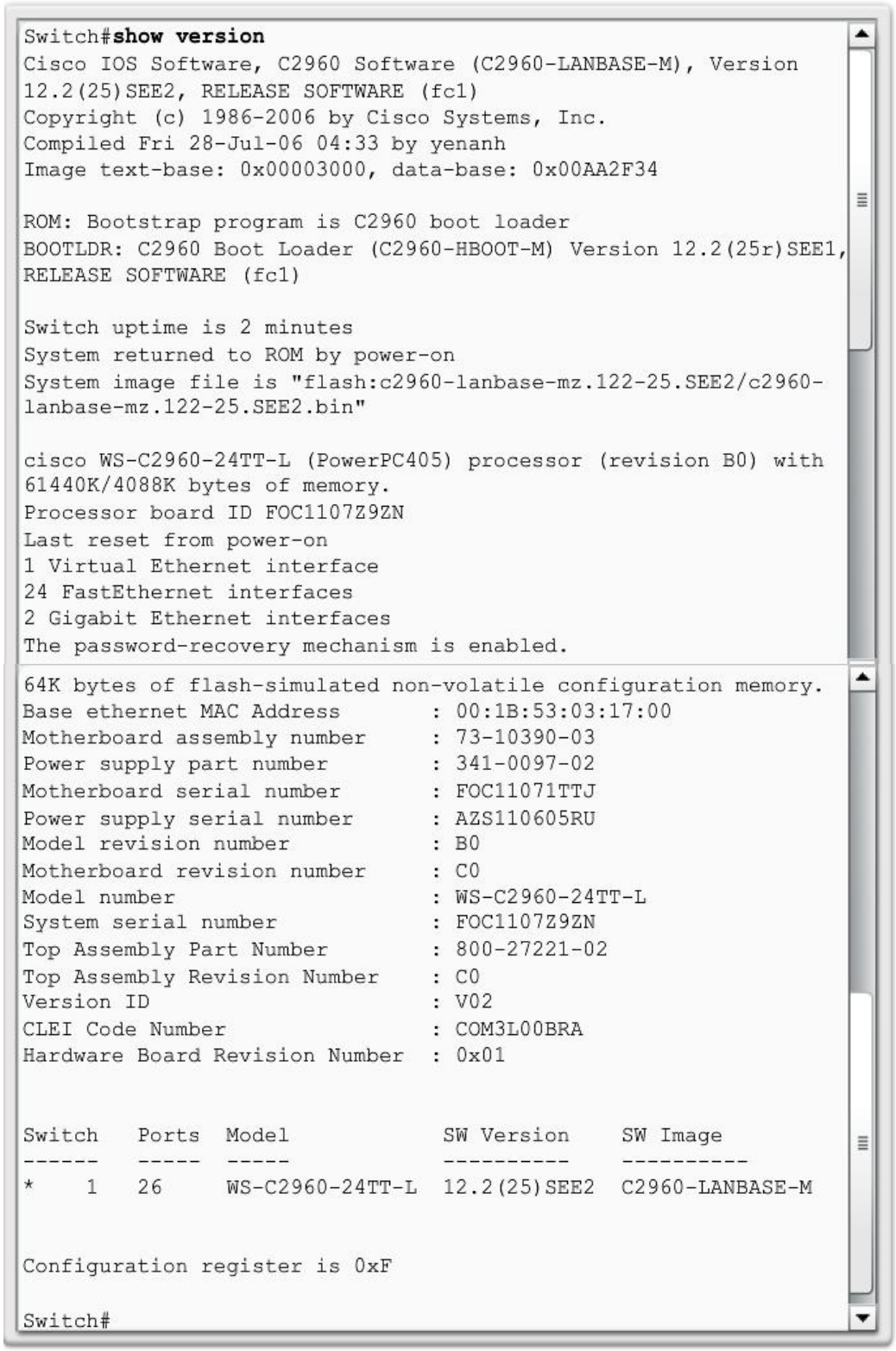


Capítulo 11: Es una red 11.3.3.3 Visualización de la configuración del switch mediante el comando show versión

En un switch, el comando show version muestra información acerca de la versión de software cargada actualmente, junto con información del hardware y del dispositivo. Algunos de los datos que muestra este comando son los siguientes:

- Versión del software: versión del software IOS.
- Versión de bootstrap: versión de bootstrap.
- Tiempo de actividad del sistema: tiempo transcurrido desde la última vez que se reinició.
- Información de reinicio del sistema: método de reinicio (por ejemplo, apagado y encendido, colapso).
- Nombre de la imagen del software: nombre del archivo de IOS.
- Plataforma de switch y tipo de procesador: número de modelo y tipo de procesador.
- Tipo de memoria (compartida/principal): memoria RAM del procesador principal y almacenamiento en búfer de E/S de paquetes compartidos.
- Interfaces de hardware: interfaces disponibles en el switch.
- Registro de configuración: establece especificaciones de arranque, la configuración de velocidad de la consola y parámetros relacionados.

En la ilustración, se muestra un ejemplo del resultado típico del comando show version que se muestra en un switch.



Capítulo 11: Es una red 11.3.4.1 Opciones del comando ipconfig

Como se muestra en la figura 1, la dirección IP del gateway predeterminado de un host se puede ver emitiendo el comando ipconfig en la línea de comandos de un equipo Windows.

Una herramienta para analizar la dirección MAC de una PC es ipconfig /all. Observe que, en la figura 2, la dirección MAC de la PC ahora aparece junto con varios detalles relacionados con el direccionamiento de capa 3 del dispositivo. Intente utilizar este comando.

Además, se puede identificar el fabricante de la interfaz de red en la PC mediante la porción de OUI de la dirección MAC. Esto se puede investigar en Internet.

El servicio del cliente DNS en las PC de Windows optimiza el rendimiento de la resolución de nombres DNS almacenando previamente los nombres resueltos en la memoria. El comando ipconfig /displaydnsmuestra todas las entradas DNS en caché en un sistema de computación Windows.

Resultado de **ipconfig** de muestra que indica la dirección de gateway predeterminado.

```
C:\>ipconfig /all
Ethernet adapter Network Connection:
        Connection-specific DNS Suffix: example.com
        Description . . . . . : Intel(R)
        PRO/Wireless 3945ABG Network Connection
        Physical Address. . . . . : 00-18-DE-C7-F3-FB
        Dhcp Enabled. . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . : 10.2.3.4
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . : 10.2.3.254
        DHCP Server . . . . . : 10.2.3.69
        DNS Servers . . . . . : 192.168.226.120
        Lease Obtained. . . . . : Thursday, May 03,
                                   2007 3:47:51 PM
        Lease Expires . . . . . : Friday, May 04,
                                   2007 6:57:11 AM
C:\>
```

Capítulo 11: Es una red 11.3.4.2 Opciones del comando arp

El comando arp permite crear, editar y mostrar las asignaciones de direcciones físicas a direcciones IPv4 conocidas. El comando arp se ejecuta desde el símbolo del sistema de Windows.

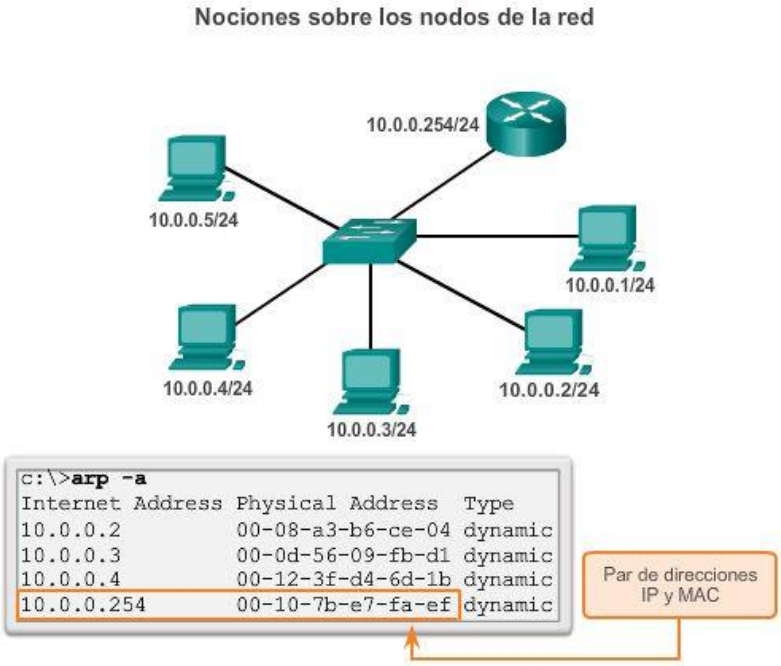
Para ejecutar un comando arp, introduzca lo siguiente en el símbolo del sistema de un host:

C:\host1> arp -a

Como se muestra en la ilustración, el comando arp –a enumera todos los dispositivos que se encuentran actualmente en la caché ARP del host, lo cual incluye la dirección IPv4, la dirección física y el tipo de direccionamiento (estático/dinámico) para cada dispositivo.

Se puede borrar la caché mediante el comando arp -d en caso de que el administrador de red desee volver a llenarla con información actualizada.

Nota: la caché ARP solo contiene información de los dispositivos a los que se accedió recientemente. Para asegurar que la caché ARP esté cargada, haga ping a un dispositivo de manera tal que tenga una entrada en la tabla ARP.



Capítulo 11: Es una red 11.3.4.3 Opciones del comando show cdp neighbors

Examine el resultado de los comandos show cdp neighbors de la figura 1, con la topología de la figura 2. Observe que R3 ha recopilado información detallada acerca de R2 y el switch conectado a la interfaz Fast Ethernet de R3.

CDP es un protocolo exclusivo de Cisco que se ejecuta en la capa de enlace de datos. Debido a que el protocolo CDP funciona en la capa de enlace de datos, es posible que dos o más dispositivos de red Cisco (como routers que admiten distintos protocolos de la capa de red) obtengan información de los demás incluso si no hay conectividad de capa 3.

Cuando arranca un dispositivo Cisco, el CDP se inicia de manera predeterminada. CDP descubre automáticamente los dispositivos Cisco vecinos que ejecutan ese protocolo, independientemente de los protocolos o los conjuntos de aplicaciones de capa 3 en ejecución. El CDP intercambia información del hardware y software del dispositivo con sus vecinos CDP conectados directamente.

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

- Identificadores de dispositivos: por ejemplo, el nombre host configurado de un switch.
- Lista de direcciones: hasta una dirección de capa de red para cada protocolo admitido.
- Identificador de puerto: el nombre del puerto local y remoto en forma de una cadena de caracteres ASCII, como por ejemplo, ethernet0

- Lista de capacidades: por ejemplo, si el dispositivo es un router o un switch
- Plataforma: plataforma de hardware del dispositivo; por ejemplo, un router Cisco serie 1841.

El comando show cdp neighbors detail muestra la dirección IP de un dispositivo vecino. El CDP revelará la dirección IP del vecino, independientemente de si puede hacer ping en el vecino o no.

Este comando es muy útil cuando dos routers Cisco no pueden enrutarse a través de su enlace de datos compartido. El comandoshow cdp neighbors detail ayuda a determinar si uno de los vecinos con CDP tiene un error de configuración IP.

En situaciones de detección de redes, la dirección IP del vecino con CDP suele ser la única información necesaria para conectarse a ese dispositivo mediante Telnet.

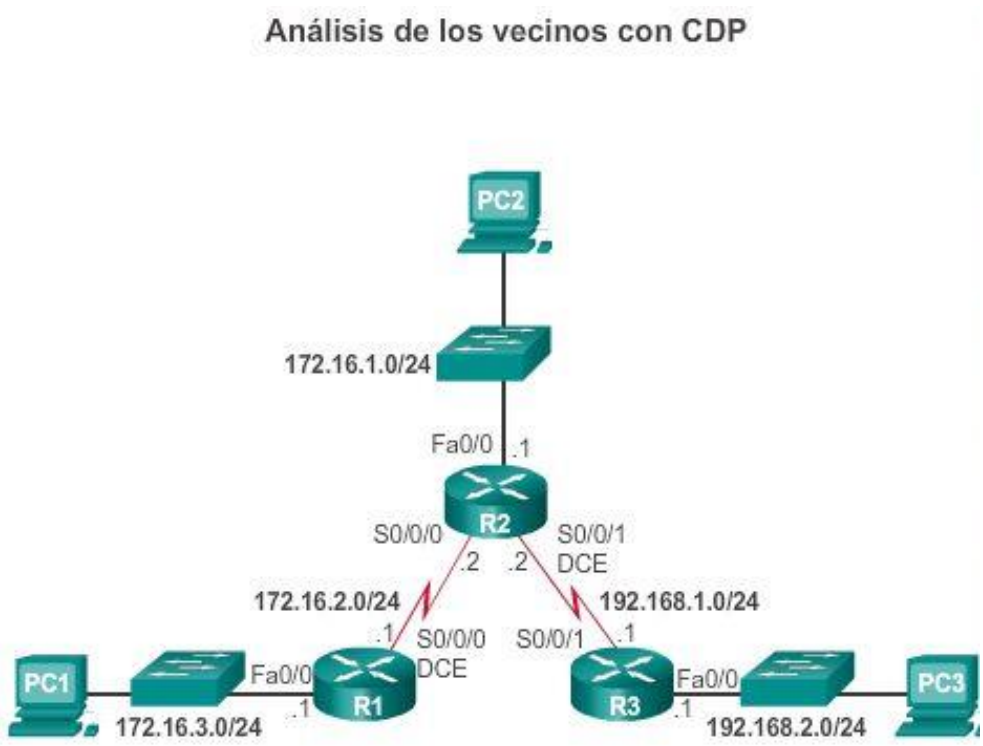
Por razones obvias, CDP puede suponer un riesgo para la seguridad. Debido a que algunas versiones de IOS envían publicaciones CDP de manera predeterminada, es importante que sepa cómo deshabilitar el CDP.

Para desactivar CDP globalmente, utilice el comando de configuración global no cdp run. Para desactivar CDP en una interfaz, utilice el comando de interfaz no cdp enable.

Análisis de los vecinos con CDP

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

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

R3#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 192.168.1.2
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: Serial0/0/1,  Port ID (outgoing port): Serial0/0/1
Holdtime : 161 sec
Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M),
Version 12.4(10b), RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''

---------------------------
Device ID: S3
Entry address(es):
Platform: cisco WS-C2950-24,  Capabilities: Switch IGMP
Interface: FastEthernet0/0,  Port ID (outgoing port):
FastEthernet0/11
Holdtime : 148 sec
```

```
Version :
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(9)EA1,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Wed 24-Apr-02 06:57 by antonino

advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload
len=27, value=00000000FFFFFFFF0
10231FF000000000000000AB769F6C0FF0000
VTP Management Domain: 'CCNA3'
Duplex: full

R3#
```



Capítulo 11: Es una red 11.3.4.4 Uso del comando show ip interface brief

De la misma manera que los comandos y las utilidades se utilizan para verificar la configuración de un host, los comandos se pueden utilizar para verificar las interfaces de los dispositivos intermediarios. Cisco IOS proporciona comandos para verificar el funcionamiento de interfaces de router y switch.

Verificación de interfaces del router

Uno de los comandos más utilizados es el comando show ip interface brief. Este comando proporciona un resultado más abreviado que el comando show ip interface. Proporciona un resumen de la información clave para todas las interfaces de red de un router.

En la figura 1, se muestra la topología que se utiliza en este ejemplo.

En la figura 2, haga clic en el botón R1. El resultado de show ip interface brief muestra todas las interfaces del router, la dirección IP asignada a cada interfaz (si las hubiera) y el estado de funcionamiento de la interfaz.

Según el resultado, la interfaz FastEthernet0/0 tiene la dirección IP 192.168.254.254. En las últimas dos columnas de esta línea, se muestra el estado de la capa 1 y de la capa 2 de esta interfaz. El valor up (activo) en la columna Status (Estado) muestra que esa interfaz opera en la capa 1. El valor up en la columna Protocol (Protocolo) indica que el protocolo de capa 2 funciona.

Observe también que la interfaz Serial 0/0/1 no se habilitó. Esto lo indica el valor administratively down(administrativamente inactiva) en la columna Status.

Como en cualquier dispositivo final, es posible verificar la conectividad de capa 3 con los comandos ping ytraceroute. En este ejemplo, tanto el comando ping como el comando trace muestran una conectividad satisfactoria.

Verificación de las interfaces del switch

En la figura 2, haga clic en el botón S1. El comando show ip interface brief también se puede utilizar para verificar el estado de las interfaces del switch. La dirección IP para el switch se aplica a una interfaz VLAN. En este caso, la interfaz Vlan1 recibió la dirección IP 192.168.254.250 y está habilitada y en funcionamiento.

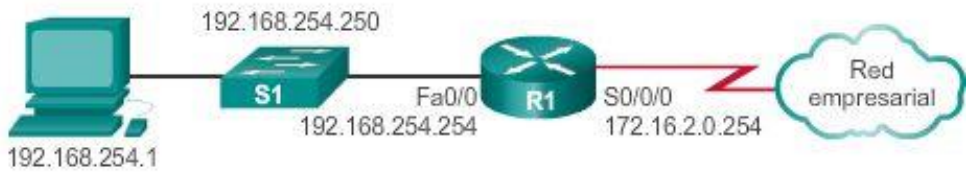
El resultado también muestra que la interfaz FastEthernet0/1 está inactiva. Esto indica que no hay ningún dispositivo conectado a la interfaz o que el dispositivo que está conectado a ella tiene una interfaz de red que no funciona.

Por otro lado, el resultado muestra que las interfaces FastEthernet0/2 y FastEthernet0/3 funcionan. Esto lo indica el valor up en las columnas Status y Protocol.

También se puede probar la conectividad de capa 3 en el switch con los comandos show ip interface brief y traceroute. En este ejemplo, tanto el comando ping como el comando trace muestran una conectividad satisfactoria.

Es importante tener en cuenta que no se requiere ninguna dirección IP para que un switch cumpla su función de reenvío de tramas en la capa 2. Se necesita una dirección IP solo si se administra el switch a través de la red mediante Telnet o SSH. Si el administrador de red planea conectarse al switch de forma remota desde una ubicación fuera de la red LAN local, también se debe configurar un gateway predeterminado.

Prueba de interfaz



Prueba de interfaz

```
R1# show ip interface brief
Interface              IP-Address      OK? Method  Status                Protocol
FastEthernet0/0        192.168.254.254 YES NVRAM   up                    up
FastEthernet0/1        unassigned      YES unset   down                  down
Serial0/0/0            172.16.0.254    YES NVRAM   up                    up
Serial0/0/1            unassigned      YES unset   administratively down down
-------------------------------------------------------------------------
R1# ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
-------------------------------------------------------------------------
R1# traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
  1 172.16.0.253 8 msec 4 msec 8 msec
  2 10.0.0.254 16 msec 16 msec 8 msec
  3 192.168.0.1 16 msec * 20 msec
```

R1 S1

Prueba de interfaz

```
S1# show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
Vlan1                  192.168.254.250 YES manual  up        up
FastEthernet0/1        unassigned      YES unset   down      up
FastEthernet0/2        unassigned      YES unset   up        up
FastEthernet0/3        unassigned      YES unset   up        up
<resultado omitido>
-------------------------------------------------------------------------
S1# ping 192.168.254.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.254.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
-------------------------------------------------------------------------
S1# traceroute 192.168.0.1
Type escape sequence to abort.
Tracing the route to 192.168.0.1
  1 192.168.254.254 4 msec 2 msec 3 msec
  2 172.16.0.253 8 msec 4 msec 8 msec
  3 10.0.0.254 16 msec 16 msec 8 msec
  4 192.168.0.1 16 msec * 20 msec
```

R1 S1

Capítulo 11: Es una red 11.4.1.1 Sistemas de archivos del router

Además de implementar y proteger una red pequeña, el administrador de red también debe administrar los archivos de configuración. La administración de los archivos de configuración es importante para la realización de copias de seguridad y la recuperación en caso de falla del dispositivo.

El sistema de archivos de Cisco IOS (IFS) proporciona una única interfaz a todos los sistemas de archivos que utiliza un router, incluidos los siguientes:

- Sistemas de archivos de memoria flash
- Sistemas de archivos de red (TFTP y FTP)
- Cualquier otra terminal para leer o escribir datos, como la memoria NVRAM, la configuración en ejecución y la memoria ROM, entre otras

Con Cisco IFS, se pueden ver y clasificar todos los archivos (imagen, archivo de texto, etcétera), incluidos los archivos en servidores remotos. Por ejemplo, es posible ver un archivo de configuración en un servidor remoto para verificar que sea el archivo de configuración correcto antes de cargarlo en el router.

Cisco IFS permite que el administrador se desplace por distintos directorios, enumere los archivos en uno de ellos y cree subdirectorios en la memoria flash o en un disco. Los directorios disponibles dependen del dispositivo.

En la figura 1, se muestra el resultado del comando show file systems. En este ejemplo, enumera todos los sistemas de archivos disponibles en un router Cisco 1941. Este comando proporciona información útil, como la cantidad de memoria disponible y libre, el tipo de sistema de archivos y los permisos. Los permisos incluyen solo lectura (ro), solo escritura (wo) y lectura y escritura (rw), los cuales se muestran en la columna Flags (Indicadores) del resultado del comando.

Si bien se enumeran varios sistemas de archivos, nos enfocaremos en los sistemas de archivos TFTP, flash y NVRAM.

Observe que el sistema de archivos flash también tiene un asterisco que lo precede. Esto indica que el sistema de archivos predeterminado actual es flash. El IOS de arranque está ubicado en la memoria flash; por lo tanto, se agrega el símbolo de almohadilla (#) a la entrada de flash para indicar que es un disco de arranque.

El sistema de archivos flash

En la figura 2, se muestra el contenido del sistema de archivos predeterminado actual, que en este caso es flash, tal como indicaba el asterisco que precedía la entrada en la ilustración anterior. Hay varios archivos ubicados en la memoria flash, pero el de mayor interés específicamente es el último de la lista: se trata del nombre del archivo de imagen de Cisco IOS actual que se ejecuta en la memoria RAM.

El sistema de archivos NVRAM

Para ver el contenido de la memoria NVRAM, se debe cambiar el sistema de archivos predeterminado actual con el comando cd (cambiar directorio), como se muestra en la figura 3. El comando pwd (directorio de trabajo actual) verifica que estemos viendo el directorio NVRAM. Finalmente, el comando dir (directorio) enumera el contenido de la memoria NVRAM. Si bien se enumeran varios archivos de configuración, el de mayor interés específicamente es el archivo de configuración de inicio.

Sistemas de archivos

```
Router#show file systems
File Systems:

       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   archive:
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
             -             -    opaque     rw   null:
             -             -   network     rw   tftp:
*    256487424     183234560      disk     rw   flash0: flash:#
             -             -      disk     rw   flash1:
        262136        254779     nvram     rw   nvram:
             -             -    opaque     wo   syslog:
             -             -    opaque     rw   xmodem:
             -             -    opaque     rw   ymodem:
             -             -   network     rw   rcp:
             -             -   network     rw   http:
             -             -   network     rw   ftp:
             -             -   network     rw   scp:
             -             -    opaque     ro   tar:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
```

Flash

```
Router#dir
Directory of flash0:/

 1 -rw-     2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
                                             19xx.cfg
 2 -rw-  3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-     1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-   122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-  1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
                                             ios-3.1.1.45-k9.pkg
 6 -rw-   415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
                                             1.1.4.176.pkg
 7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00 c1900-
                                             universalk9-
                                             mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

NVRAM

```
Router#cd nvram:
Router#pwd
nvram:/
Router#dir
Directory of nvram:/

  253  -rw-        1156      <no date>  startup-config
  254  ----           5      <no date>  private-config
  255  -rw-        1156      <no date>  underlying-config
    1  -rw-        2945      <no date>  cwmp_inventory
    4  ----          58      <no date>  persistent-data
    5  -rw-          17      <no date>  ecfm_ieee_mib
    6  -rw-         559      <no date>  IOS-Self-Sig#1.cer

262136 bytes total (254779 bytes free)
```

Capítulo 11: Es una red 11.4.1.2 Sistemas de archivos del switch

Con el sistema de archivos flash del switch Cisco 2960, se pueden copiar los archivos de configuración y archivar (subir y descargar) imágenes de software.

El comando para ver los sistemas de archivos en un switch Catalyst es el mismo que se utiliza en los routers Cisco: show file systems, como se muestra en la ilustración.

Los switches y routers Cisco admiten muchos comandos UNIX básicos: cd para cambiar a un sistema de archivos o un directorio, dir para mostrar los directorios en un sistema de archivos y pwd para mostrar el directorio de trabajo.

Switch Cisco 2960

```
Switch#show file systems
File Systems:

      Size(b)     Free(b)      Type  Flags  Prefixes
*    32514048    20887552     flash     rw   flash:
           -           -    opaque     rw      vb:
           -           -    opaque     ro      bs:
           -           -    opaque     rw  system:
           -           -    opaque     rw  tmpsys:
       65536       48897     nvram     rw   nvram:
           -           -    opaque     ro  xmodem:
           -           -    opaque     ro  ymodem:
           -           -    opaque     rw    null:
           -           -    opaque     ro     tar:
           -           -   network     rw    tftp:
           -           -   network     rw     rcp:
           -           -   network     rw    http:
           -           -   network     rw     ftp:
           -           -   network     rw     scp:
           -           -   network     rw   https:
           -           -    opaque     ro     cns:
```

Capítulo 11: Es una red 11.4.2.1 Creación de copias de seguridad y restauración mediante archivos de texto

Copia de seguridad de las configuraciones con captura de texto (Tera Term)

Los archivos de configuración se pueden guardar o archivar en un archivo de texto mediante Tera Term.

Como se muestra en la figura, los pasos son:

Paso 1. En el menú File, haga clic en Log.

Paso 2. Elija la ubicación para guardar el archivo. Tera Term comenzará a capturar texto.

Paso 3. Una vez que comienza la captura, ejecute el comando show running-config o show startup-config en la petición de entrada de EXEC privilegiado. El texto que aparece en la ventana de la terminal se colocará en el archivo elegido.

Paso 4. Cuando la captura haya finalizado, seleccione Close (Cerrar) en la ventana Log (Registro) de TeraTerm.

Paso 5. Observe el archivo para verificar que no esté dañado.

Restauración de las configuraciones de texto

Una configuración se puede copiar de un archivo a un dispositivo. Cuando se copia desde un archivo de texto y se pega en la ventana de una terminal, el IOS ejecuta cada línea del texto de configuración como si fuera un comando. Esto significa que el archivo necesitará edición para asegurar que las contraseñas encriptadas estén en forma de texto y que se eliminen los mensajes de IOS y el texto de no comando, como "--More--". Este proceso se analiza en la práctica de laboratorio.

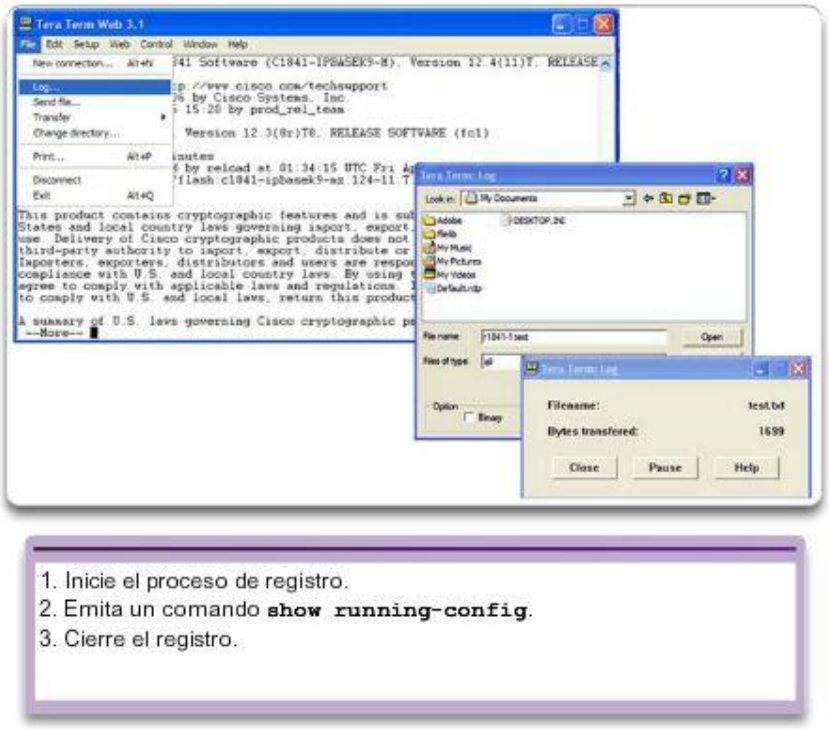
A su vez, en la CLI, el dispositivo debe establecerse en el modo de configuración global para recibir los comandos del archivo de texto que se pegan en la ventana de la terminal.

Cuando se usa Tera Term, los pasos son los siguientes:

Paso 1. En el menú File (Archivo), haga clic en Send (Enviar) para enviar el archivo.
Paso 2. Ubique el archivo que debe copiar en el dispositivo y haga clic en Open.
Paso 3. Tera Term pegará el archivo en el dispositivo.

El texto en el archivo estará aplicado como comandos en la CLI y pasará a ser la configuración en ejecución en el dispositivo. Éste es un método conveniente para configurar manualmente un router.

Cómo guardar en un archivo de texto en Tera Term



Capítulo 11: Es una red 11.4.2.2 Creación de copias de seguridad y restauración mediante TFTP

Copia de seguridad de las configuraciones mediante TFTP

Las copias de los archivos de configuración se deben almacenar como archivos de copia de seguridad en caso de que se produzca un problema. Los archivos de configuración se pueden almacenar en un servidor de protocolo trivial de transferencia de archivos (TFTP) o en una unidad USB. Un archivo de configuración también tendría que incluirse en la documentación de red.

Para guardar la configuración en ejecución o la configuración de inicio en un servidor TFTP, utilice el comandocopy running-config tftp o copy startup-config tftp, como se muestra en la ilustración. Siga estos pasos para realizar una copia de seguridad de la configuración en ejecución en un servidor TFTP:

Paso 1. Introduzca el comando copy running-config tftp.
Paso 2. Ingrese la dirección IP del host en el cual se almacenará el archivo de configuración.
Paso 3. Ingrese el nombre que se asignará al archivo de configuración.
Paso 4. Presione Intro para confirmar cada elección.

Restauración de las configuraciones mediante TFTP

Para restaurar la configuración en ejecución o la configuración de inicio desde un servidor TFTP, utilice el comando copy tftp running-config o copy tftp startup-config. Siga estos pasos para restaurar la configuración en ejecución desde un servidor TFTP:

Paso 1. Introduzca el comando copy tftp running-config.

Paso 2. Introduzca la dirección IP del host en el que está almacenado el archivo de configuración.

Paso 3. Ingrese el nombre que se asignará al archivo de configuración.

Paso 4. Presione Intro para confirmar cada elección.

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm]
Writing tokyo.2 !!!!!! [OK]
```

Capítulo 11: Es una red 11.4.2.3 Uso de puertos USB en un router Cisco

La característica de almacenamiento de bus serial universal (USB) habilita a determinados modelos de routers Cisco para que admitan unidades flash USB. La característica flash USB proporciona una capacidad de almacenamiento secundario optativa y un dispositivo de arranque adicional. Las imágenes, las configuraciones y demás archivos se pueden copiar en la memoria flash USB Cisco y desde esta con la misma confiabilidad con la que se almacenan y se recuperan archivos con una tarjeta Compact Flash. Además, los routers de servicios integrados modulares pueden arrancar con cualquier imagen del software Cisco IOS guardada en la memoria flash USB.

Los módulos de memoria flash USB Cisco están disponibles en versiones de 64 MB, 128 MB y 256 MB.

Para ser compatible con un router Cisco, una unidad flash USB debe tener formato FAT16. De lo contrario, el comando show file systems muestra un error que indica que el sistema de archivos es incompatible.

A continuación, se presenta un ejemplo del uso del comando dir en un sistema de archivos USB:

Router# dir usbflash0:

Directory of usbflash0:/

1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)

Lo ideal es que la memoria flash USB pueda contener varias copias de las configuraciones de Cisco IOS y varias configuraciones del router. La memoria flash USB permite que un administrador mueva y copie fácilmente esos archivos y configuraciones de IOS de un router a otro. En numerosas ocasiones, el proceso de copiado puede ser mucho más rápido que a través de una LAN o una WAN. Tenga en cuenta que es posible que el IOS no reconozca el tamaño correcto de la memoria flash USB, pero eso no significa necesariamente que la memoria flash no sea compatible. Además, los puertos USB de un router generalmente son USB 2.0, como los que se muestran en la ilustración.

Capítulo 11: Es una red 11.4.2.4 Creación de copias de seguridad y restauración mediante USB

Copia de seguridad de las configuraciones mediante una unidad flash USB

Al realizar copias de seguridad en un puerto USB, se recomienda emitir el comando show file systemspara verificar que la unidad USB esté presente y confirmar el nombre, como se muestra en la figura 1.

A continuación, utilice el comando copy run usbflash0:/ para copiar el archivo de configuración a la unidad flash USB. Asegúrese de utilizar el nombre de la unidad flash tal como se indica en el sistema de archivos. La barra es optativa, pero indica el directorio raíz de la unidad flash USB.

El IOS le solicitará el nombre de archivo. Si el archivo ya existe en la unidad flash USB, el router solicitará la confirmación de sobrescritura, como se ve en la figura 2.

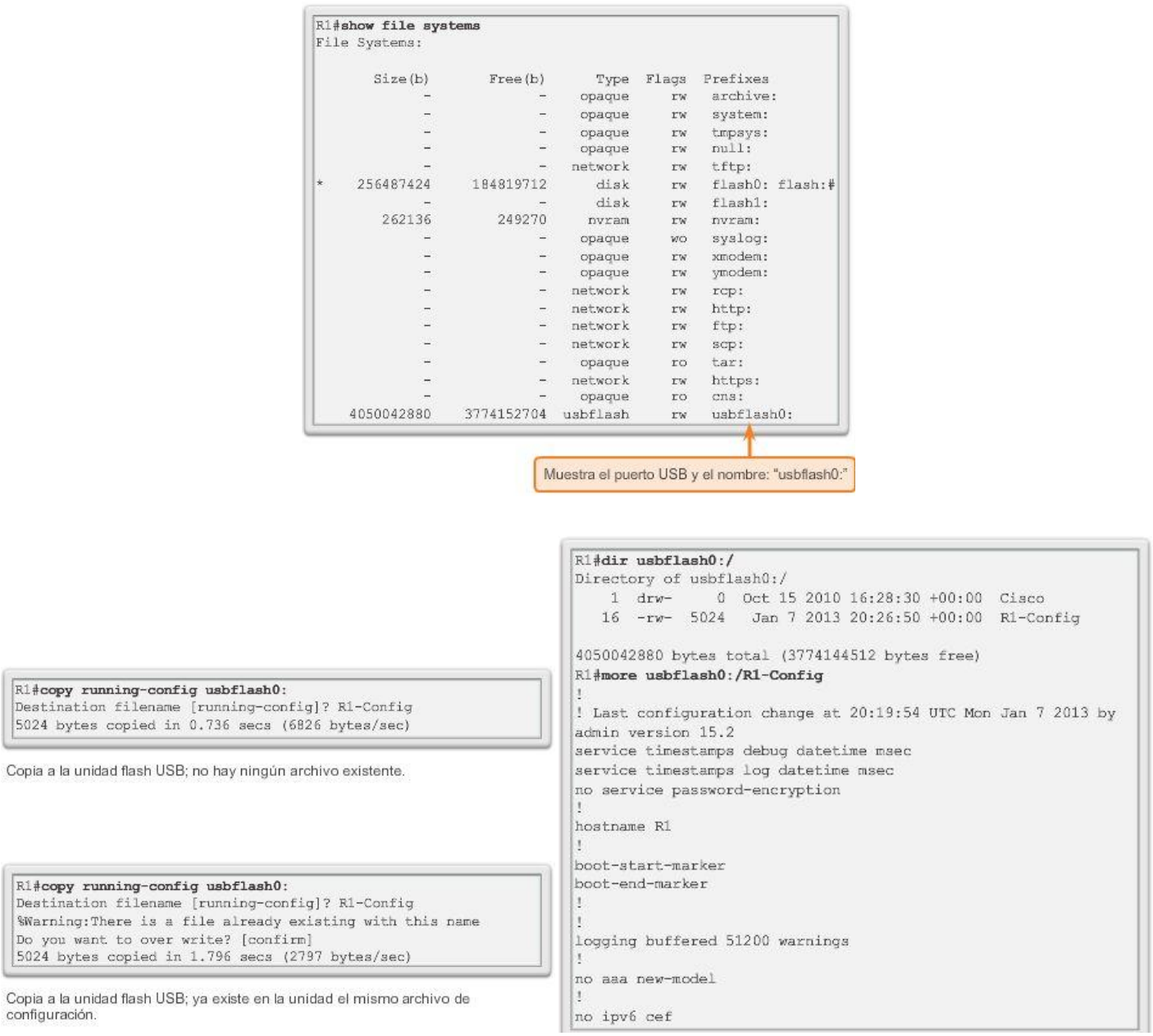
Utilice el comando dir para ver el archivo en la unidad USB, y el comando more para ver el contenido, como se muestra en la figura 3.

Restauración de las configuraciones mediante una unidad flash USB

Para volver a copiar el archivo, se deberá editar el archivo USB R1-Config con un editor de texto para transformarlo en un archivo de configuración válido; de lo contrario, hay muchas entradas que son comandos no válidos y no aparecerá ninguna interfaz.

R1# copy usbflash0:/R1-Config running-config

Destination filename [running-config]?



Capítulo 11: Es una red 11.5.1.1 Dispositivo Multi-Function

El uso de redes no se limita a las pequeñas empresas y a las grandes organizaciones.

Otro entorno en el que cada vez se aprovecha más la tecnología de red es el hogar. Las redes domésticas se utilizan para proporcionar conectividad y uso compartido de Internet entre varios sistemas de computación personales y computadoras portátiles en el hogar. También permiten que las personas aprovechen diversos servicios, como el uso compartido de una impresora de red, el almacenamiento centralizado de fotos, música y películas en un dispositivo de almacenamiento conectado a la red (NAS) y el acceso de otros dispositivos para usuarios finales, como tablet PC, teléfonos celulares e incluso electrodomésticos, como un televisor, a servicios de Internet.

Una red doméstica es muy similar a la red de una pequeña empresa. Sin embargo, la mayoría de las redes domésticas y muchas redes de pequeñas empresas no requieren dispositivos de gran volumen, como routers y switches dedicados. Los dispositivos de menor escala son suficientes, siempre que proporcionen la misma

funcionalidad de enrutamiento y conmutación. Por este motivo, muchas redes domésticas y de pequeñas empresas utilizan el servicio de un dispositivo multifunción.

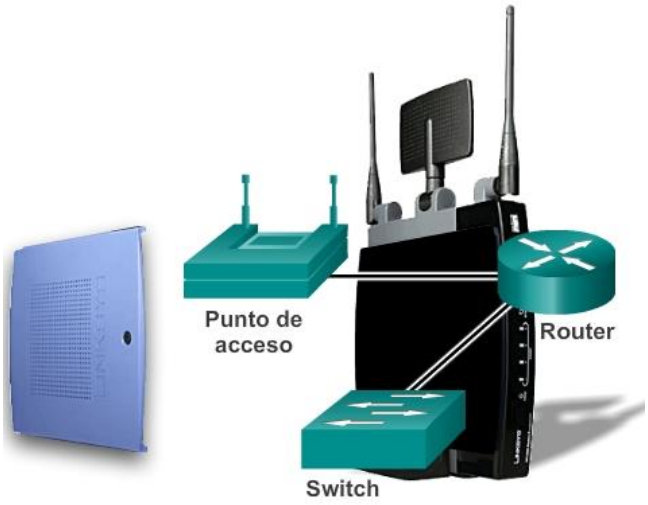
A los fines de este curso, los dispositivos multifunción se denominarán routers integrados.

Un router integrado es como tener varios dispositivos diferentes conectados entre sí. Por ejemplo: la conexión entre el switch y el router sigue existiendo, pero se produce internamente. Cuando se reenvía un paquete desde un dispositivo hacia otro en la misma red local, el switch integrado reenvía automáticamente el paquete al dispositivo de destino. No obstante, si se reenvía un paquete a un dispositivo en una red remota, el switch integrado reenvía el paquete a la conexión del router interno. Luego, el router interno determina cuál es el mejor camino y reenvía el paquete en consecuencia.

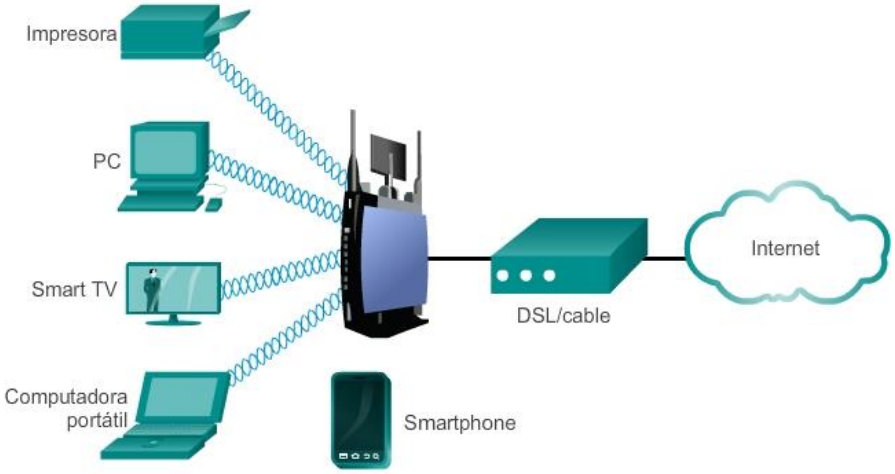
La mayoría de los routers integrados ofrecen tanto capacidades de conmutación por cable como conectividad inalámbrica y sirven como punto de acceso (AP) en la red inalámbrica, como el que se muestra en la figura 1. La conectividad inalámbrica es una forma popular, flexible y rentable de que los hogares y las empresas proporcionen servicios de red a los dispositivos finales.

En las figuras 2 y 3, se enumeran algunas ventajas y consideraciones comunes respecto del uso de la tecnología inalámbrica.

Además de admitir el enrutamiento, la conmutación y la conectividad inalámbrica, un router integrado puede ofrecer muchas funciones adicionales, las cuales incluyen: servicio de DHCP, un firewall e, incluso, servicios de almacenamiento conectado a la red.



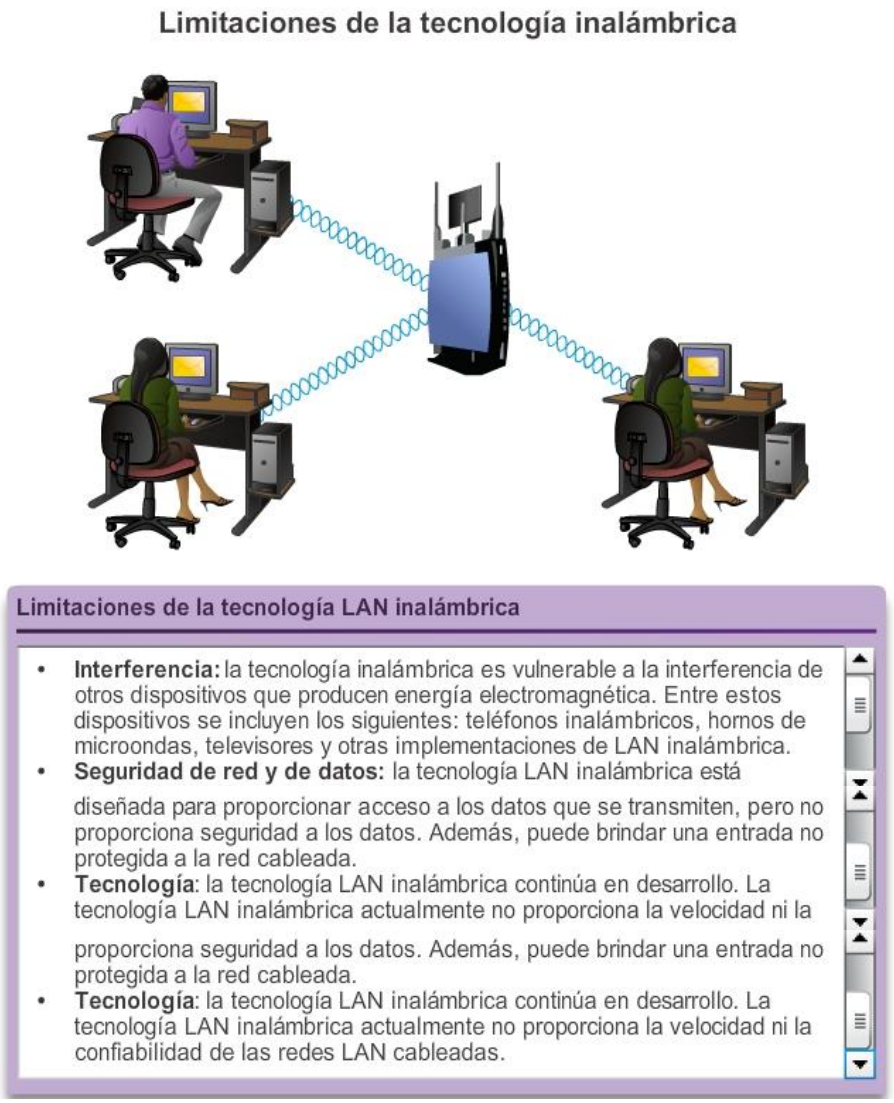
Ventajas de la tecnología inalámbrica



Beneficios de la tecnología LAN inalámbrica

- **Movilidad:** permite que tanto los clientes estacionarios como los clientes móviles se conecten fácilmente.
- **Escalabilidad:** se puede expandir fácilmente para permitir que se conecten más usuarios y para aumentar el área de cobertura.
- **Flexibilidad:** proporciona conectividad en cualquier momento y lugar.
- **Ahorro en costos:** los costos de los equipos continúan disminuyendo a medida que la tecnología avanza.
- **Menor tiempo de instalación:** la instalación de un único equipo puede proporcionar conectividad a un gran número de personas.
- **Confiabilidad en entornos adversos:** fácil de instalar en entornos

medida que la tecnología avanza.
- **Menor tiempo de instalación:** la instalación de un único equipo puede proporcionar conectividad a un gran número de personas.
- **Confiabilidad en entornos adversos:** fácil de instalar en entornos hostiles y de emergencia.



Capítulo 11: Es una red 11.5.1.2 Tipos de routers integrados

Los routers integrados pueden ser desde dispositivos pequeños, diseñados para aplicaciones de oficinas hogareñas y pequeñas empresas, hasta dispositivos más eficaces, que se pueden usar en sucursales de empresas.

Un ejemplo de este tipo de router integrado es un router inalámbrico Linksys, como el que se muestra en la ilustración. Este tipo de routers integrados tienen un diseño simple y, por lo general, no tiene componentes independientes, lo que reduce el costo del dispositivo. Sin embargo, si se produce una falla, no es posible reemplazar componentes individuales dañados. De este modo, crean un único punto de falla y no están optimizados para ninguna función en particular.

Otro ejemplo de router integrado es el router de servicio integrado (ISR) de Cisco. La familia de productos ISR de Cisco ofrece una amplia gama de productos, entre ellos los dispositivos diseñados para entornos de oficinas pequeñas y hogareñas o para redes más grandes. Muchos de los ISR ofrecen modularidad y tienen componentes individuales para cada función, por ejemplo un componente de switch y un componente de router. Esto permite agregar, reemplazar y actualizar componentes individuales según sea necesario.

Todos los routers integrados permiten opciones de configuración básicas como contraseñas y direcciones IP, y opciones de configuración de DHCP, que son las mismas independientemente de si el dispositivo se utiliza para conectar hosts por cable o inalámbricos.

No obstante, si se utiliza la funcionalidad inalámbrica, se necesitan parámetros de configuración adicionales, como la configuración del modo inalámbrico, el SSID y el canal inalámbrico.

Capítulo 11: Es una red 11.5.1.3 Capacidad inalámbrica

Modo inalámbrico

El modo inalámbrico se refiere a la configuración del estándar inalámbrico IEEE 802.11 que utilizará la red. Existen cuatro enmiendas al estándar IEEE 802.11, que describen distintas características para las comunicaciones inalámbricas; estas son 802.11a, 802.11b, 802.11g y 802.11n. En la figura 1, se muestra más información sobre cada estándar.

La mayoría de los routers inalámbricos integrados son compatibles con las versiones 802.11b, 802.11g y 802.11n. Las tres tecnologías son compatibles, pero todos los dispositivos en la red deben funcionar en el mismo estándar común a todos los dispositivos. Por ejemplo: si un router 802.11n está conectado a una computadora portátil con 802.11n, la red funciona en un estándar 802.11n. Sin embargo, si se agrega una impresora inalámbrica 802.11b a la red, el router y la computadora portátil revierten al estándar 802.11b, que es más lento, para todas las comunicaciones. Por lo tanto, mantener dispositivos inalámbricos más antiguos en la red provoca que toda la red funcione más despacio. Es importante tener esto en cuenta al decidir si se mantienen dispositivos inalámbricos más antiguos o no.

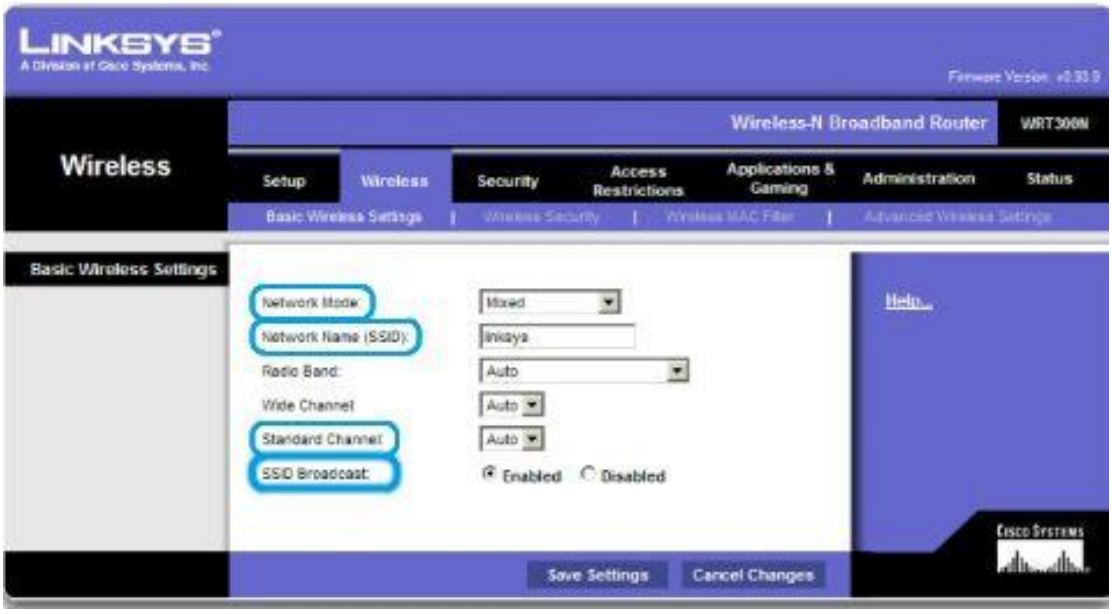
Identificador de conjunto de servicios (SSID)

Puede haber muchas otras redes inalámbricas en su zona. Es importante que los dispositivos inalámbricos se conecten a la red WLAN correcta. Esto se realiza mediante un identificador del servicio (SSID, Service Set Identifier).

El SSID es un nombre alfanumérico que distingue mayúsculas de minúsculas para su red inalámbrica doméstica. El nombre puede tener hasta 32 caracteres de longitud. El SSID se utiliza para comunicar a los dispositivos inalámbricos a qué WLAN pertenecen y con qué otros dispositivos pueden comunicarse. Independientemente del tipo de instalación WLAN, todos los dispositivos inalámbricos en una WLAN pueden configurarse con el mismo SSID a fin de poder realizar la comunicación.

Canal inalámbrico

Los canales se crean al dividir el espectro de RF disponible. Cada canal puede transportar una conversación diferente. Esto es similar a la manera en que los distintos canales de televisión se transmiten por un único medio. Varios AP pueden funcionar muy cerca unos de otros siempre que utilicen diferentes canales para la comunicación.



Capítulo 11: Es una red 11.5.1.4 Seguridad básica de la red inalámbrica

Antes de conectar el AP a la red o al ISP, se deben planificar y configurar las medidas de seguridad.

Como se muestra en la figura 1, algunas de las medidas de seguridad más básicas incluyen lo siguiente:

- Modificación de los valores predeterminados para el SSID, los nombres de usuario y las contraseñas
- Desactivación de la transmisión del SSID
- Configuración de la encriptación mediante WEP o WPA

La encriptación es el proceso de transformar datos de manera que, aunque sean interceptados, queden inutilizables.

Protocolo de equivalencia por cable (WEP, Wired Equivalency Protocol)

El protocolo WEP es una característica de seguridad avanzada que encripta el tráfico de la red a medida que este se desplaza por el aire. WEP utiliza claves preconfiguradas para encriptar y descifrar datos, como se muestra en la figura 2.

Una clave WEP se introduce como una cadena de números y letras, y generalmente consta de 64 ó 128 bits. En algunos casos, el WEP admite también claves de 256 bits. Para simplificar la creación y la introducción de

estas claves, muchos dispositivos incluyen la opción por contraseña. La opción por contraseña es una manera fácil de recordar la palabra o frase usada para generar automáticamente una clave.

A fin de que el WEP funcione, el AP (y cualquier otro dispositivo inalámbrico que tenga habilitado el acceso a la red) deberá tener la misma clave WEP introducida. Sin esta clave, los dispositivos no podrán comprender las transmisiones inalámbricas.

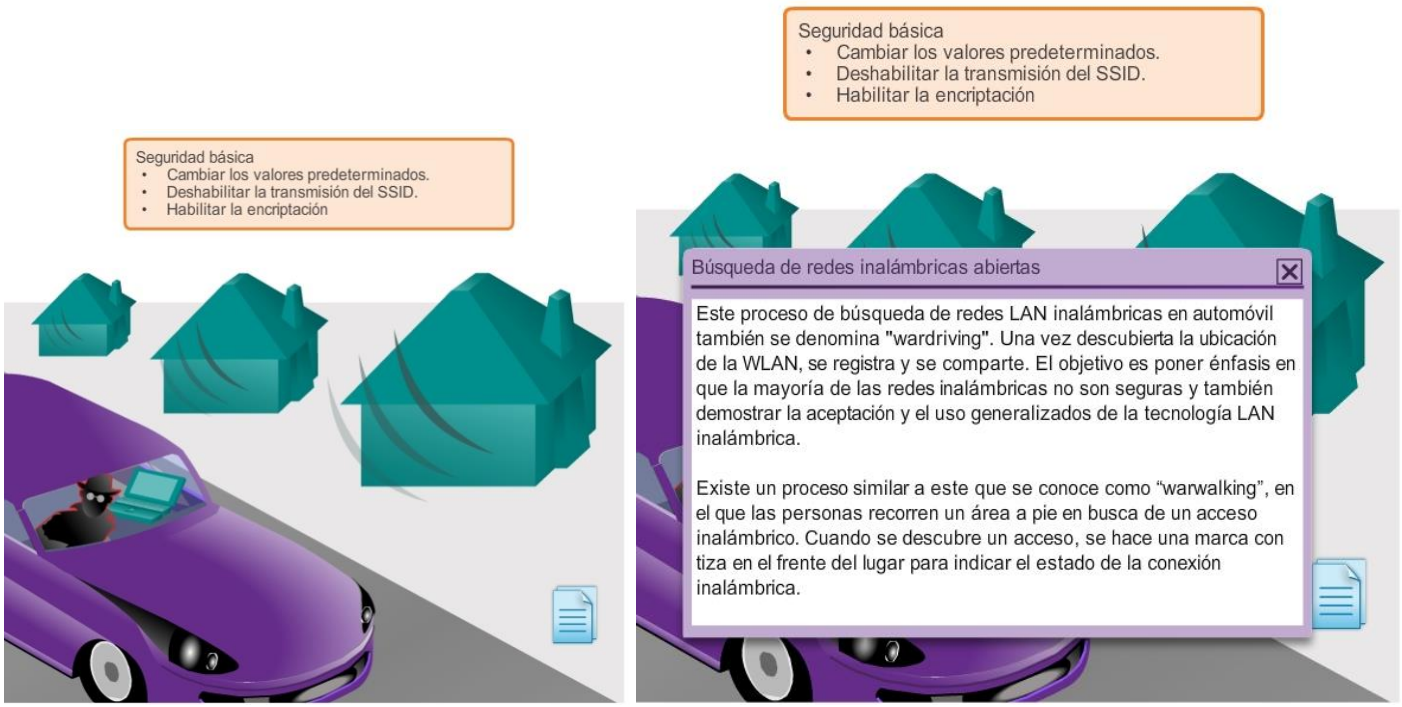
WEP tiene puntos débiles, por ejemplo, el uso de una clave estática en todos los dispositivos con WEP habilitado. Existen aplicaciones disponibles que los atacantes pueden utilizar para descubrir la clave WEP. Estas aplicaciones se encuentran disponibles fácilmente en Internet. Una vez que el atacante ha extraído la clave, tiene acceso completo a toda la información transmitida.

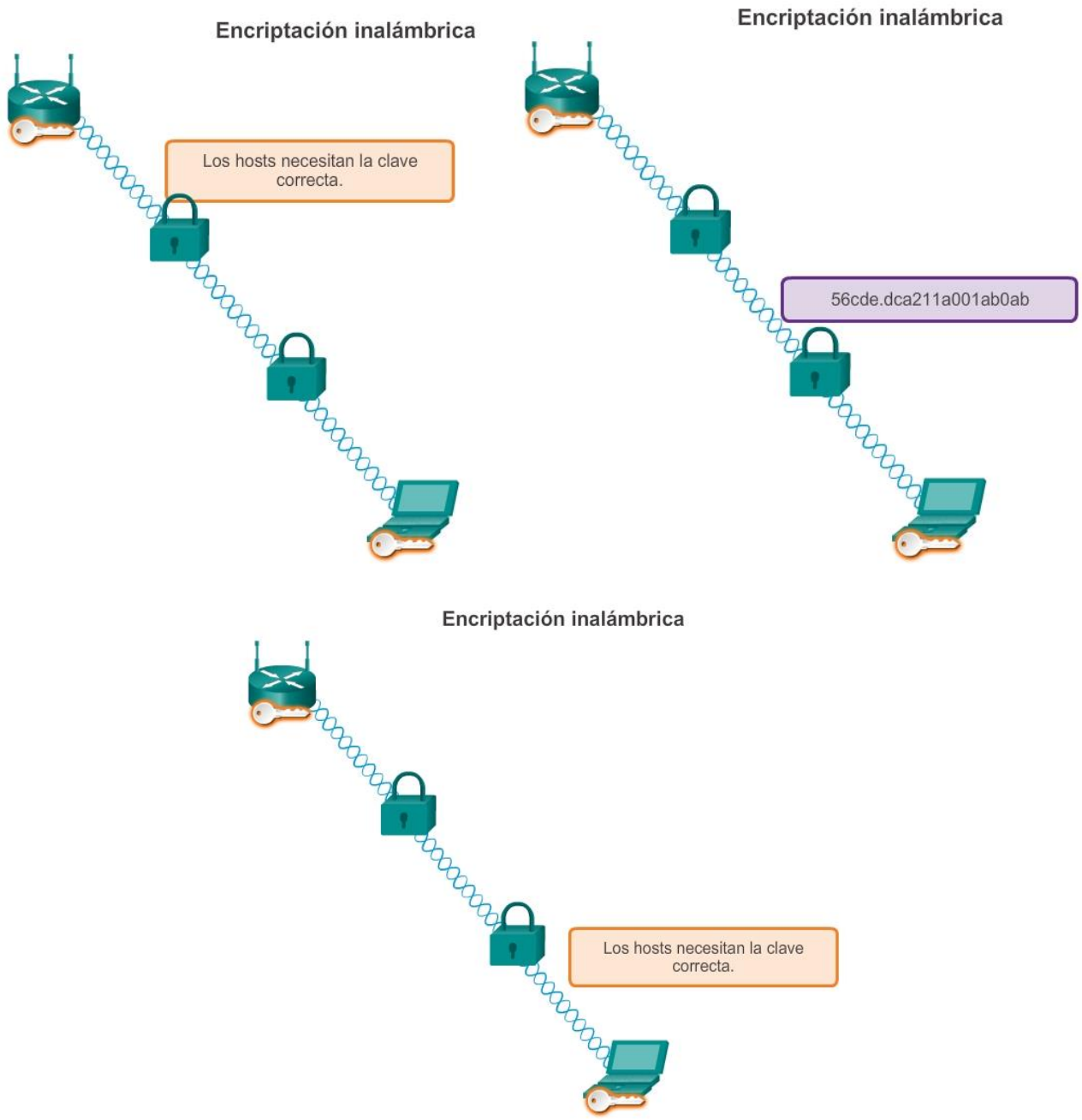
Una manera de superar este punto débil es cambiar la clave frecuentemente. Otra manera es usar una forma de encriptación más avanzada y segura, conocida como acceso protegido Wi-Fi (WPA, Wi-Fi Protected Access).

Acceso protegido Wi-Fi (WPA)

El WPA también utiliza claves de encriptación de 64 a 256 bits. Sin embargo, el WPA, a diferencia del WEP, genera nuevas claves dinámicas cada vez que un cliente establece una conexión con el AP. Por esta razón el WPA se considera más seguro que el WEP, ya que es mucho más difícil de decodificar.

Existen varias implementaciones de seguridad más que se pueden configurar en un AP inalámbrico, incluidos el filtrado de direcciones MAC, la autenticación y el filtrado de tráfico. Sin embargo, estas implementaciones de seguridad exceden el ámbito de este curso.





Capítulo 11: Es una red 11.5.2.1 Configuración del router integrado

Un router inalámbrico Linksys es un dispositivo común utilizado en redes domésticas y de pequeñas empresas. En este curso, se utilizará para demostrar las configuraciones básicas de un router integrado. Un dispositivo Linksys típico ofrece cuatro puertos Ethernet para conectividad por cable y, además, actúa como punto de acceso inalámbrico. El dispositivo Linksys también funciona como servidor de DHCP y miniservidor Web que admite una interfaz gráfica de usuario (GUI) basada en Web.

Acceso a un router Linksys y configuración

Para acceder inicialmente al router, conecte un cable de una PC a uno de los puertos Ethernet para LAN del router, como se muestra en la ilustración. Una vez establecida la conexión por cable, el dispositivo que se conecta obtendrá automáticamente la información de direccionamiento IP del router integrado, incluida una dirección de gateway predeterminado.

La dirección de gateway predeterminado es la dirección IP del dispositivo Linksys. Revise la configuración de la red de computadoras con el comando ipconfig /all para obtener esta dirección. Ahora puede escribir esa dirección IP en un explorador Web de la PC para acceder a la GUI de configuración basada en Web.

El dispositivo Linksys tiene una configuración predeterminada que habilita servicios de conmutación y de enrutamiento básico. También está configurado de manera predeterminada como servidor de DHCP.

Las tareas de configuración básica, como el cambio del nombre de usuario y contraseña predeterminados, de la dirección IP predeterminada de Linksys e, incluso, de los rangos predeterminados de direcciones IP de DHCP, se deben realizar antes de que se conecte el AP a una red activa.

Capítulo 11: Es una red 11.5.2.2 Habilitación de la conectividad inalámbrica

Para habilitar la conectividad inalámbrica, se debe configurar el modo inalámbrico, el SSID, el canal de RF y cualquier mecanismo de encriptación de seguridad deseado.

Primero, seleccione el modo inalámbrico correcto, como se muestra en la ilustración. Al seleccionar el modo, o el estándar inalámbrico, cada modo incluye una sobrecarga determinada. Si todos los dispositivos en la red utilizan el mismo estándar, seleccionar el modo asociado a ese estándar limita la cantidad de sobrecarga que se genera. También aumenta la seguridad, dado que no permite que se conecten dispositivos con estándares diferentes. No obstante, si necesitan acceder a la red dispositivos que utilizan estándares diferentes, se debe seleccionar el modo mixto. El rendimiento de la red disminuirá debido a la sobrecarga adicional ocasionada por admitir todos los modos.

A continuación, establezca el SSID. Todos los dispositivos que deseen participar en la WLAN deben tener el mismo SSID. Por cuestiones de seguridad, se debe modificar el SSID predeterminado. Para permitir que los clientes detecten la WLAN fácilmente, se transmite el SSID de manera predeterminada. Se puede deshabilitar la característica de transmisión del SSID. Si no se transmite el SSID, los clientes inalámbricos necesitarán configurar este valor manualmente.

El canal de RF utilizado para el router integrado se debe elegir teniendo en cuenta las demás redes inalámbricas que se encuentren alrededor.

Las redes inalámbricas adyacentes deben utilizar canales que no se superpongan, a fin de optimizar el rendimiento. La mayoría de los puntos de acceso ahora ofrecen una opción para permitir que el router localice automáticamente el canal menos congestionado.

Por último, seleccione el mecanismo de encriptación que prefiera e introduzca una clave o una frase de contraseña.

Capítulo 11: Es una red 11.5.2.3 Configuración de un cliente inalámbrico

Configuración de un cliente inalámbrico

Un host inalámbrico, o cliente, se define como cualquier dispositivo que contenga un software de cliente inalámbrico y una NIC inalámbrica. Este software cliente le permite al hardware participar en la WLAN. Los dispositivos incluyen algunos smartphones, computadoras portátiles y de escritorio, impresoras, televisores, sistemas de juego y tablet PC.

Para que un cliente inalámbrico se conecte a la WLAN, las opciones de configuración del cliente deben coincidir con las del router inalámbrico. Esto incluye el SSID, la configuración de seguridad y la información del canal (si este se configuró manualmente). Esta configuración se especifica en el software de cliente.

El software cliente inalámbrico utilizado puede estar integrado por software al sistema operativo del dispositivo o puede ser un software de utilidad inalámbrica, independiente y que se puede descargar, diseñado específicamente para interactuar con la NIC inalámbrica.

Una vez que se configure el software cliente, verifique el enlace entre el cliente y el AP.

Abra la pantalla de información del enlace inalámbrico para ver datos como la velocidad de datos de la conexión, el estado de la conexión y el canal inalámbrico utilizado, como se muestra en la ilustración. Si está disponible, la característica Información de enlace muestra la potencia de señal y la calidad de la señal inalámbrica actuales.

Además de verificar el estado de la conexión inalámbrica, verifique que los datos realmente puedan transmitirse. Una de las pruebas más comunes para verificar si la transmisión de datos se realiza correctamente es la prueba de ping. Si el ping se realiza correctamente se puede realizar la transmisión de datos.

Capítulo 11: Es una red 11.6.1.3 Resumen

Para cumplir con los requisitos de los usuarios, incluso las redes pequeñas requieren planificación y diseño, como se muestra en la ilustración. La planificación asegura que se consideren debidamente todos los requisitos, factores de costo y opciones de implementación. La confiabilidad, la escalabilidad y la disponibilidad son partes importantes del diseño de una red.

Para admitir y ampliar una red pequeña, se necesita estar familiarizado con los protocolos y las aplicaciones de red que se ejecutan en ella. Los analizadores de protocolos permiten que los profesionales de red recopilen información estadística sobre los flujos de tráfico en una red rápidamente. La información recopilada por el analizador de protocolos se analiza de acuerdo con el origen y el destino del tráfico, y con el tipo de tráfico que se envía.

Los técnicos de red pueden utilizar este análisis para tomar decisiones acerca de cómo administrar el tráfico de manera más eficiente. Los protocolos de red comunes incluyen DNS, Telnet, SMTP, POP, DHCP, HTTP y FTP.

Es necesario tener en cuenta las amenazas y vulnerabilidades de seguridad al planificar la implementación de una red. Se deben proteger todos los dispositivos de red. Esto incluye routers, switches, dispositivos para usuarios finales e, incluso, dispositivos de seguridad. Se deben proteger las redes contra softwares malintencionados, como virus, caballos de Troya y gusanos. Los softwares antivirus pueden detectar la mayoría de los virus y muchas aplicaciones de caballo de Troya, y evitar que se propaguen en la red. La manera más eficaz de mitigar un ataque de gusanos consiste en descargar las actualizaciones de seguridad del proveedor del sistema operativo y aplicar parches a todos los sistemas vulnerables.

También se deben proteger las redes contra los ataques de red. Los ataques de red se pueden clasificar en tres categorías principales: de reconocimiento, de acceso y por denegación de servicio. Existen varias maneras de proteger la red contra los ataques de red.

- Los servicios de seguridad de red de autenticación, autorización y contabilidad (AAA o “triple A”) proporcionan el marco principal para configurar el control de acceso en dispositivos de red. AAA es un modo de controlar quién tiene permitido acceder a una red (autenticar), controlar lo que las personas pueden hacer mientras se encuentran allí (autorizar) y observar las acciones que realizan mientras acceden a la red (contabilizar).

- El firewall es una de las herramientas de seguridad más eficaces disponibles para la protección de los usuarios internos de la red contra amenazas externas. El firewall reside entre dos o más redes y controla el tráfico entre ellas, además de evitar el acceso no autorizado.

- Para proteger los dispositivos de red, es importante utilizar contraseñas seguras. Además, al acceder a los dispositivos de red de forma remota, se recomienda habilitar SSH en vez del protocolo Telnet, que no es seguro.

Una vez que se implementó la red, el administrador debe poder supervisar y mantener la conectividad de red. Existen varios comandos para este fin. Para probar la conectividad de red a destinos locales y remotos, se suelen utilizar comandos como ping, telnet y traceroute.

En los dispositivos Cisco IOS, se puede utilizar el comando show version para verificar y resolver problemas de algunos de los componentes básicos de hardware y software que se utilizan durante el proceso de arranque.

Para ver información de todas las interfaces de red en un router, se utiliza el comandoshow ip interface. También se puede utilizar el comando show ip interface brief para ver un resultado más abreviado que el del comando show ip interface. Cisco Discovery Protocol (CDP) es un protocolo exclusivo de Cisco que se ejecuta en la capa de enlace de datos. Debido a que el protocolo CDP funciona en la capa de enlace de datos, es posible que dos o más dispositivos de red Cisco (como routers que admiten distintos protocolos de la capa de red) obtengan información de los demás incluso si no hay conectividad de capa 3.

Los archivos de configuración de Cisco IOS como startup-config o running-config se deben archivar. Estos archivos pueden guardarse en un archivo de texto o almacenarse en un servidor TFTP.

Algunos modelos de routers también tienen un puerto USB, y se puede crear la copia de seguridad de un archivo en una unidad USB. Si es necesario, esos archivos se pueden copiar en el router o switch desde el servidor TFTP o la unidad USB.

El uso de redes no se limita a las pequeñas empresas y a las grandes organizaciones. Otro entorno en el que cada vez se aprovecha más la tecnología de red es el hogar. Una red doméstica es muy similar a la red de una pequeña empresa. Sin embargo, la mayoría de las redes domésticas (y muchas redes de pequeñas empresas) no requieren dispositivos de gran volumen, como routers y switches dedicados.

En lugar de esto, la mayoría de las redes domésticas utilizan un único dispositivo multifunción. A los fines de este curso, los dispositivos multifunción se denominarán routers integrados.

La mayoría de los routers integrados ofrecen tanto capacidades de conmutación por cable como conectividad inalámbrica y sirven como punto de acceso (AP) en la red inalámbrica. Para habilitar la conectividad inalámbrica, se debe configurar el modo inalámbrico, el SSID, el canal de RF y cualquier mecanismo de encriptación de seguridad deseado.

Al planificar una red, tenga en cuenta…

- Costo
- Puertos
- Velocidad
- Capacidad de expansión
- Facilidad de administración

Red típica de una pequeña empresa